Avaya Solution & Interoperability Test Lab

Configuring Cisco Adaptive Security Appliance (ASA) using Cisco Adaptive Security Device Manager (ASDM) VPN Wizard to Support Avaya VPNremote Phones – Issue 1.1

Abstract

These Application Notes describe the steps to configure the Cisco Adaptive Security Appliance to support IPSec VPN tunnel termination and XAuth authentication of the Avaya VPNremote Phone. The configuration steps utilize the VPN Wizard tool of the Cisco Adaptive Security Device Manager.

TABLE OF CONTENTS

1. Introduction

These Application Notes describe the steps to configure the Cisco Adaptive Security Appliance, referred to as “ASA” throughout the remainder of these Application Notes, to support IPSec VPN (Virtual Private Network) tunnel termination and XAuth (eXtended Authentication) authentication of the Avaya VPNremote Phone. The configuration steps utilize the VPN Wizard tool of the Cisco Adaptive Security Device Manager (ASDM) application. The Cisco ASDM application provides a graphical user interface to the ASA. The VPN Wizard configures the following VPN elements on the ASA to support VPNremote Phones:

- VPN Tunnel Group
- Pre-shared Key
- User Authentication
- User Accounts
- IP Address Pool
- Security Associations
- IPSec Encryption and Authentication Algorithms

The full command line configuration of the ASA for the sample configuration is provided in Appendix A as a reference.

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. An end user experiences the same IP telephone features as if the phone were 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 an ASA model 5520. However, these configuration steps can be applied to other ASA 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 ASA using IKE with 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 ASA and create a temporary secure path to allow the VPNremote Phone user to present credentials (username/password) to the ASA. After the VPNremote Phone user authentication is successful, the ASA assigns an IP address to the VPNremote Phone from a pre-configured IP Address Pool. The ASA local user authentication mechanism is used in the sample configuration.

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 1.** The Main Campus location contains the ASA functioning as perimeter security device and VPN head-end. The Phone Configuration File Server and DNS Server are all running on the same physical server on the trusted enterprise LAN. The Avaya S8710 Server and Avaya G650 Media Gateway are also located at the Main Campus.

The Avaya VPNremote Phones are located in the public network and are configured to establish an IPSec tunnel to the Public (outside) IP address of the ASA. The ASA assigns IP addresses to the VPNremote Phones. 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 and DNS server. The VPNremote Phone then initiates an H.323 registration with Avaya Communication Manager.

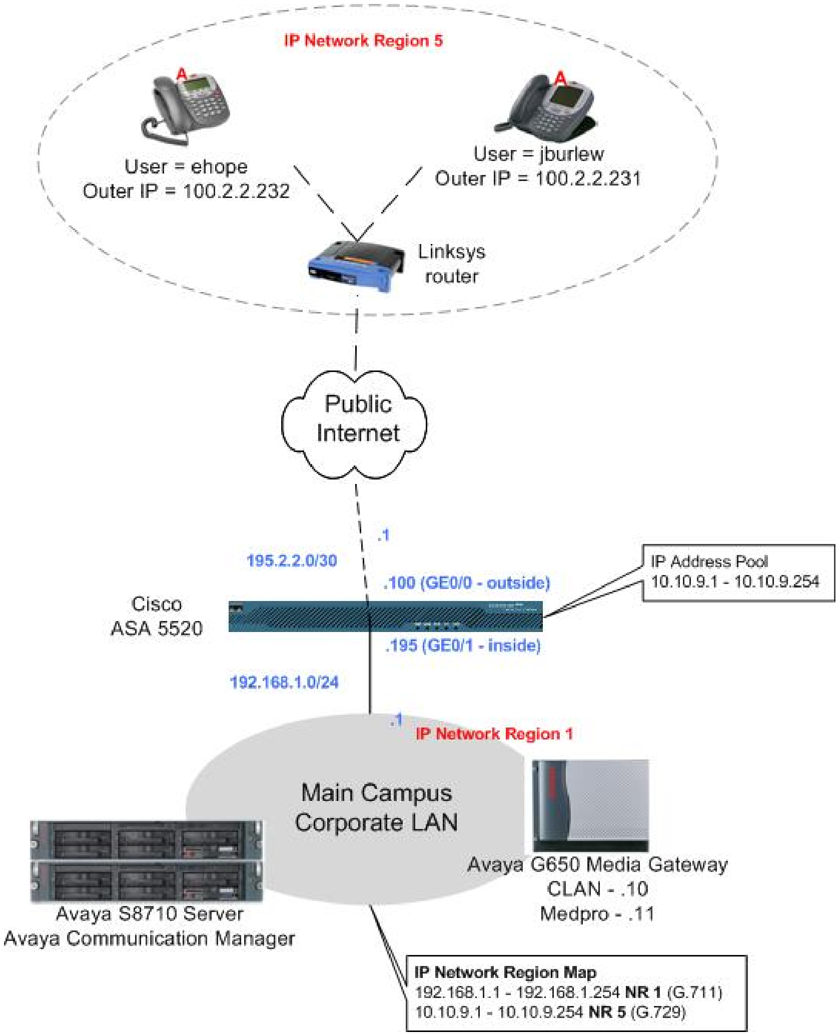


Figure 1: Network Diagram

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 Server	Avaya Communication Manager 5.1.1 (R015x.01.1.415.1) and service patch 16402
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_4 – (a10b**VPN**232_4.bin)
Avaya 4625SW IP Telephones	R2.5.2_4 – (a25**VPN**252_4.bin)
Cisco ASA model 5520	8.0(3)
Cisco Adaptive Security Device Manager	6.1(5)

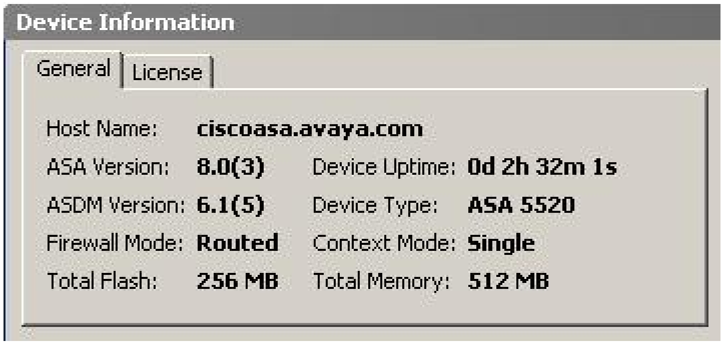
Table 1 – Software/Hardware Version Information

4. Cisco ASA Configuration

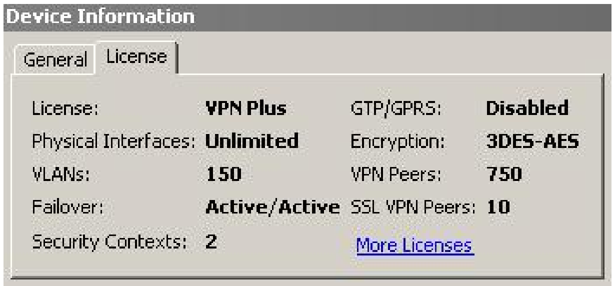
These Application Notes assume that the ASA is fully operational and configured to allow the Cisco ASDM to make configuration changes. See [8] for additional information.

4.1. VPN Wizard

1. From the **ASDM Home** screen, verify the version of the ASA, as shown in the Device Information pane, with the ASA 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 [7] and [8] for additional information. Also verify the status and configuration of the network interfaces as shown in the Interface Status pane.



