



Configuring Cisco PIX Security Appliance with Microsoft Internet Authentication Service and Active Directory using RADIUS to Support Avaya VPNremote Phones – Issue 1.0

Abstract

These Application Notes describe the steps to configure a Cisco PIX Security Appliance to support IPSec VPN tunnel termination of the Avaya VPNremote Phone. The PIX Security Appliance is configured to use the RADIUS protocol with the Microsoft Internet Authentication Service in conjunction with Microsoft Active Directory for authentication of VPNremote Phone users.

The Cisco Adaptive Security Device Manager (ASDM) is used to configure the PIX Security Appliance.

TABLE OF CONTENTS

1.	INTRODUCTION.....	3
2.	NETWORK TOPOLOGY	4
3.	EQUIPMENT AND SOFTWARE VALIDATED.....	5
4.	MICROSOFT ACTIVE DIRECTORY CONFIGURATION.....	6
4.1.	CREATE USER ACCOUNTS	6
4.2.	CREATE USER GROUP	9
4.3.	ADD USERS TO GROUP	11
5.	MICROSOFT IAS CONFIGURATION.....	12
5.1.	RADIUS CLIENT.....	12
5.2.	REMOTE ACCESS POLICY	14
5.3.	RADIUS PORT NUMBER.....	19
6.	CISCO PIX CONFIGURATION	20
6.1.	AAA (RADIUS)	21
6.2.	IP ADDRESS POOL	27
6.3.	TUNNEL GROUP POLICY	28
6.4.	TUNNEL GROUP.....	31
6.5.	IKE	36
6.6.	IPSec	38
6.7.	DEFAULT ROUTE	41
6.8.	VPNREMOTE PHONE TO VPNREMOTE PHONE DIRECT AUDIO	42
7.	AVAYA COMMUNICATION MANAGER CONFIGURATION.....	43
7.1.	IP CODEC SET CONFIGURATION	43
7.2.	IP NETWORK MAP CONFIGURATION	44
7.3.	IP NETWORK REGION CONFIGURATION	45
7.4.	ADD STATION.....	47
8.	AVAYA VPNREMOTE PHONE CONFIGURATION.....	48
8.1.	VPNREMOTE PHONE FIRMWARE.....	48
8.2.	CONFIGURING AVAYA VPNREMOTE PHONE	48
9.	VERIFICATION.....	52
9.1.	VPNREMOTE PHONE IPSec STATISTICS.....	52
9.2.	PIX LOGGING	52
9.3.	IAS LOGGING	53
9.4.	AVAYA COMMUNICATION MANAGER "LIST REGISTERED-IP-STATIONS"	55
9.5.	AVAYA COMMUNICATION MANAGER "STATUS STATION"	55
10.	TROUBLESHOOTING.....	56
10.1.	INCORRECT VPNREMOTE PHONE USER NAME (AD).....	57
10.2.	INCORRECT VPNREMOTE PHONE USER PASSWORD (AD).....	58
10.3.	USER ACCOUNT: REMOTE ACCESS PERMISSION DISABLED (AD)	59
10.4.	USER ACCOUNT NOT ADDED TO GROUP (AD).....	60
10.5.	INCORRECT AUTHENTICATION METHOD (IAS)	61
10.6.	INCORRECT RADIUS CLIENT IP ADDRESS (IAS).....	61
10.7.	IAS / PIX MISMATCHED SHARED SECRET (IAS).....	62
11.	CONCLUSION.....	62
12.	REFERENCES.....	63

1. Introduction

These Application Notes describe the steps to configure a Cisco PIX Security Appliance, referred to as “PIX” throughout the remainder of these Application Notes, to support IPsec VPN (Virtual Private Network) tunnel termination of the Avaya VPNremote Phone. The PIX is configured to use the RADIUS (Remote Authentication Dial In User Service) protocol with the Microsoft Internet Authentication Service (IAS) in conjunction with Microsoft Active Directory (AD) for authentication of VPNremote Phone users. The Cisco Adaptive Security Device Manager (ASDM) application provides a Graphical User Interface to the PIX and is used to configure the PIX in these Application Notes.

The Avaya VPNremote™ Phone is a software based IPsec VPN client integrated into the firmware of an Avaya 4600 Series IP Telephone. This capability allows the Avaya IP Telephone to be plugged in and used over a secure IPsec VPN from any broadband Internet connection. The end user experiences the same IP telephone features as if the phone was being used in the office. Avaya IP Telephone models supporting the Avaya VPNremote Phone firmware include the 4610SW, 4620SW, 4621SW, 4622SW and 4625SW.

Release 2 of the Avaya VPNremote Phone, used in these Application Notes, extends the support of head-end VPN gateways to include Cisco security platforms. The configuration steps described in these Application Notes utilize a PIX model 525. However, these configuration steps can be applied to other PIX models using the software version specified in **Table 1**.

XAuth is a draft RFC developed by the Internet Engineering Task Force (IETF) based on the Internet Key Exchange (IKE) protocol. The VPNremote Phone communicates with the PIX using IKE with a pre-shared key. XAuth allows security gateways to perform user authentication in a separate phase after the IKE authentication phase 1 exchange is complete. The VPNremote Phone uses the pre-shared key to authenticate with the PIX and creates a temporary secure path to allow the VPNremote Phone user to present credentials (username/password) to the PIX. The PIX passes the VPNremote Phone user credentials to the Microsoft IAS / AD server using the RADIUS protocol for authentication and policy checking. After the VPNremote Phone user authentication is successful, the PIX assigns an IP address to the VPNremote Phone from a pre-configured IP Address Pool.

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 1**. The Main Campus location contains the PIX functioning as perimeter security device and VPN head-end. The Avaya WebLM License Manager, Phone Configuration File Server, Microsoft IAS, Microsoft AD, and DNS Server are all running on the same physical Windows 2003 Server connected to the trusted enterprise LAN. The Avaya S8710 Media Server and Avaya G650 Media Gateway are also located at the Main Campus.

The Avaya VPNremote Phones are located in the public network and configured to establish an IPSec tunnel to the Public (outside) IP address of the PIX. The PIX assigns IP addresses to the VPNremote Phones after successful authentication. The assigned IP addresses, also known as the inner addresses, will be used by the VPNremote Phones when communicating inside the IPSec tunnel and in the private corporate network to Avaya Communication Manager. Once the IPSec tunnel is established, the VPNremote Phone accesses the Phone Configuration File Server, DNS server, and WebLM server. The VPNremote Phone then initiates an H.323 registration with Avaya Communication Manager.

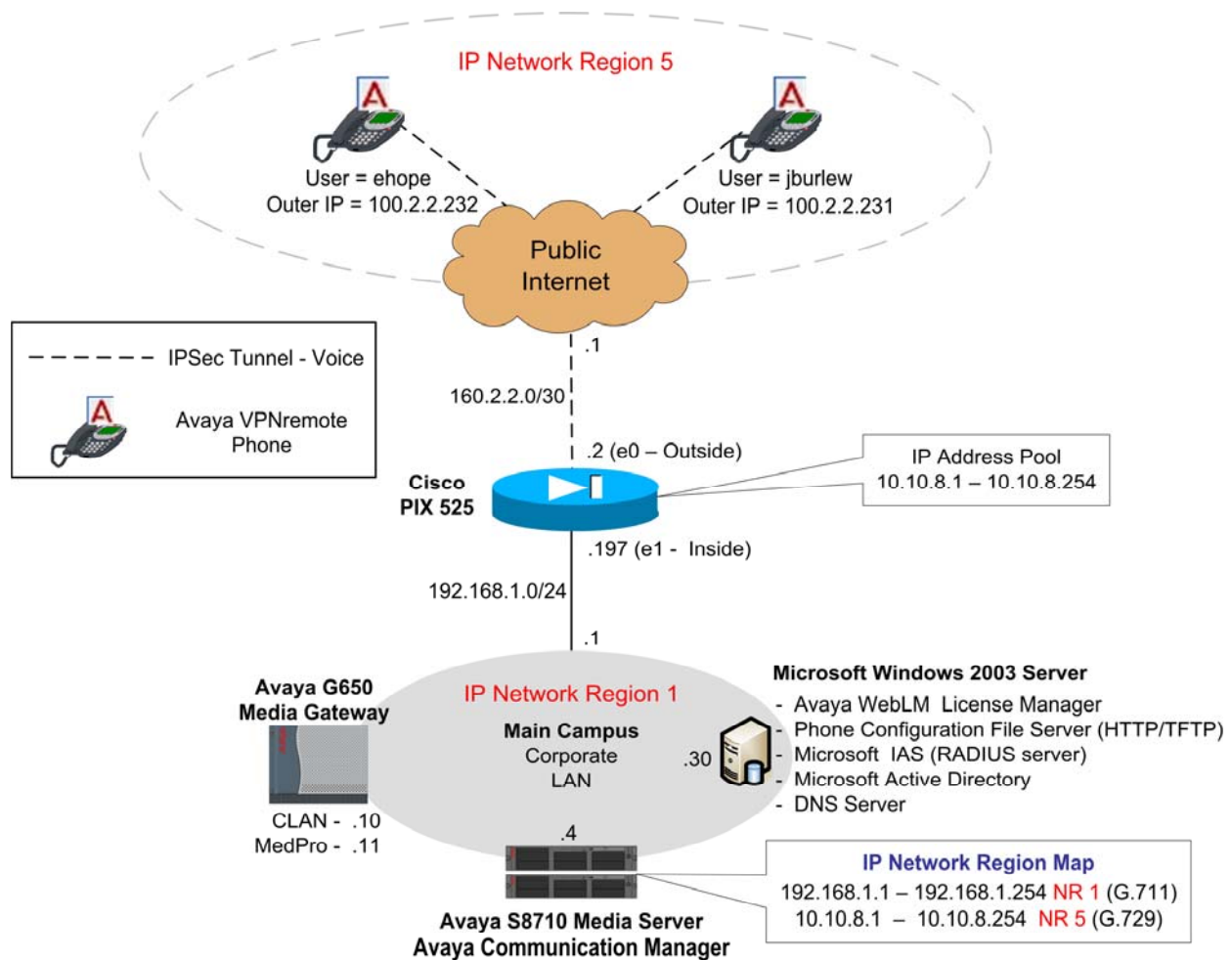


Figure 1: Network Diagram

3. Equipment and Software Validated

The information in these Application Notes is based on the software and hardware versions list in **Table 1** below.

Equipment	Software Version
Avaya S8710 Media Server	Avaya Communication Manager 3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MedPro (TN2302AP)	FW 022 (HW6) FW 016 (HW1) FW 108 (HW12)
Avaya 4610SW IP Telephones	R2.3.2 – Release 2 (a10bVPN232_1.bin)
Avaya 4625SW IP Telephones	R2.5.2 – Release 2 (a25VPN252_1.bin)
Avaya WebLM License Manager	V4.3
Cisco PIX model 525	7.2(1)
Cisco Adaptive Security Device Manager	5.2(1)
Microsoft Internet Authentication Service	Windows 2003 Server IAS Version 5.2.3790
Microsoft Active Directory - User and Computers	Windows 2003 Server AD Version 5.2.3790

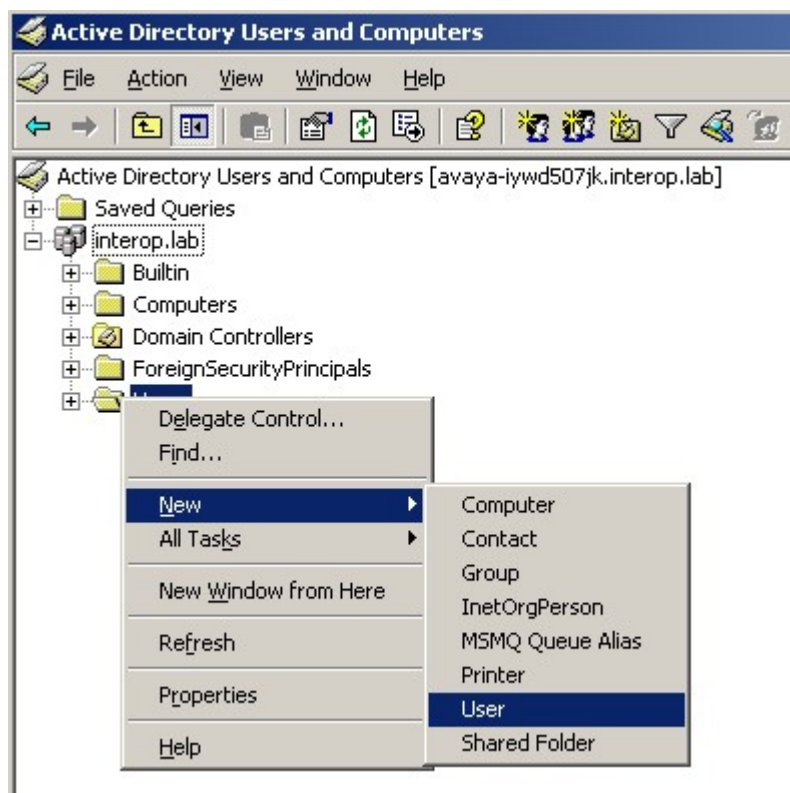
Table 1 – Software/Hardware Version Information

4. Microsoft Active Directory Configuration

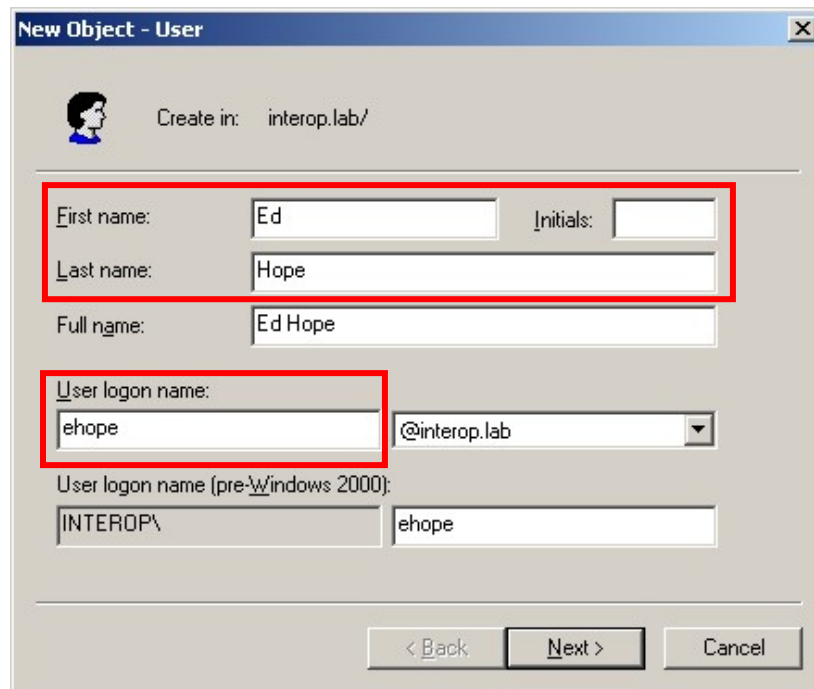
4.1. Create User Accounts

The steps below create a new user account for one of the VPNremote Phones shown in **Figure 1**. These Application Notes assume Active Directory is installed and operational.

1. On the Microsoft Windows 2003 Server running Active Directory, open the **Active Directory Users and Computers** application window by selecting **Start > All Programs > Administrative Tools > Active Directory Users and Computers**. Right click the **Users** folder and select **New > User** from the pop-up menu as shown below. Alternatively, the **Create New Users** icon from the tool bar can be used.

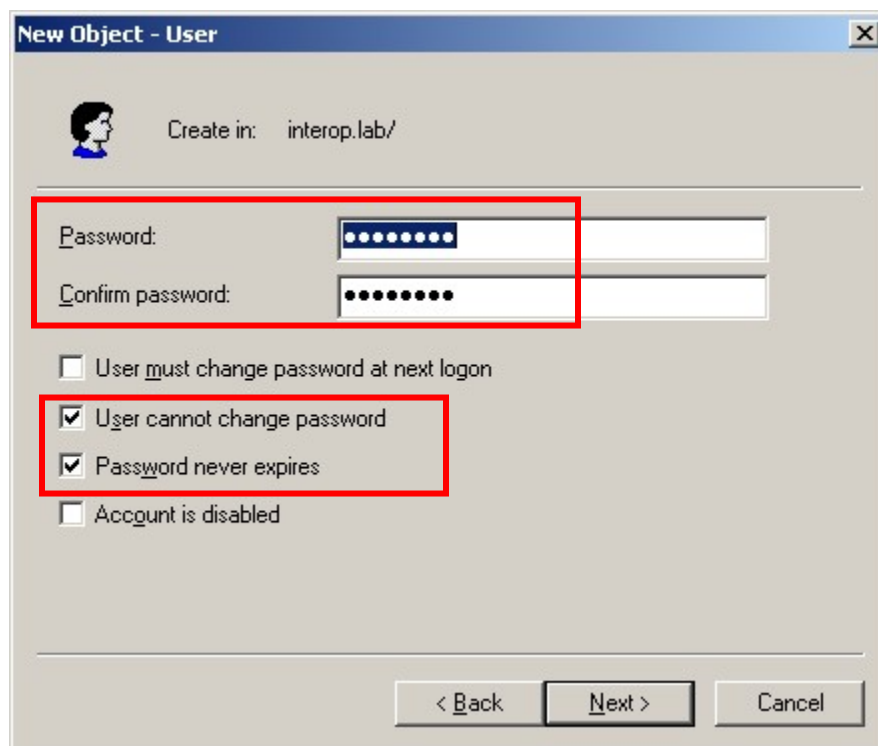


2. Enter the user information as highlighted below. All remaining fields may be left default. Click **Next** to continue.



The 'New Object - User' dialog box is shown. The 'Create in:' field is set to 'interop.lab/'. The 'First name:' field contains 'Ed' and the 'Last name:' field contains 'Hope'. The 'Full name:' field displays 'Ed Hope'. The 'User logon name:' field contains 'ehope' and the domain dropdown is set to '@interop.lab'. The 'User logon name (pre-Windows 2000):' field contains 'INTEROP\ehope'. The 'Next >' button is highlighted.

