CHAPTER 10

VPN Client Configuration Examples

This chapter provides examples that show how to configure interoperability between a PIX Firewall and PIX Firewall-supported VPN clients. The following VPN clients are supported within version 6.0 or later of the PIX Firewall:

Note Although PIX Firewall version 6.0 supports the following VPN clients, we strongly suggest that you use the Cisco VPN Client version 3.0.

- Cisco Secure VPN Client version 1.1 or later
- Cisco VPN 3000 Client version 2.5 or later
- Cisco VPN Client version 3.0
- Windows 2000 Client

This chapter includes the following sections:

- Configuring Interoperability with a Cisco Secure VPN Client Version 1.1
- Configuring Interoperability with a Cisco VPN 3000 Client and a Cisco VPN Client Version 3.0
- Configuring and Using Xauth with RSA Ace/Server and RSA SecurID
- Configuring Interoperability with a Windows 2000 Client

Configuring Interoperability with a Cisco Secure VPN Client Version 1.1

This section provides one example of how to configure the PIX Firewall and the Cisco VPN Client for interoperability. The example shows use of the following supported features:

- Extended Authentication (Xauth) for user authentication
- IKE Mode Config for VPN Client IP address assignment
- Wildcard pre-shared key for IKE authentication (the most commonly used method for IKE authentication among VPN users)

For more information about Xauth, see “Configuring Extended Authentication (Xauth)” within Chapter 8, “Advanced Configurations.” For more information about IKE Mode Config, see “Configuring IKE Mode Config (Dynamic IP Address Assignment for VPN Client)” within the Chapter 8, “Advanced Configurations.”

Note An example of certificate use for IKE authentication is not covered in this chapter.

VPN Client Access with Extended Authentication, IKE Mode Config, and Wildcard Pre-Shared Key

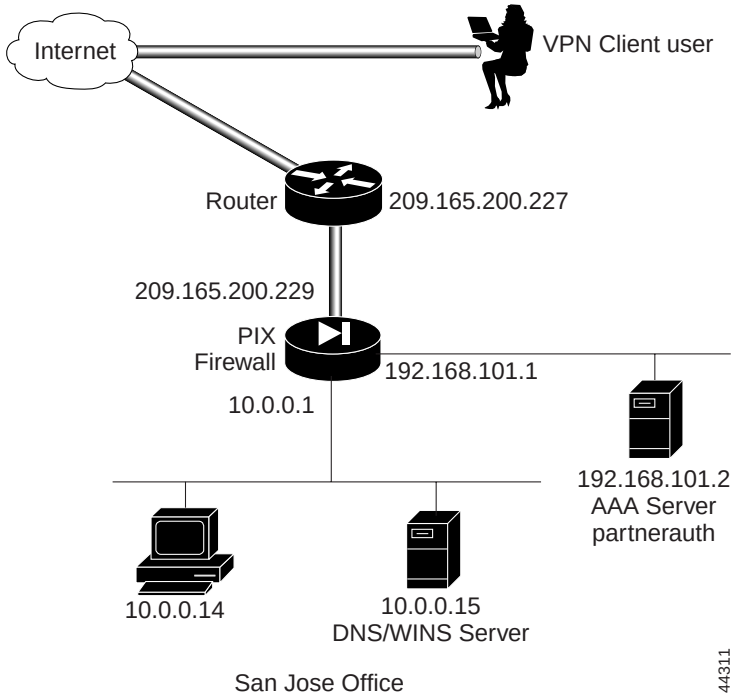
The example in this section shows use of Extended Authentication (Xauth), IKE Mode Config and a wildcard, pre-shared key for IKE authentication between a PIX Firewall and a Cisco Secure VPN Client.

This section includes the following topics:

- Configuring the PIX Firewall
- Configuring the Cisco Secure VPN Client Version 1.1

Figure 10-1 illustrates the example network.

Figure 10-1 VPN Client Access



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 set into a static crypto map set:

```
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
```

Table 10-1 provides the complete PIX Firewall configuration.

Table 10-1 PIX Firewall with VPN Client and Manual IP Address

Configuration	Description

`nameif ethernet0 outside security0`
`nameif ethernet1 inside security100`
`nameif ethernet2 dmz security10`
	PIX Firewall provides **nameif** command statements for the inside and outside interfaces in the default configuration. This example shows the default name for the perimeter interface "dmz."

`enable password 8Ry2YjIyt7RRXU24 encrypted` `passwd 2KFQnbNIdI.2KYOU encrypted`	Default values for the privileged mode password and the Telnet password.
`hostname SanJose`	Define a host name for the PIX Firewall.
`domain-name example.com`	Set the domain name.

`fixup protocol ftp 21`
`fixup protocol http 80`
`fixup protocol smtp 25`
`fixup protocol h323 1720`
`fixup protocol rsh 514`
`fixup protocol sqlnet 1521`
	Default **fixup protocol** values that define port usage.

`names`
`pager lines 24`
`no logging on`
	Default values that let you use names instead of IP addresses, display 24 lines of text before you are prompted to continue, and disable syslog output.

`interface ethernet0 auto`
`interface ethernet1 auto`
`interface ethernet2 auto`
	Default interface definitions indicating that each Ethernet interface has automatic sensing capabilities to determine line speed and duplex.

`mtu outside 1500`
`mtu inside 1500`
`mtu dmz 1500`
	Set the maximum transmission unit values for the Ethernet interfaces.

`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`
	The IP addresses for each PIX Firewall interface.

`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`
	Default values to disable failover.

`arp timeout 14400`	Default value specifying that the ARP cache be reinitialized every four hours.
`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`	Let users on the inside interface start connections on an interface with a lower security level.

`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`
	Create access lists that define the virtual IP addresses for the VPN clients.

`nat 0 access-list 80`	Configure NAT 0.

Table 10-1 PIX Firewall with VPN Client and Manual IP Address (continued)

Configuration	Description
`global (outside) 1 209.165.200.45-209.165.200.50 netmask 255.255.255.224`	Establish a pool of global addresses on the outside interface for translated addresses to use when users on the inside start connections to the outside.
`route outside 0.0.0.0 0.0.0.0 209.165.200.227 1`	Set the default route to be the router on the outside.

`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`
	Default timeout values.

`ip local pool dealer 192.168.15.1-192.168.15.5`	Create a pool of IP addresses that remote users access after they are authenticated by the AAA server.

`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`
	Establish the AAA parameters. The first two command statements enable access to the TACACS+ and RADIUS protocols. The next command statement associates the partnerauth protocol to TACACS+.

`no snmp-server location`
`no snmp-server contact`
`snmp-server community public`
`no snmp-server enable traps`
	Default values to disable SNMP.