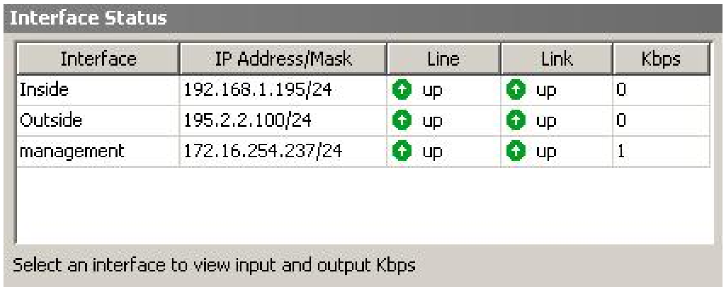
Host Name: ciscoasa.avaya.com
ASA Version: 8.0(3) Device Uptime: 0d 2h 32m 1s
ASDM Version: 6.1(5) Device Type: ASA 5520
Firewall Mode: Routed Context Mode: Single
Total Flash: 256 MB Total Memory: 512 MB



Device Information

General | License

License:	**VPN Plus**	GTP/GPRS:	**Disabled**
Physical Interfaces:	**Unlimited**	Encryption:	**3DES-AES**
VLANs:	**150**	VPN Peers:	**750**
Failover:	**Active/Active**	SSL VPN Peers:	**10**
Security Contexts:	**2**	More Licenses	

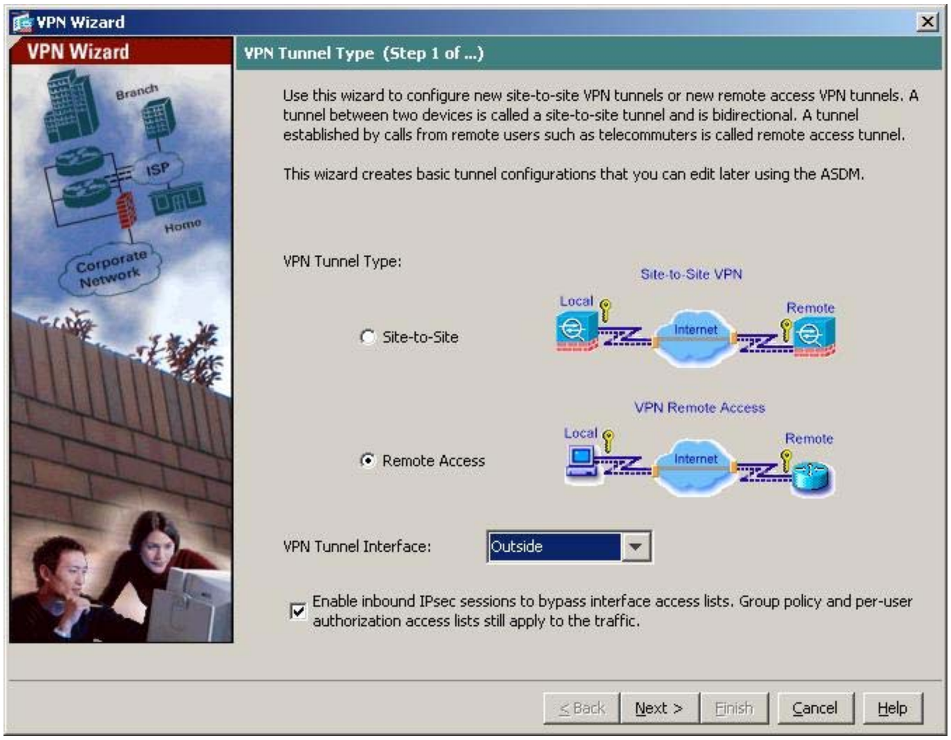


Interface Status

Interface	IP Address/Mask	Line	Link	Kbps
Inside	192.168.1.195/24	up	up	0
Outside	195.2.2.100/24	up	up	0
management	172.16.254.237/24	up	up	1

Select an interface to view input and output Kbps

2. To start the VPN Wizard, select **Wizards > IPSec VPN Wizard** from the ASDM top toolbar. Select **Remote Access** for the VPN Tunnel Type and **Outside** for VPN Tunnel Interface. All remaining fields can be left at default values. Click **Next** to continue.



VPN Tunnel Type (Step 1 of ...)

Use this wizard to configure new site-to-site VPN tunnels or new remote access VPN tunnels. A tunnel between two devices is called a site-to-site tunnel and is bidirectional. A tunnel established by calls from remote users such as telecommuters is called remote access tunnel.

This wizard creates basic tunnel configurations that you can edit later using the ASDM.

VPN Tunnel Type:

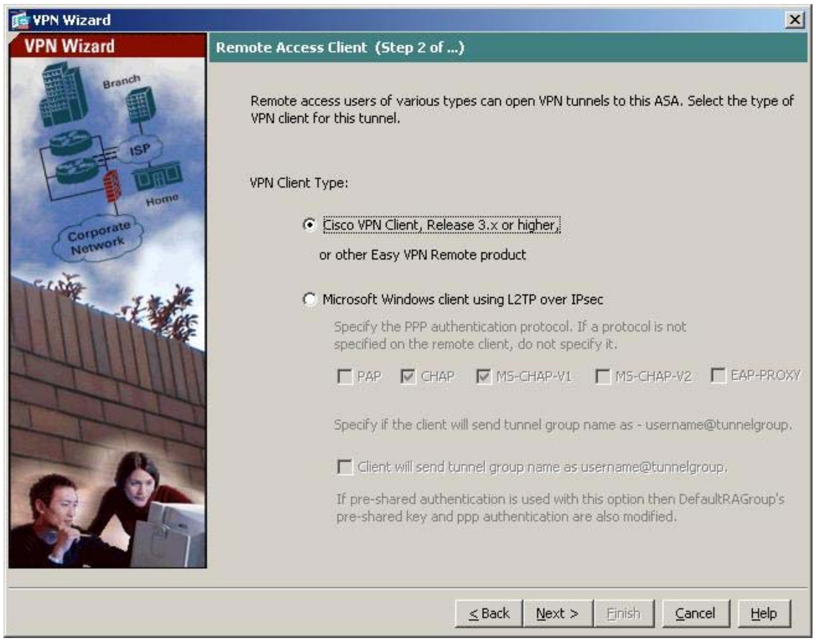
○ Site-to-Site

● Remote Access

VPN Tunnel Interface: Outside

☑ Enable inbound IPsec sessions to bypass interface access lists. Group policy and per-user authorization access lists still apply to the traffic.

3. Maintain the default selection of **Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product**. Click **Next** to continue.



Remote Access Client (Step 2 of ...)

Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.

VPN Client Type:

● Cisco VPN Client, Release 3.x or higher, or other Easy VPN Remote product

○ Microsoft Windows client using L2TP over IPsec

Specify the PPP authentication protocol. If a protocol is not specified on the remote client, do not specify it.

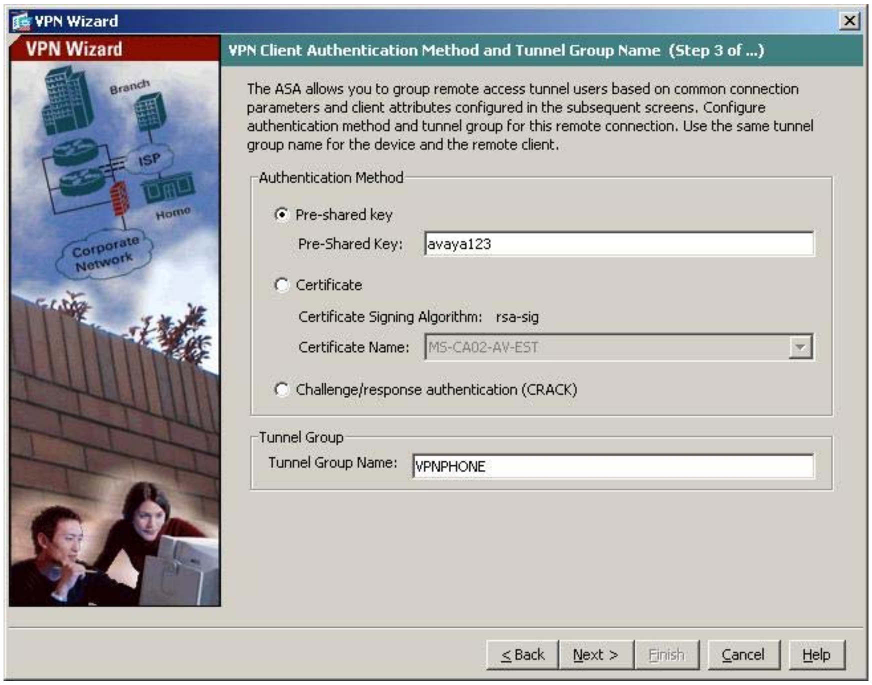
□ PAP ☑ CHAP ☑ MS-CHAP-V1 □ MS-CHAP-V2 □ EAP-PROXY

Specify if the client will send tunnel group name as - username@tunnelgroup.