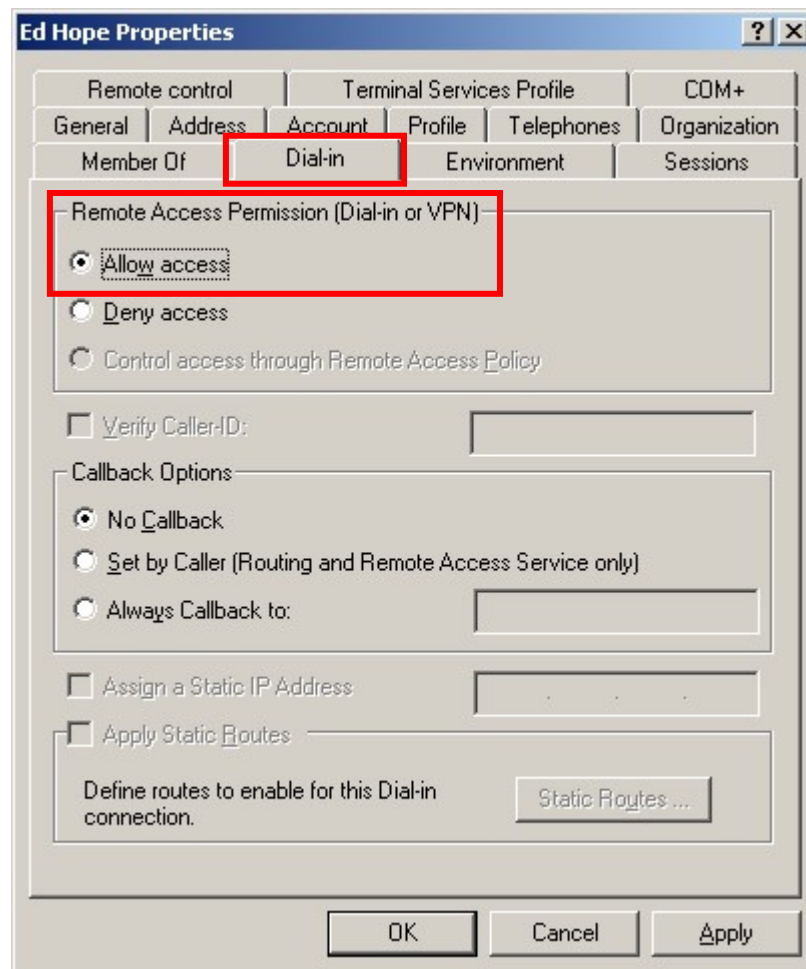
3. Enter the password and the password policy options shown below. Click **Next** to continue then **Finish**.



The 'New Object - User' dialog box is shown. The 'Password:' and 'Confirm password:' fields are highlighted with a red box. The 'User must change password at next logon' checkbox is unchecked. The 'User cannot change password' and 'Password never expires' checkboxes are checked. The 'Account is disabled' checkbox is unchecked. The 'Next >' button is highlighted.

4. The new account is now created with default properties, to allow this account to request authentication remotely, via an IPsec tunnel to the PIX, the account's Remote Access Permission must be enabled as shown below.

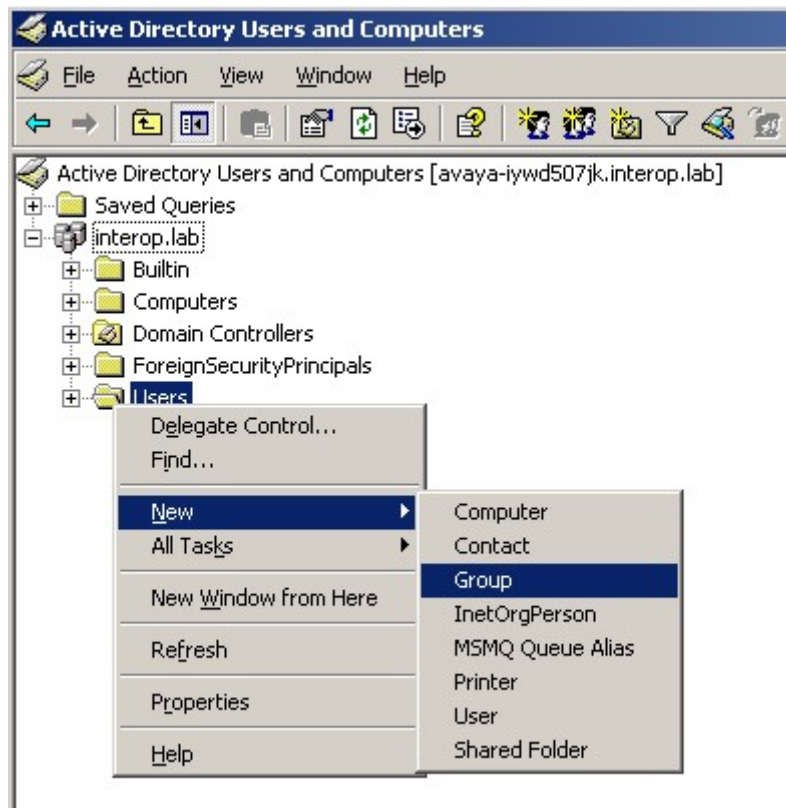
Edit the properties of the newly created user account by right click the account name under the Users folder. Select Properties from the pop-up window. Select the **Dial-in** tab then the **Allow access** option. All remaining fields can be left as default. Click **OK** to save and exit the user Properties window.



4.2. Create User Group

The steps below create a new user group to allow all VPNremote Phone user accounts to be grouped together and used by IAS to apply a consistent access policy.

1. From the **Active Directory Users and Computers** window, right click the **Users** folder and select the **New > Group** from the pop-up menu as shown below. Alternatively, the **Create New Group** icon from the tool bar can be used.



2. Enter a descriptive group name as highlighted below. All remaining fields may be left default. Click **OK**.

New Object - Group

Create in: interop.lab/

Group name:
VPNphone Users

Group name (pre-Windows 2000):
VPNphone Users

Group scope:

- ☐ Domain local
- ☒ Global
- ☐ Universal

Group type:

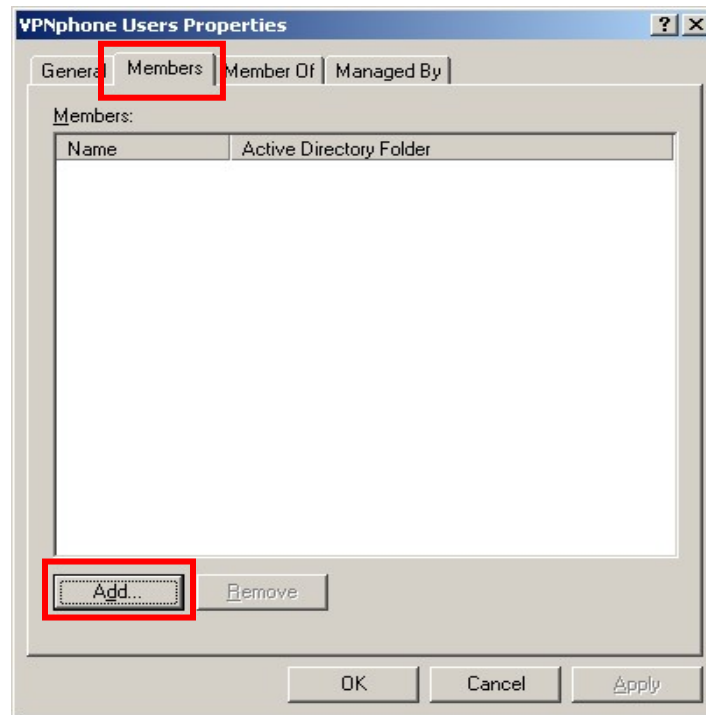
- ☒ Security
- ☐ Distribution

OK Cancel

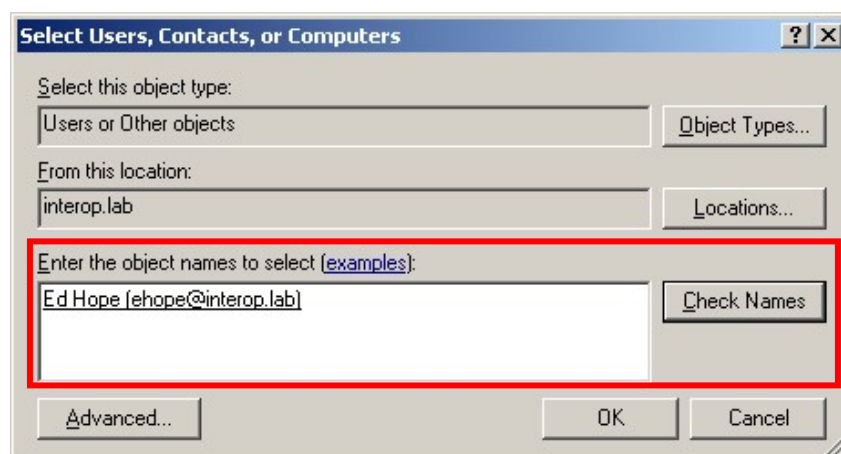
4.3. Add Users to Group

The steps below add the newly created user to the newly created user group.

1. Edit the properties of the newly created user group by right click the group name under the Users folder. Select **Properties** from the pop-up window. From the Properties window, select the **Members** tab then the **Add** button.



2. Enter the user name to add to the group. Entering the first few letters of the user name then clicking the **Check Names** button is a short cut for speed and accuracy. Click **OK** to save, then click **OK** again to exit the Group Properties window.

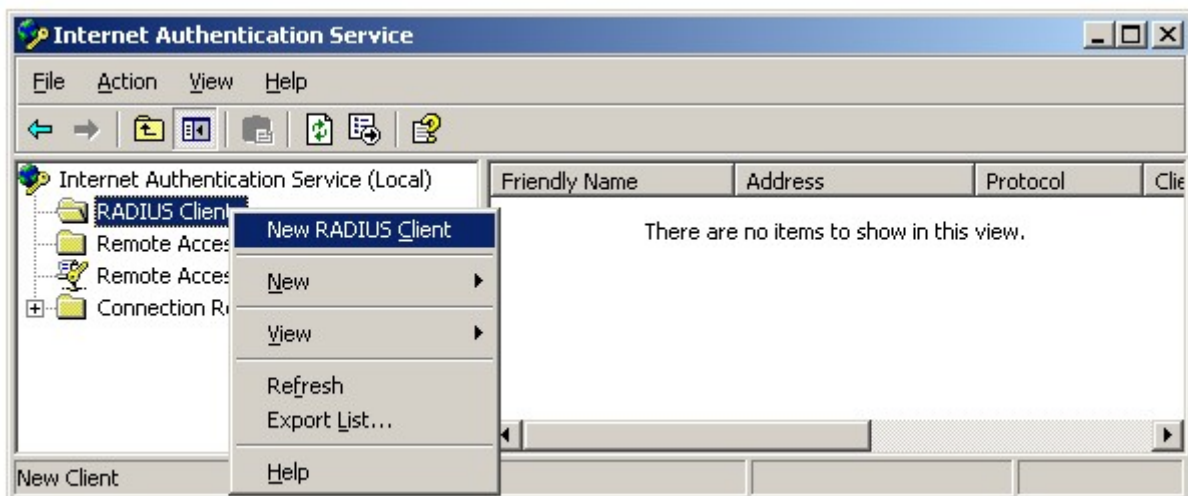


5. Microsoft IAS Configuration

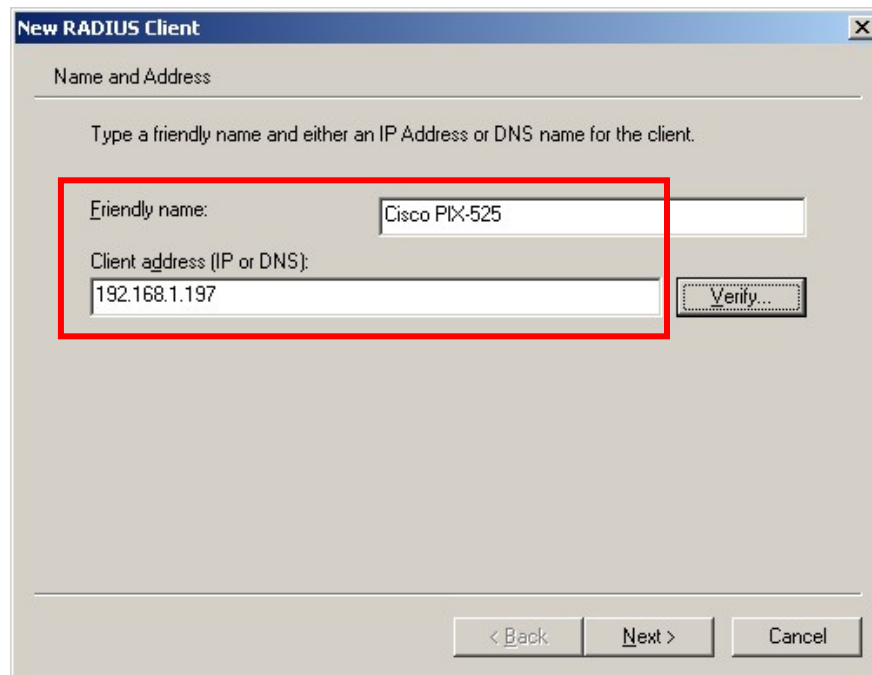
The steps below add the PIX to the IAS configuration as a RADIUS client. This enables IAS to exchange RADIUS messages with the PIX. These Application Notes assume the Microsoft Internet Authentication Service is installed and operational.

5.1. RADIUS Client

1. Open the IAS application window by selecting **Start > All Programs > Administrative Tools > IAS**. Right click **RADIUS Clients** and select **New Radius Client** from the pop-up menu as shown below.

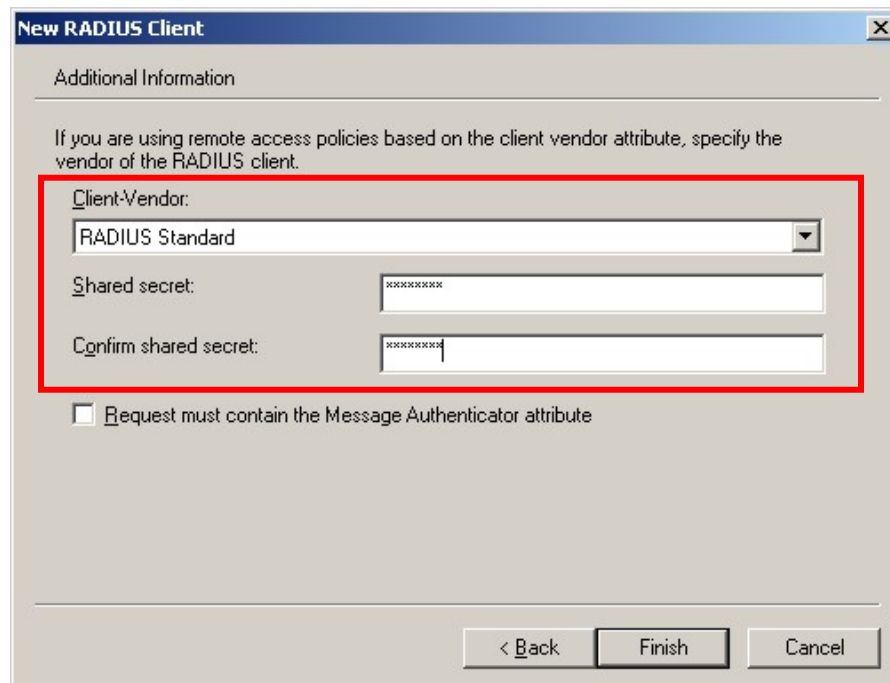


2. Enter a descriptive name for the PIX and the IP address of the inside interface of the PIX for IAS to communicate with. Click **Next** to continue.



The dialog box is titled "New RADIUS Client" and has a tab labeled "Name and Address". Below the tab is a text label: "Type a friendly name and either an IP Address or DNS name for the client." There are two text input fields: "Friendly name:" with the value "Cisco PIX-525" and "Client address (IP or DNS):" with the value "192.168.1.197". A "Verify..." button is located to the right of the client address field. At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel". A red rectangle highlights the "Friendly name" and "Client address" fields.

3. Enter a **Shared secret** text string. This shared secret is used by the PIX and IAS to authenticate each other for RADIUS communications. All remaining fields may be left default. Click **Finish**.

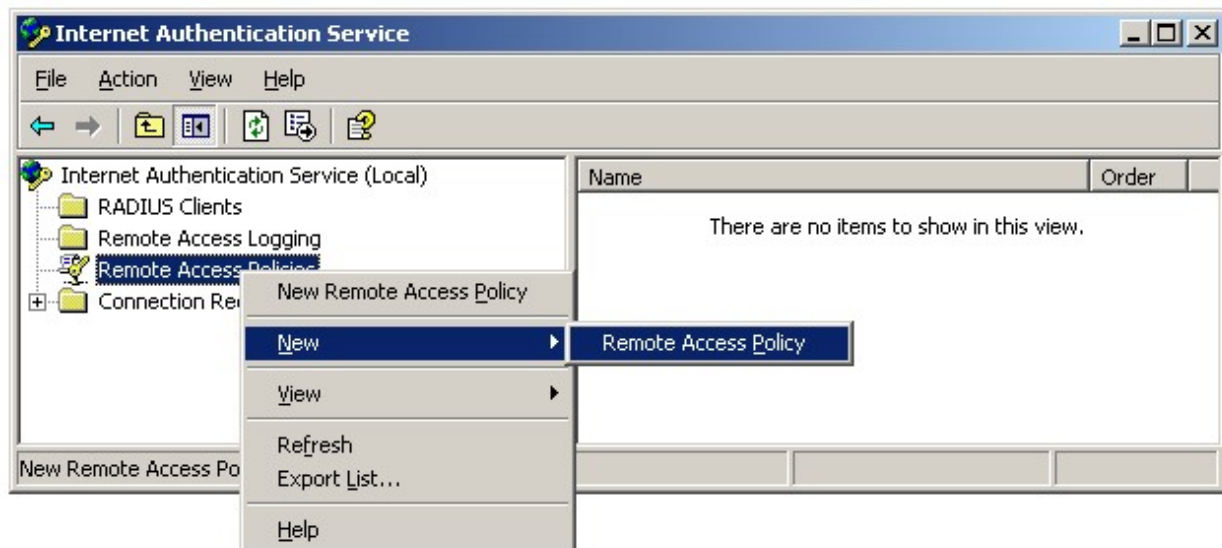


The dialog box is titled "New RADIUS Client" and has a tab labeled "Additional Information". Below the tab is a text label: "If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client." There are three text input fields: "Client-Vendor:" with a dropdown menu showing "RADIUS Standard", "Shared secret:" with a masked input (xxxxxxxx), and "Confirm shared secret:" with a masked input (xxxxxxxx). A checkbox labeled "Request must contain the Message Authenticator attribute" is located below the input fields. At the bottom of the dialog are three buttons: "< Back", "Finish", and "Cancel". A red rectangle highlights the "Client-Vendor", "Shared secret", and "Confirm shared secret" fields.