`crypto map partner-map client configuration address initiate`	Specify the IKE Mode Configuration parameters.
`isakmp client configuration address-pool local dealer outside`	Establish association to local pool of IP addresses.
`crypto ipsec transform-set strong-des esp-3des esp-sha-hmac`	Create a transform set for Triple DES, ESP, SHA, and HMAC.
`crypto dynamic-map cisco 4 set transform-set strong-des`	Create a dynamic crypto map that associates the access list and the transform set.
`crypto map partner-map 20 ipsec-isakmp dynamic cisco`	Define a crypto map that enables the ISAKMP policy.
`crypto map partner-map client authentication partnerauth`	Enable Xauth. Be sure to specify the same AAA server name within the **crypto map client authentication** command statement as was specified in the **aaa-server** command statement.
`crypto map partner-map interface outside`	Apply the crypto map to the outside interface.
`isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0`	Create a wildcard, pre-shared key.

`isakmp enable outside`
`isakmp policy 8 authentication pre-share`
`isakmp policy 8 encryption 3des`
`isakmp policy 8 hash md5`
	Create the ISAKMP policy on the outside interface, to handle pre-shared keys, to have Triple DES encryption, and to provide an MD5 hash for additional security.

`sysopt connection permit-ipsec`	Implicitly permit IPSec connections through the PIX Firewall.
`telnet timeout 5` `terminal width 80`	Default values for how long a Telnet console session can be idle and that a console session should display up to 80 characters wide on the console computer.

Configuring the Cisco Secure VPN Client Version 1.1

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

- **a.** Under **Select Phase 1 Negotiation Mode**, click **Main Mode**.
- **b.** 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:

- **a.** Authentication Method—Click **Pre-shared Key**.
- **b.** Encrypt Alg—Click **Triple DES**.
- **c.** Hash Alg—Click **MD5**.

d. SA Life—Click **Unspecified** to accept the default values.

e. 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:

a. Select the **Encapsulation Protocol (ESP)** check box.

b. Encryption Alg—Click **Triple DES**.

c. Hash Alg—Click **SHA-1**.

d. 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 in 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.

An example of a typical View Log session follows:

```
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
```

Configuring Interoperability with a Cisco VPN 3000 Client and a Cisco VPN Client Version 3.0

Remote access VPN users employing the Cisco VPN 3000 Client version 2.5 or later, or the Cisco VPN Client version 3.0, can now securely access their private enterprise network through the PIX Firewall.

Unlike the Cisco Secure VPN Client, the Cisco VPN 3000 Client requires the gateway to push policy information to the Cisco VPN 3000 client. To support the Cisco VPN 3000 Client, the IKE Mode Config feature within the PIX Firewall has been extended to include the downloading of DNS, WINS, default domain, and split tunnel mode attributes to the Cisco VPN 3000 Client. The split tunnel mode allows the PIX Firewall to direct packets to a network interface in clear text form or over an IPSec tunnel in encrypted form.

The **vpngroup** command set allows you to configure Cisco VPN 3000 Client policy attributes to be associated with a VPN group name and downloaded to the Cisco VPN 3000 Client(s) that are part of the given group. These new commands' purpose is to configure the Cisco VPN 3000 Client policy groups. See the **vpngroup** command page within the Chapter 12, "Command Reference," for more information about these commands.

This section shows two examples of how to configure the PIX Firewall and the Cisco VPN 3000 Client for interoperability. The steps for configuring the Cisco VPN 3000 Client version 2.5 and the Cisco VPN Client version 3.0, are the same, except where noted.

The first 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

The second example shows use of the following supported features:

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

For more information about Xauth, see "Configuring Extended Authentication (Xauth)" within Chapter 8, "Advanced Configurations." For more information about IKE Mode Config, see "Configuring IKE Mode Config (Dynamic IP Address Assignment for VPN Client)" within Chapter 8, "Advanced Configurations." For more information about RADIUS authorization, see "RADIUS Authorization Feature" within the **aaa** command page of Chapter 5, "Command Reference" in the *Configuration Guide for the Cisco Secure PIX Firewall Version 6.0*.

Note If the Cisco Secure VPN Client is already installed on the computer, uninstall it from your computer and ensure all directories containing this VPN Client application are cleared of it before you install the Cisco VPN 3000 Client or the Cisco VPN Client version 3.0.

This section includes the following topics:

- VPN Client Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Wildcard Pre-Shared Key
- VPN Client Access with Extended Authentication, IKE Mode Config, and Digital Certificates

VPN Client Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Wildcard Pre-Shared Key

The example in 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 a Cisco VPN 3000 Client.

With the **vpngroup** command set, you configure the PIX Firewall for a specified group of Cisco VPN 3000 Client users with the following parameters:

- group name for a given group of Cisco VPN 3000 Client users.
- 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 that you enter within the **Group Password** field of the Cisco VPN 3000 Client while configuring your group access information for a connection entry.

- a pool of local addresses to be assigned to the VPN group.
- an IP address of a DNS server to download to the Cisco VPN 3000 Client. (optional)

- an IP address of a WINS server to download to the Cisco VPN 3000 Client. (optional)
- a default domain name to download to the Cisco VPN 3000 Client. (optional)
- enable split tunneling on the PIX Firewall allowing both encrypted and clear traffic between the Cisco VPN 3000 Client and the PIX Firewall. (optional)

Note If split tunneling is not enabled, all traffic between the Cisco VPN 3000 Client and the PIX Firewall will be encrypted.

- the inactivity timeout for the Cisco VPN 3000 Client. The default is 30 minutes. (optional)

On the Cisco VPN 3000 Client, you would configure the vpngroup name and group password to match that which you configured on the PIX Firewall.

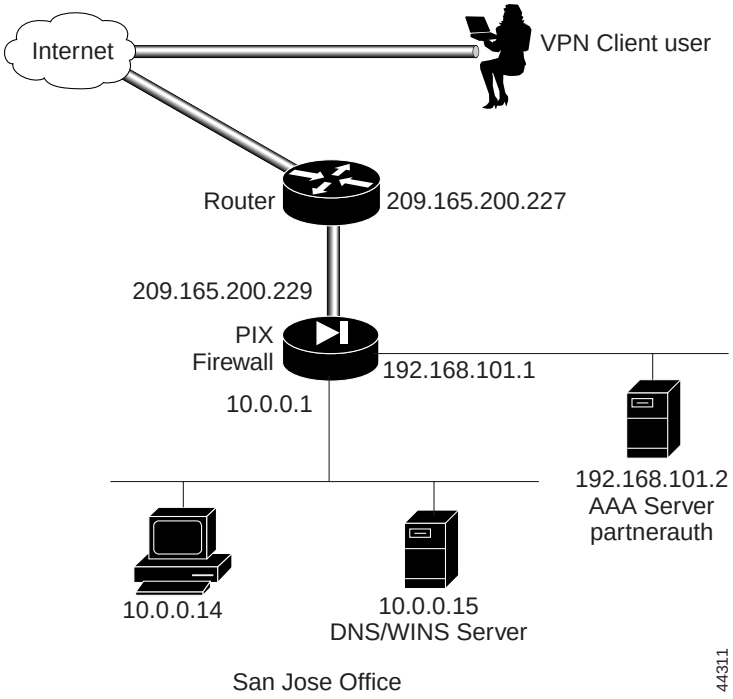
When the Cisco VPN 3000 Client initiates ISAKMP with the PIX Firewall, the VPN group name and pre-shared key are sent to the PIX Firewall. The PIX Firewall then uses the group name to look up the configured client policy attributes for the given Cisco VPN 3000 Client and downloads the matching policy attributes to the client during the IKE negotiation.

