

# PIX/ASA 7.x and Cisco VPN Client 4.x with Windows 2003 IAS RADIUS (Against Active Directory) Authentication Configuration Example

Document ID: 70330

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

### Background Information

#### Configure

- Network Diagram
- Configurations
- VPN Client 4.8 Configuration
- Microsoft Windows 2003 Server with IAS Configuration

### Password Expiry Feature

#### Verify

- AAA Authentication
- show Commands

### Troubleshoot

- Clear Security Associations
- Troubleshooting Commands
- Sample debug Output

### Related Information

## Introduction

This sample configuration shows how to set up the remote access VPN connection between a Cisco VPN Client (4.x for Windows) and the PIX 500 Series Security Appliance 7.x. The remote VPN Client user authenticates against the Active Directory using a Microsoft Windows 2003 Internet Authentication Service (IAS) RADIUS server.

Refer to Cisco Secure PIX Firewall 6.x and Cisco VPN Client 3.5 for Windows with Microsoft Windows 2000 and 2003 IAS RADIUS Authentication in order to learn more about the same scenario in PIX 6.x with Cisco VPN Client 3.5.

Refer to IPsec Between a VPN 3000 Concentrator and a VPN Client 4.x for Windows using RADIUS for User Authentication and Accounting Configuration Example to establish an IPsec tunnel between a Cisco VPN 3000 Concentrator and a Cisco VPN Client 4.x for Windows using RADIUS for user authentication and accounting.

Refer to Configuring IPsec Between a Cisco IOS Router and a Cisco VPN Client 4.x for Windows Using RADIUS for User Authentication to configure a connection between a router and the Cisco VPN Client 4.x using RADIUS for user authentication.

# Prerequisites

## Requirements

Ensure that you meet this requirement before you attempt this configuration:

- The PIX 500 Series Security Appliance is reachable from the Internet.
- Enable the IAS server to read user objects in Active Directory. Refer to Microsoft – Checklist: Configuring IAS for dial-up and VPN access for more information on IAS.

## Components Used

The information in this document is based on these software and hardware versions:

- PIX 515E Series Security Appliance Software Release 7.1(1)
- Cisco VPN Client version 4.8 for Windows
- Windows 2003 Server with IAS

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Related Products

This configuration can also be used with the Cisco ASA 5500 Series Security Appliance.

## Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

## Background Information

Remote access VPNs address the requirement of the mobile workforce to securely connect to the organization's network. Mobile users are able to set up a secure connection using the VPN Client software installed on their PCs. The VPN Client initiates a connection to a central site device configured to accept these requests. In this example, the central site device is a PIX 500 Series Security Appliance that uses dynamic crypto maps.

In this configuration example, an IPsec tunnel is configured with these elements:

- Crypto maps applied to the outside interfaces on the PIX.
- Extended authentication (xauth) of the VPN Clients against a RADIUS database.
- Dynamic assignment of a private IP address from a pool to VPN Clients.
- The **nat 0 access-list** command functionality, which allows hosts on a LAN to use private IP addresses with a remote user and still get a Network Address Translation (NAT) address from the PIX to visit an untrusted network.

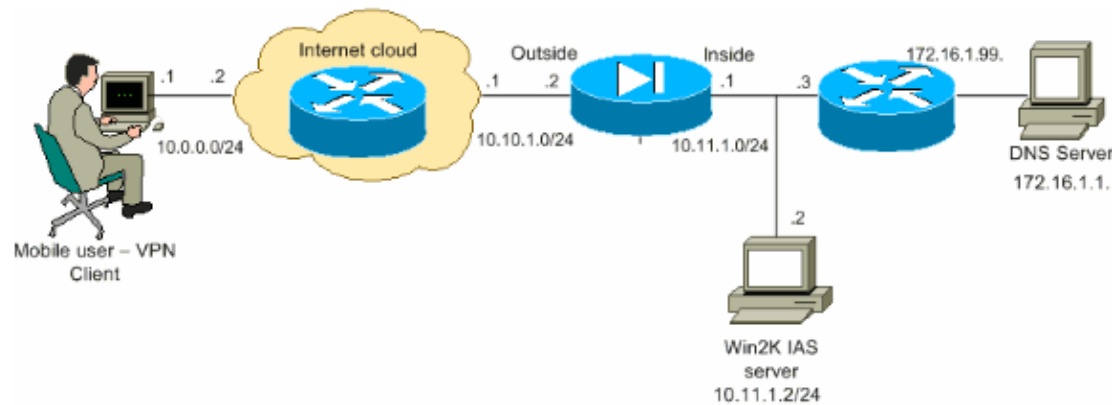
## Configure

In this section, you are presented with the information to configure the remote access VPN connection with xauth using the Windows 2003 IAS server.

**Note:** Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

## Network Diagram

This document uses this network setup:



## Configurations

This document uses these configurations:

- PIX 515E Security Appliance Configuration
- Cisco VPN Client 4.8 for Windows Configuration
- Microsoft Windows 2003 Server with IAS Configuration