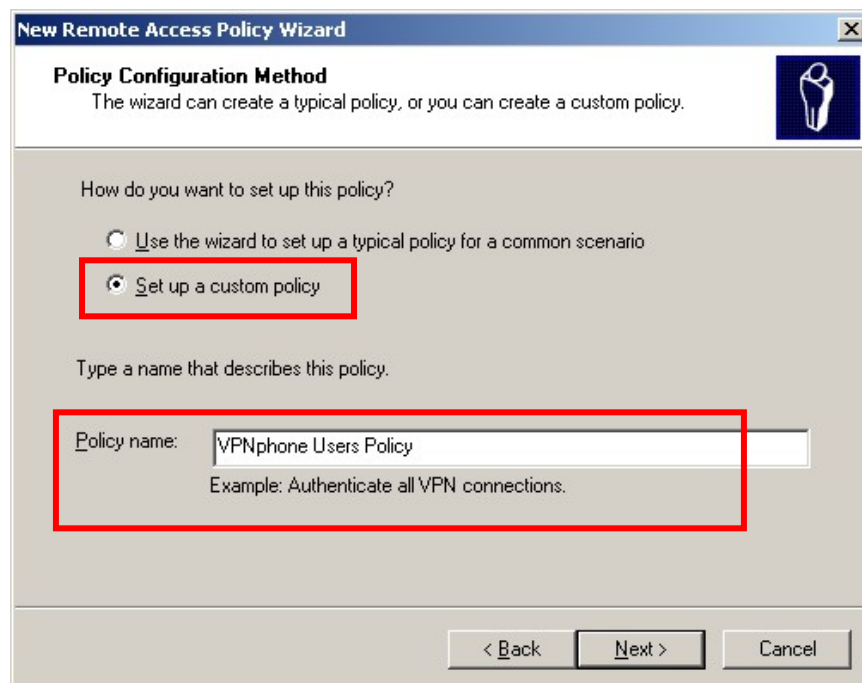
5.2. Remote Access Policy

The steps below create a new access policy to be used for RADIUS requests coming from the PIX on behalf of VPNremote Phones users.

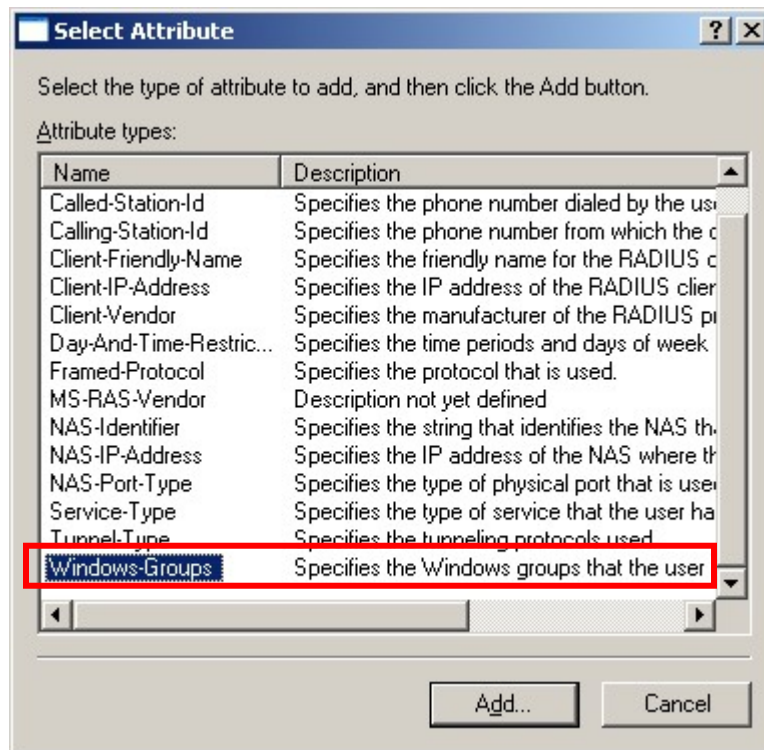
1. From the IAS main application window, right click **Remote Access Policies** and select **New > Radius Access Policy** from the pop-up menu to start the New Remote Access Policy Wizard.



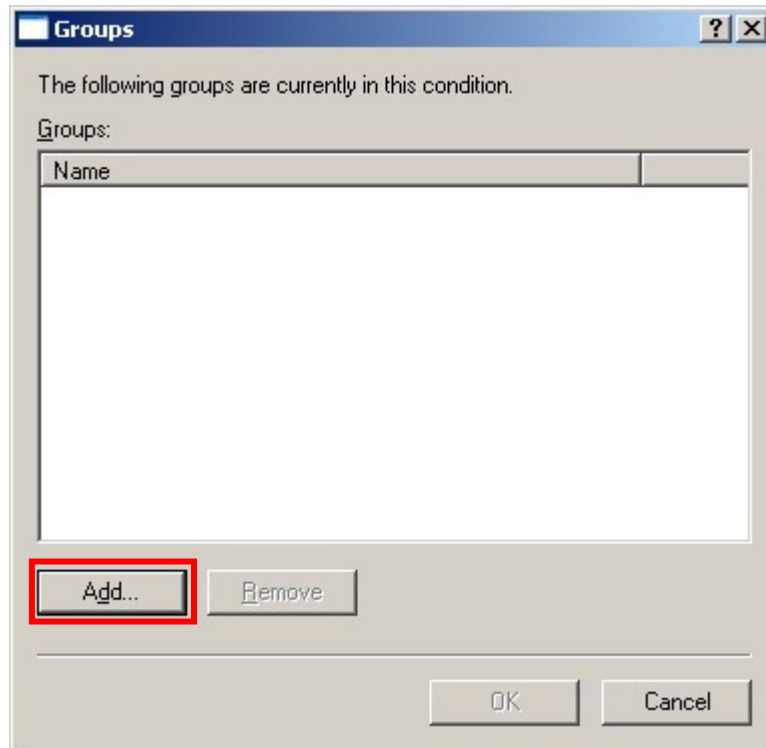
2. Select **Set up a custom policy** and enter a descriptive policy name. Click **Next** to continue.



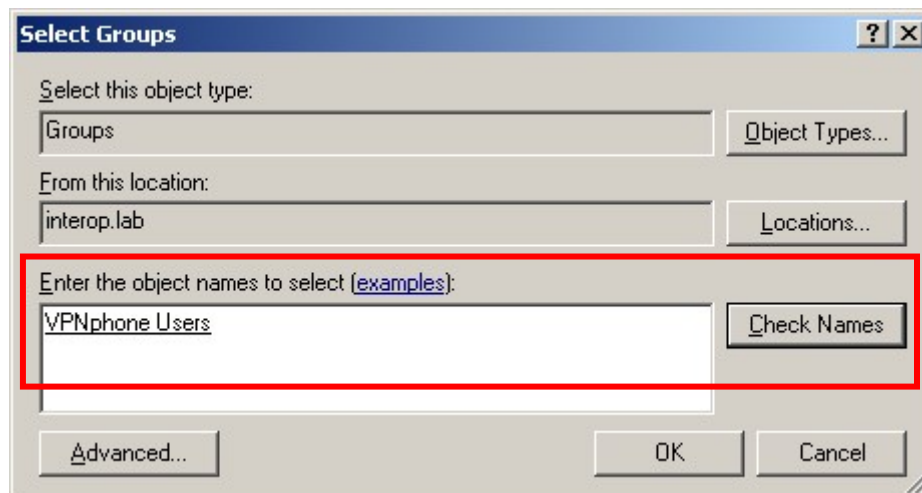
3. From the Policy Conditions window, click **Add** (not shown). Select the attributes to be applied to this access policy. The **Windows-Groups** attribute is used in the sample configuration as show below. Click **Add**.



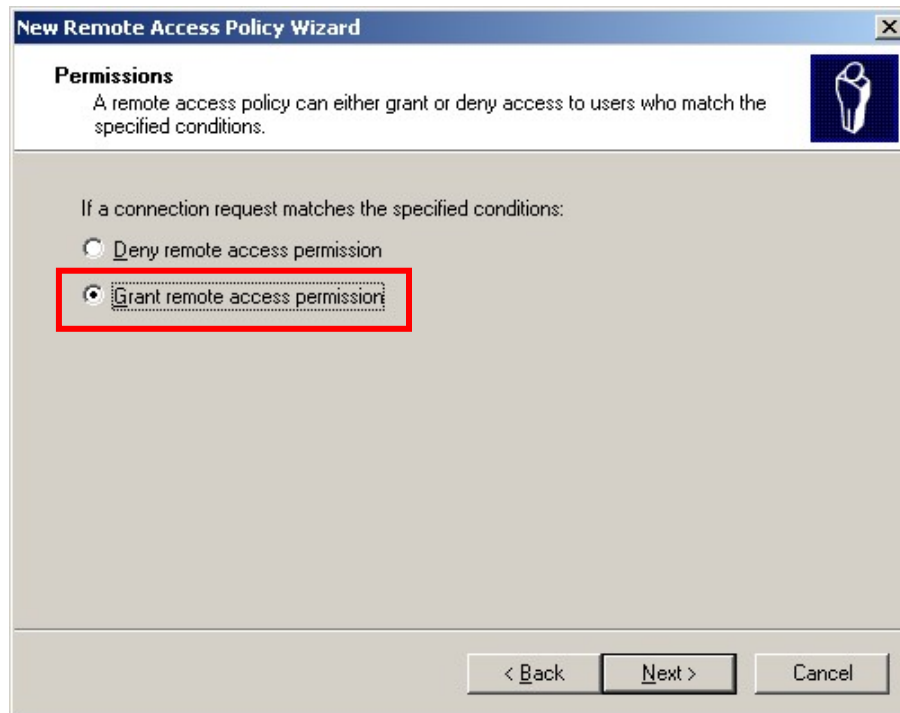
4. The Active Directory VPNphone Users group is added to this access policy as shown below. Click **Add**.



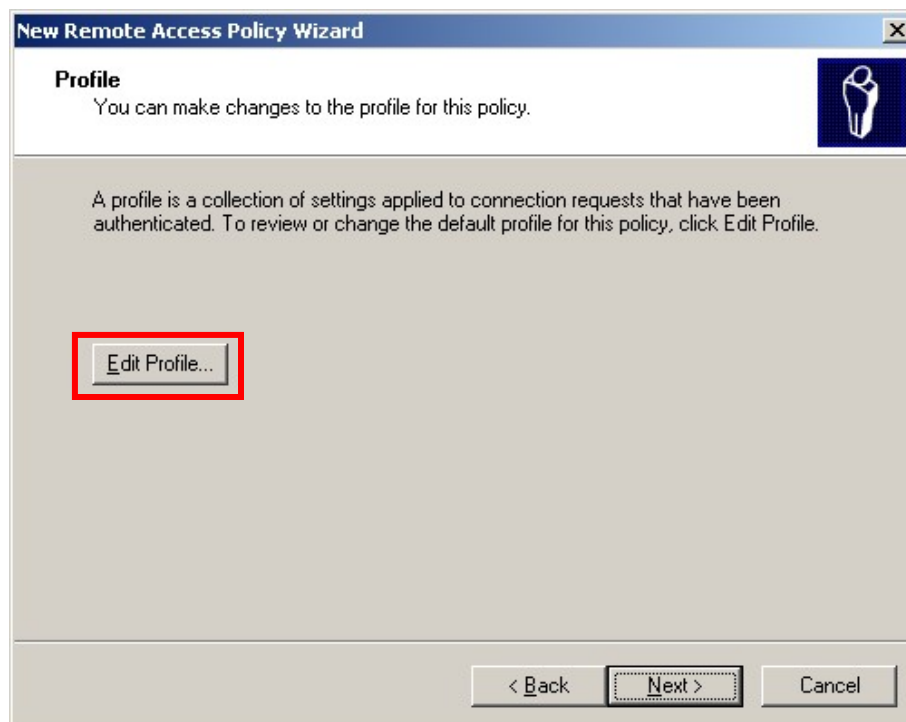
5. Enter the group name created in Section 4.2. Entering the first few letters of the group name then clicking the **Check Names** button is a short cut for speed and accuracy. Click **OK**, followed by **OK** and then **Next** to continue.



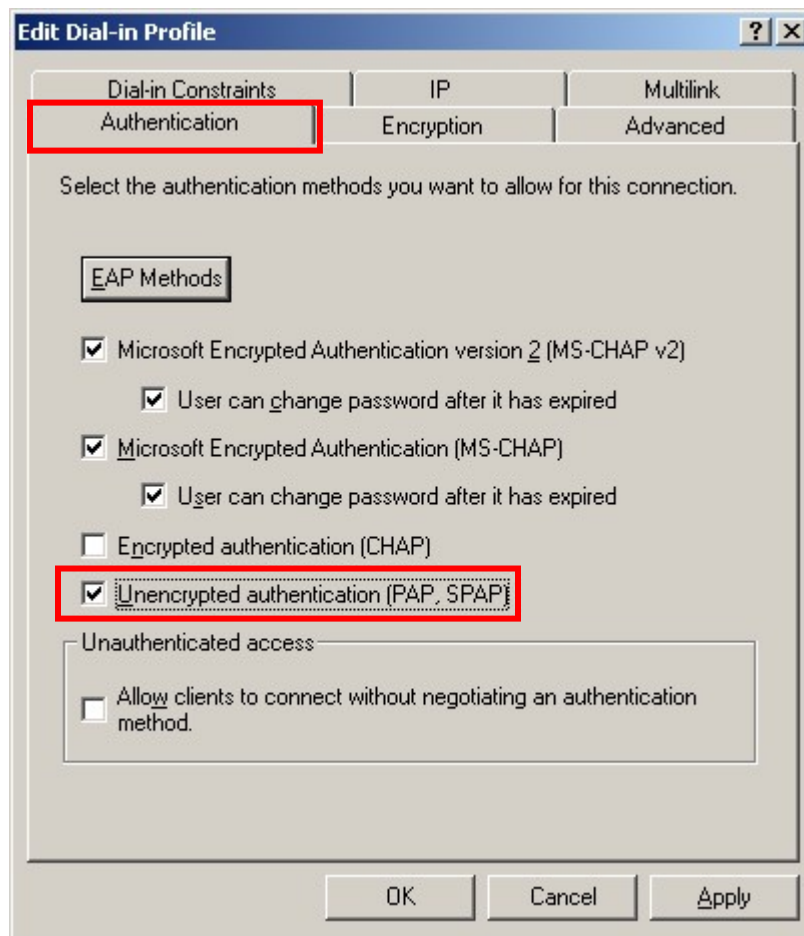
6. Enable remote access permissions. Click **Next** to continue.



7. Click **Edit Profile**.



8. Select the **Authentication** tab. Ensure **Unencrypted authentication (PAP, SPAP)** is enabled with a check mark. Click **OK**, followed by **OK** and then **Finished** to complete the wizard.



5.3. RADIUS Port Number

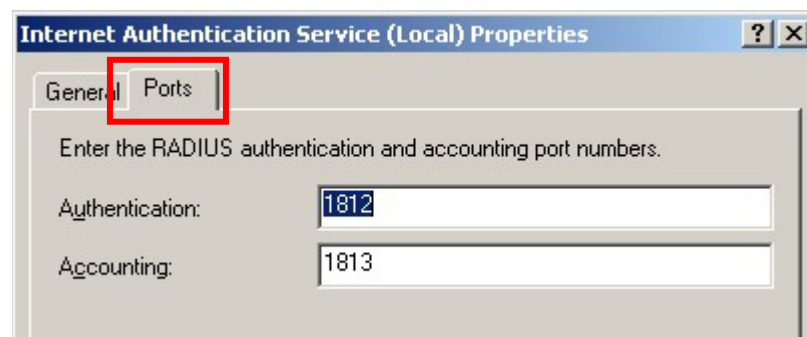
IAS must use a common UDP port number when communicating with RADIUS clients such as the PIX. By default, IAS uses UDP port number 1812 for RADIUS. Port 1812 is the officially assigned port number for RADIUS as stated in the RADIUS standard, RFC 2865 [9].

The following step describes how to verify the default port number IAS is configured to use for the RADIUS protocol.

1. From the IAS main application window, right click **Internet Authentication Services** and select **Properties** from the pop-up menu.



2. Select the Ports tab and note the configured port numbers.



6. Cisco PIX Configuration

These Application Notes assume both the PIX and Cisco ASDM application are installed and operational.

From the **ASDM Home** screen, compare the version of the PIX, as shown in the Device Information pane, with the PIX software version listed in Table 1. Select the **License** tab to identify the IPsec encryption algorithms licensed for use. Encryption algorithms other than DES require the installation of an enhanced encryption license from Cisco. See [9] for additional information. Also verify the status and configuration of the network interfaces as shown in the Interface Status pane.