This section includes the following topics:

- Configuring the PIX Firewall
- Configuring the Cisco VPN 3000 Client

Figure 10-2 illustrates the example network.

Figure 10-2 Cisco VPN 3000 Client Access



Configuring the PIX Firewall

Follow these steps to configure the PIX Firewall to interoperate with the Cisco VPN 3000 Client using Xauth, IKE Mode Config, AAA Authorization with RADIUS, and 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 3000 Client version 3.0 or above, you must include the following command in this step: `isakmp policy 8 group 2`

Step 3 Configure a wildcard, pre-shared key:

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

Step 4 Create an access list that defines the PIX Firewall local network(s) requiring IPSec protection:

```
access-list 80 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0
```

Step 5 Create access lists that define the services the VPN clients are authorized to use with the RADIUS server:

```
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. Your entry in the authentication server would then be **acl=100**.

Step 6 Configure NAT 0:

```
nat (inside) 0 access-list 80
```

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

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

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 IKE Mode Config related parameters:

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

Note To configure the Cisco VPN 3000 Client version 2.5, you must include the following command in this step: `crypto map partner-map client configuration address initiate`

Step 13 Configure Cisco VPN 3000 Client policy attributes to download to the Cisco VPN 3000 Client:

```
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 the Cisco VPN 3000 Client as part of the Group access information. See Step 9 within “Configuring the Cisco VPN 3000 Client.”

Step 14 Tell PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

Table 10-2 provides the complete PIX Firewall configuration.

Table 10-2 VPN Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Wildcard Pre-Shared Key

Configuration	Description

`nameif ethernet0 outside security0`
`nameif ethernet1 inside security100`
`nameif ethernet2 dmz security10`
	PIX Firewall provides **nameif** command statements for the inside and outside interfaces in the default configuration. This example shows the default name for the perimeter interface “dmz.”

`enable password 8Ry2YjIyt7RRXU24 encrypted` `passwd 2KFQnbNIdI.2KYOU encrypted`	Default values for the privileged mode password and the Telnet password.
`hostname SanJose`	Define a host name for the PIX Firewall.
`domain-name example.com`	Set the domain name.

`fixup protocol ftp 21`
`fixup protocol http 80`
`fixup protocol smtp 25`
`fixup protocol h323 1720`
`fixup protocol rsh 514`
`fixup protocol sqlnet 1521`
	Default **fixup protocol** values that define port usage.

`names`
`pager lines 24`
`no logging on`
	Default values that let you use names instead of IP addresses, display 24 lines of text before you are prompted to continue, and disable syslog output.

`interface ethernet0 auto`
`interface ethernet1 auto`
`interface ethernet2 auto`
	Default interface definitions indicating that each Ethernet interface has automatic sensing capabilities to determine line speed and duplex.

Table 10-2 VPN Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Wildcard Pre-Shared Key (continued)

Configuration	Description

`mtu outside 1500`
`mtu inside 1500`
`mtu dmz 1500`
	Set the maximum transmission unit values for the Ethernet interfaces.

`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`
	The IP addresses for each PIX Firewall interface.

`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`
	Default values to disable failover.

`arp timeout 14400`	Default value specifying that the ARP cache be reinitialized every four hours.
`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`	Let users on the inside interface start connections on an interface with a lower security level.
`access-list 80 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0`	Create an access list that defines the PIX Firewall local network(s) requiring IPSec protection. To be used for split tunnelling.

`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`
	Create access lists that define the services the VPN Clients are authorized to use with the RADIUS server.

`nat (inside) 0 access-list 80`	Configure NAT 0.
`global (outside) 1 209.165.200.45-209.165.200.50 netmask 255.255.255.224`	Establish a pool of global addresses on the outside interface for translated addresses to use when users on the inside start connections to the outside.
`route outside 0.0.0.0 0.0.0.0 209.165.200.227 1`	Set the default route to be the router on the outside.

`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`
	Default timeout values.

`ip local pool dealer 10.1.1.1-10.1.1.254`	Create a pool of IP addresses that remote users access after they are authenticated by the AAA server.

`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`
	Establish the AAA parameters. The first two command statements enable access to the TACACS+ and RADIUS protocols. The next command statement associates the partnerauth protocol to TACACS+.

`no snmp-server location`
`no snmp-server contact`
`snmp-server community public`
`no snmp-server enable traps`
	Default values to disable SNMP.

`crypto map partner-map client configuration address initiate`[1]	Specify the IKE Mode Configuration parameters.
`crypto ipsec transform-set strong-des esp-3des esp-sha-hmac`	Create a transform set for Triple DES, ESP, SHA, and HMAC.
`crypto dynamic-map cisco 4 set transform-set strong-des`	Create a dynamic crypto map that associates the access list and the transform set.

Table 10-2 VPN Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Wildcard Pre-Shared Key (continued)

Configuration	Description
`crypto map partner-map 20 ipsec-isakmp dynamic cisco`	Define a crypto map that enables the ISAKMP policy.
`crypto map partner-map client authentication partnerauth`	Enable the Extended Authentication feature. Be sure to specify the same AAA server name within the **crypto map client authentication** command statement as was specified in the **aaa-server** command statement.
`crypto map partner-map interface outside`	Apply the crypto map to the outside interface.
`isakmp key cisco1234 address 0.0.0.0 netmask 0.0.0.0`	Create a wildcard, pre-shared key.

`isakmp enable outside`
`isakmp policy 8 authentication pre-share`
`isakmp policy 8 encryption 3des`
`isakmp policy 8 hash md5`
`isakmp policy 8 group 2`[2]
	Create the ISAKMP policy on the outside interface, to handle pre-shared keys, to have Triple DES encryption, and to provide an MD5 hash for additional security.

`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`
	Configure Cisco VPN 3000 Client policy attributes to download to the Cisco VPN 3000 Client.

`sysopt connection permit-ipsec`	Implicitly permit IPSec connections through the PIX Firewall.
`telnet timeout 5` `terminal width 80`	Default values for how long a Telnet console session can be idle and that a console session should display up to 80 characters wide on the console computer.