### PIX 515E Security Appliance

```
PIX Version 7.1(1)
!
hostname PIX

!--- Specify the domain name for the Security Appliance.

domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names

!--- Configure the outside and inside interfaces.

!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.10.1.2 255.255.255.0
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.11.1.1 255.255.255.0
!

!--- Output is suppressed.

!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
```

```
!--- Specify the interface which points toward the DNS server
!--- to enable the PIX to use DNS.

dns domain-lookup inside
dns server-group DefaultDNS
  timeout 30

!--- Specify the location of the DNS server in the DefaultDNS group.

name-server 172.16.1.1

domain-name cisco.com

!--- This access list is used for a nat zero command that prevents
!--- traffic which matches the access list from undergoing NAT.

access-list 101 extended permit ip 172.16.0.0 255.255.0.0 10.16.20.0 255.255.255.00

pager lines 24
logging buffer-size 500000
logging console debugging
logging monitor errors
mtu outside 1500
mtu inside 1500

!--- Create a pool of addresses from which IP addresses are assigned
!--- dynamically to the remote VPN Clients.

ip local pool vpnclient 10.16.20.1-10.16.20.5

no failover
icmp permit any outside
icmp permit any inside
no asdm history enable
arp timeout 14400

!--- NAT 0 prevents NAT for networks specified in the ACL 101.
!--- The nat 1 command specifies Port Address Translation (PAT)
!--- using 10.10.1.5 for all other traffic.

global (outside) 1 10.10.1.5
nat (inside) 0 access-list 101
nat (inside) 1 0.0.0.0 0.0.0.0
route outside 10.10.0.0 255.255.255.0 10.10.1.1 1
route outside 0.0.0.0 0.0.0.0 10.11.1.1 1
route inside 172.16.0.0 255.255.0.0 10.11.1.3 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00
timeout mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute

!--- Create the AAA server group "vpn" and specify the protocol as RADIUS.
!--- Specify the IAS server as a member of the "vpn" group and provide the
!--- location and key.
```

```
aaa-server vpn protocol radius
aaa-server vpn host 10.11.1.2
key cisco123

!--- Create the VPN users' group policy and specify the DNS server IP address
!--- and the domain name in the group policy.

group-policy vpn3000 internal
group-policy vpn3000 attributes
dns-server value 172.16.1.1
default-domain value cisco.com

!--- In order to identify remote access users to the Security Appliance,
!--- you can also configure usernames and passwords on the device
!--- in addition to using AAA.

username vpn3000 password nPtKy7KDCerzhKeX encrypted
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!--- PHASE 2 CONFIGURATION ---!
!--- The encryption types for Phase 2 are defined here.
!--- A single DES encryption with
!--- the md5 hash algorithm is used.

crypto ipsec transform-set my-set esp-des esp-md5-hmac

!--- Defines a dynamic crypto map with
!--- the specified encryption settings.

crypto dynamic-map dynmap 10 set transform-set my-set

!--- Enable Reverse Route Injection (RRI), which allows the Security Appliance
!--- to learn routing information for connected clients.

crypto dynamic-map dynmap 10 set reverse-route

!--- Binds the dynamic map to the IPsec/ISAKMP process.

crypto map mymap 10 ipsec-isakmp dynamic dynmap

!--- Specifies the interface to be used with
!--- the settings defined in this configuration.

crypto map mymap interface outside

!--- PHASE 1 CONFIGURATION ---!

!--- This configuration uses ISAKMP policy 10.
!--- Policy 65535 is included in the configuration by default.
```

```
!--- The configuration commands here define the Phase  
!--- 1 policy parameters that are used.
```

```
isakmp enable outside  
isakmp policy 10 authentication pre-share  
isakmp policy 10 encryption des  
isakmp policy 10 hash md5  
isakmp policy 10 group 2  
isakmp policy 10 lifetime 1000
```

```
isakmp policy 65535 authentication pre-share  
isakmp policy 65535 encryption 3des  
isakmp policy 65535 hash sha  
isakmp policy 65535 group 2  
isakmp policy 65535 lifetime 86400
```

```
!--- The Security Appliance provides the default tunnel groups  
!--- for remote access (DefaultRAGroup).
```

```
tunnel-group DefaultRAGroup general-attributes  
authentication-server-group (outside) vpn
```

```
!--- Create a new tunnel group and set the connection  
!--- type to IPsec remote access (ipsec-ra).
```

```
tunnel-group vpn3000 type ipsec-ra
```

```
!--- Associate the vpnclient pool to the tunnel group using the address pool.  
!--- Associate the AAA server group (VPN) with the tunnel group.
```

```
tunnel-group vpn3000 general-attributes  
address-pool vpnclient  
authentication-server-group vpn  
default-group-policy vpn3000
```

```
!--- Enter the pre-shared-key to configure the authentication method.
```

```
tunnel-group vpn3000 ipsec-attributes  
pre-shared-key *
```

```
telnet timeout 5  
ssh timeout 5  
console timeout 0
```

```
!  
class-map inspection_default  
match default-inspection-traffic  
!
```

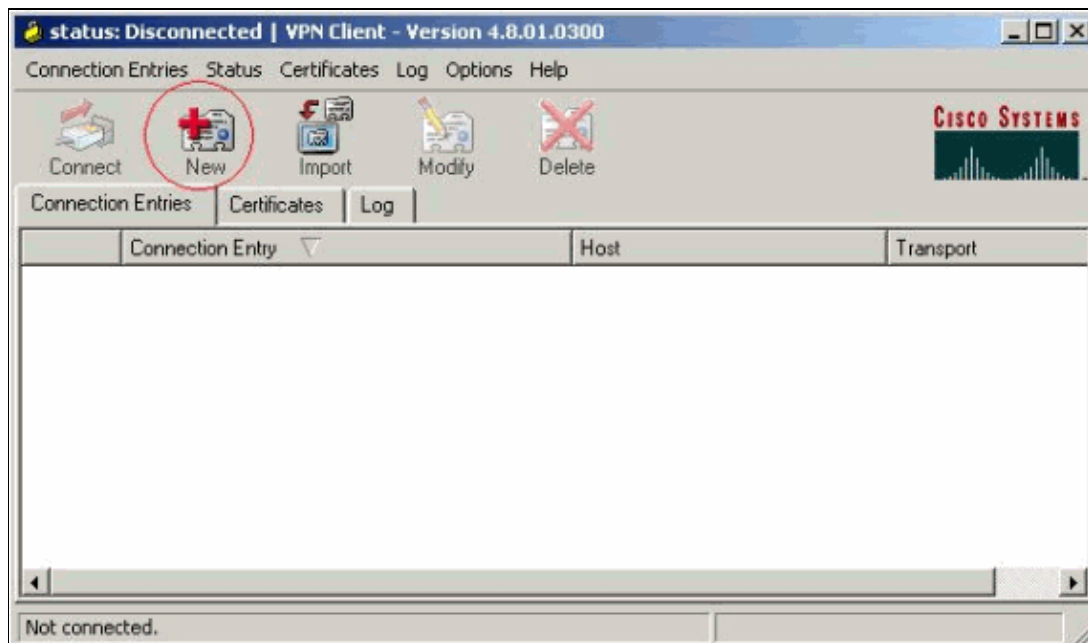
```
policy-map global_policy  
class inspection_default  
inspect dns maximum-length 512  
inspect ftp  
inspect h323 h225  
inspect h323 ras  
inspect netbios  
inspect rsh  
inspect rtsp
```

```
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global
Cryptochecksum:ecb58c5d8ce805b3610b198c73a3d0cf
: end
```