Device Information

General | License

Host Name:	pixfirewall.default.domain.invalid		
PIX Version:	7.2(1)	Device Uptime:	25d 20h 20m 59s
ASDM Version:	5.2(1)	Device Type:	PIX 525
Firewall Mode:	Routed	Context Mode:	Single
Total Flash:	16 MB	Total Memory:	128 MB

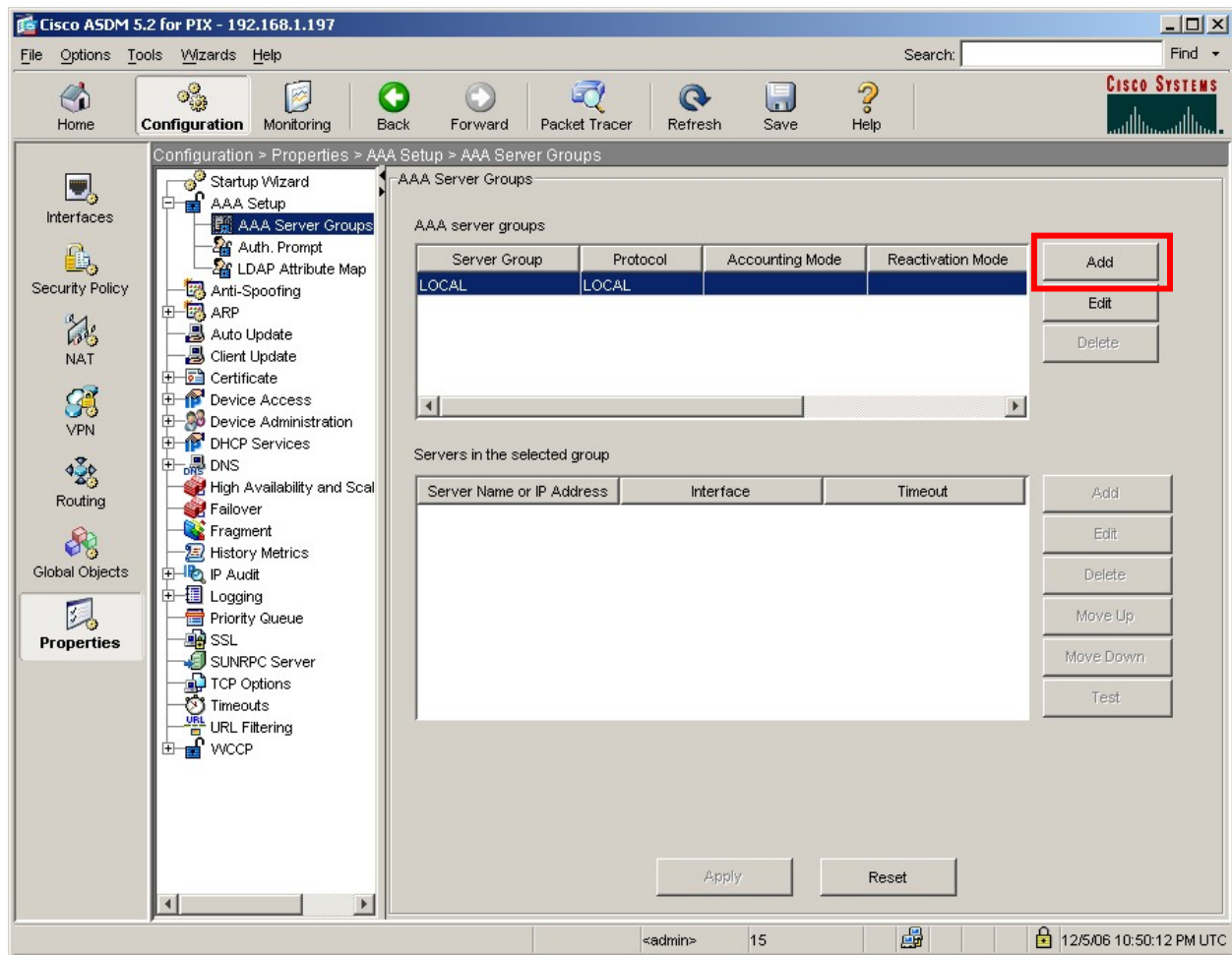
Device Information			
General		License	
Encryption:	3DES-AES	GTP/GPRS:	Disabled
Failover:	Disabled	VPN Peers:	Unlimited
Max VLANs:	25	Max Physical Interfaces:	6
License:	Restricted(R)		

Interface Status				
Interface	IP Address/Mask	Line	Link	Kbps
inside	192.168.1.197/24	↑ up	↑ up	1
outside	160.2.2.2/30	↑ up	↑ up	0

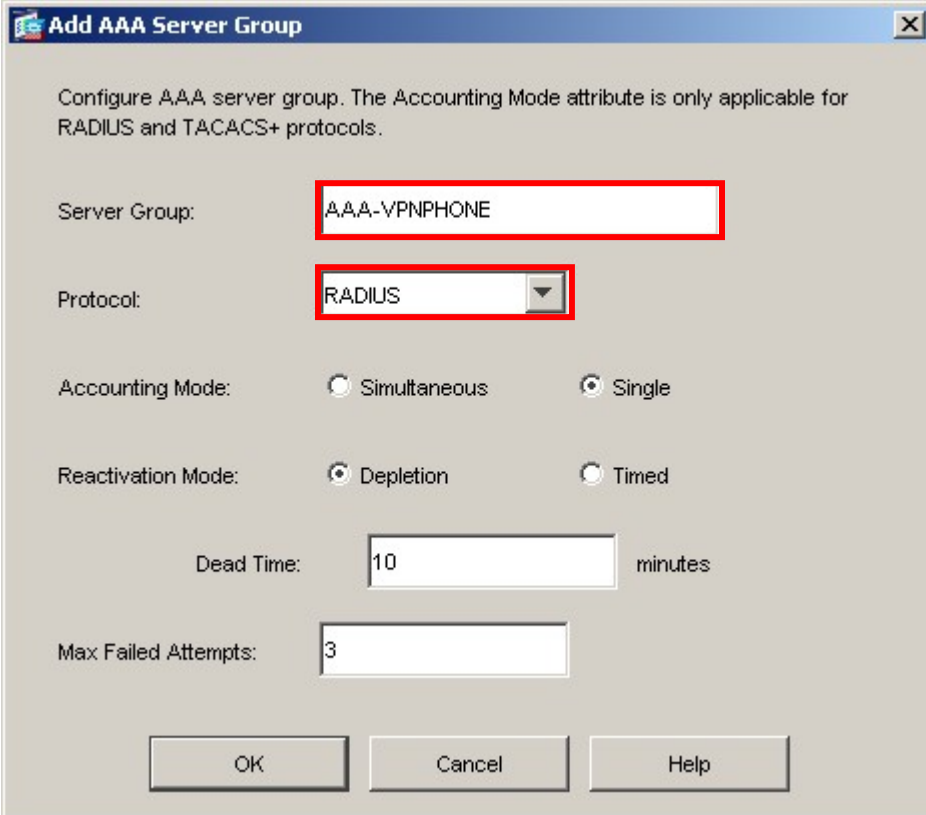
6.1. AAA (RADIUS)

The steps below create a new AAA Server Group and add the Microsoft IAS server to the group as a RADIUS Server.

1. From the ASDM GUI, select **Configuration > Properties > AAA Setup > AAA Server Groups**. Click **Add**.



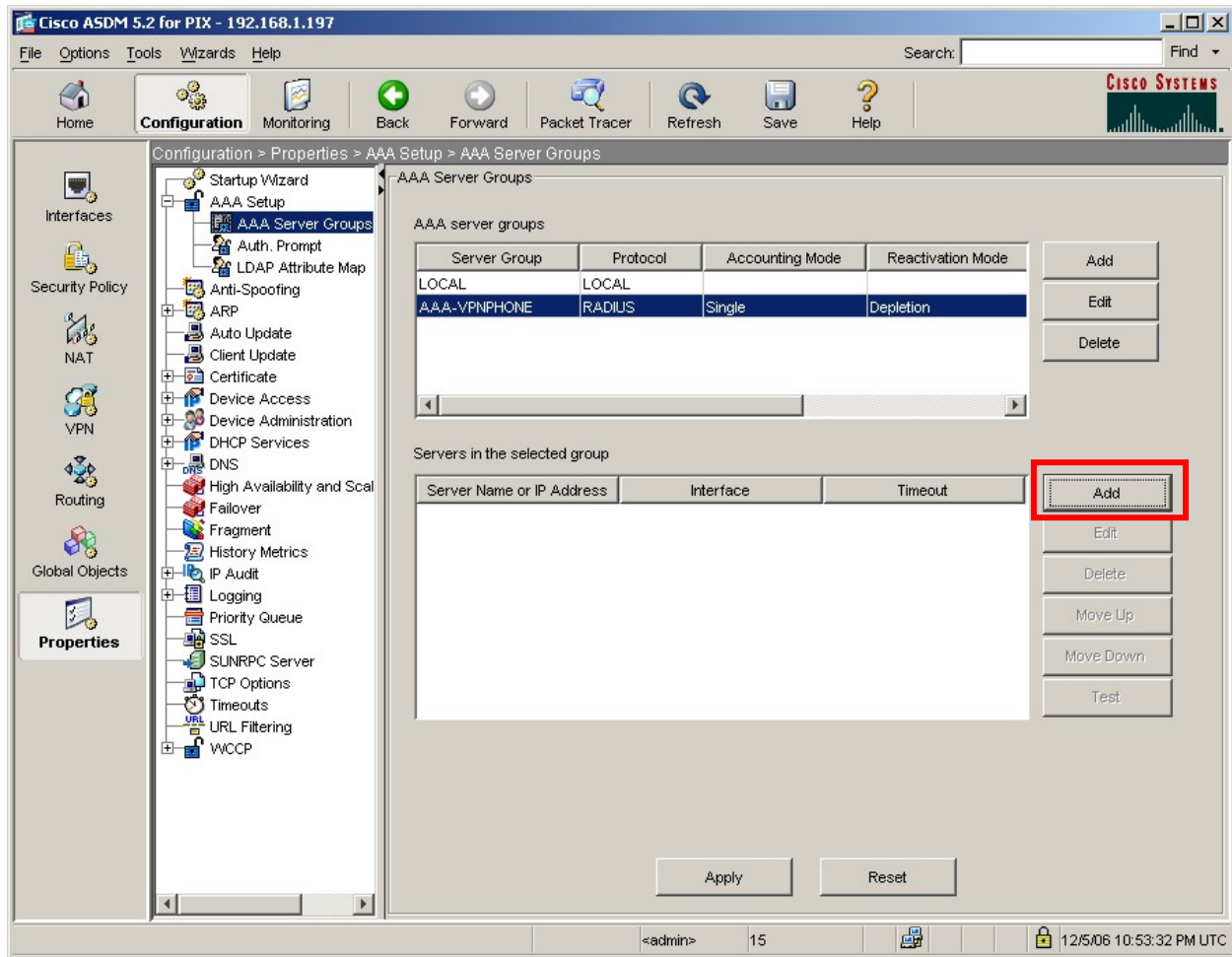
2. Enter a descriptive Server Group name and select **RADIUS** from the Protocol drop down menu. All remaining fields can be left as default. Click **OK**.



The image shows a Windows-style dialog box titled "Add AAA Server Group". It contains the following fields and options:

- Server Group:** A text box containing "AAA-VPNPHONE".
- Protocol:** A dropdown menu with "RADIUS" selected.
- Accounting Mode:** Two radio buttons: "Simultaneous" (unselected) and "Single" (selected).
- Reactivation Mode:** Two radio buttons: "Depletion" (selected) and "Timed" (unselected).
- Dead Time:** A text box containing "10" followed by the label "minutes".
- Max Failed Attempts:** A text box containing "3".
- Buttons:** "OK", "Cancel", and "Help" at the bottom.

3. Highlight the newly created AAA Server Group and click the lower **Add** button to add the Microsoft IAS server to the new server group as shown below.



4. Select the PIX network interface to use when communicating with the Microsoft IAS server and enter the IAS server's IP address or FQDN if DNS is used.

For RADIUS Parameters, the Server Authentication and Accounting Port numbers must match the Port numbers used by the IAS server. See Section 5.3.

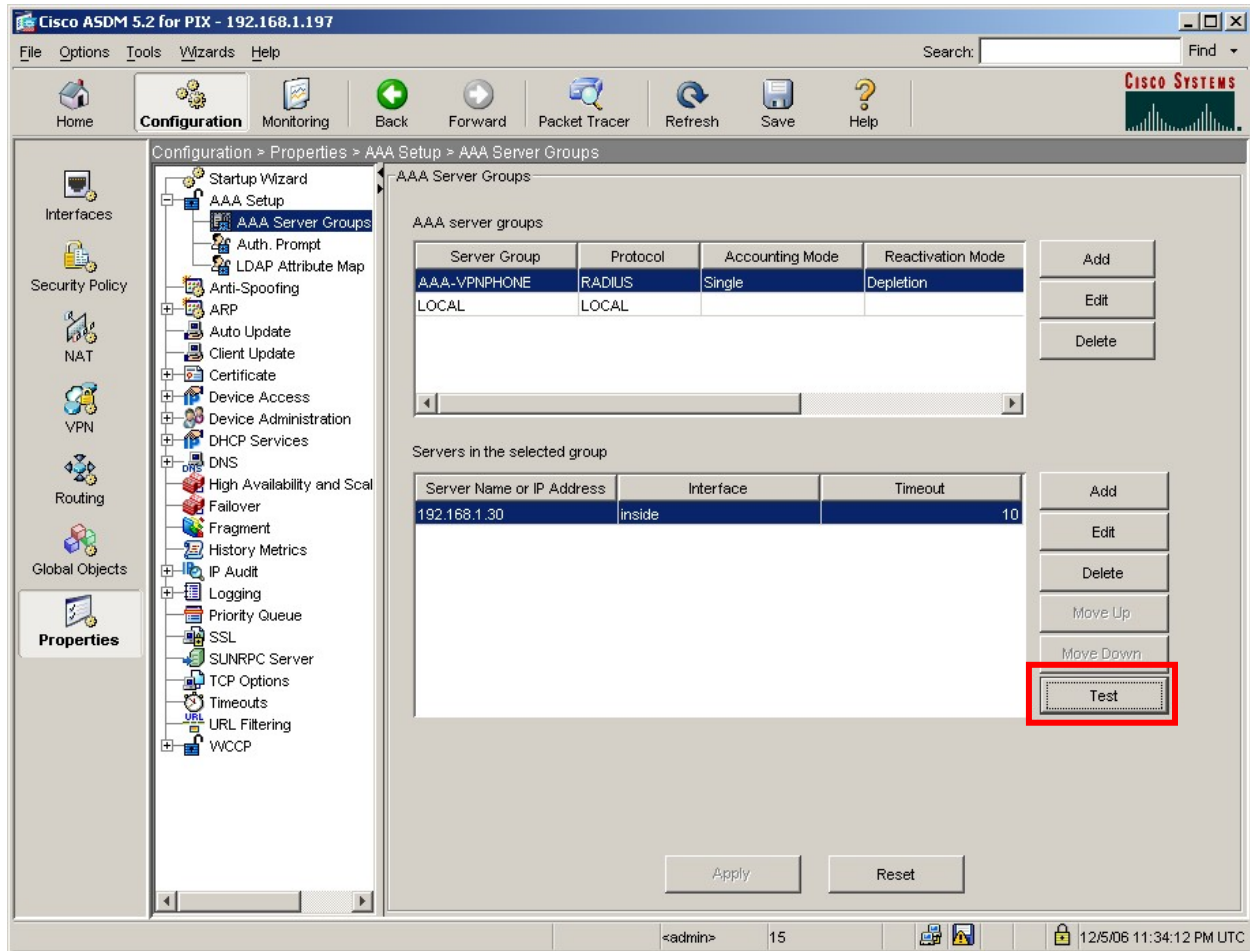
The Server Secret Key entered here must match the Shared Secret Key configured in IAS. See Section 5.1.

Note: Although the Accounting service is not being used in the sample configuration, it is recommended to change the Accounting Port number to match IAS.

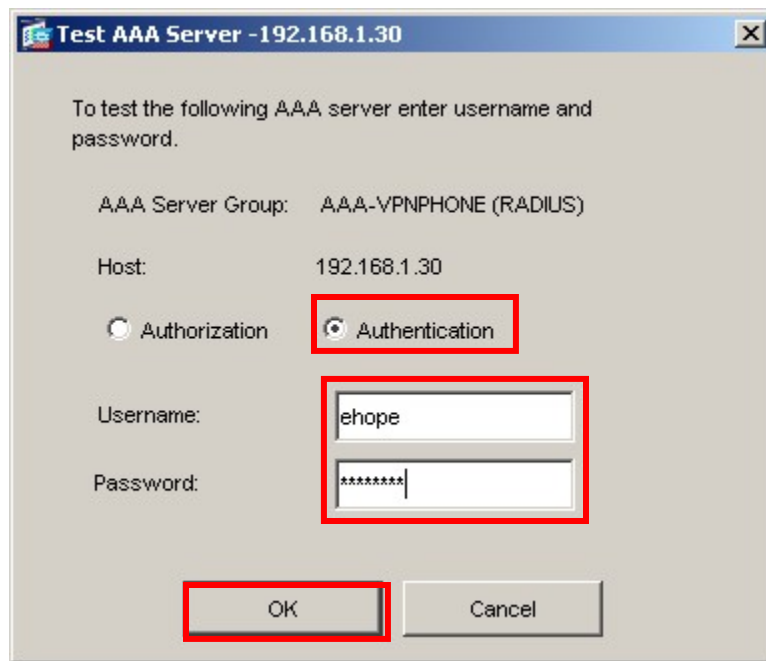
All remaining fields can be left as default. Click **OK**, then click **Apply** to save changes.

The screenshot shows the 'Add AAA Server' dialog box. The 'Server Group' is set to 'AAA-VPNPHONE'. The 'Interface Name' is 'inside'. The 'Server Name or IP Address' is '192.168.1.30'. The 'Timeout' is '10 seconds'. The 'RADIUS Parameters' section is expanded, showing 'Server Authentication Port' as '1812', 'Server Accounting Port' as '1813', 'Retry Interval' as '10 seconds', 'Server Secret Key' as 'avaya123', 'Common Password' as an empty field, and 'ACL Netmask Convert' as 'Standard'. The fields for 'Interface Name', 'Server Name or IP Address', 'Server Authentication Port', 'Server Accounting Port', and 'Server Secret Key' are highlighted with red rectangles. The 'OK', 'Cancel', and 'Help' buttons are at the bottom.

5. At this point, the AAA configuration on the PIX is complete. To verify the RADIUS configuration and connectivity to the Microsoft IAS RADIUS server, click the **Test** button as shown below.

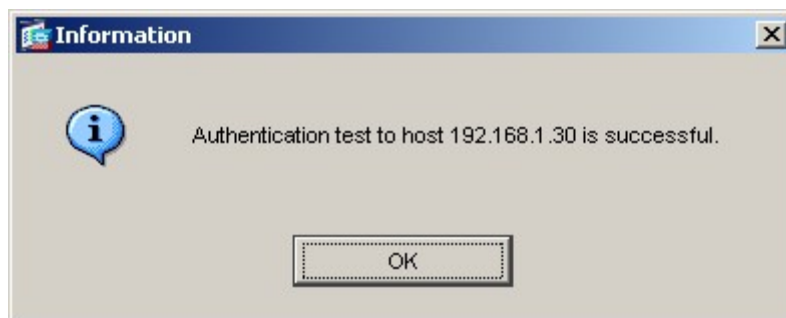


6. Select **Authentication** and enter the username and password of a valid user configured in Active Directory, Section 4.1. Click **OK** to initiate the test.