1. This command is only required to configure the Cisco VPN 3000 Client version 2.5.
2. This command is only required to configure the Cisco VPN Client version 3.0 or above.

Configuring the Cisco VPN 3000 Client

This section describes how to configure the Cisco VPN 3000 Client to match the configurations within "Configuring the PIX Firewall," in the previous section. It is assumed the Cisco VPN 3000 Client is already installed on your system and is configured for general use. You can find the Cisco VPN 3000 Client documentation online at the following website:

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

For the Cisco VPN 3000 Client to gain VPN access to the PIX Firewall using a pre-shared key, you must create one connection entry for the Cisco VPN 3000 Client to use that identifies the following:

- the 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 chapter "Configuring the VPN Client" in the *VPN 3000 Client User Guide* for the detailed steps to follow when configuring the Cisco VPN 3000 Client.

Follow these steps to configure the Cisco VPN 3000 Client to interoperate with the PIX Firewall:

Step 1 Click **Start**>**Programs**>**Cisco Systems VPN 3000 Client**>**VPN Dialer**.

Step 2 At the VPN Client main dialog box, click **New**.

The first New Connection Entry Wizard dialog box appears.

Step 3 Enter a unique name for the connection.

Step 4 (Optional) Enter a description of this connection.

Step 5 Click **Next**.

The second New Connection Entry Wizard dialog box appears.

Step 6 Enter the host name or IP address of the remote PIX Firewall you want to access.

Step 7 Click **Next**.

The third New Connection Entry Wizard dialog box appears.

Step 8 Click **Group Access Information**.

Step 9 Enter the name of the VPN group to which you belong and the password for you VPN group.

The password displays in asterisks.

Step 10 Click **Next**.

The fourth New Connection Entry Wizard dialog box appears.

Step 11 Review the connection entry name.

Step 12 Click **Finish**.

VPN Client Access with Extended Authentication, IKE Mode Config, and Digital Certificates

This example shows use of Xauth, IKE Mode Config, and digital certificates for IKE authentication between a PIX Firewall and a Cisco VPN 3000 Client. 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 Both the PIX Firewall and the Cisco VPN 3000 Client are required to 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.

Note The PIX Firewall supports CA servers developed by VeriSign, Entrust, Baltimore Technologies, and Microsoft. See Chapter 11, “CA Configuration Examples,” for examples on how to interoperate with each of the 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 Cisco VPN 3000 Client users the following:

- a pool of local addresses to be assigned to the VPN group
- an IP address of a DNS server to download to the Cisco VPN 3000 Client (optional)
- an IP address of a WINS server to download to the Cisco VPN 3000 Client (optional)
- a default domain name to download to the Cisco VPN 3000 Client (optional)
- enable split tunneling on the PIX Firewall allowing both encrypted and clear traffic between the Cisco VPN 3000 Client and the PIX Firewall. (optional)

Note If split tunnelling is not enabled, all traffic between the Cisco VPN 3000 Client and the PIX Firewall will be encrypted.

- the inactivity timeout for the Cisco VPN 3000 Client. The default is 30 minutes. (optional)

On the Cisco VPN 3000 Client, configure the client to obtain a digital certificate. After obtaining the certificate, set up your Cisco VPN 3000 Client connection entry to use the digital certificate.

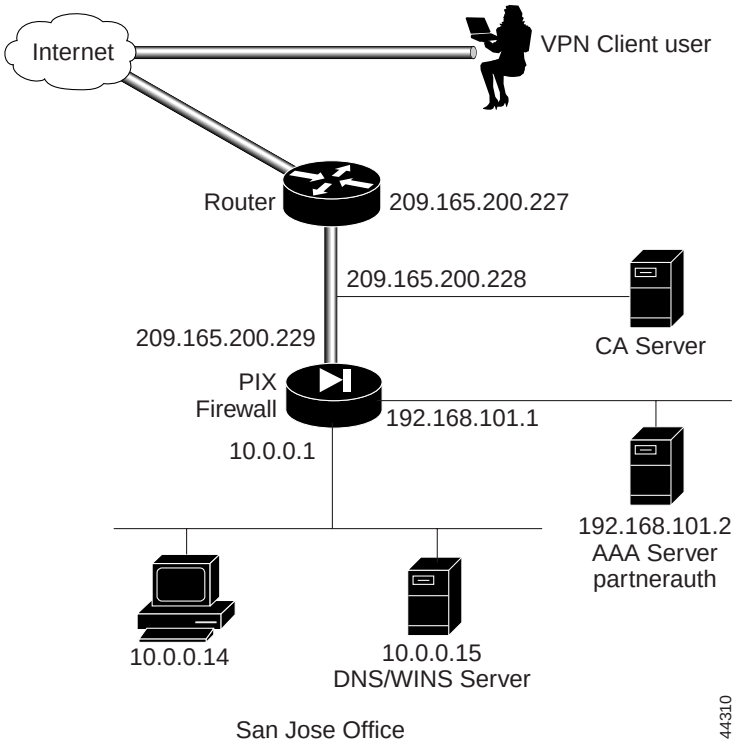
When the Cisco VPN 3000 Client initiates ISAKMP with the PIX Firewall, the digital certificate is sent to the PIX Firewall. The PIX Firewall uses the digital certificate to look up the configured client policy attributes for the given Cisco VPN 3000 Client and downloads the matching policy attributes to the client during the IKE negotiation.

This section includes the following topics:

- Configuring the PIX Firewall
- Configuring the Cisco VPN 3000 Client

Figure 10-3 illustrates the example network.

Figure 10-3 Cisco VPN 3000 Client Access



Configuring the PIX Firewall

Follow these steps to configure the PIX Firewall to interoperate with the Cisco VPN 3000 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 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. Before entering this command, contact your CA administrator because they will have to authenticate your PIX Firewall manually before granting its certificate(s):

```
ca enroll abcd cisco
```

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

Step 12 Create an access list that defines the PIX Firewall 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 13 Configure NAT 0:

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

Step 14 Configure a transform set that defines how the traffic will be protected:

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

Step 15 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 16 Add the dynamic crypto map set into a static crypto map set:

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

Step 17 Apply the crypto map to the outside interface:

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

Step 18 Tell PIX Firewall to implicitly permit IPSec traffic:

```
sysopt connection permit-ipsec
```

Step 19 Enable Xauth:

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

Step 20 Configure IKE Mode Config related parameters:

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

Step 21 Configure Cisco VPN 3000 Client policy attributes to download to the Cisco VPN 3000 Client:

```
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 access-list 90
vpngroup superteam idle-time 1800
```

Table 10-3 provides the complete PIX Firewall configuration.