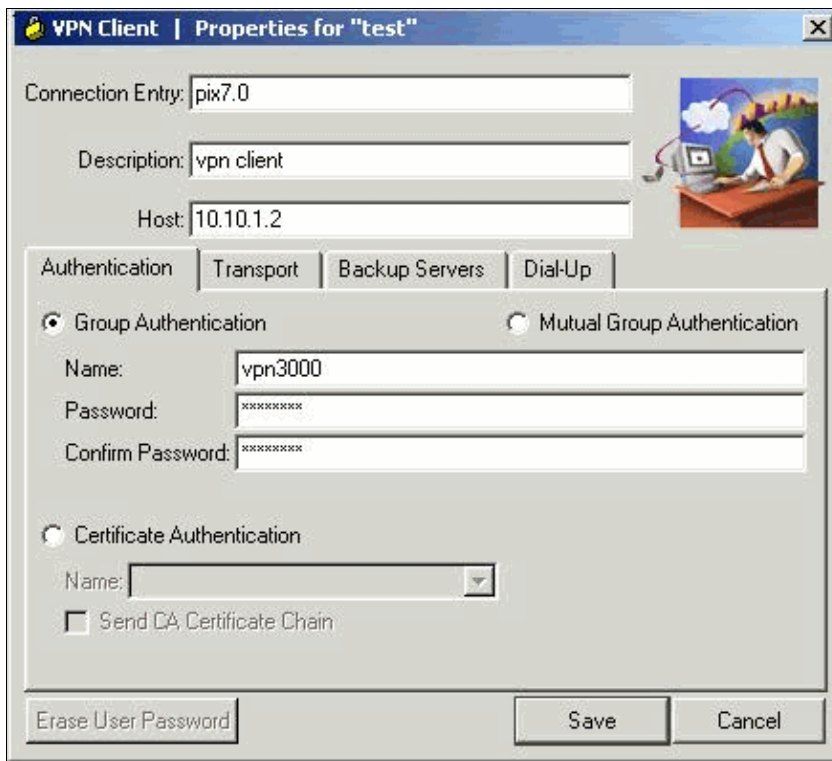
## VPN Client 4.8 Configuration

Complete these steps to configure the VPN Client 4.8.

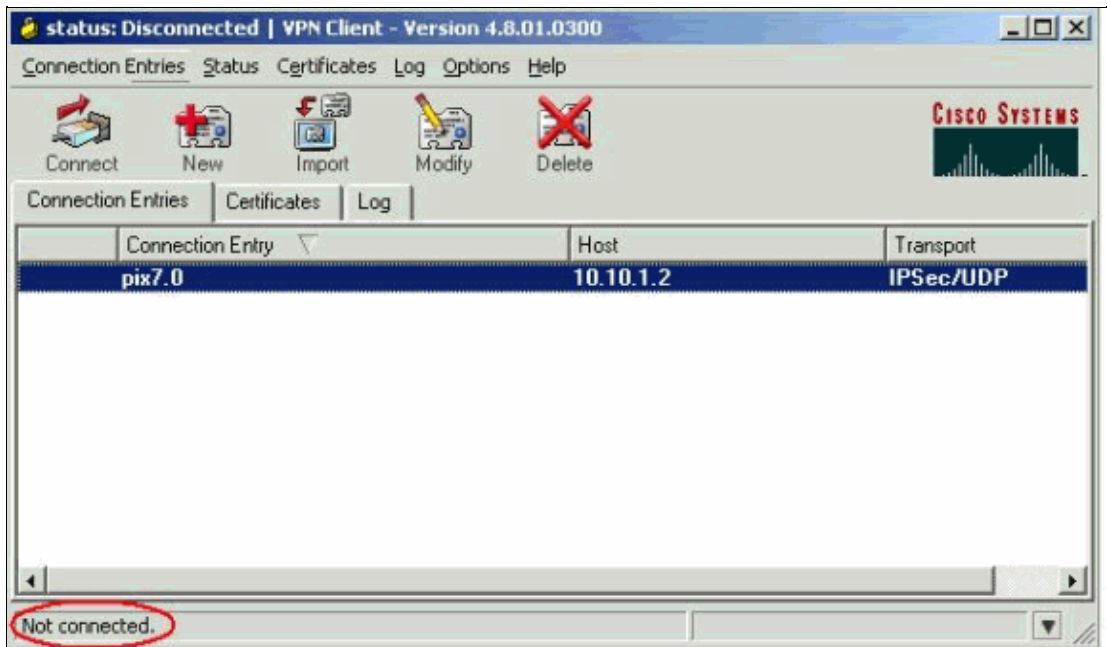
1. Select **Start > Programs > Cisco Systems VPN Client > VPN Client**.
2. Click **New** to launch the Create New VPN Connection Entry window.