7. The following window appears if the RADIUS authentication request to the Microsoft IAS and Active Directory server is successful. Click **OK** to continue.

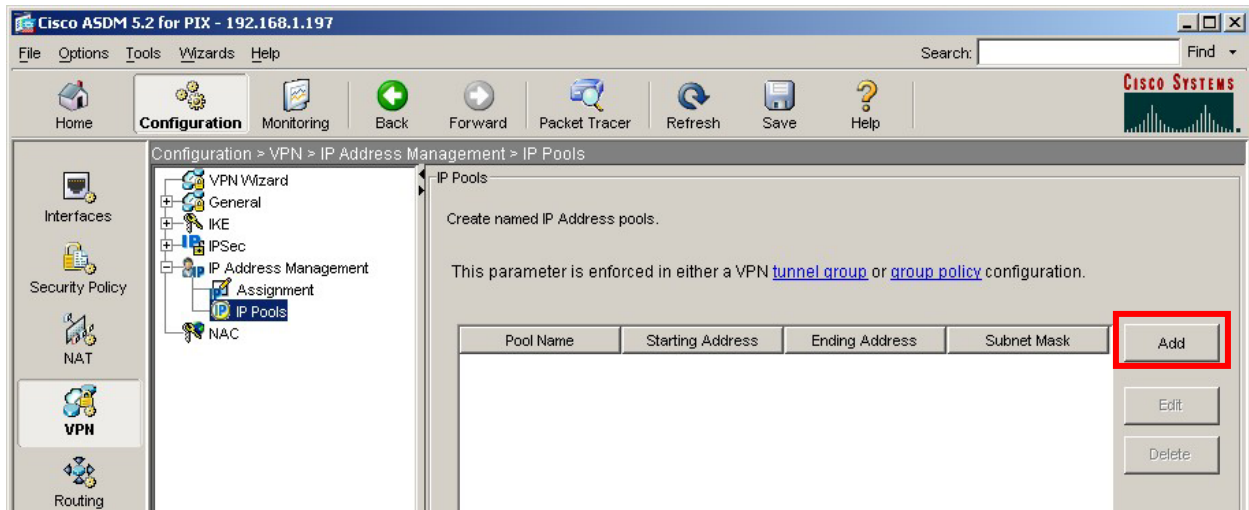
If the test fails, verify the Microsoft IAS and Active Directory configuration as well as the PIX AAA configuration steps above. See Section 10 for troubleshooting tips.



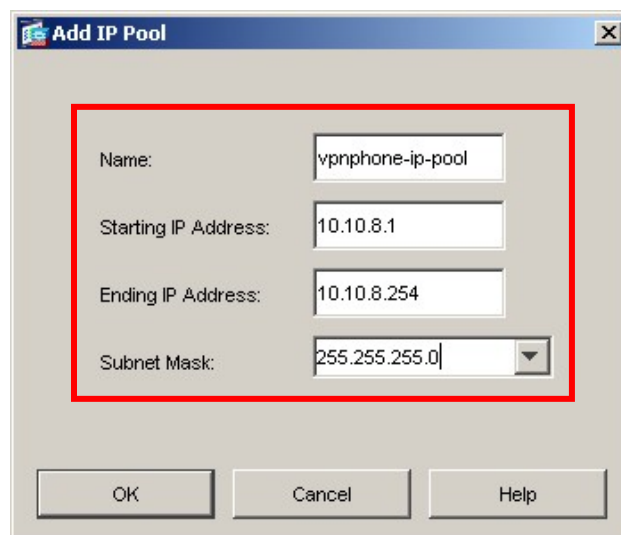
6.2. IP Address Pool

The steps below create an IP Address Pool for the PIX to use for assigning IP addresses to VPNremote Phones as the “inner address” when an IPSec tunnel is successfully established.

1. From the ASDM GUI, select **Configuration > VPN > IP Address Management > IP Pools**. Click **Add**.



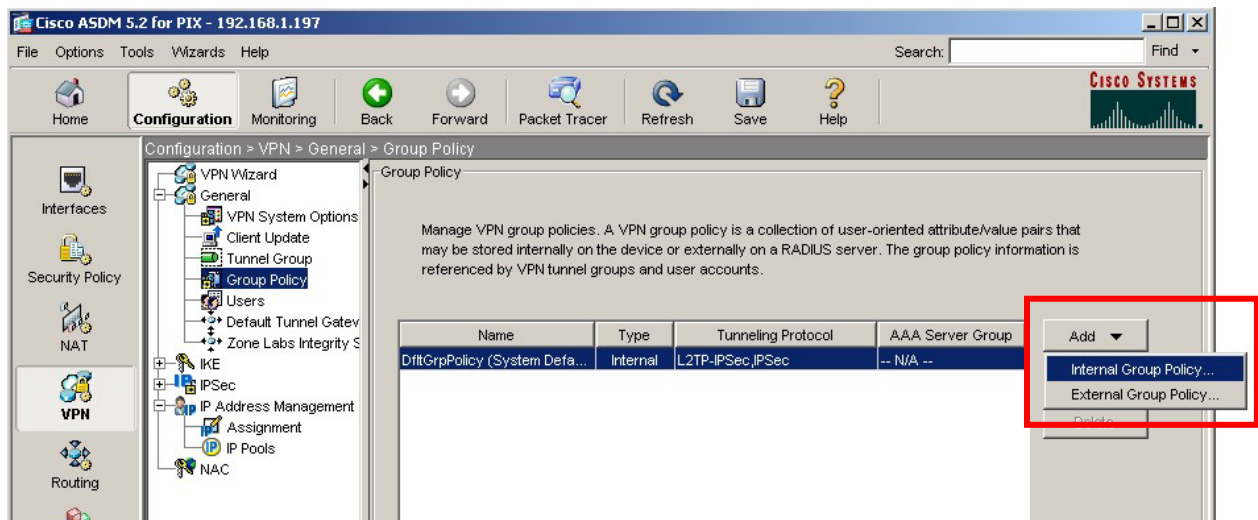
2. Enter a descriptive name and the IP address range to be assigned to VPNremote Phones. This address range must not overlap with any addresses on the private enterprise network and must be routable within the enterprise network. Click **OK** to complete.



6.3. Tunnel Group Policy

The steps below create a Group Policy to be used for VPNremote phones. Creating a VPNremote Phone Group Policy allows for easier management of VPNremote Phones.

1. From the ASDM GUI, select **Configuration > VPN > General > Group Policy**. Click the **Add** button then **Internal Group Policy** from the drop down menu that appears.



2. Configure the highlighted fields shown below. All remaining fields may be left as default. Click the **IPSec** tab to continue.

Add Internal Group Policy

Name:

General | **IPSec** | Client Configuration | Client Firewall | Hardware Client | NAC

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Tunneling Protocols: ☐ Inherit ☒ IPSec ☐ L2TP over IPSec

Filter: ☒ Inherit Manage...

Connection Settings

Access Hours: ☒ Inherit Manage...

Simultaneous Logins: ☐ Inherit

Maximum Connect Time: ☒ Inherit ☐ Unlimited minutes

Idle Timeout: ☒ Inherit ☐ Unlimited minutes

Servers

DNS Servers: ☐ Inherit Primary: Secondary:

WINS Servers: ☒ Inherit Primary: Secondary:

DHCP Scope: ☒ Inherit

OK Cancel Help

3. Configure the highlighted fields shown below. All remaining fields may be left as default. It is recommended to disable **Re-authentication on IKE Re-key** especially for VPNremote Phone implementations that do not allow user passwords to be stored in flash memory. Users would have to re-renter their password into the VPNremote Phone every time an IKE re-key occurs. **IP Compression** and **Perfect Forward Secrecy** are not enabled on the VPNremote Phone. Click **OK** to complete.

The screenshot shows the 'Add Internal Group Policy' dialog box with the 'Client Configuration' tab selected. The 'Name' field is set to 'VPNPHONE-grp'. The 'Client Access Rules' section is expanded, showing an 'Inherit' checkbox checked. The 'Re-authentication on IKE Re-key', 'IP Compression', and 'Perfect Forward Secrecy' settings are highlighted with a red box, showing 'Inherit' unchecked and 'Disable' selected. The 'Tunnel Group Lock' is set to 'Inherit'.

Name:

General | **IPSec** | Client Configuration | Client Firewall | Hardware Client | NAC

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Re-authentication on IKE Re-key: ☐ Inherit ☐ Enable ☒ Disable

IP Compression: ☐ Inherit ☐ Enable ☒ Disable

Perfect Forward Secrecy: ☐ Inherit ☐ Enable ☒ Disable

Tunnel Group Lock: ☒ Inherit

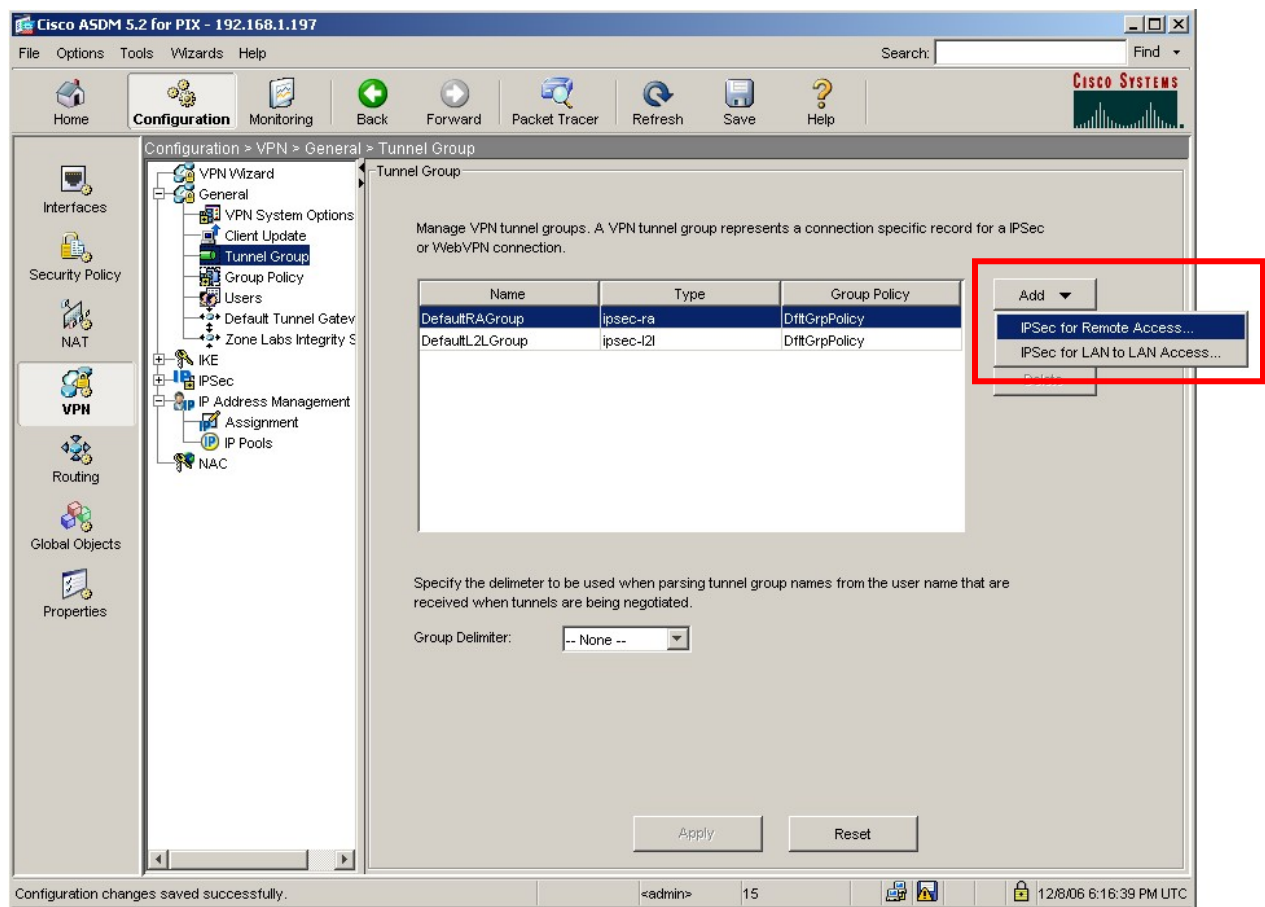
Client Access Rules

☒ Inherit *Configure up to 25 client access rules.*

6.4. Tunnel Group

The steps below create a Tunnel Group to be used for VPNremote phones. The Tunnel Group allows a single security association to be used for IKE Phase 1 with all VPNremote Phones. This makes for easier management of VPNremote Phone devices from the PIX perspective. Because a single IKE security association is used for all VPNremote Phones assigned to the same tunnel group, a limited amount of PIX resources are used.

1. From the ASDM GUI, select **Configuration > VPN > General > Tunnel Group**. Click the **Add** button then **IPSec for Remote Access** from the drop down menu that appears.



2. Configure the highlighted fields shown below. All remaining fields can be left as default. The Group Policy created in the Section 6.3 is assigned to this Tunnel Group. Click the **Authentication** tab to continue.

The screenshot shows the 'Add Tunnel Group' dialog box. The 'Name' field is highlighted with a red box and contains the text 'VPNPHONE'. The 'Type' field contains 'ipsec-ra'. Below the tabs, the 'Group Policy' dropdown is also highlighted with a red box and shows 'VPNPHONE-grp'. The 'Authentication' tab is selected. The 'Basic' tab is also visible. The 'Password Management' section is expanded, showing options for overriding account-disabled indication and enabling password expiration notifications.

Add Tunnel Group

Name: Type:

General | IPsec | PPP

Configure general access attributes from the following sub-tabs.

Basic | Authentication | Authorization | Accounting | Client Address Assignment | Advanced

Group Policy:

☐ Strip the realm from username before passing it on to the AAA server

☐ Strip the group from username before passing it on to the AAA server

Password Management

☐ Override account-disabled indication from AAA server

☐ Enable notification upon password expiration to allow user to change password

☐ Enable notification prior to expiration Notify days prior to expiration

OK Cancel Help

3. Configure the highlighted fields shown below. All remaining fields can be left as default. The Authentication Server created in the Section 6.1 is assigned to this Tunnel Group. Click the **Client Address Assignment** tab to continue.

Add Tunnel Group

Name: Type:

General | IPsec | PPP

Configure general access attributes from the following sub-tabs.

Basic | Authentication | Authorization | Accounting | Client Address Assignment | Advanced

To set authentication server group per interface, go to the Advanced tab.

Authentication Server Group:

☐ Use LOCAL if Server Group fails

NAC Authentication Server Group:

OK Cancel Help

4. Configure the highlighted fields shown below. All remaining fields can be left as default. The IP Address Pool created in the Section 6.2 is assigned to this Tunnel Group by selecting **vpnphone-ip-pool** from the Available Pools list then clicking the **Add >>** button. Click the **IPSec** tab to continue.

Add Tunnel Group

Name: Type:

General | IPSec | PPP

Configure general access attributes from the following sub-tabs.

Basic | Authentication | Authorization | Accounting | Client Address Assignment | Advanced

To specify whether to use DHCP or address pools for address assignment, go to Configuration > VPN > IP Address Management > Assignment.

DHCP Servers

IP Address:

Address Pools

To configure interface-specific address pools, go to the Advanced tab.

Available Pools Assigned pools

5. Configure the highlighted fields shown below. All remaining fields can be left as default. The Pre-Shared Key value entered here will also be entered into the VPNremote Phone and stored in flash memory. The Pre-Shared Key is used for Phase 1 IKE authentication of the VPNremote Phone device. Extended Authentication (XAuth) is the Authentication mechanism used between the VPNremote Phone and the PIX for the user of the VPNremote Phone. XAuth will utilize Microsoft IAS and Active Directory for the user authentication. The VPNremote phone does not respond to keepalives. Click **OK** when complete.