□ Client will send tunnel group name as username@tunnelgroup.

If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.

4. Enter the "Pre-shared Key" value and the "Tunnel Group Name" to be used by the Avaya VPNremote Phones, then click **Next** to continue. VPNPHONE is the default group name used by the VPNremote Phones. However, any group name can be used as long as the VPNremote Phone configuration matches. See Section 6.2.



VPN Client Authentication Method and Tunnel Group Name (Step 3 of ...)

The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client.

Authentication Method

● Pre-shared key

Pre-Shared Key: avaya123

○ Certificate

Certificate Signing Algorithm: rsa-sig

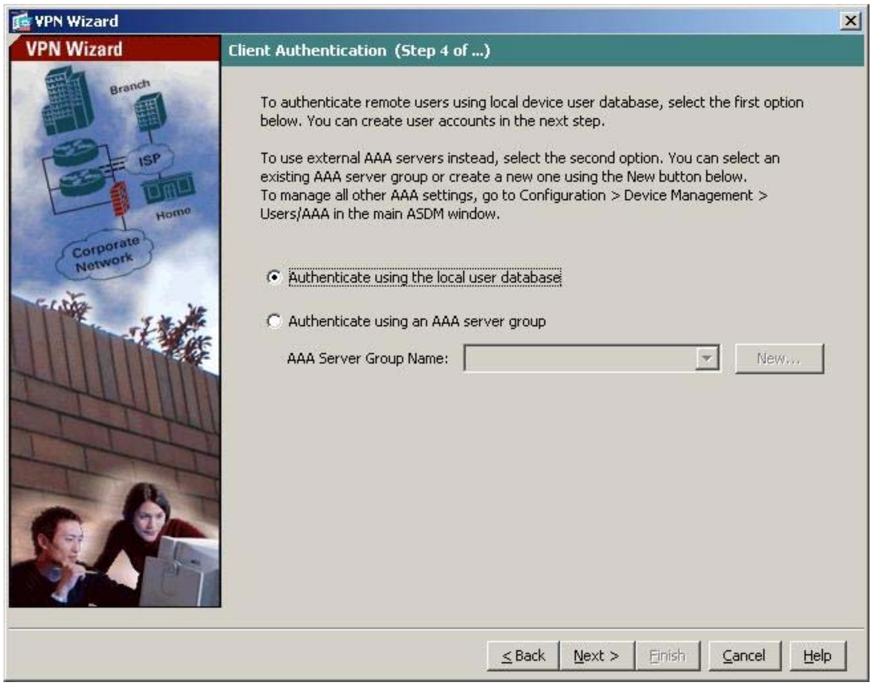
Certificate Name: MS-CA02-AV-EST

○ Challenge/response authentication (CRACK)

Tunnel Group

Tunnel Group Name: VPNPHONE

5. The internal ASA user authentication database is used in the sample configuration. However, an external authentication server can be used. Maintain the default **Authenticate using the local user database** and click **Next** to continue.



Client Authentication (Step 4 of ...)

To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step.

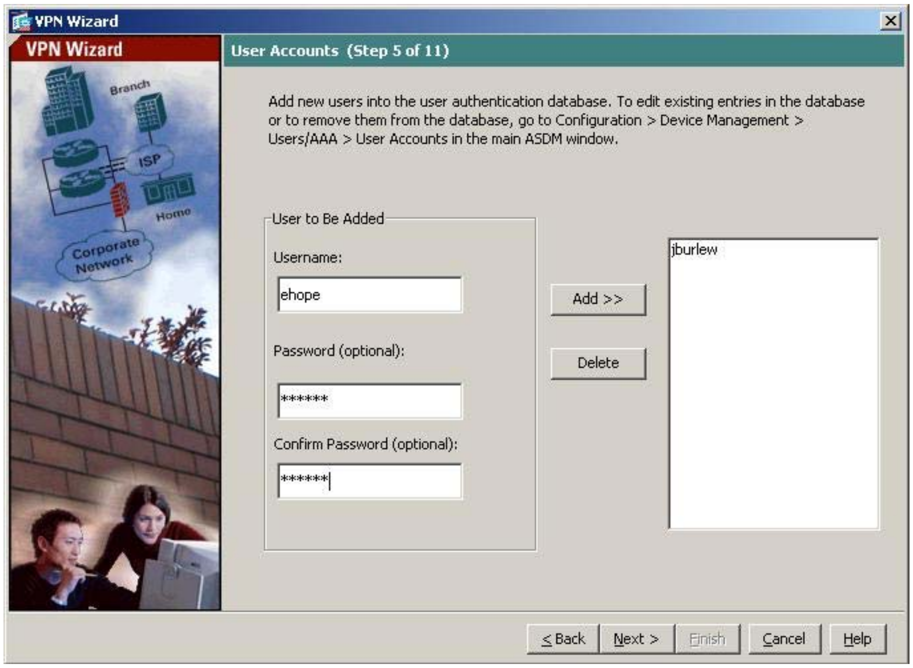
To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below.
To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.

● Authenticate using the local user database

○ Authenticate using an AAA server group

AAA Server Group Name:

6. Enter the Username and Password of a VPNremote Phone user and click **Add**. Two user accounts, ehope and jburlew, are created in the sample configuration. When all VPNremote Phone user accounts have been entered, click **Next** to continue.



User Accounts (Step 5 of 11)

Add new users into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Device Management > Users/AAA > User Accounts in the main ASDM window.

User to Be Added

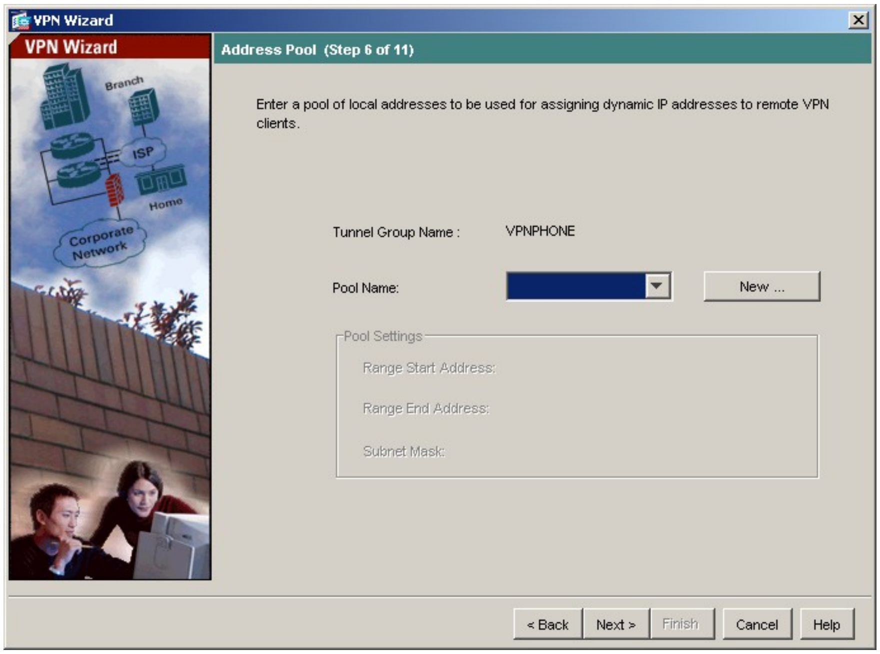
Username: ehope

Password (optional): ******

Confirm Password (optional): ******

jburlew

7. Click the **New** button to create a new IP address pool.



Address Pool (Step 6 of 11)

Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.