3. Enter the name of the Connection Entry along with a description. Enter the outside IP address of the PIX Firewall in the Host box. Then enter the VPN Group name and password and click **Save**.



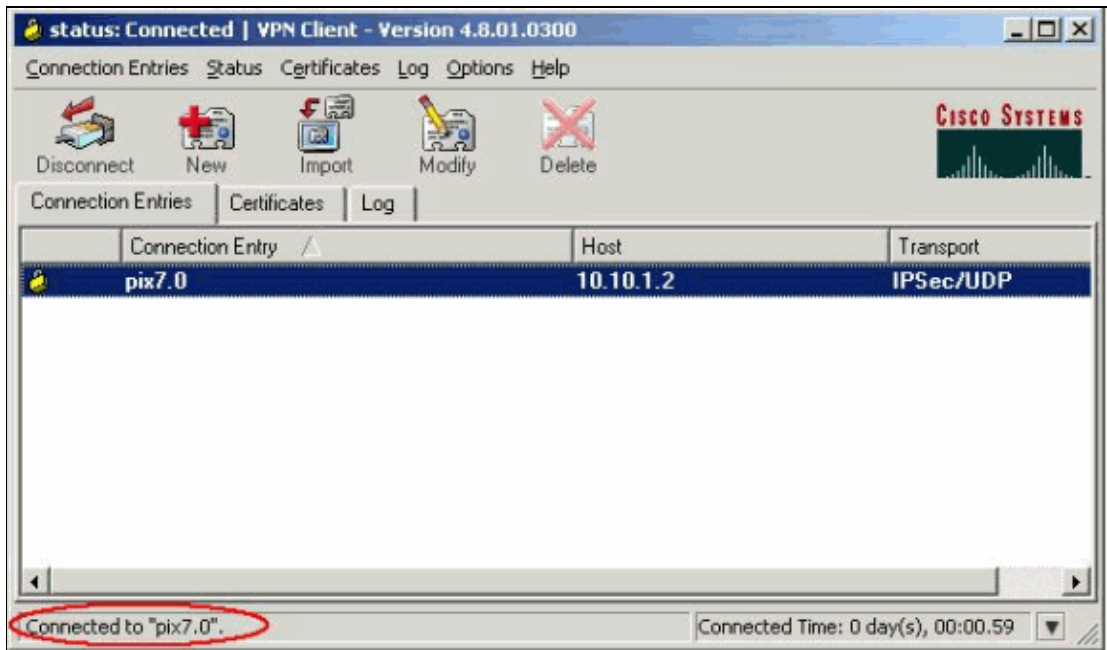
4. Click on the connection you would like to use and click **Connect** from the VPN Client main window.



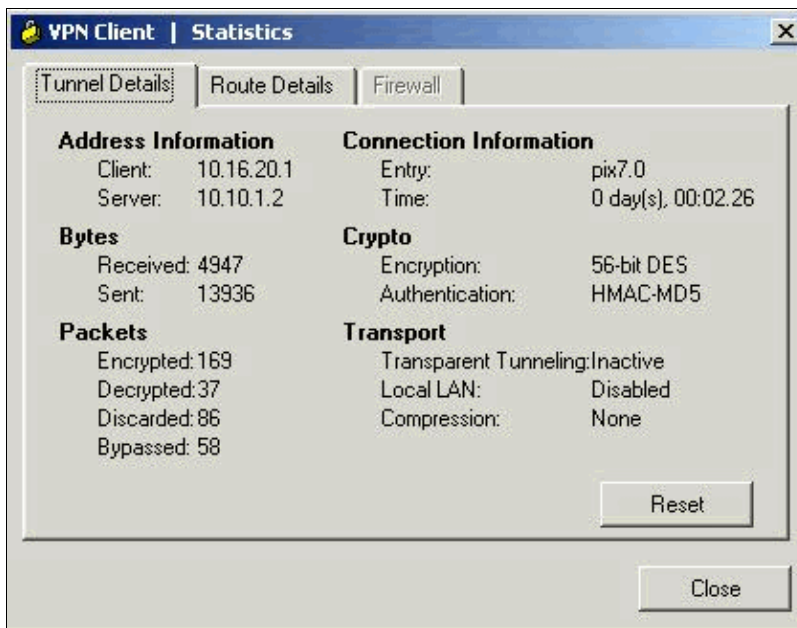
5. When prompted, enter the Username and Password information for xauth and click **OK** to connect to the remote network.



6. The VPN Client gets connected with the PIX at the central site.



7. Select **Status > Statistics** to check the tunnel statistics of the VPN Client.



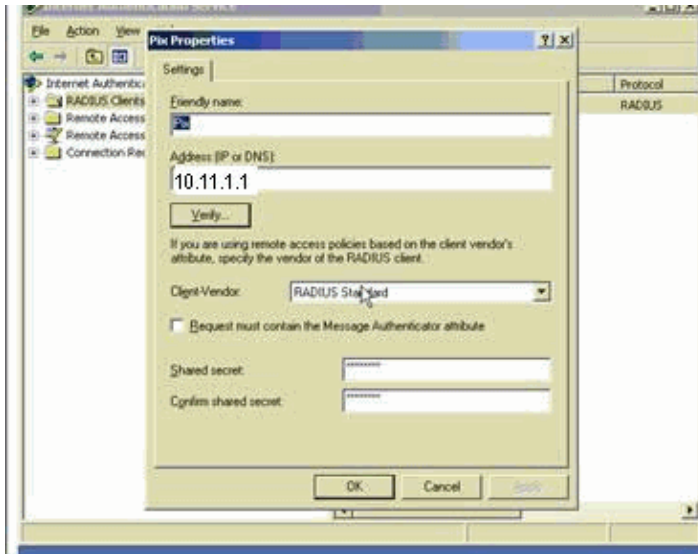
## Microsoft Windows 2003 Server with IAS Configuration

Complete these steps to configure the Microsoft Windows 2003 server with IAS.