Add Tunnel Group

Name: Type:

General | IPsec | PPP

Pre-shared Key: Trustpoint Name:

Authentication Mode: IKE Peer ID Validation:

☐ Enable sending certificate chain

ISAKMP Keepalive

☒ Disable keepalives

☐ Monitor keepalives

Confidence Interval: (seconds) Retry Interval: (seconds)

☐ Head end will never initiate keepalive monitoring

Interface-Specific Authentication Mode

Interface: Add >>

Authentication Mode: << Remove

Client Type	VPN Client Revisions	Image URL
All Windows Platforms		
Windows 95/98/ME		
Windows NT4.0/2000/XP		
VPN3002 Hardware Client		

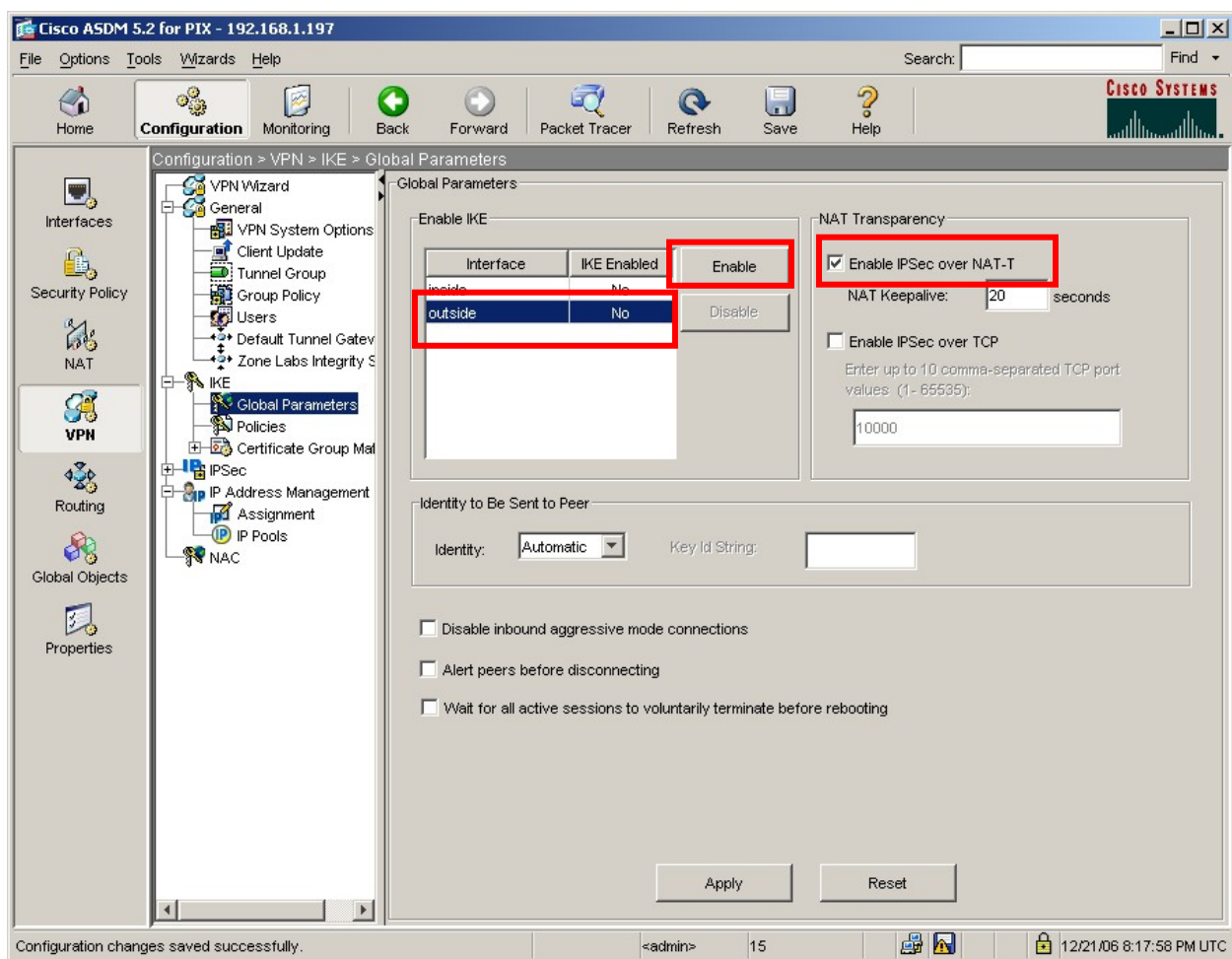
OK Cancel Help

6.5. IKE

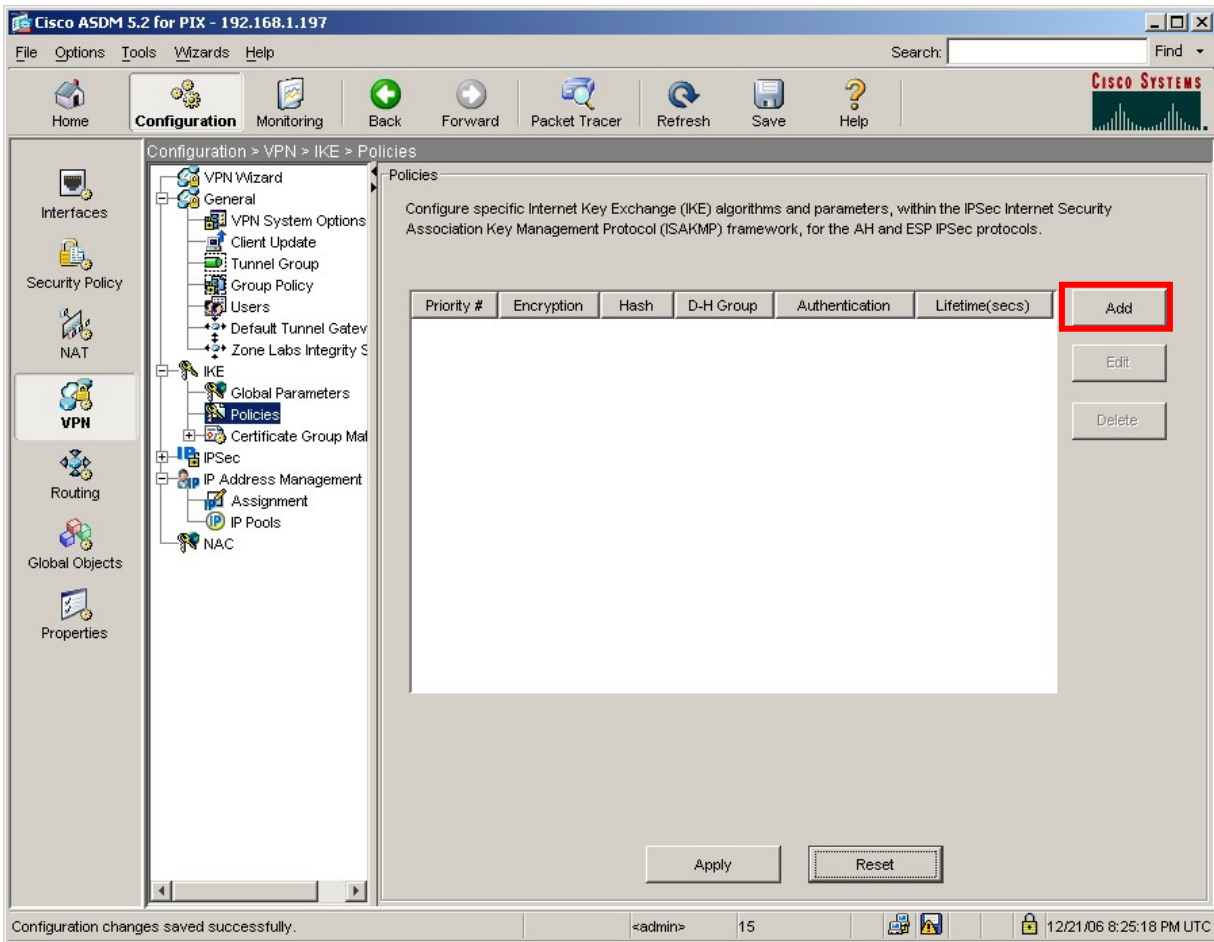
The steps below set the following IKE global parameters: a new IKE security policy used in the sample configuration is created, IKE is configured to use the outside interface of the PIX and IPSec over NAT-T, NAT Transparency, is enabled. NAT-T is enabled to ensure VPNremote Phones placed behind NAT devices (i.e. D-link, NetGear and Linksys) will operate successfully. The IKE policy is defined as well.

1. From the ASDM GUI, select **Configuration > VPN > IKE > Global Parameters**. Configure the highlighted fields shown below. All remaining fields can be left as default. Click **Apply** when complete.

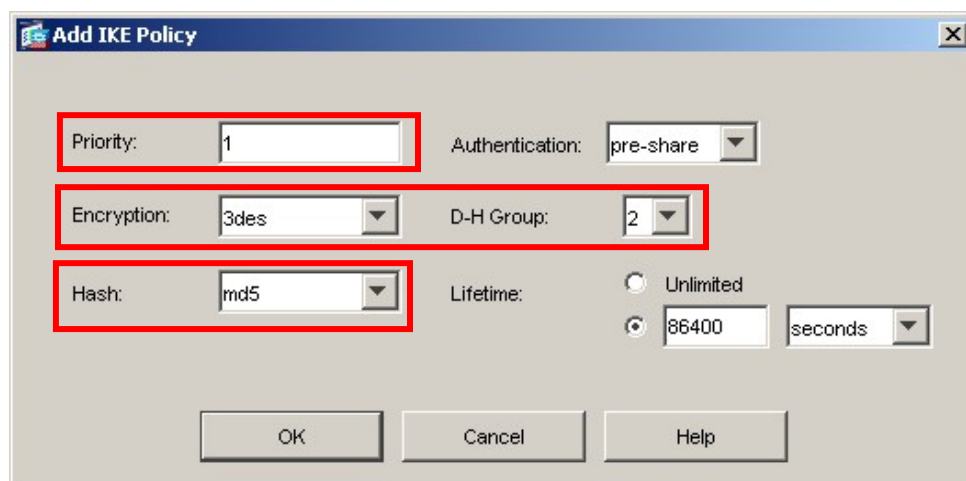
Note: After selecting the **Enable** button to enable IKE for an interface, the IKE Enabled status changes from No to Yes for the associated interface.



2. Select **Configuration > VPN > IKE > Policies**. Click the **Add** button as shown below.



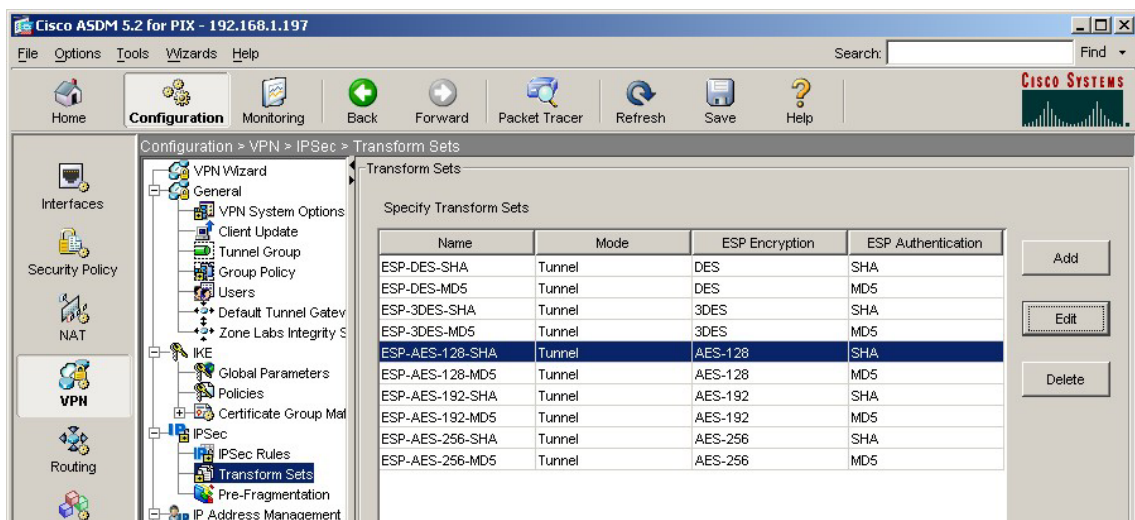
3. Configure the highlighted fields shown below. All remaining fields may be left as default. Click **OK** to continue then **Apply** to save configuration.



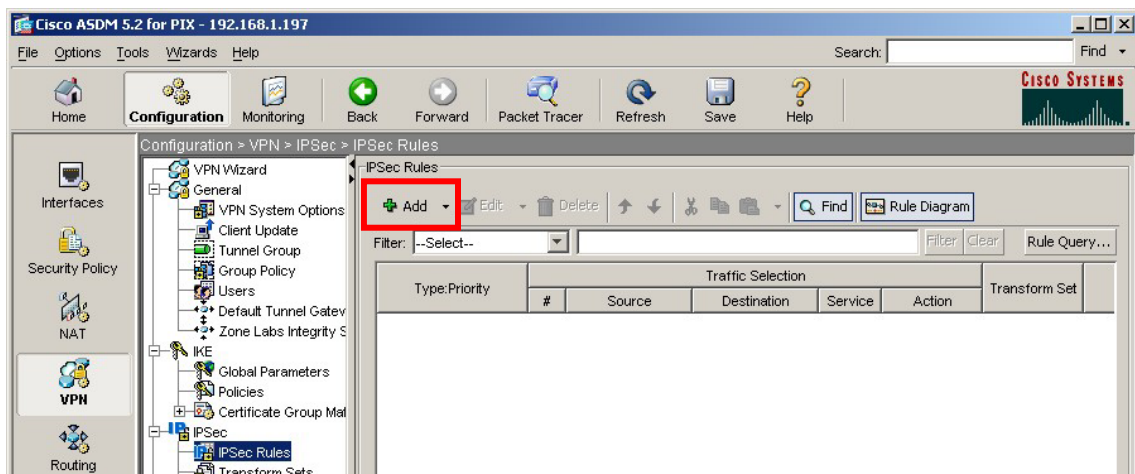
6.6. IPSec

The steps below create a security policy for negotiating IPSec, Phase 2, security associations with the VPNremote Phone. The policy is associated with a transformer set which identifies the IPSec encryption and hash algorithms to offer in the Phase 2 negotiation; ESP-AES-128-SHA is used in the sample configuration. The policy type of dynamic is used for remote access clients with dynamically assigned IP addresses. The priority value is used to prioritize the order of IPSec rule execution.

1. Select **Configuration > VPN > IPSec > Transform Sets**. Verify the Transform Set(s) to be used for IPSec are listed. Several Transformer Sets are defined by the system by default. As previously mentioned, the ESP-AES-128-SHA system defined Transformer Set is used in the sample configuration.



2. Select **Configuration > VPN > IPSec > IPSec Rules**. Click the **Add** button to create a new IPSec Rule.



3. Configure the highlighted fields shown below. All remaining fields may be left as default. Highlight the desired Transform Set from the drop-down list then click **Add>>**. Although multiple Transformer Sets can be included in a IPSec rule, only one is used in the sample configuration. Click the **Traffic Selection** tab to continue.

Create IPSec Rule

Tunnel Policy (Crypto Map) - Basic | Tunnel Policy (Crypto Map) - Advanced | Traffic Selection

Interface: **outside** | Policy Type: **dynamic** | Priority: **20**

Transform Sets

Transform Set to Be Added:

ESP-AES-128-SHA

ESP-DES-SHA
ESP-DES-SHA
ESP-DES-MD5
ESP-3DES-SHA
ESP-3DES-MD5
ESP-AES-128-MD5
ESP-AES-192-SHA
ESP-AES-192-MD5

Add >>

Remove

Move Up

Move Down

Dynamic Crypto Map Entries

IP Address of Peer to Be Added:

Add >>

Remove

Move Up

Move Down

☐ Enable Perfect Forwarding Security

Diffie-Hellman Group:

OK Cancel Help

4. Configure the highlighted fields shown below. All remaining fields may be left as default. Click **OK** to complete.

The screenshot shows the 'Create IPsec Rule' dialog box with the following configuration:

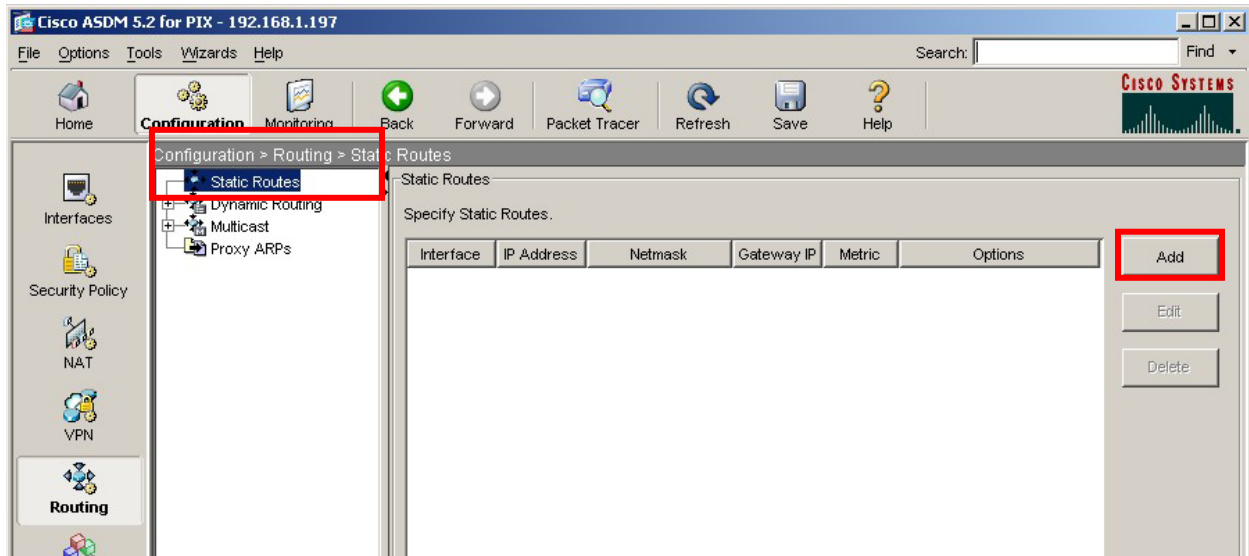
- Tunnel Policy (Crypto Map) - Basic** tab is selected.
- Interface and Action:**
 - Interface: **outside** (highlighted with a red box)
 - Action: **Protect** (indicated by a green checkmark)
- Source:**
 - Type: **any** (highlighted with a red box)
- Destination:**
 - Type: **any** (highlighted with a red box)
- Protocol and Service:**
 - Protocol: **ip**
- Rule Flow Diagram:** A diagram showing traffic flow from 'any' to 'outside' through a central router icon, with a green checkmark and 'Protect' label below it.
- Options:**
 - Time Range: **(any)**
 - Description: (empty text field)

Buttons at the bottom: **OK**, **Cancel**, **Help**.

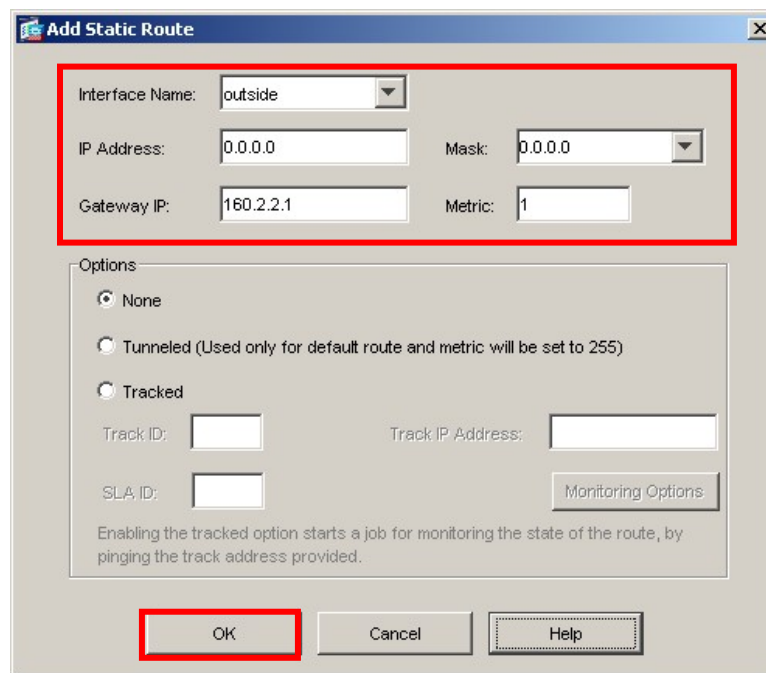
6.7. Default route

The default route must be set on the PIX. The default route is set to the outside (public) interface for the sample configuration.