Tunnel Group Name : VPNPHONE

Pool Name:

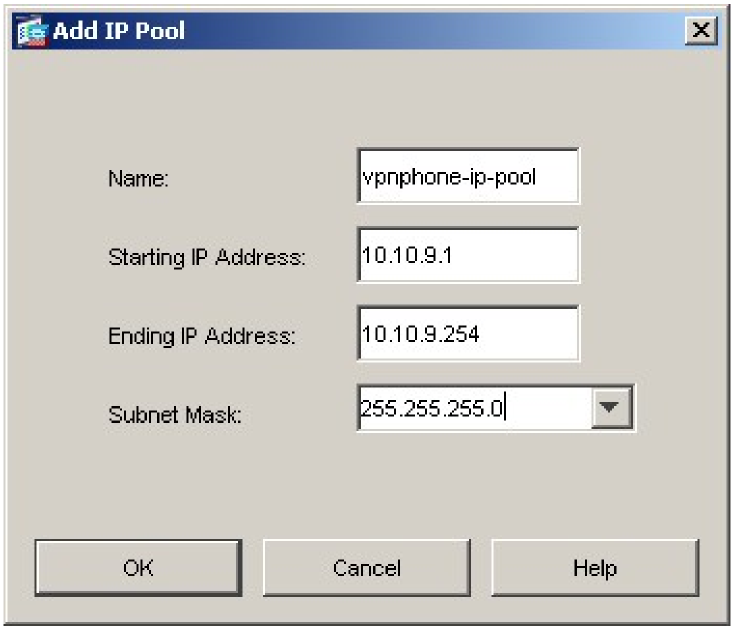
Pool Settings

Range Start Address:

Range End Address:

Subnet Mask:

8. Enter a descriptive name and the IP address range to be assigned to VPNremote Phones as the "inner address". This address range must not overlap with any addresses on the private enterprise network and must be routable within the enterprise network. Click **OK** and then click **Next** at the Address Pool window to continue.



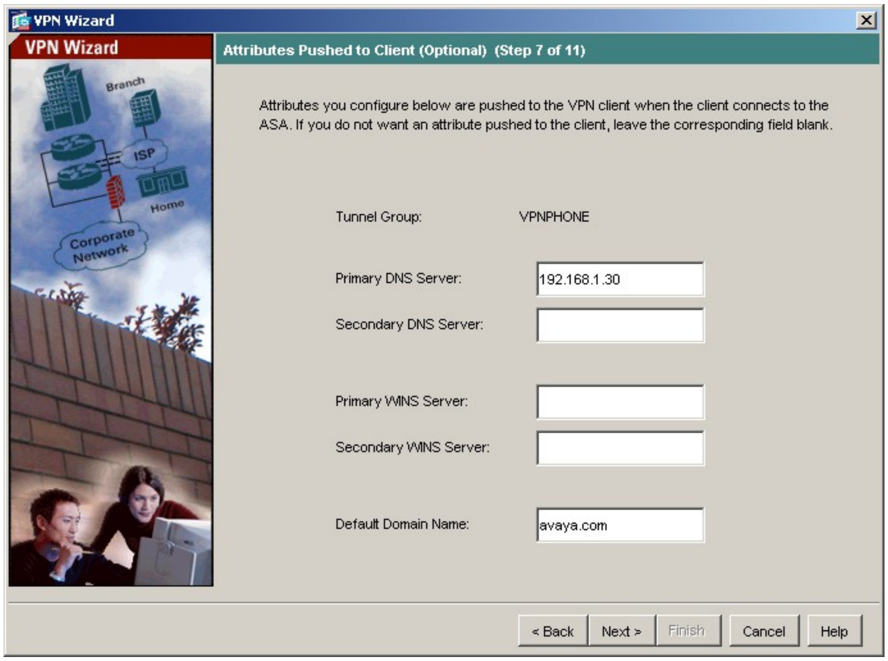
Name: vpnphone-ip-pool

Starting IP Address: 10.10.9.1

Ending IP Address: 10.10.9.254

Subnet Mask: 255.255.255.0

9. Enter the DNS, WINS and Domain information to be used by the VPNremote Phone while accessing the enterprise network through the IPSec tunnel. Values entered below are specific to the sample network used for these Application Notes. Click **Next** when complete.



Attributes Pushed to Client (Optional) (Step 7 of 11)

Attributes you configure below are pushed to the VPN client when the client connects to the ASA. If you do not want an attribute pushed to the client, leave the corresponding field blank.

Tunnel Group: VPNPHONE

Primary DNS Server: 192.168.1.30

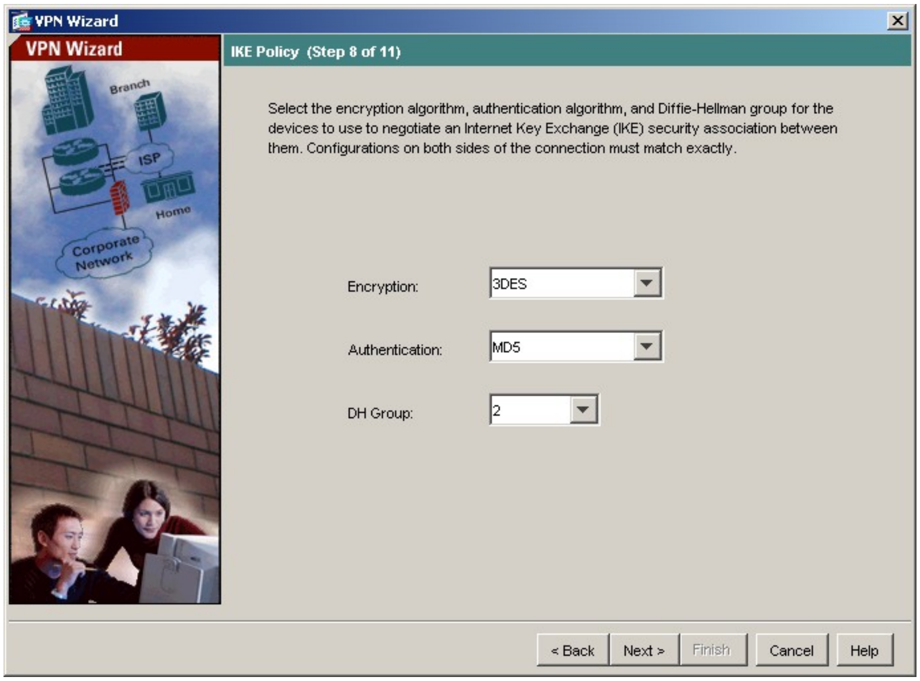
Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

Default Domain Name: avaya.com

10. Select the IKE security association parameters from the drop-down lists. Click **Next** to continue.



IKE Policy (Step 8 of 11)