Table 10-3 VPN Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Digital Certificates

Configuration	Description

`nameif ethernet0 outside security0`
`nameif ethernet1 inside security100`
`nameif ethernet2 dmz security10`
	PIX Firewall provides **nameif** command statements for the inside and outside interfaces in the default configuration. This example shows the default name for the perimeter interface "dmz."

`enable password 8Ry2YjIyt7RRXU24 encrypted` `passwd 2KFQnbNIdI.2KYOU encrypted`	Default values for the privileged mode password and the Telnet password.
`hostname SanJose`	Define a host name for the PIX Firewall.
`domain-name example.com`	Set the domain name.

`fixup protocol ftp 21`
`fixup protocol http 80`
`fixup protocol smtp 25`
`fixup protocol h323 1720`
`fixup protocol rsh 514`
`fixup protocol sqlnet 1521`
	Default **fixup protocol** values that define port usage.

`names`
`pager lines 24`
`no logging on`
	Default values that let you use names instead of IP addresses, display 24 lines of text before you are prompted to continue, and disable syslog output.

`interface ethernet0 auto`
`interface ethernet1 auto`
`interface ethernet2 auto`
	Default interface definitions indicating that each Ethernet interface has automatic sensing capabilities to determine line speed and duplex.

`mtu outside 1500`
`mtu inside 1500`
`mtu dmz 1500`
	Set the maximum transmission unit values for the Ethernet interfaces.

Table 10-3 VPN Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Digital Certificates (continued)

Configuration	Description

`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`
	The IP addresses for each PIX Firewall interface.

`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`
	Default values to disable failover.

`arp timeout 14400`	Default value specifying that the ARP cache be reinitialized every four hours.
`nat (inside) 1 0.0.0.0 0.0.0.0 0 0`	Let users on the inside interface start connections on an interface with a lower security level.
`access-list 90 permit ip 10.0.0.0 255.255.255.0 10.1.1.0 255.255.255.0`	Create an access list that defines the PIX Firewall local network(s) requiring IPSec protection. To be used for split tunnelling.

`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`
	Create access lists that define the services the VPN clients are authorized to use with the RADIUS server.

`nat (inside) 0 access-list 90`	Configure NAT 0.
`global (outside) 1 209.165.200.45-209.165.200.50 netmask 255.255.255.224`	Establish a pool of global addresses on the outside interface for translated addresses to use when users on the inside start connections to the outside.
`route outside 0.0.0.0 0.0.0.0 209.165.200.227 1`	Set the default route to be the router on the outside.

`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`
	Default timeout values.

`ip local pool dealer 10.1.1.1-10.1.1.254`	Create a pool of IP addresses that remote users access after they are authenticated by the AAA server.

`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`
	Establish the AAA parameters. The first two command statements enable access to the TACACS+ and RADIUS protocols. The next command statement associates the partnerauth protocol to TACACS+.

`no snmp-server location`
`no snmp-server contact`
`snmp-server community public`
`no snmp-server enable traps`
	Default values to disable SNMP.

`crypto map partner-map client configuration address initiate`[1]	Specify the IKE Mode Configuration parameters.
`crypto ipsec transform-set strong-des esp-3des esp-sha-hmac`	Create a transform set for Triple DES, ESP, SHA, and HMAC.
`crypto dynamic-map cisco 4 set transform-set strong-des`	Create a dynamic crypto map that associates the access list and the transform set.
`crypto map partner-map 20 ipsec-isakmp dynamic cisco`	Define a crypto map that enables the ISAKMP policy.

Table 10-3 VPN Access with Extended Authentication, RADIUS Authorization, IKE Mode Config, and Digital Certificates (continued)

Configuration	Description
`crypto map partner-map client authentication partnerauth`	Enable Xauth. Be sure to specify the same AAA server name within the **crypto map client authentication** command statement as was specified in the **aaa-server** command statement.
`crypto map partner-map interface outside`	Apply the crypto map to the outside interface.

`isakmp enable outside`
`isakmp policy 8 encryption 3des`
`isakmp policy 8 hash md5`
`isakmp policy 8 authentication rsa-sig`
	Create the ISAKMP policy on the outside interface, to handle digital certificates, to have Triple DES encryption, and to provide an MD5 hash for additional security.

`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`
	Configure Cisco VPN 3000 Client policy attributes to download to the Cisco VPN 3000 Client.

`ca identity abcd 209.165.200.228 209.165.200.228` `ca configure abcd ra 1 100 crloptional`	Define CA-related enrollment commands.
`sysopt connection permit-ipsec`	Implicitly permit IPSec connections through the PIX Firewall.
`telnet timeout 5` `terminal width 80`	Default values for how long a Telnet console session can be idle and that a console session should display up to 80 characters wide on the console computer.

1. This command is only required to configure the Cisco VPN 3000 Client, version 2.5.

Configuring the Cisco VPN 3000 Client

This section describes how to configure the Cisco VPN 3000 Client to match the configurations within "Configuring the PIX Firewall," in the previous section. It is assumed the Cisco VPN 3000 Client is already installed on your system and is configured for general use. You can find the Cisco VPN 3000 Client documentation online at the following website:

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

For the Cisco VPN 3000 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:

- the 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 Cisco VPN 3000 Client.)

Note When configuring the VPN 3000 Client certificate, be sure to match the VPN group name you specified within the associated **vpngroup** commands in your PIX Firewall configuration. To specify a VPN group name within the VPN 3000 Client certificate, enter the name of the VPN group in the "Organization Unit" (OU) field. The PIX Firewall will use this VPN group name to match a given VPN Client's policy. For example, you would enter "superteam" in the OU field if the name of your VPN group is "superteam". You would use "superteam" as the VPN group name to configure on the PIX Firewall using the **vpngroup** commands.

This section does not cover how to obtain a digital certificate for the Cisco VPN 3000 Client. For information about obtaining a certificate for the Cisco VPN 3000 Client, refer to the chapter "Obtaining a Certificate" within the *VPN 3000 Client User Guide*.

To obtain the detailed steps to follow when configuring the Cisco VPN 3000 Client, refer to the chapter "Configuring the VPN Client" in the *VPN 3000 Client User Guide*.

Follow these steps to configure the Cisco VPN 3000 Client:

Step 1 Click **Start**>**Programs**>**Cisco Systems VPN 3000 Client>VPN Dialer**.

Step 2 At the Cisco VPN 3000 Client main dialog box, click **New**.

The first New Connection Entry Wizard dialog box appears.

Step 3 Enter a unique name for the connection.

Step 4 (Optional) Enter a description of this connection.

Step 5 Click **Next**.

The second New Connection Entry Wizard dialog box appears.

Step 6 Enter the host name or IP address of the remote PIX Firewall you want to access.

Step 7 Click **Next**.

The third New Connection Entry Wizard dialog box appears.

Step 8 Click **Certificate**.