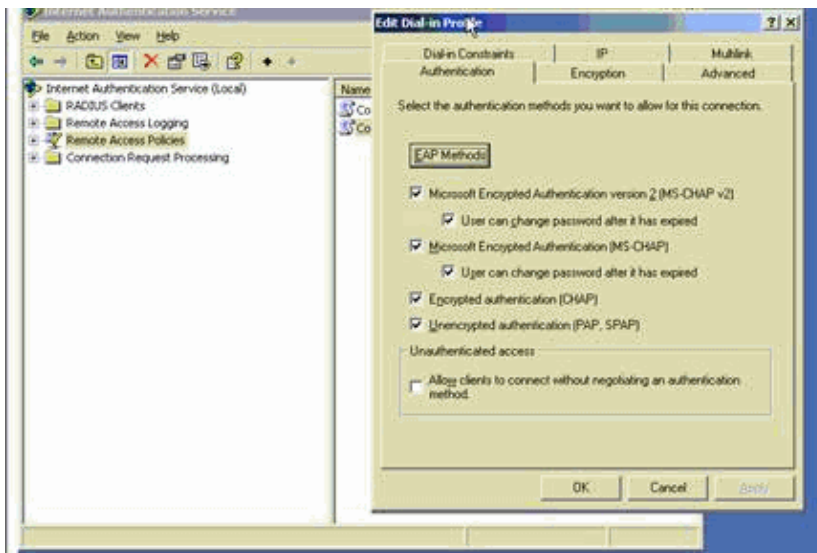
**Note:** These steps assume that IAS is already installed on the local machine. If not, add this through **Control Panel > Add/Remove Programs**.

1. Select **Administrative Tools > Internet Authentication Service** and right-click on **RADIUS Client** to add a new RADIUS client. When you have typed the client information, click **OK**.

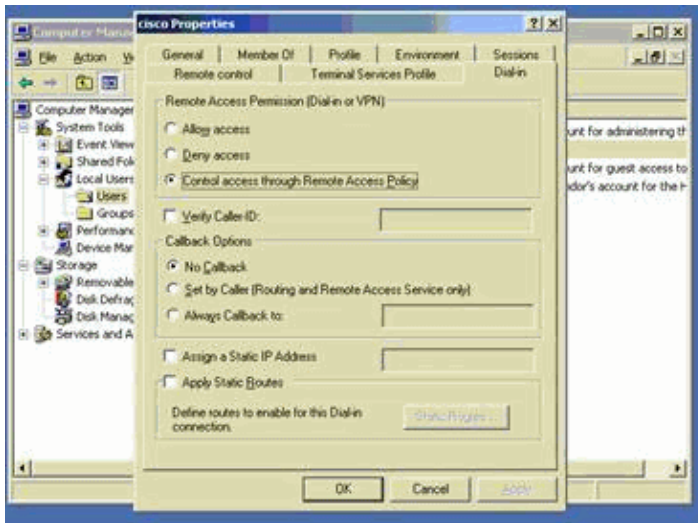
This example shows a client named **Pix** with an IP address of 10.11.1.1. Client-Vendor is set to **RADIUS Standard**, and the shared secret is **cisco123**.



2. Go to **Remote Access Policies**, right-click on **Connections to Other Access Servers**, and select **Properties**.
  3. Ensure that the option for **Grant Remote Access Permissions** is selected.
  4. Click **Edit Profile** and check these settings:
    - ◆ On the **Authentication** tab, check **Unencrypted authentication (PAP, SPAP), MS-CHAP, and MS-CHAP-v2**.
    - ◆ On the **Encryption** tab, ensure that the option for **No Encryption** is selected.
- Click **OK** when you are finished.



5. Select **Administrative Tools > Computer Management > System Tools > Local Users and Groups**, right-click on **Users** and select **New Users** to add a user into the local computer account.
  6. Add a user with Cisco password **password1** and check this profile information:
    - ◆ On the **General** tab, ensure that the option for **Password Never Expired** is selected instead of the option for **User Must Change Password**.
    - ◆ On the **Dial-in** tab, select the option for **Allow access** (or leave the default setting of **Control access through Remote Access Policy**).
- Click **OK** when you are finished.



## Password Expiry Feature

The security appliance supports password management for the RADIUS and LDAP protocols. It supports the `password-expire-in-days` option for LDAP only.

You can configure **password management** for IPSec remote access and SSL VPN tunnel-groups.

When you configure the **password-management** command, the security appliance notifies the remote user at login that the current password of the user is about to expire or has expired. The security appliance then offers the user the opportunity to change the password. If the current password has not yet expired, the user can still log in with that password.

This command is valid for AAA servers that support such notification. The security appliance ignores this command if RADIUS or LDAP authentication has not been configured.

When a user password expires and the user attempts to log with a VPN client to the ASA, the `Password needs to be changed but password management disabled` error message appears on the Cisco client software. Enable `Password-Management` with the **password-management** command in the tunnel group general attributes mode in order to resolve this issue.