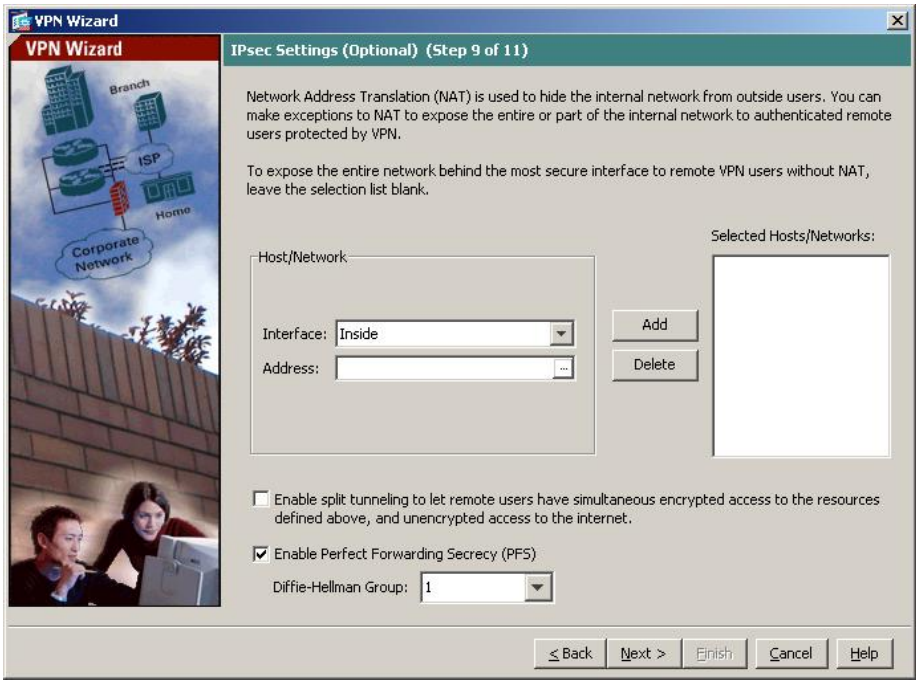
Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.

Encryption: 3DES

Authentication: MD5

DH Group: 2

11. Maintain the default **Address Translation Exemption and Split Tunneling** options and click **Next** to continue.



IPsec Settings (Optional) (Step 9 of 11)

Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN.

To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the selection list blank.

Host/Network

Interface: Inside

Address:

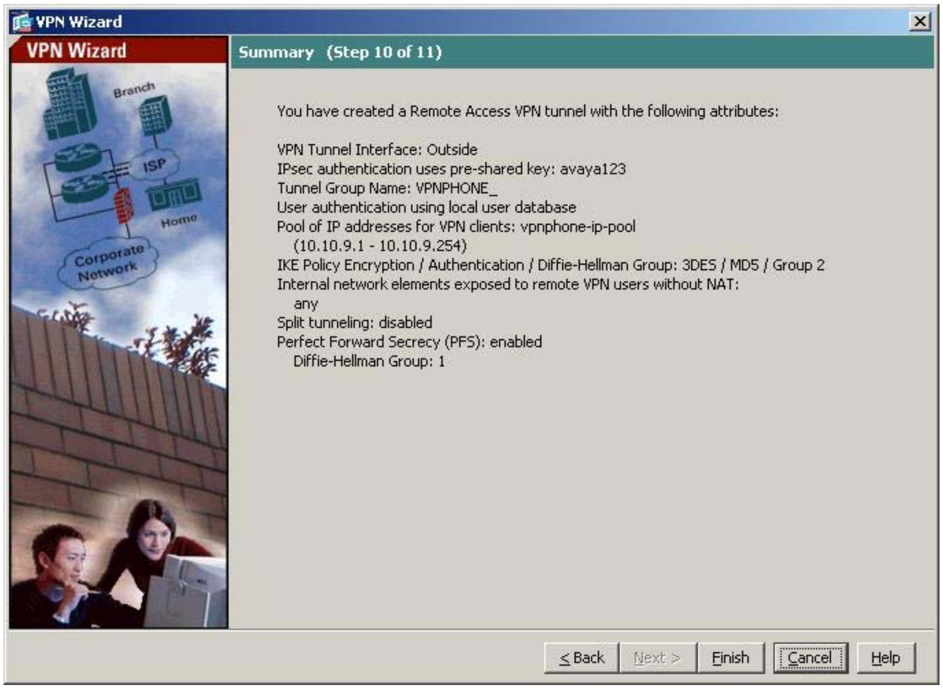
Selected Hosts/Networks:

☐ Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.

☑ Enable Perfect Forwarding Secrecy (PFS)

Diffie-Hellman Group: 1

12. Verify the VPN Tunnel options and click **Finish** to complete.



Summary (Step 10 of 11)

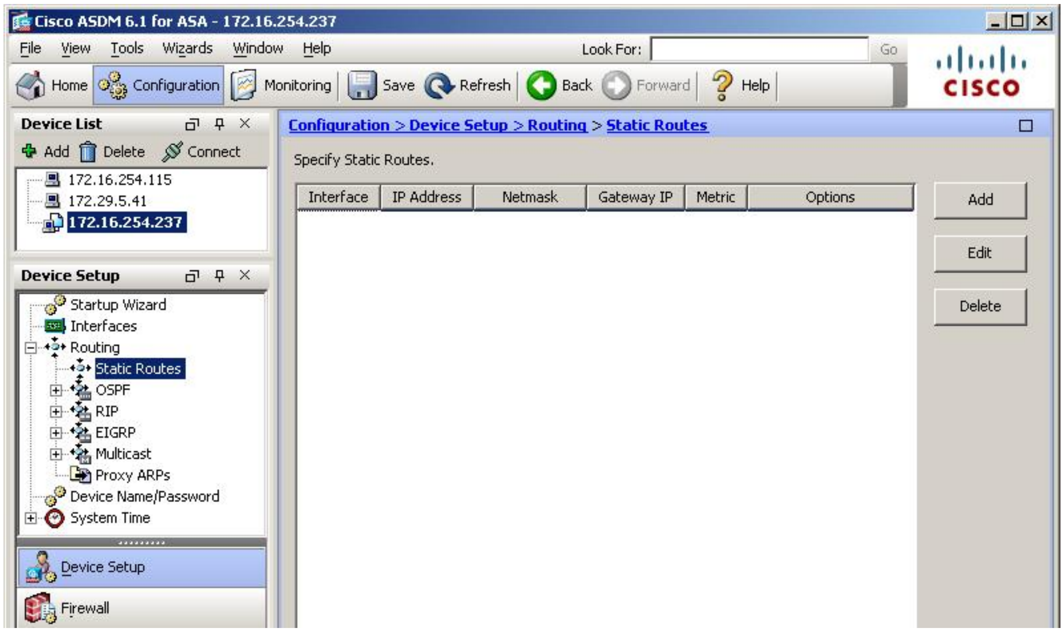
You have created a Remote Access VPN tunnel with the following attributes:

VPN Tunnel Interface: Outside
IPsec authentication uses pre-shared key: avaya123
Tunnel Group Name: VPNPHONE_
User authentication using local user database
Pool of IP addresses for VPN clients: vpnphone-ip-pool
  (10.10.9.1 - 10.10.9.254)
IKE Policy Encryption / Authentication / Diffie-Hellman Group: 3DES / MD5 / Group 2
Internal network elements exposed to remote VPN users without NAT:
  any
Split tunneling: disabled
Perfect Forward Secrecy (PFS): enabled
  Diffie-Hellman Group: 1

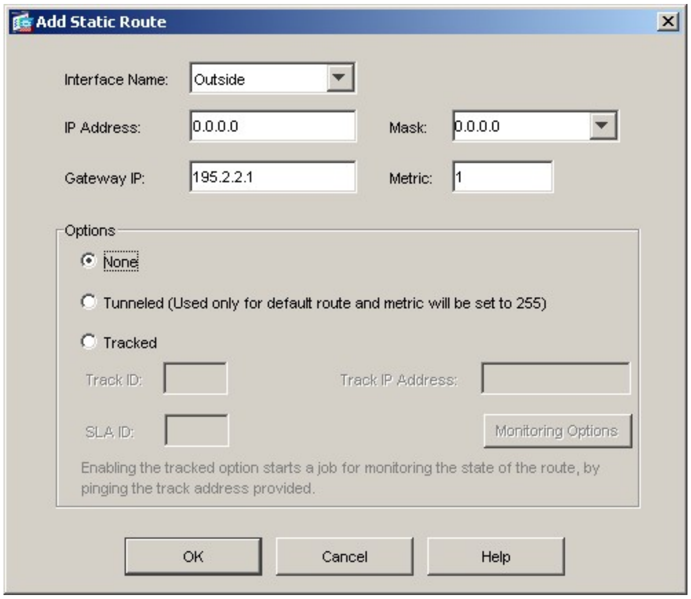
4.2. Default Route

The default route must be set on the ASA. The default route was 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 195.2.2.1 is the ISP next hop router as shown in **Figure 1**. Click **OK**.