Step 9 Click the name of the certificate you are using.

Step 10 Click **Next**.

The fourth New Connection Entry Wizard dialog box appears.

Step 11 Review the connection entry name.

Step 12 Click **Finish**.

Configuring and Using Xauth with RSA Ace/Server and RSA SecurID

This section contains the following topics:

- Terminology
- Introduction
- PIX Firewall Configuration
- SecurID with Cisco VPN Clients

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 RSA SercurID Standard Card, Key Fob, 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 must enter 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 Secure VPN Client version 1.1, the Cisco VPN 3000 Client version 2.5, and the Cisco VPN Client version 3.0, which are supported by PIX Firewall. SecureId 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:

1. The token is Enabled.
2. The token is in the Next Tokencode Mode.
3. The token is in the 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 isakmp policy and define 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 command **crypto map newmap client token authentication partner-auth** is optional for the Cisco VPN Client version 3.0, 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 3.0, 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 and the Cisco VPN Client version 3.0, the vpngroup Command configuration is also needed.

```
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 Clients

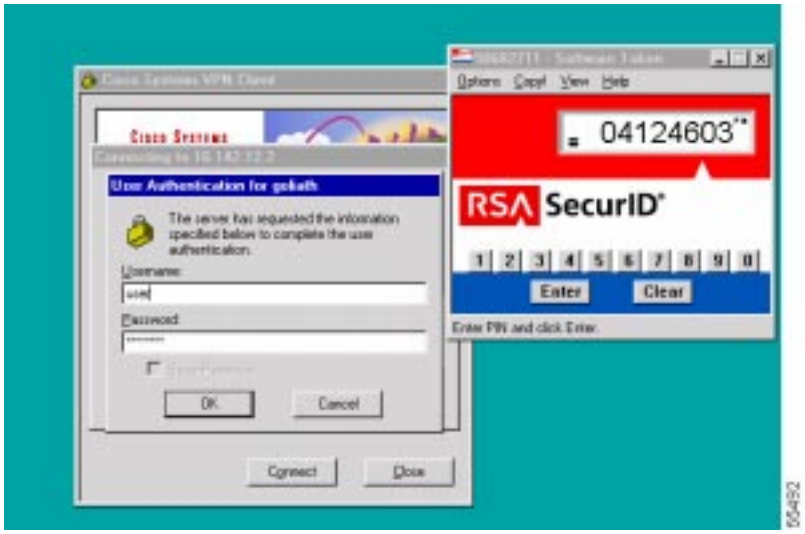
This section provides a reference for using the VPN clients in the different token modes discussed in the section, “Introduction”, which lists using the Software Token and Pinpad methods for authentication.

Cisco VPN Client Version 3.0

1. Token is enabled:

When a connection is being established to the PIX Firewall with the Cisco VPN Client version 3.0, 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 10-4).

Figure 10-4



2. Token is in 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 (see Figure 10-5).

Figure 10-5

3. Token is in 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).

Case1: 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 had a PIN before and needs to change the PIN.

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 (See Figure 10-5). 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.

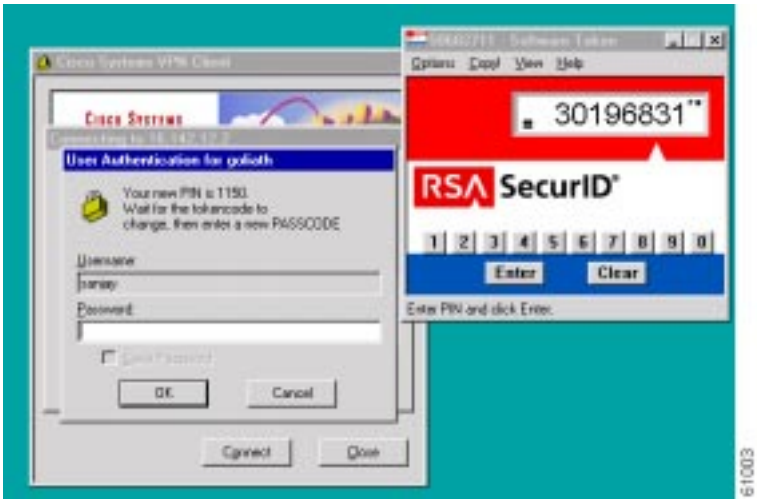
The next prompt requires the user to enter the password using the new PIN. Enter the newly created PIN in the **Software Token** dialog box or Pinpad and use the value thus obtained (See Figure 10-6).

For a system generated PIN:

Figure 10-6

A **y** must be entered at this point. The server then sends a PIN message to the user. Enter the next tokencode using the new PIN (see Figure 10-7).

Figure 10-7

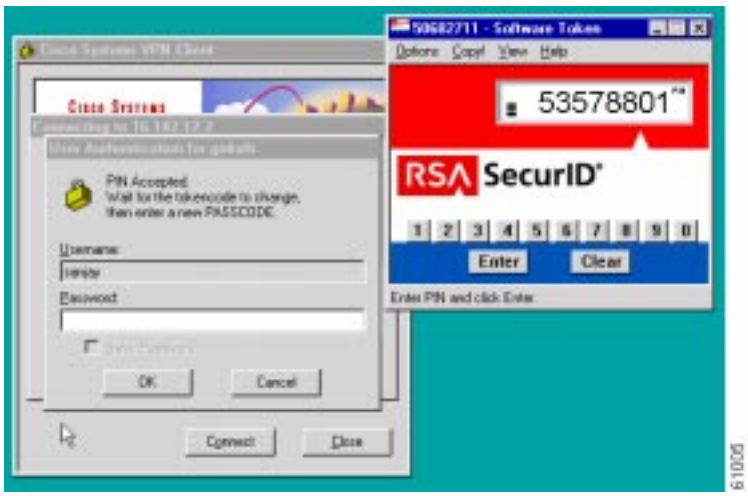