This is a sample configuration to configure LDAP:

```
aaa-server LDAP-AD protocol ldap
aaa-server LDAP-AD host <IP-of-Windows-AD>
server-port 636
ldap-base-dn <AD base DN>
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-dn <login user DN>
ldap-login-password <password for login user DN>
ldap-over-ssl enable
```

This is a sample configuration for Password-Expiry :

```
tunnel-group <Tunnel-group> type remote-access
tunnel-group <Tunnel-group> general-attributes
authentication-server-group LDAP-AD
default-group-policy DfltGrpPolicy
password-management password-expire-in-days <number of days>
```

**Note:** In PIX/ASA, the CHAP, MS-CHAP-v1 and MS-CHAP-v2 can be used for RADIUS authentication with an IAS server as PAP. In order to make use of these protocols, you need to use the Password Expiry feature. Use the **password-management** command in order to set up the password expiration feature in the tunnel group general attributes mode.

## Verify

### AAA Authentication

From the PIX, use the *Test* keyword with the **aaa authentication** command in global configuration mode in order to verify the user authentication with the AAA server. After you enter the command, the PIX prompts you to enter the username and password to validate. When the user credential is verified and it is valid, you receive the Authentication Successful message.

```
pix(config-aaa-server-host)#test aaa authentication radius host 10.11.1.2

Username: administrator
Password: *****

INFO: Attempting Authentication test to IP address <10.11.1.2> (timeout: 12 seconds)
INFO: Authentication Successful
```

### show Commands

Use this section to confirm your configuration works properly.

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

- **show crypto isakmp sa** Shows all current IKE Security Associations (SAs) at a peer.
- **show crypto ipsec sa** Shows the settings used by current SAs.

```
PIX#show crypto ipsec sa

                                interface: outside
Crypto map tag: dynmap, seq num: 10, local addr: 10.10.1.2

local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (10.16.20.1/255.255.255.255/0/0)
current_peer: 10.0.0.1, username: administrator
dynamic allocated peer ip: 10.16.20.1

#pkts encaps: 33, #pkts encrypt: 33, #pkts digest: 33
#pkts decaps: 33, #pkts decrypt: 33, #pkts verify: 33
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
#send errors: 0, #recv errors: 0

local crypto endpt.: 10.10.1.2, remote crypto endpt.: 10.0.0.1

path mtu 1500, ipsec overhead 60, media mtu 1500
current outbound spi: CA8BF3BC

inbound esp sas:
spi: 0xE4F08D9F (3840970143)
transform: esp-des esp-md5-hmac
in use settings ={RA, Tunnel, }
slot: 0, conn_id: 1, crypto-map: dynmap
sa timing: remaining key lifetime (sec): 28689
```

```
IV size: 8 bytes
replay detection support: Y
outbound esp sas:
spi: 0xCA8BF3BC (3398169532)
transform: esp-des esp-md5-hmac
in use settings = {RA, Tunnel, }
slot: 0, conn_id: 1, crypto-map: dynmap
sa timing: remaining key lifetime (sec): 28687
IV size: 8 bytes
replay detection support: Y
```

## Troubleshoot

This section provides information you can use to troubleshoot your configuration. Sample debug output is also shown.

### Clear Security Associations

When you troubleshoot, be sure to clear existing Security Associations after you make a change. In the privileged mode of the PIX, use these commands:

- **clear [crypto] ipsec sa** Deletes the active IPsec SAs. The keyword **crypto** is optional.
- **clear [crypto] isakmp sa** Deletes the active IKE SAs. The keyword **crypto** is optional.

### Troubleshooting Commands

The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

**Note:** Refer to Important Information on Debug Commands before you use **debug** commands.

- **debug crypto ipsec** Displays the IPsec negotiations of Phase 2.
- **debug crypto isakmp** Displays the ISAKMP negotiations of Phase 1.

### Sample debug Output

- PIX Firewall
- VPN Client 3.5 for Windows

#### PIX Firewall

```
PIX#debug crypto isakmp 7
PIX# May 22 22:32:25 [IKEv1]: IP = 10.0.0.1, IKE_DECODE RECEIVED Message (msgid=
9117fc3d) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length :
80
May 22 22:32:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, processing hash payload
May 22 22:32:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, processing notify payload
May 22 22:32:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1

!--- Dead-Peer-Detection Exchange

0.0.0.1, Received keep-alive of type DPD R-U-THERE (seq number 0x36a6342)
May 22 22:32:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x36a6342)
May 22 22:32:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
```