Add Static Route

Interface Name: Outside

IP Address: 0.0.0.0 Mask: 0.0.0.0

Gateway IP: 195.2.2.1 Metric: 1

Options

● None

○ Tunneled (Used only for default route and metric will be set to 255)

○ Tracked

Track ID: Track IP Address:

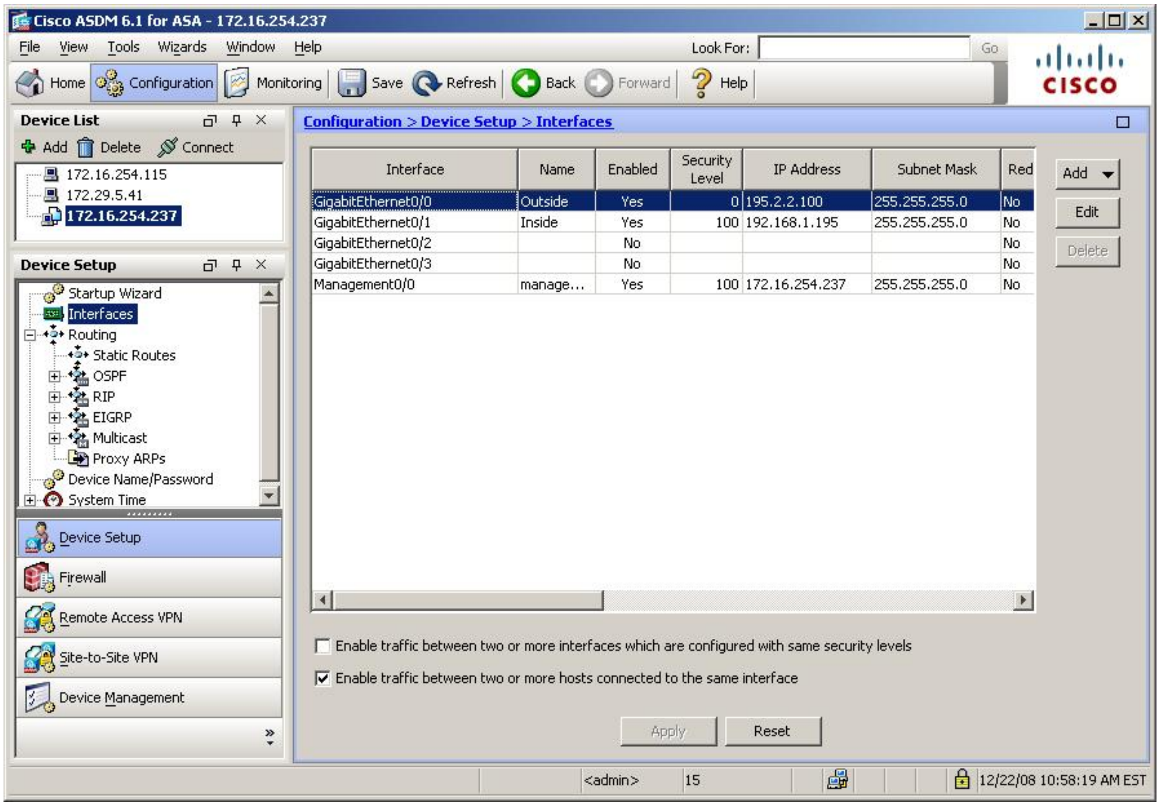
SLA ID: Monitoring Options

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

4.3. 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 ASA, the **Enable traffic between two or more hosts connected to the same interface** ASA 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 towards the bottom of the screen next to **Enable traffic between two or more hosts connected to the same interface**. Click **Apply** to save.



Interface	Name	Enabled	Security Level	IP Address	Subnet Mask	Red
GigabitEthernet0/0	Outside	Yes	0	195.2.2.100	255.255.255.0	No
GigabitEthernet0/1	Inside	Yes	100	192.168.1.195	255.255.255.0	No
GigabitEthernet0/2		No				No
GigabitEthernet0/3		No				No
Management0/0	manage...	Yes	100	172.16.254.237	255.255.255.0	No

☐ Enable traffic between two or more interfaces which are configured with same security levels

☑ Enable traffic between two or more hosts connected to the same interface

5. Avaya Communication Manager Configuration

This section shows the necessary steps to configure Avaya Communication Manager for VPNremote Phones. It is assumed that the basic configuration of 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).

As shown in **Figure 1**, VPNremote Phones are assigned to IP Network Region 5 using the IP address range of the ASA 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.

5.1. 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:
```

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

```
list ip-codec-set

                                IP CODEC SETS

Codec  Codec 1     Codec 2     Codec 3     Codec 4     Codec 5
Set

  1    G.711MU
  2    G.729
  3
  4
```

5.2. IP Network Map Configuration

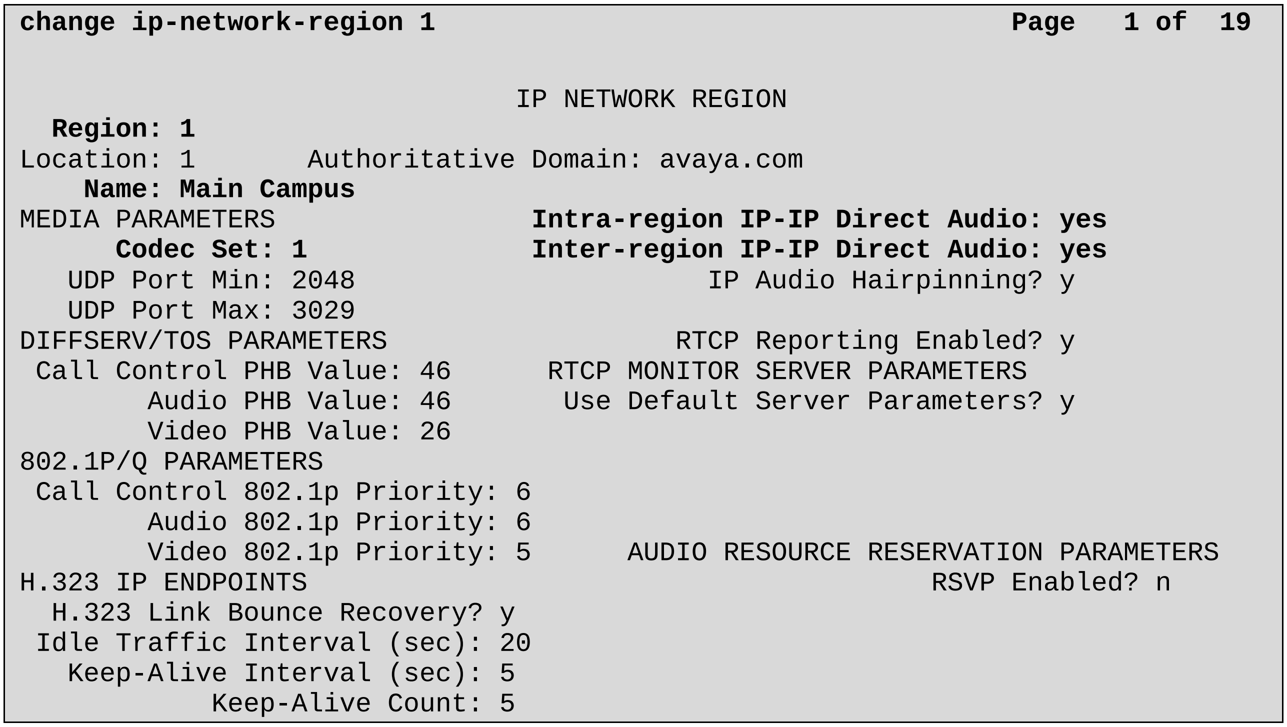
Use the **`change ip-network-map`** command to define the IP address to Network Region mapping for VPNremote Phones.