The user creates the PIN, or the user is required to create the PIN if the user enters **n** in the prompt that asks whether the system should generate the PIN or when the user is required to create the PIN.

Figure 10-8

After the PIN is entered, and is accepted by the server, another **Software Token** dialog box appears (see Figure 10-8).

Figure 10-9



Enter the next tokencode, using the new PIN, in the **Software Token** dialog box (see Figure 10-9).

Cisco VPN 3000 Client Version 2.5

1. Token is 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 10-10).

Figure 10-10

2. Token is in 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 (see Figure 10-11).

Figure 10-11

3. Token is in 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).

Case1: 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 had a PIN before, and needs to change the PIN.

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 promp, 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.

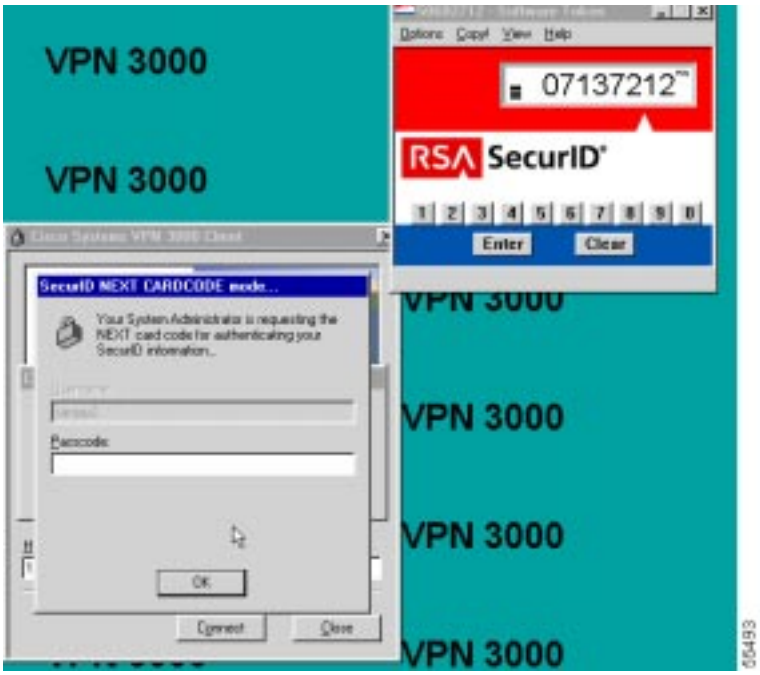
The prompt following thereafter requires the user to enter the passcode using the new PIN. Use the newly created PIN on the **Software Token** dialog box or on the Pinpad and use the value thus obtained. On a Windows NT operating system, enter the new PIN in the **SecurID New Pin Mode** dialog box (see Figure 10-12).

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

Figure 10-12

The next prompt requests that the user enter the next tokencode using the new PIN (see Figure 10-13).

Figure 10-13

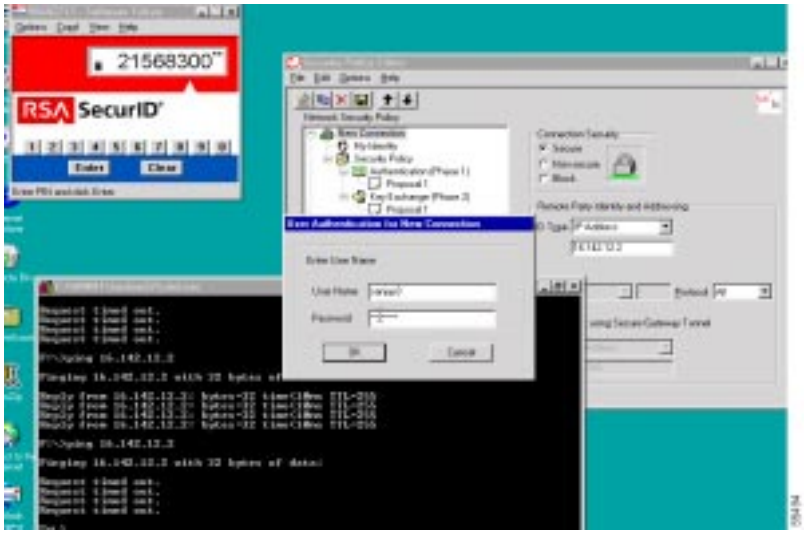


Cisco Secure VPN Client 1.1 (3DES)

1. Token is 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 10-14).

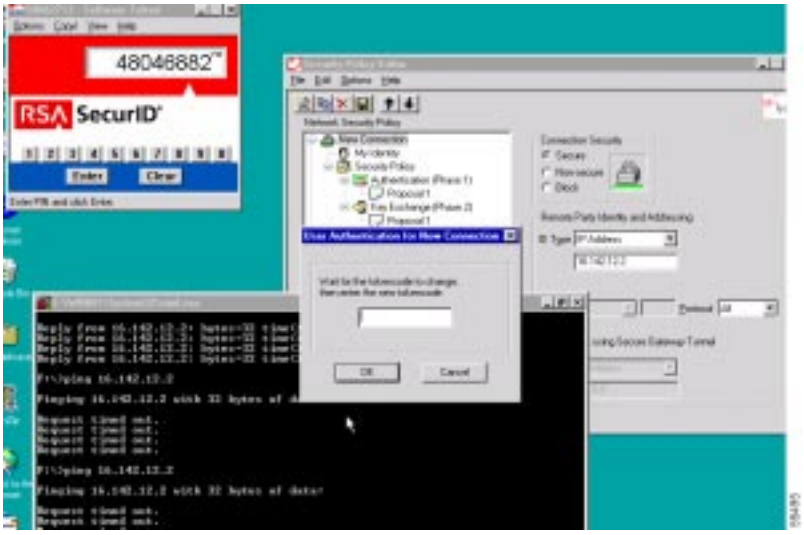
Figure 10-14



2. Token is in 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 (see Figure 10-15).

Figure 10-15



3. Token is in 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).

Case1: 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 had a PIN previously assigned and needs to change the PIN.

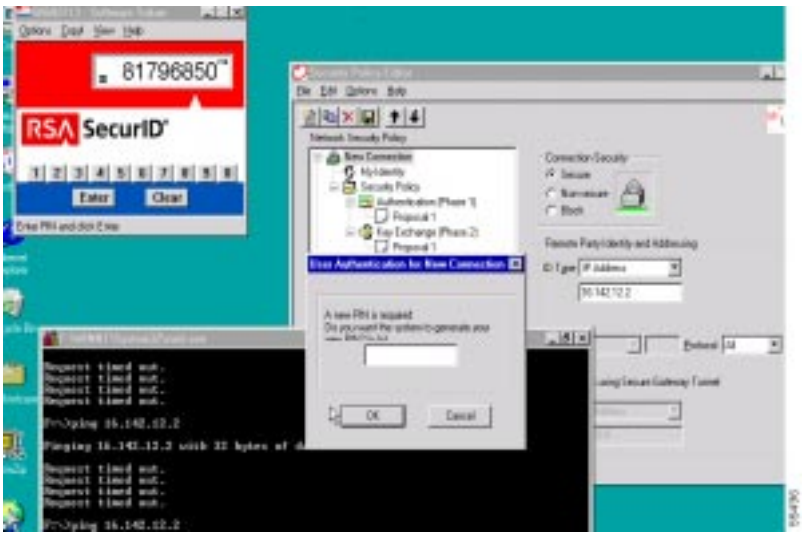
In this case, enter the PIN in the **Software Token** dialog box or on the Pinpad, and use the value thus obtained as the password.

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 (see Figure 10-16).

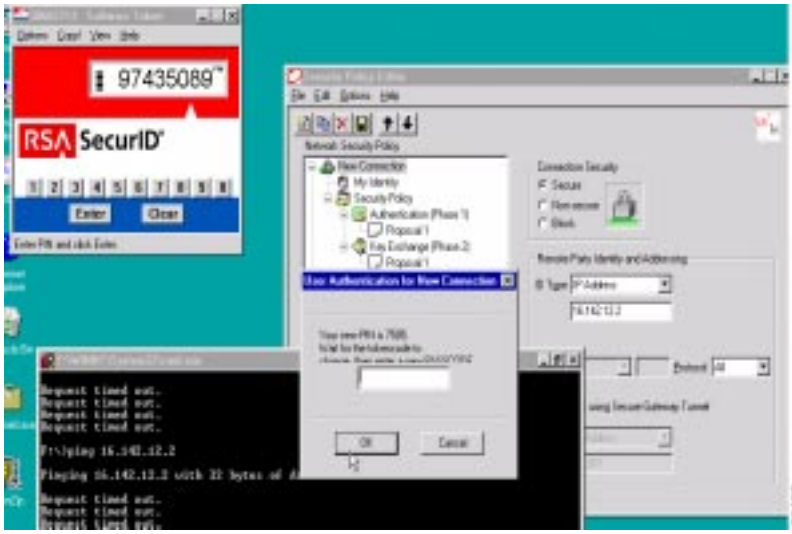
1. For the system generated PIN:

Figure 10-16



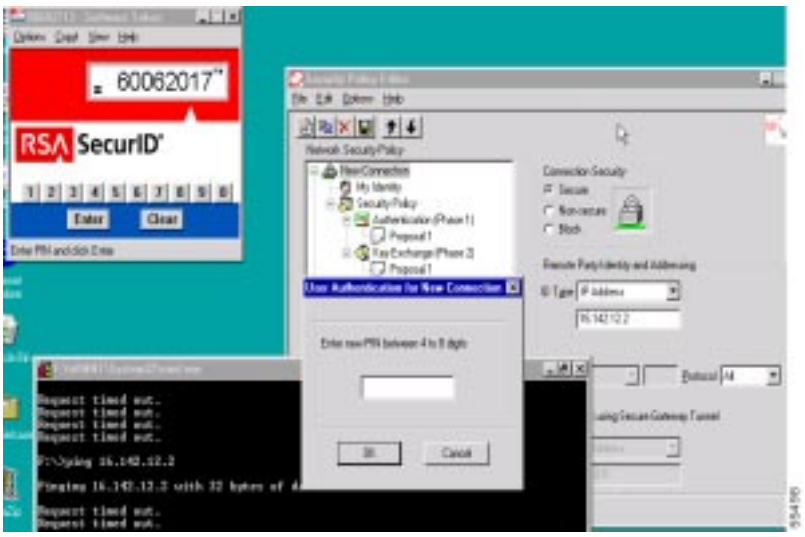
When a **y** is entered, the system sends the PIN and requires the user to use the PIN to enter the next tokencode (see Figure 10-17).

Figure 10-17



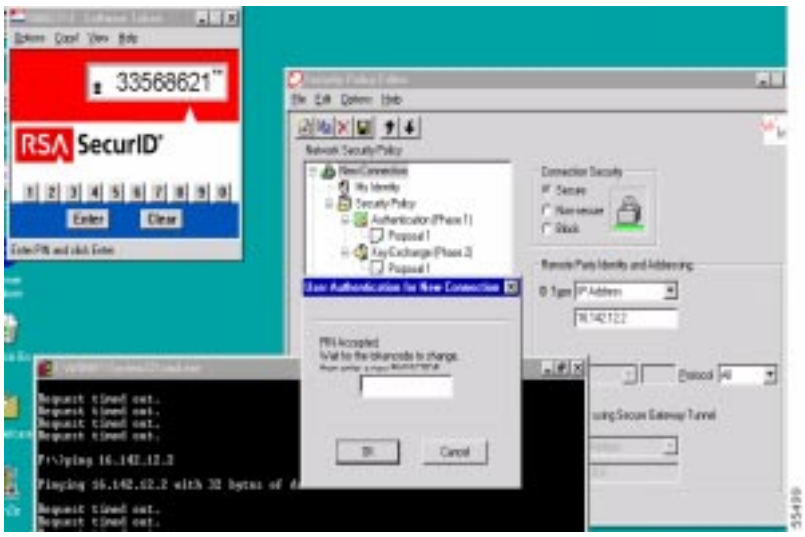
2. The user creates the PIN, or a user-created PIN is required. When **n** is entered in the **Generate PIN** dialog box, or if the user is required to generate the PIN, the **User Authentication for New Connection** dialog box appears (see Figure 10-18).