0.0.0.1, constructing blank hash payload  
May 22 22:32:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, constructing qm hash payload  
May 22 22:32:25 [IKEv1]: IP = 10.0.0.1, IKE\_DECODE SENDING Message (msgid=4c047e39) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80  
May 22 22:32:36 [IKEv1]: IP = 10.0.0.1, IKE\_DECODE RECEIVED Message (msgid=a1063306) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80  
May 22 22:32:36 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, processing hash payload  
May 22 22:32:36 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, processing notify payload  
May 22 22:32:36 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, Received keep-alive of type DPD R-U-THERE (seq number 0x36a6343)  
May 22 22:32:36 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x36a6343)  
May 22 22:32:36 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, constructing blank hash payload  
May 22 22:32:36 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, constructing qm hash payload  
May 22 22:32:36 [IKEv1]: IP = 10.0.0.1, IKE\_DECODE SENDING Message (msgid=ceada919) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80  
May 22 22:32:47 [IKEv1]: IP = 10.0.0.1, IKE\_DECODE RECEIVED Message (msgid=ab66b5e2) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80  
May 22 22:32:47 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, processing hash payload  
May 22 22:32:47 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, processing notify payload  
May 22 22:32:47 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, Received keep-alive of type DPD R-U-THERE (seq number 0x36a6344)  
May 22 22:32:47 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x36a6344)  
May 22 22:32:47 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, constructing blank hash payload  
May 22 22:32:47 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, constructing qm hash payload  
May 22 22:32:47 [IKEv1]: IP = 10.0.0.1, IKE\_DECODE SENDING Message (msgid=b5341ba5) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80  
May 22 22:32:58 [IKEv1]: IP = 10.0.0.1, IKE\_DECODE RECEIVED Message (msgid=22d77ee7) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80  
May 22 22:32:58 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, processing hash payload  
May 22 22:32:58 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, processing notify payload  
May 22 22:32:58 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, Received keep-alive of type DPD R-U-THERE (seq number 0x36a6345)  
May 22 22:32:58 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x36a6345)  
May 22 22:32:58 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, constructing blank hash payload  
May 22 22:32:58 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, constructing qm hash payload  
May 22 22:32:58 [IKEv1]: IP = 10.0.0.1, IKE\_DECODE SENDING Message (msgid=8d688bd2) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80  
May 22 22:33:14 [IKEv1]: IP = 10.0.0.1, IKE\_DECODE RECEIVED Message (msgid=f949ae6) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80  
May 22 22:33:14 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, processing hash payload  
May 22 22:33:14 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, processing notify payload  
May 22 22:33:14 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, Received keep-alive of type DPD R-U-THERE (seq number 0x36a6346)  
May 22 22:33:14 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x36a6346)  
May 22 22:33:14 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1  
0.0.0.1, constructing blank hash payload  
May 22 22:33:14 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1

```
0.0.0.1, constructing qm hash payload
May 22 22:33:14 [IKEv1]: IP = 10.0.0.1, IKE_DECODE SENDING Message (msgid=fd9fef
25) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
May 22 22:33:25 [IKEv1]: IP = 10.0.0.1, IKE_DECODE RECEIVED Message (msgid=54d3b
543) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
May 22 22:33:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, processing hash payload
May 22 22:33:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, processing notify payload
May 22 22:33:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, Received keep-alive of type DPD R-U-THERE (seq number 0x36a6347)
May 22 22:33:25 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x36a6347)
May 22 22:33:26 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, constructing blank hash payload
May 22 22:33:26 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, constructing qm hash payload
May 22 22:33:26 [IKEv1]: IP = 10.0.0.1, IKE_DECODE SENDING Message (msgid=4d4102
0b) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
May 22 22:33:37 [IKEv1]: IP = 10.0.0.1, IKE_DECODE RECEIVED Message (msgid=af7ad
910) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
May 22 22:33:37 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, processing hash payload
May 22 22:33:37 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, processing notify payload
May 22 22:33:37 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, Received keep-alive of type DPD R-U-THERE (seq number 0x36a6348)
May 22 22:33:37 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, Sending keep-alive of type DPD R-U-THERE-ACK (seq number 0x36a6348)
May 22 22:33:37 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, constructing blank hash payload
May 22 22:33:37 [IKEv1 DEBUG]: Group = vpn3000, Username = administrator, IP = 1
0.0.0.1, constructing qm hash payload
May 22 22:33:37 [IKEv1]: IP = 10.0.0.1, IKE_DECODE SENDING Message (msgid=84cd22
35) with payloads : HDR + HASH (8) + NOTIFY (11) + NONE (0) total length : 80
```

PIX#debug crypto ipsec 7

*!--- Deletes the old SAs.*

```
PIX# IPSEC: Deleted inbound decrypt rule, SPI 0xA7E3E225
  Rule ID: 0x0243DD38
IPSEC: Deleted inbound permit rule, SPI 0xA7E3E225
  Rule ID: 0x024BA720
IPSEC: Deleted inbound tunnel flow rule, SPI 0xA7E3E225
  Rule ID: 0x02445A48
IPSEC: Deleted inbound VPN context, SPI 0xA7E3E225
  VPN handle: 0x018F68A8
IPSEC: Deleted outbound encrypt rule, SPI 0xB9C97D06
  Rule ID: 0x024479B0
IPSEC: Deleted outbound permit rule, SPI 0xB9C97D06
  Rule ID: 0x0243E9E0
IPSEC: Deleted outbound VPN context, SPI 0xB9C97D06
  VPN handle: 0x0224F490
```

*!--- Creates new SAs.*

```
IPSEC: New embryonic SA created @ 0x02448B38,
  SCB: 0x024487E0,
  Direction: inbound
  SPI      : 0xE4F08D9F
  Session ID: 0x00000001
  VPIF num : 0x00000001
  Tunnel type: ra
```