```
change ip-network-map                                          Page   1 of  32
                         IP ADDRESS MAPPING

                                                               Emergency
                                     Subnet                    Location
 From IP Address  (To IP Address   or Mask)  Region    VLAN   Extension
 10 .10 .9  .1    10 .10 .9  .254             5        n
    .   .   .        .   .   .                         n
    .   .   .        .   .   .                         n
    .   .   .        .   .   .                         n
```

5.3. IP Network Region Configuration

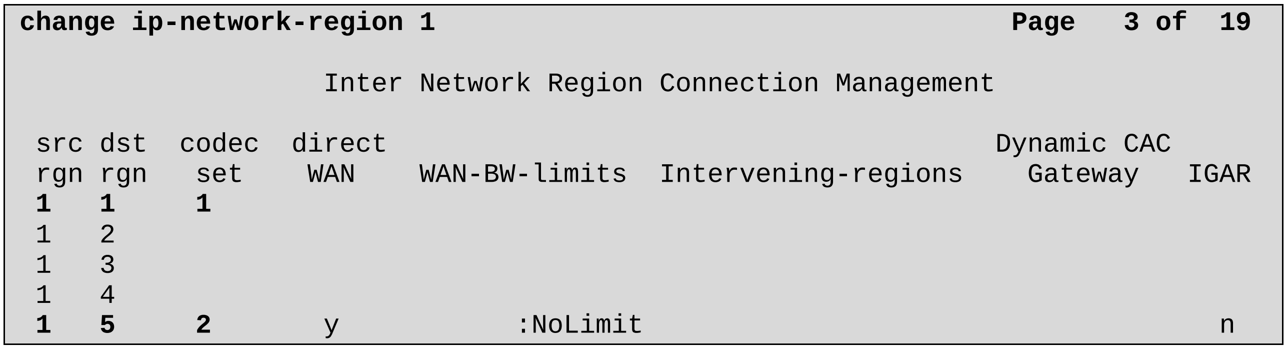
Use the **change ip-network-region *n*** command to configure IP Network Region parameters where ***n*** is the IP Network Region number. Configure the highlighted fields shown below. All remaining fields can be left at the default values.

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 5.1, 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 - ASA
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
```

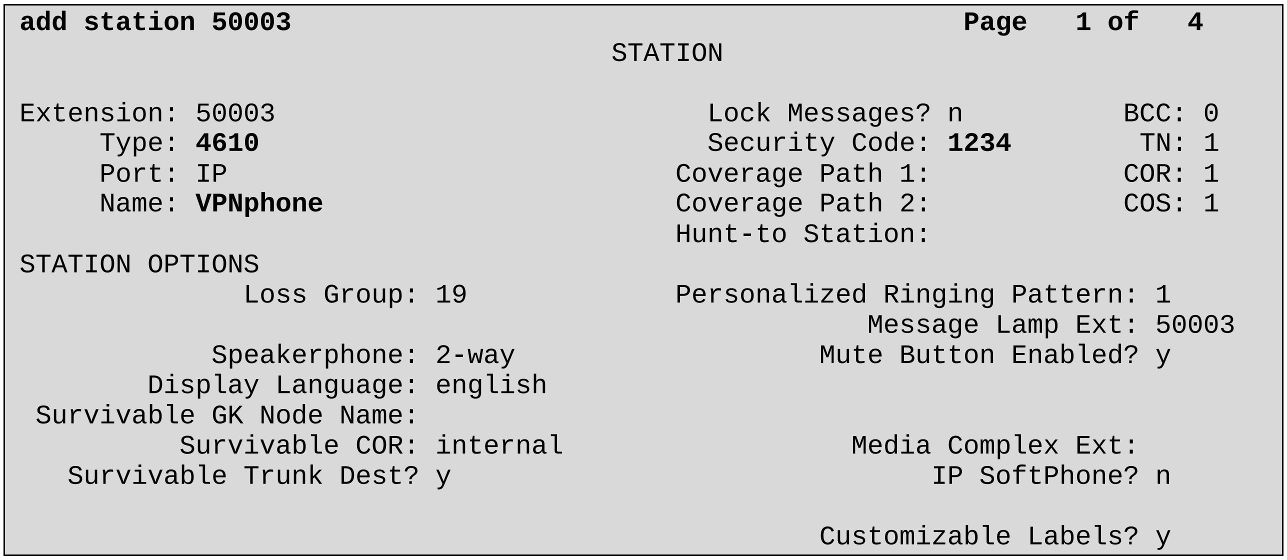
Page 3 defines the codec set to use for inter-region calls. Avaya VPNremote Phones are mapped to Region 5. Calls between IP Network Region 5 and IP Network Region 1 will also use Codec Set 2 (G.729).

```
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
```

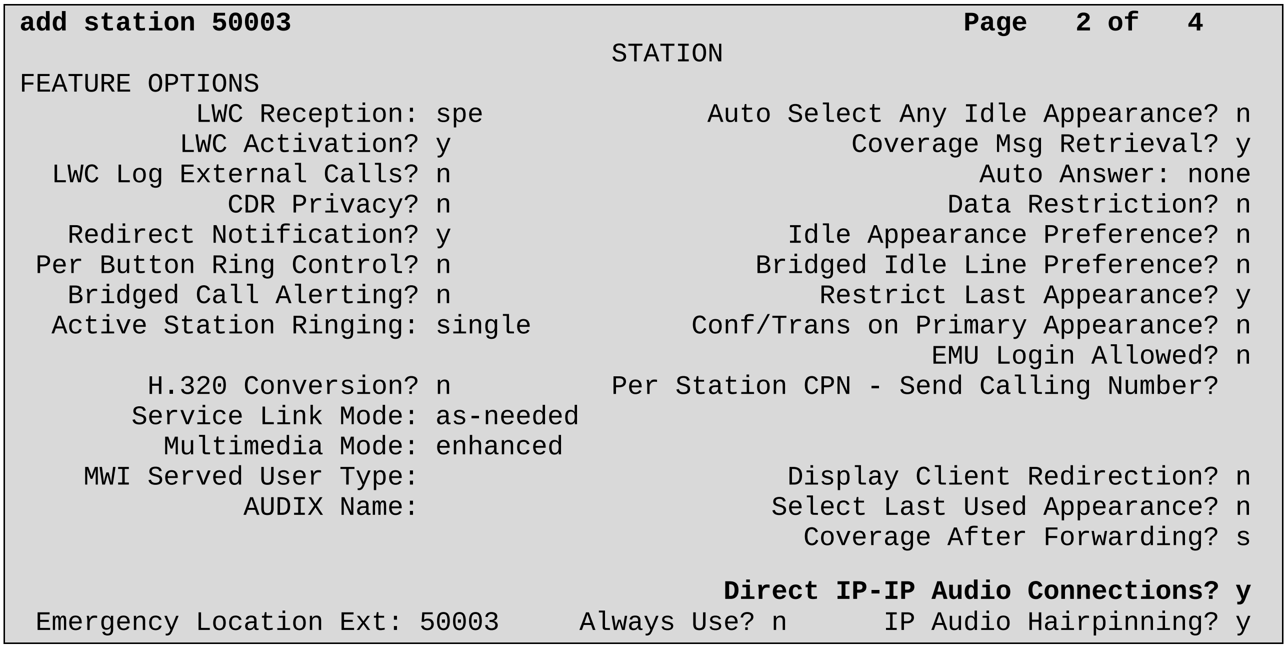
5.4. Add Station

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 4.3.



```
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
```

6. Avaya VPNremote Phone Configuration

6.1. 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 selecting 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.