Figure 10-18



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 (see Figure 10-19).

Figure 10-19



Configuring Interoperability with a Windows 2000 Client

This section provides an example of how to configure the PIX Firewall for interoperability with a Windows 2000 client. The example shows the use of IPSec with L2TP, which requires that IPSec be configured in transport mode. Refer to the "Configuring L2TP with IPSec in Transport Mode" section in Chapter 8, "Advanced Configurations," for IPSec transport mode configuration information. For detailed command reference information, refer to Chapter 12, "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 Chapter 12, "Command Reference." For information on obtaining certificates for RSA signature authentication from various CA vendors, refer to Chapter 11, "CA Configuration Examples."

This section contains the following topics:

- Troubleshooting
- Windows 2000 Client Access Utilizing IPSec with L2TP

Troubleshooting

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 "oakley".

Step 4 Create the DWORD "EnableLogging".

Step 5 Set the "EnableLogging" value to "1".

Step 6 Stop and Start the IPSec Policy Agent (**Start>Programs>Administrative Tools>Services**). The debug file will be found at "%windir%\debug\oakley.log".

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

Basic L2TP/IPSec Troubleshooting in Windows 2000

Windows 2000 Client Access Utilizing IPSec with L2TP

This section provides an IPSec with L2TP configuration example.

Configuring the PIX Firewall

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

Note In this example, PIX Firewall uses PAP and AAA authentication. No **conduit** commands are included, as the **sysopt connection permit-l2tp** option is set in Step 23. This command also permits L2TP traffic.

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

```
ca enroll abcd cisco
```

"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 transfom-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 must be selected on the trasform 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 set into a static crypto map set:

```
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
vpdn group 1 client accounting 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 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 3.0 or the Cisco VPN 3000 Client version 2.5 or later is installed. You must disable the *Cisco VPN Service* for the Cisco VPN Client version 3.0, or the *ANetIKE Service* for the Cisco VPN 3000 Client version 2.5 or later from the Services panel in Windows 2000 (**Start>Programs>Administrative Tools>Services**). You must then restart the IPSec Policy Agent Service from the **Services** panel, and reboot the machine.