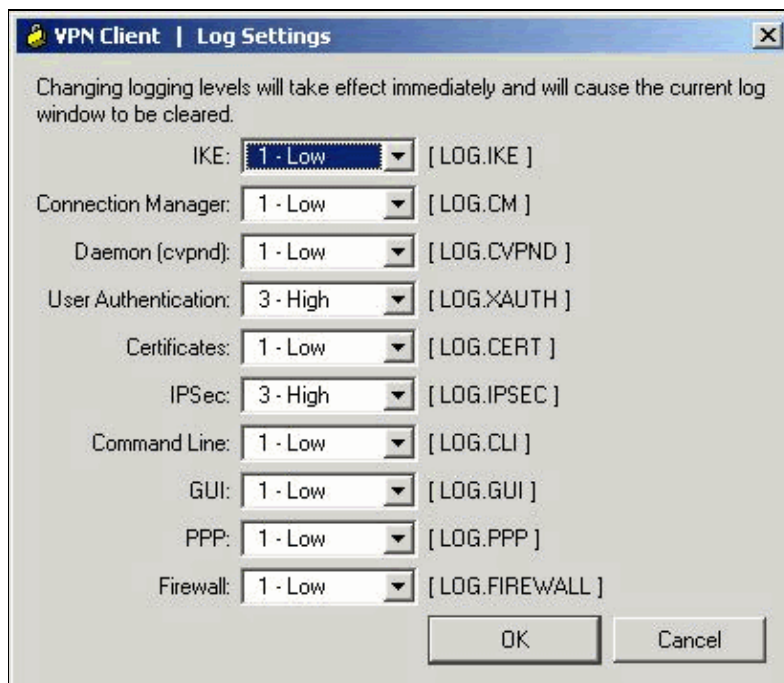
```
Protocol : esp
Lifetime : 240 seconds
IPSEC: New embryonic SA created @ 0x02446750,
SCB: 0x02511DD8,
Direction: outbound
SPI : 0xCA8BF3BC
Session ID: 0x00000001
VPIF num : 0x00000001
Tunnel type: ra
Protocol : esp
Lifetime : 240 seconds
IPSEC: Completed host OBSA update, SPI 0xCA8BF3BC
IPSEC: Creating outbound VPN context, SPI 0xCA8BF3BC
Flags: 0x00000005
SA : 0x02446750
SPI : 0xCA8BF3BC
MTU : 1500 bytes
VCID : 0x00000000
Peer : 0x00000000
SCB : 0x02511DD8
Channel: 0x014A42F0
IPSEC: Completed outbound VPN context, SPI 0xCA8BF3BC
VPN handle: 0x024B9868
IPSEC: New outbound encrypt rule, SPI 0xCA8BF3BC
Src addr: 0.0.0.0
Src mask: 0.0.0.0
Dst addr: 10.16.20.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 0
Use protocol: false
SPI: 0x00000000
Use SPI: false
IPSEC: Completed outbound encrypt rule, SPI 0xCA8BF3BC
Rule ID: 0x024B9B58
IPSEC: New outbound permit rule, SPI 0xCA8BF3BC
Src addr: 10.10.1.2
Src mask: 255.255.255.255
Dst addr: 10.0.0.1
Dst mask: 255.255.255.255
Src ports
Upper: 0
Lower: 0
Op : ignore
Dst ports
Upper: 0
Lower: 0
Op : ignore
Protocol: 50
Use protocol: true
SPI: 0xCA8BF3BC
Use SPI: true
IPSEC: Completed outbound permit rule, SPI 0xCA8BF3BC
Rule ID: 0x024E7D18
IPSEC: Completed host IBSA update, SPI 0xE4F08D9F
IPSEC: Creating inbound VPN context, SPI 0xE4F08D9F
Flags: 0x00000006
SA : 0x02448B38
SPI : 0xE4F08D9F
```

MTU : 0 bytes  
VCID : 0x00000000  
Peer : 0x024B9868  
SCB : 0x024487E0  
Channel: 0x014A42F0  
IPSEC: Completed inbound VPN context, SPI 0xE4F08D9F  
VPN handle: 0x024D90A8  
IPSEC: Updating outbound VPN context 0x024B9868, SPI 0xCA8BF3BC  
Flags: 0x00000005  
SA : 0x02446750  
SPI : 0xCA8BF3BC  
MTU : 1500 bytes  
VCID : 0x00000000  
Peer : 0x024D90A8  
SCB : 0x02511DD8  
Channel: 0x014A42F0  
IPSEC: Completed outbound VPN context, SPI 0xCA8BF3BC  
VPN handle: 0x024B9868  
IPSEC: Completed outbound inner rule, SPI 0xCA8BF3BC  
Rule ID: 0x024B9B58  
IPSEC: Completed outbound outer SPD rule, SPI 0xCA8BF3BC  
Rule ID: 0x024E7D18  
IPSEC: New inbound tunnel flow rule, SPI 0xE4F08D9F  
Src addr: 10.16.20.1  
Src mask: 255.255.255.255  
Dst addr: 0.0.0.0  
Dst mask: 0.0.0.0  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 0  
Use protocol: false  
SPI: 0x00000000  
Use SPI: false  
IPSEC: Completed inbound tunnel flow rule, SPI 0xE4F08D9F  
Rule ID: 0x0243DD38  
IPSEC: New inbound decrypt rule, SPI 0xE4F08D9F  
Src addr: 10.0.0.1  
Src mask: 255.255.255.255  
Dst addr: 10.10.1.2  
Dst mask: 255.255.255.255  
Src ports  
Upper: 0  
Lower: 0  
Op : ignore  
Dst ports  
Upper: 0  
Lower: 0  
Op : ignore  
Protocol: 50  
Use protocol: true  
SPI: 0xE4F08D9F  
Use SPI: true  
IPSEC: Completed inbound decrypt rule, SPI 0xE4F08D9F  
Rule ID: 0x02440628  
IPSEC: New inbound permit rule, SPI 0xE4F08D9F  
Src addr: 10.0.0.1  
Src mask: 255.255.255.255  
Dst addr: 10.10.1.2  
Dst mask: 255.255.255.255  
Src ports

```
Upper: 0
Lower: 0
Op   : ignore
Dst ports
Upper: 0
Lower: 0
Op   : ignore
Protocol: 50
Use protocol: true
SPI: 0xE4F08D9F
Use SPI: true
IPSEC: Completed inbound permit rule, SPI 0xE4F08D9F
Rule ID: 0x0251A970
```

## VPN Client 4.8 for Windows

Select **Log > Log settings** to enable the log levels in the VPN Client.



Select **Log > Log Window** to view the log entries in the VPN Client.



## Related Information

- [Cisco PIX 500 Series Security Appliances](#)
- [Cisco PIX Firewall Software](#)
- [Cisco Secure PIX Firewall Command References](#)
- [RADIUS Support Page](#)
- [IPsec Negotiation/IKE Protocols Support Page](#)
- [Cisco VPN Client Support Page](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco Systems](#)

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Oct 13, 2008

Document ID: 70330

---