1. Navigate to **Configuration > Routing > Static Routes** and click the **Add** button.



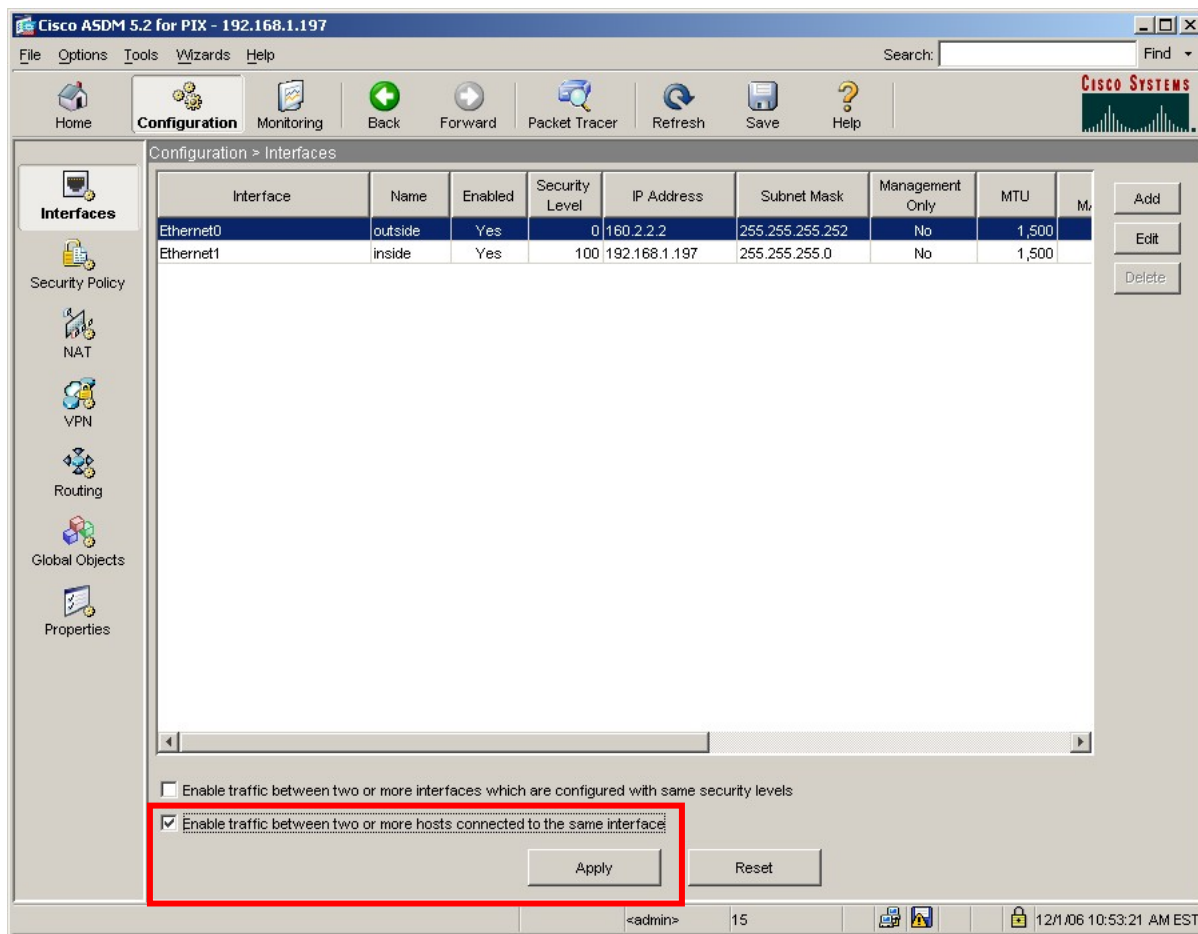
2. The IP address of 0.0.0.0 with a Mask of 0.0.0.0 signifies the default route. The IP address of 160.2.2.1 is the ISP next hop router as shown in the network diagram, **Figure 1**. Click **OK** to continue then **Apply** to save configuration.



6.8. VPNremote Phone to VPNremote Phone Direct Audio

The path taken by RTP audio packets of a VPNremote Phone can be controlled in the same way as a traditional Avaya IP Phone using the IP-IP Direct Audio features of Avaya Communication Manager. If it is desirable for the RTP audio packets to go directly between two VPNremote Phones with VPN tunnels to the same PIX, the **Enable traffic between two or more hosts connected to the same interface** PIX configuration option must be enabled. This is in addition to configuring the proper IP-IP Direct Audio options on Avaya Communication Manager.

1. Navigate to **Configuration > Interfaces** and select the check box next to **Enable traffic between two or more hosts connected to the same interface**. Click **Apply** to save.



7. Avaya Communication Manager Configuration

This section shows the necessary steps in configuring Avaya Communication Manager for VPNremote Phones. It is assumed that the basic configuration on Avaya Communication Manager has already been completed. See [3] for additional information. All commands discussed in this section are executed on Avaya Communication Manager using the System Access Terminal (SAT). After the completion of the configuration in this section, perform a **save translation** command to make the changes permanent.

As shown in **Figure 1**, VPNremote Phones are assigned to IP Network Region 5 using the IP address range of the PIX IP Address Pool. IP Network Region 5 is then assigned a codec set configured with the G.729 codec. The Main Campus is assigned to IP Network Region 1 using the G.711 codec.

7.1. IP Codec Set Configuration

Use the **change ip-codec-set n** command to configure IP Codec Set parameters where **n** is the IP Codec Set number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

1. Use the **change ip-codec-set 1** command to define a codec set for the G.711 codec as shown below.

change ip-codec-set 1				Page	1 of	2
IP Codec Set						
Codec Set: 1						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size(ms)			
1: G.711MU	n	2	20			
2:						
3:						

2. Use the **change ip-codec-set 2** command to define a codec set for the G.729 (30ms) codec as shown below.

change ip-codec-set 2				Page	1 of	2
IP Codec Set						
Codec Set: 2						
Audio	Silence	Frames	Packet			
Codec	Suppression	Per Pkt	Size(ms)			
1: G.729	n	3	30			
2:						
3:						

- Use the `list ip-codec-set` command to verify the codec assignments.

```
list ip-codec-set
```

IP CODEC SETS					
Codec Set	Codec 1	Codec 2	Codec 3	Codec 4	Codec 5
1	G.711MU				
2	G.729				
3					
4					

7.2. IP Network Map Configuration

Use the `change ip-network-map` command to define the IP address to Network Region mapping for VPNremote Phones. This IP address range should match the IP address range used in the PIX IP Address Pool in Section 6.2.

```
change ip-network-map
```

Page 1 of 32

IP ADDRESS MAPPING

From IP Address	(To IP Address	Subnet or Mask)	Region	VLAN	Emergency Location Extension
10 .10 .8 .1	10 .10 .8 .254		5	n	
.	.	.		n	
.	.	.		n	
.	.	.		n	

7.3. IP Network Region Configuration

Use the **change ip-network-region n** command to configure IP Network Region parameters where **n** is the IP Network Region number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

Intra-region and **Inter-region IP-IP Direct Audio** determines the flow of RTP audio packets. Setting these fields to “yes” enables the most efficient audio path to be taken. **Codec Set 1**, defined in Section 7.1, is used within IP Network Region 1.

change ip-network-region 1		Page 1 of 19
IP NETWORK REGION		
Region: 1		
Location: 1		Authoritative Domain: avaya.com
Name: Main Campus		
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes
Codec Set: 1		Inter-region IP-IP Direct Audio: yes
UDP Port Min: 2048		IP Audio Hairpinning? y
UDP Port Max: 3029		
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? y
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS
Audio PHB Value: 46		Use Default Server Parameters? y
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS		RSVP Enabled? n
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

Page 3 of the IP-Network-Region form, shown below, defines the codec set to use for inter-region calls. Avaya VPNremote Phones are mapped to Region 5. Calls within IP Network Region 1 use Codec Set 1 (G.711MU) while calls between IP Network Region 1 and IP Network Region 5 use Codec Set 2 (G.729).

change ip-network-region 1		Page 3 of 19					
Inter Network Region Connection Management							
src	dst	codec	direct			Dynamic CAC	
rgn	rgn	set	WAN	WAN-BW-limits	Intervening-regions	Gateway	IGAR
1	1	1					
1	2						
1	3						
1	4						
1	5	2	y	:NoLimit			n

Use the **change ip-network-region 5** command to configure IP Network Region 5 parameters. Configure the highlighted fields shown below. Calls within IP Network Region 5 (i.e., a VPNremote Phone calling another VPNremote Phone) use Codec Set 2 (G.729). All remaining fields can be left at the default values.

change ip-network-region 5		Page 1 of 19	
IP NETWORK REGION			
Region: 5			
Location:		Authoritative Domain: avaya.com	
Name: VPNphones - PIX			
MEDIA PARAMETERS		Intra-region IP-IP Direct Audio: yes	
Codec Set: 2		Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048		IP Audio Hairpinning? y	
UDP Port Max: 3029			
DIFFSERV/TOS PARAMETERS		RTCP Reporting Enabled? y	
Call Control PHB Value: 46		RTCP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46		Use Default Server Parameters? y	
Video PHB Value: 26			
802.1P/Q PARAMETERS			
Call Control 802.1p Priority: 6			
Audio 802.1p Priority: 6			
Video 802.1p Priority: 5		AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS		RSVP Enabled? n	
H.323 Link Bounce Recovery? y			
Idle Traffic Interval (sec): 20			
Keep-Alive Interval (sec): 5			
Keep-Alive Count: 5			

Page 3 defines the codec set to use for inter-region calls. Avaya VPNremote Phones are mapped to Region 5. Calls between IP Network Region 5 and IP Network Region 1 will also use Codec Set 2 (G.729).

change ip-network-region 5						Page	3 of	19
Inter Network Region Connection Management								
src	dst	codec	direct				Dynamic CAC	
rgn	rgn	set	WAN	WAN-BW-limits	Intervening-regions	Gateway	IGAR	
5	1	2	y	:NoLimit				n
5	2							
5	3							
5	4							
5	5	2						

7.4. Add Station

An Avaya VPNremote Phone is administered the same as any other IP telephone within Avaya Communication Manager. Even though the Avaya VPNremote Phone is physically located remote from the corporate network, the Avaya VPNremote Phone will behave the same as other Avaya IP telephones located locally on the corporate LAN once the VPN tunnel has been established. The VPNremote Phone can be administered as a bridged extension, typically bridged to the user's phone in the corporate office, or as a single dedicated extension. The latter is used for the VPNremote phone in the sample configuration.

The screens below show the first two **add station** pages for the 4610SW VPNremote Phone used for these Application Notes. The **Direct IP-IP Audio Connections** option on **Page 2** must be set to **y** to take advantage of the configuration in Section 7.3.

add station 50003		Page 1 of 4
STATION		
Extension: 50003	Lock Messages? n	BCC: 0
Type: 4610	Security Code: 1234	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: VPNphone	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 50003	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: english		
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? n	
	Customizable Labels? y	

add station 50003		Page 2 of 4
STATION		
FEATURE OPTIONS		
LWC Reception: spe	Auto Select Any Idle Appearance? n	
LWC Activation? y	Coverage Msg Retrieval? y	
LWC Log External Calls? n	Auto Answer: none	
CDR Privacy? n	Data Restriction? n	
Redirect Notification? y	Idle Appearance Preference? n	
Per Button Ring Control? n	Bridged Idle Line Preference? n	
Bridged Call Alerting? n	Restrict Last Appearance? y	
Active Station Ringing: single	Conf/Trans on Primary Appearance? n	
	EMU Login Allowed? n	
H.320 Conversion? n	Per Station CPN - Send Calling Number?	
Service Link Mode: as-needed		
Multimedia Mode: enhanced		
MWI Served User Type:	Display Client Redirection? n	
AUDIX Name:	Select Last Used Appearance? n	
	Coverage After Forwarding? s	
	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 50003	Always Use? n	IP Audio Hairpinning? y

8. Avaya VPNremote Phone Configuration

8.1. VPNremote Phone Firmware

The Avaya VPNremote Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. See [1] and [2] for details on installing VPNremote Phone firmware. The firmware version of Avaya IP telephones can be identified by viewing the version displayed on the phone upon boot up or when the phone is operational by pressing the **OPTIONS** hard button > **View IP Settings** soft button > **Miscellaneous** soft button > **Right arrow** hard button. The Application file name displayed denotes the installed firmware version.

As displayed in **Table 1**, VPNremote Phone firmware includes the letters **VPN** in the name. This allows for easy identification of firmware versions incorporating VPN capabilities.

8.2. Configuring Avaya VPNremote Phone

The Avaya VPNremote Phone configuration can be administered centrally from an HTTP/TFTP server or locally on the phone. These Application Notes utilize the local phone configuration method for all VPNremote Phone parameters with the exception of the WebLM License Manager URL. The WebLM License Manager URL cannot be set from the local phone configuration menu as of the firmware release used in these Application Notes and must be set from a centralized HTTP/TFTP server. The **NVWEBLMURL** variable of the 46xxvpnsetting.txt script file located on the HTTP/TFTP server defines the WebLM License Manager URL, which the VPNremote Phones use to acquire a license. See [1], [2] and [5] for additional information.

The following shows the **NVWEBLMURL** setting used in the 46xxvpnsetting.txt script file for these Application Notes:

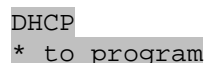
SET NVWEBLMURL http://192.168.1.30:8080/webLM/LicenseServer

The following steps describe how to configure the VPNremote Phone VPN parameters locally from the telephone.

1. There are two methods available to access the **VPN Configuration Options** menu from the VPNremote Phone.

- a. **During Telephone Boot:**

During the VPNremote Phone boot up, the option to press the * key to enter the local configuration mode is displayed on the telephones screen as shown below.



DHCP
* to program

When the * key is pressed, several configuration parameters are presented such as the phone's IP Address, the Call Server's IP Address, etc. Press the # key to accept the current settings, or enter an appropriate value and press the # key. The final configuration option displayed is the VPN Start Mode option shown below. Press the * key to enter the VPN Options menu.

```
VPN Start Mode: Boot
*=Modify    #=OK
```

b. During Telephone Operation:

While the VPNremote Phone is in an operational state, registered with Avaya Communication Manager, press the following key sequence on the telephone to enter VPN configuration mode:

Mute-V-P-N-M-O-D-# (Mute-8-7-6-6-6-3-#)

The following is displayed:

```
VPN Start Mode: Boot
*=Modify    #=OK
```

Press the * key to enter the VPN Options menu.

- The VPN configuration options menu is displayed. The configuration values for the VPNremote Phone of user ehope, used in the sample configuration, are shown in **Table 2** below.

Note: The values entered below are case sensitive.

Press the ► hard button on the Phone to access the next screen of configuration options. Phone models with larger displays (e.g., 4621SW) will present more configuration options per page.

Configuration Options	Value	Description
Server:	160.2.2.2	IP address of the PIX Public interface
User Name:	ehope	User created in Section 4.1
Password:	*****	Must match user password entered in Section 4.1
Group Name:	VPNPHONE	Group name created in Section 6.4
Group PSK:	***** (avaya123)	Must match pre-shared key entered in Section 6.4
VPN Start Mode:	BOOT	IPSec tunnel dynamically starts on Phone power up

Configuration Options	Value	Description
Password Type:	Save in Flash	User is not prompted at phone boot up.
Encapsulation	4500-4500	Default value to enable NAT Traversal
Syslog Server:	-	Locally log phone events
IKE Parameters:	DH2-3DES-MD5	Must match IKE SA set in Section 6.5
IKE ID Type:	KEY-ID	Specifies the format of the Group Name
Diffie-Hellman Grp	2	Can be set to “Detect” to accept PIX settings
Encryption Alg:	3DES	Can be set to “Any” to accept PIX settings
Authentication Alg:	MD5	Can be set to “Any” to accept PIX settings
IKE Xchg Mode:	Aggressive	Mode used for Phase 1 Negotiations
IKE Config Mode:	Enable	Enables IKE
IPSec Parameters:	NOPFS-AES128-SHA1	Must match IPSec proposals from Section 6.6
Encryption Alg:	AES-128	Can be set to “Any” to accept PIX settings
Authentication Alg:	SHA1	Can be set to “Any” to accept PIX settings
Diffie-Hellman Grp	NONE	Can be set to “Detect” to accept PIX settings
Protected Net:		
Remote Net #1:	0.0.0.0/0	Access to all private nets
Copy TOS:	Yes	Maintain Phones TOS setting on Corp Network for QoS
File Srvr:	192.168.1.30	TFTP/HTTP Phone File Srv
Connectivity Check:	First Time	Test initial IPSec connectivity

Table 2 – VPNremote Phone Configuration

3. The VPNremote Phone can interoperate with several VPN head-end vendors. The VPNremote Phone must be told which VPN head-end vendor will be used so the appropriate protocol dialogs can take place. This is done by setting the **VPN Configuration Profile** on the VPNremote Phone.

Press the **Profile** softtbutton at the bottom of the VPNremote Phones display while in the VPN Options mode. The **VPN Configuration Profile** options, shown below, are displayed. If a Profile other then Cisco is already chosen, press the Modify soft button to see this list.

- **Avaya Security Gateway**
- **Cisco Xauth with PSK**
- **Juniper Xauth with PSK**
- **Generic PSK**

Press the button aligned with the **Cisco Xauth with PSK** profile option then press the **Done** soft button.

When all VPN configuration options have been set, press the **Done** soft button. The following is displayed. Press # to save the configuration and reboot phone.

```
Save new values ?
*=no  #=yes
```

9. Verification

9.1. VPNremote Phone IPSec Statistics

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional (Dial-tone), from the telephone keypad, press the **OPTIONS** hard button (with √ icon). From the telephone keypad, press the ► hard button until the **VPN Status...** option appears. Select **VPN Status...**. The VPN statistics of the active IPSec tunnel will be displayed. Use the ► hard button to access the next screen. Press the **Refresh** soft button to update the displayed statistics.

The list below shows the statistics from the VPNremote phone used in the sample configuration.

VPN Status...	
PKT S/R	448/419
FRAG RCVD	0
Comp/Decomp	0/0
Auth Failures	0
Recv Errors	0
Send Errors	0
Gateway	160.2.2.2
Outer IP	100.2.2.232
Inner IP	10.10.8.1
Gateway Version	0.0.0
Inactivity Timeout	0
AES128-SHA-1 days	

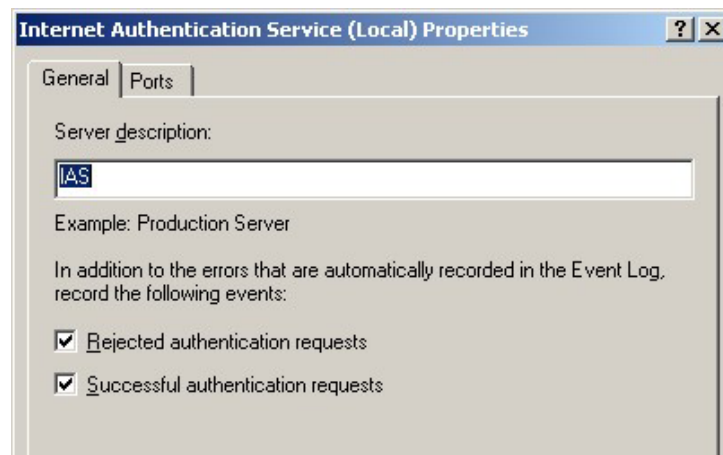
9.2. PIX Logging

The PIX **Real-time Log Viewer** displays the current event log contents of the PIX. The Real-time Log Viewer snapshots shown below contain key log events specific to the VPNremote Phone. Log entries of particular interest are highlighted in bold.

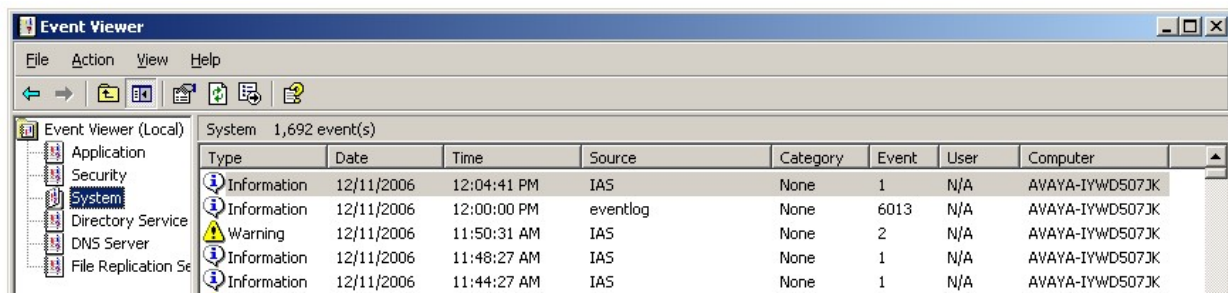
To access the PIX Real-time Log Viewer, select **Monitoring > Logging > Real-time Log Viewer** then the **View** button. See [4] for PIX log output examples with Avaya VPNremote Phone.

9.3. IAS Logging

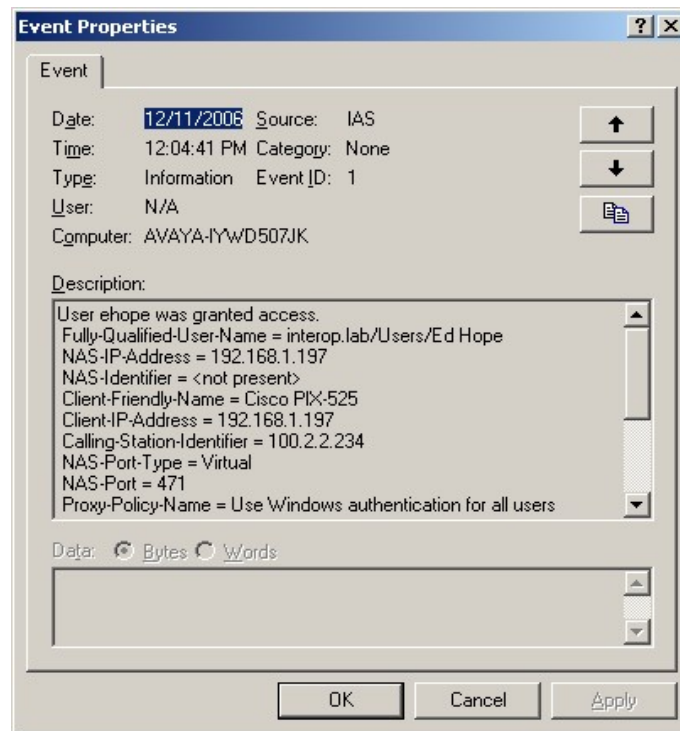
To enable logging of IAS events in the Windows Event Log, IAS must be running as a Windows service. Additionally, the following IAS options must be enabled to log Rejected and Successful authentication attempts to the event log. The IAS properties window is accessible by right clicking **Internet Authentication Services (Local)** > **Properties** from the IAS application window.



The Windows Event Viewer provides access to the Windows Event Log. IAS entries are categorized as System events. See events with a Source of IAS. The following screen shows an example of several IAS events.



Double clicking an event will display the event detail as shown in the window below for a successfully authenticated VPNremote Phone user.



To assist the reader, the full event description is shown in a separate window below.

```
Event Type: Information
Event Source:      IAS
Event Category:    None
Event ID:          1
Date:              12/11/2006
Time:              12:04:41 PM
User:              N/A
Computer:          AVAYA-IYWD507JK
Description:
User ehope was granted access.
Fully-Qualified-User-Name = interop.lab/Users/Ed Hope
NAS-IP-Address = 192.168.1.197
NAS-Identifier = <not present>
Client-Friendly-Name = Cisco PIX-525
Client-IP-Address = 192.168.1.197
Calling-Station-Identifier = 100.2.2.234
NAS-Port-Type = Virtual
NAS-Port = 471
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = VPNphone Users Policy
Authentication-Type = PAP
EAP-Type = <undetermined>
```

9.4. Avaya Communication Manager “list registered-ip-stations”

The Avaya Communication Manager **list registered-ip-stations** command, run from the SAT, can be used to verify the registration status of the VPNremote Phones and associated parameters as highlighted below.

list registered-ip-stations							
REGISTERED IP STATIONS							
Station	Set	Product	Prod	Station	Net Orig	Gatekeeper	TCP
Ext	Type	ID	Rel	IP Address	Rgn Port	IP Address	Skt
24074	4625	IP_Phone	2.500	10.10.8.1	5	192.168.1.10	Y
50003	4610	IP_Phone	2.300	10.10.8.2	5	192.168.1.10	Y
50020	4602+	IP_Phone	2.300	192.168.1.242	1	192.168.1.10	Y

9.5. Avaya Communication Manager “status station”

The Avaya Communication Manager **status station *nnn*** command, where ***nnn*** is a station extension, can be run from the SAT to verify the current status of an administered station. The **Service State: in-service/off-hook** shown on Page 1 below indicates the VPNremote Phone with extension 50003 is participating in an active call.

status station 50003		Page 1 of 6	
GENERAL STATUS			
Administered Type:	4610	Service State:	in-service/off-hook
Connected Type:	4610	TCP Signal Status:	connected
Extension:	50003		
Port:	S00004	Parameter Download:	complete
Call Parked?	no	SAC Activated?	no
Ring Cut Off Act?	no	CF Destination Ext:	
Active Coverage Option:	1		
EC500 Status:	N/A	Off-PBX Service State:	N/A
Message Waiting:			
Connected Ports:	S00029		
User Cntrl Restr: none		HOSPITALITY STATUS	
Group Cntrl Restr: none		Awaken at:	
		User DND: not activated	
		Group DND: not activated	
		Room Status: non-guest room	

Page 4, abridged below, displays the audio status of an **active call between two VPNremote Phones**. The highlighted fields shown below indicate the following:

- Other-end IP Addr value is from the PIX IP Address Pool indicating the call is with another VPNremote Phone.
- Audio RTP packets are going direct between VPNremote Phones.
- Both stations are in IP Network Region 5.
- G.729A codec is being used.

status station 50003										Page 4 of 6		
AUDIO CHANNEL												
Port: S00004												
		Switch							IP		IP	
		Port		Other-end IP Addr		:Port		Set-end IP Addr		:Port		
G.729		Audio:		10. 10. 8. 1		:2138		10. 10. 8. 2		:2934		
Node Name:												
Network Region:		5							5			
Audio Connection Type: ip-direct												

Page 4, abridged below, displays the audio status of an **active call between a VPNremote Phone and a Main Campus IP telephone**. The highlighted fields indicate the following:

- Other-end IP Addr value indicates the call is with an IP telephone at the Main Campus.
- Audio RTP packets are going direct between VPNremote Phone and the IP telephone.
- Call is between IP Network Region 1 and IP Network Region 5.
- G.729A codec is being used.

status station 50003					Page 4 of 6		
AUDIO CHANNEL							
Port: S00004							
Switch		IP			IP		
Port		Other-end IP Addr	:Port	Set-end IP Addr	:Port		
G.729	Audio:	192.168. 1.242	:2678	10. 10. 8. 2	:2934		
Node Name:							
Network Region:		1			5		
Audio Connection Type: ip-direct							

10. Troubleshooting

This section offers some common configuration mismatches to assist in troubleshooting. The focus of this section is on RADIUS user authentication with Microsoft IAS and AD. See [4] for PIX log output examples and troubleshooting with Avaya VPNremote Phone. The text below is from the Description field of the Microsoft Windows 2003 Server event log running the IAS and Active Directory applications.

10.1. Incorrect VPNremote Phone User Name (AD)

The following log entry is a result of a VPNremote Phone user name not found in Active Directory; **ehop** instead of **ehope**. See Section 4.1.

```
Event Type: Warning
Event Source: IAS
Event Category: None
Event ID: 2
Date: 12/12/2006
Time: 12:01:28 PM
User: N/A
Computer: AVAYA-IYWD507JK
Description:
User ehop was denied access.
Fully-Qualified-User-Name = INTEROP\ehop
NAS-IP-Address = 192.168.1.197
NAS-Identifier = <not present>
Called-Station-Identifier = 160.2.2.2
Calling-Station-Identifier = 100.2.2.234
Client-Friendly-Name = Cisco PIX-525
Client-IP-Address = 192.168.1.197
NAS-Port-Type = Virtual
NAS-Port = 472
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = <undetermined>
Authentication-Type = PAP
EAP-Type = <undetermined>
Reason-Code = 16
Reason = Authentication was not successful because an unknown user
name or incorrect password was used.
```

10.2. Incorrect VPNremote Phone User Password (AD)

The following log entry is a result of an incorrect VPNremote Phone user password for user ehope in Active Directory. See Section 4.1.

```
Event Type: Warning
Event Source:      IAS
Event Category:    None
Event ID:          2
Date:              12/12/2006
Time:              12:03:57 PM
User:              N/A
Computer:          AVAYA-IYWD507JK
Description:
User ehope was denied access.
Fully-Qualified-User-Name = INTEROP\ehope
NAS-IP-Address = 192.168.1.197
NAS-Identifier = <not present>
Called-Station-Identifier = 160.2.2.2
Calling-Station-Identifier = 100.2.2.234
Client-Friendly-Name = Cisco PIX-525
Client-IP-Address = 192.168.1.197
NAS-Port-Type = Virtual
NAS-Port = 473
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = <undetermined>
Authentication-Type = PAP
EAP-Type = <undetermined>
Reason-Code = 16
Reason = Authentication was not successful because an unknown user
name or incorrect password was used.
```

10.3. User Account: Remote Access Permission Disabled (AD)

The following log entry is a result of a VPNremote Phone user account, ehope, not enabled for remote authentication in Active Directory. See Section 4.1 Step 4.

```
Event Type: Warning
Event Source:      IAS
Event Category:    None
Event ID:          2
Date:              12/12/2006
Time:              12:06:34 PM
User:              N/A
Computer:          AVAYA-IYWD507JK
Description:
User ehope was denied access.
Fully-Qualified-User-Name = interop.lab/Users/Ed Hope
NAS-IP-Address = 192.168.1.197
NAS-Identifier = <not present>
Called-Station-Identifier = 160.2.2.2
Calling-Station-Identifier = 100.2.2.234
Client-Friendly-Name = Cisco PIX-525
Client-IP-Address = 192.168.1.197
NAS-Port-Type = Virtual
NAS-Port = 474
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = VPNphone Users Policy
Authentication-Type = PAP
EAP-Type = <undetermined>
Reason-Code = 65
Reason = The connection attempt failed because remote access
permission for the user account was denied. To allow remote access,
enable remote access permission for the user account, or, if the user
account specifies that access is controlled through the matching remote
access policy, enable remote access permission for that remote access
policy.
```

10.4. User Account Not Added to Group (AD)

The following log entry is a result of a VPNremote Phone user account, ehope, not added to the user group in Active Directory. See Section 4.3.

```
Event Type: Warning
Event Source:      IAS
Event Category:    None
Event ID:          2
Date:              12/12/2006
Time:              12:08:14 PM
User:              N/A
Computer:          AVAYA-IYWD507JK
Description:
User ehope was denied access.
Fully-Qualified-User-Name = INTEROP\ehope
NAS-IP-Address = 192.168.1.197
NAS-Identifier = <not present>
Called-Station-Identifier = 160.2.2.2
Calling-Station-Identifier = 100.2.2.234
Client-Friendly-Name = Cisco PIX-525
Client-IP-Address = 192.168.1.197
NAS-Port-Type = Virtual
NAS-Port = 475
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = <undetermined>
Authentication-Type = PAP
EAP-Type = <undetermined>
Reason-Code = 48
Reason = The connection attempt did not match any remote access
policy.
```

10.5. Incorrect Authentication Method (IAS)

The following log entry is a result of a mismatch in the IAS Remote Access Policy Authentication methods with the PIX (i.e. **Unencrypted authentication (PAP, SPAP)** was not enabled). See Section 5.2 Step 8.

```
Event Type: Warning
Event Source:      IAS
Event Category:    None
Event ID:          2
Date:              12/12/2006
Time:              12:15:36 PM
User:              N/A
Computer:          AVAYA-IYWD507JK
Description:
User ehope was denied access.
Fully-Qualified-User-Name = interop.lab/Users/Ed Hope
NAS-IP-Address = 192.168.1.197
NAS-Identifier = <not present>
Called-Station-Identifier = 160.2.2.2
Calling-Station-Identifier = 100.2.2.234
Client-Friendly-Name = Cisco PIX-525
Client-IP-Address = 192.168.1.197
NAS-Port-Type = Virtual
NAS-Port = 478
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = VPNphone Users Policy
Authentication-Type = PAP
EAP-Type = <undetermined>
Reason-Code = 66
Reason = The user attempted to use an authentication method that is
not enabled on the matching remote access policy.
```

10.6. Incorrect RADIUS client IP Address (IAS)

The following log entry is a result of a RADIUS request from an unknown source. The error below was caused by an incorrectly entered RADIUS Client IP address in IAS for the PIX. 192.168.1.196 was entering in IAS instead of 192.168.1.197. See Section 5.1 Step 2.

```
Event Type: Error
Event Source:      IAS
Event Category:    None
Event ID:          13
Date:              12/12/2006
Time:              12:33:03 PM
User:              N/A
Computer:          AVAYA-IYWD507JK
Description:
A RADIUS message was received from the invalid RADIUS client IP address
192.168.1.197.
```

10.7. IAS / PIX Mismatched Shared Secret (IAS)

The following log entry is a result of a mismatch in the IAS Shared Secret, see **Section 5.1 Step 3**, and the PIX Server Secret Key, see **Section 6.1 Step 4**.

```
Event Type: Warning
Event Source:      IAS
Event Category:    None
Event ID:          2
Date:              12/12/2006
Time:              12:36:07 PM
User:              N/A
Computer:          AVAYA-IYWD507JK
Description:
User ehope was denied access.
Fully-Qualified-User-Name = INTEROP\ehope
NAS-IP-Address = 192.168.1.197
NAS-Identifier = <not present>
Called-Station-Identifier = 160.2.2.2
Calling-Station-Identifier = 100.2.2.234
Client-Friendly-Name = Cisco PIX-525
Client-IP-Address = 192.168.1.197
NAS-Port-Type = Virtual
NAS-Port = 486
Proxy-Policy-Name = Use Windows authentication for all users
Authentication-Provider = Windows
Authentication-Server = <undetermined>
Policy-Name = <undetermined>
Authentication-Type = PAP
EAP-Type = <undetermined>
Reason-Code = 16
Reason = Authentication was not successful because an unknown user
name or incorrect password was used.
```

11. Conclusion

The Avaya VPNremote Phone combined with Cisco PIX Security Appliance, Microsoft Active Directory and Microsoft Internet Authentication Service provides a secure solution for remote worker telephony over any broadband Internet connection. The Avaya VPNremote Phone XAuth implementation for Cisco security appliances (utilizing the **Cisco Xauth with PSK** profile) demonstrated successful interoperability with the Cisco PIX model 525 Security Appliance, Microsoft IAS and Microsoft AD.

12. References

- [1] *Avaya VPNremote for the 4600 Series IP Telephones Release 2.0 Administrator Guide*, Doc ID: 19-600753
- [2] *VPNremote for 46xx Series IP Telephone Installation and Deployment Guide*, Doc ID: 1022006
- [3] *Administrators Guide for Avaya Communication Manager*, Doc ID: 03-300509
- [4] *Configuring Cisco PIX Security Appliance using Cisco Adaptive Security Device Manager (ASDM) VPN Wizard to Support Avaya VPNremote™ Phones – Issue 1.0*, Avaya Application Note
- [5] *Configuring Cisco VPN Concentrator to Support Avaya VPNremote™ Phones – Issue 1.0*, Avaya Application Note
- [6] *Application Notes for Configuring Avaya WebLM License Manager for Avaya VPNremote™ Phone Release 2 – Issue 1.0*, Avaya Application Note
- [7] **Avaya Application Notes and Resources Web Site:**
<http://www.avaya.com/gcm/master-usa/en-us/resource/>
- [8] **Avaya Product Support Web Site:**
<http://support.avaya.com/japple/css/japple?PAGE=Home>
- [9] **RCF 2865** – Remote Authentication Dial In User Service (RADIUS)
<http://www.ietf.org/rfc/rfc2865.txt?number=2865>

©2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com