6.2. 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.

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.

2. 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:	**195.2.2.100**	IP address of the ASA Public interface
User Name:	**ehope**	User created in **ASA VPN Wizard**
Password:	********	Must match user password entered in **ASA VPN Wizard**
Group Name:	**VPNPHONE**	Group name created in **ASA VPN Wizard**
Group PSK:	******** (avaya123)	Must match pre-shared key entered in **ASA VPN Wizard**
VPN Start Mode:	**BOOT**	IPSec tunnel dynamically starts on Phone power up
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 **ASA VPN Wizard**.

Configuration Options	Value	Description
IKE ID Type:	**KEY-ID**	Specifies the format of the Group Name
Diffie-Hellman Grp	**2**	Can be set to "Detect" to accept ASA settings
Encryption Alg:	**3DES**	Can be set to "Any" to accept ASA settings
Authentication Alg:	**MD5**	Can be set to "Any" to accept ASA settings
IKE Xchg Mode:	**Aggressive**	Mode used for Phase 1 Negotiations
IKE Config Mode:	**Enable**	Enables IKE
IPSec Parameters:	**DH2-AES128-SHA1**	
Encryption Alg:	**AES-128**	Can be set to "Any" to accept ASA settings
Authentication Alg:	**SHA1**	Can be set to "Any" to accept ASA settings
Diffie-Hellman Grp	**2**	Can be set to "Detect" to accept ASA settings
Protected Net:		
Remote Net #1:	**0.0.0.0/0**	Access to all private nets
Copy TOS:	**Yes**	RE-write TOS bit value to outside IP header 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 configured with the VPN head-end vendor to 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** soft button 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, and 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 the phone.

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

7. Verification

7.1. VPNremote Phone IPSec Statistics

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, 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. Press 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	**195.2.2.100**
Outer IP	**100.2.2.232**
Inner IP	**10.10.9.1**
Gateway Version	**0.0.0**
Inactivity Timeout	**0**
AES128-SHA-1 days	

7.2. 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 10.10.9.1        5           192.168.1.10    y
50003    4610    IP_Phone   2.300 10.10.9.2        5           192.168.1.10    y
50020    4602+   IP_Phone   2.300 192.168.1.242    1           192.168.1.10    y
```

7.3. 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
```

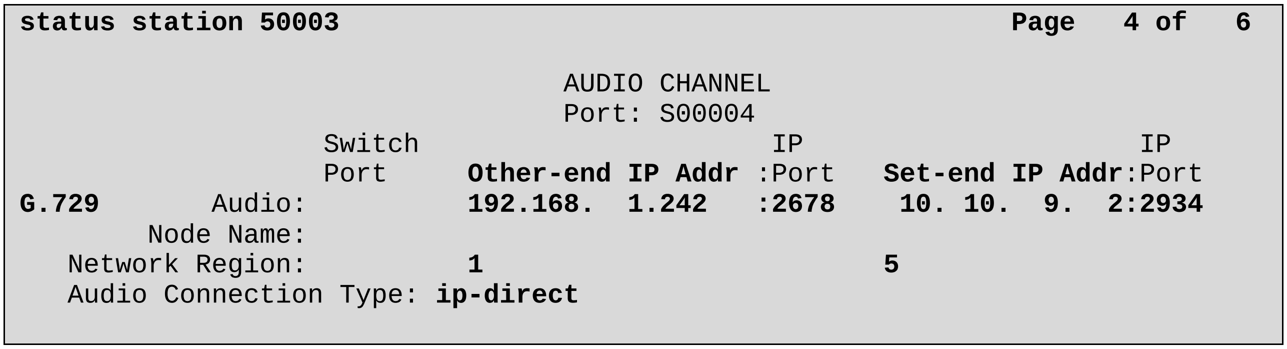
Page 4, abridged below, displays the audio status of an **active call between two VPNremote Phones**. The highlighted fields shown below indicate the following:

- Other-end IP Addr value is from the ASA 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.  9.  1   :2138    10. 10.  9.   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.  9.  2:2934
        Node Name:
   Network Region:          1                         5
   Audio Connection Type: ip-direct
```

7.4. ASA Logging

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

To access the ASA Real-time Log Viewer, select **Monitoring > Logging > Real-time Log Viewer,** and then click the **View** button.

7.4.1. Successful IKE Phase1, IKE Phase2 and XAuth User Authentication

This section shows events logged for a single Avaya VPNremote Phone successfully authenticating and establishing an IPSec tunnel. The log entries containing the text **unknown** or **unsupported transaction mode** are a normal result of the IPSec negotiation exchange between the ASA and the VPNremote Phone (i.e., not indicative of a problem).

Log Messages
AAA user authentication Successful : local database : user = ehope
AAA group policy for user ehope is being set to VPNPHONE
AAA retrieved user specific group policy (VPNPHONE) for user = ehope
AAA retrieved default group policy (VPNPHONE) for user = ehope
AAA transaction status ACCEPT : user = ehope
DAP: User ehope, Addr 100.2.2.232, Connection IPSec: The following DAP records were selected for this connection: DfltAccessPolicy
Built inbound UDP connection 360 for Outside:100.2.2.232/63121 (100.2.2.232/63121) to NP Identity Ifc:195.2.2.100/500 (195.2.2.100/500)
Built inbound UDP connection 361 for Outside:100.2.2.232/63122 (100.2.2.232/63122) to NP Identity Ifc:195.2.2.100/500 (195.2.2.100/500)
Group = VPNPHONE, Username = ehope, IP = 100.2.2.232, Received unsupported transaction mode attribute: 5
Group = VPNPHONE, Username = ehope, IP = 100.2.2.232, Received unsupported transaction mode attribute: 6
Group = VPNPHONE, Username = ehope, IP = 100.2.2.232, Client Type: Client Application Version:
Group = VPNPHONE, Username = ehope, IP = 100.2.2.232, **Assigned private IP address 10.10.9.4 to remote user**
Built inbound UDP connection 362 for Outside:100.2.2.232/63124 (100.2.2.232/63124) to NP Identity Ifc:195.2.2.100/500 (195.2.2.100/500)
Group = VPNPHONE, Username = ehope, IP = 100.2.2.232, **PHASE 1 COMPLETED**
IP = 100.2.2.232, Keep-alives configured on but peer does not support keep-alives (type = None)
Built inbound UDP connection 363 for Outside:100.2.2.232/63125 (100.2.2.232/63125) to NP Identity Ifc:195.2.2.100/500 (195.2.2.100/500)
Group = VPNPHONE, Username = ehope, IP = 100.2.2.232, Duplicate Phase 2 packet detected. No last packet to retransmit.
Group = VPNPHONE, Username = ehope, IP = 100.2.2.232, Overriding Initiator's IPSec rekeying duration from 432000 to 28800 seconds
Built inbound UDP connection 364 for Outside:100.2.2.232/63128 (100.2.2.232/63128) to NP Identity Ifc:195.2.2.100/500 (195.2.2.100/500)
IPSEC: An outbound remote access SA (SPI= 0x281FF2D9) between 195.2.2.100 and 100.2.2.232 (user= ehope) has been created.

Group = VPNPHONE, Username = ehope, IP = 100.2.2.232, Security negotiation complete for User (ehope) Responder, Inbound SPI = 0xe84beb20, Outbound SPI = 0x281ff2d9
IPSEC: An inbound remote access SA (SPI= 0xE84BEB20) between 195.2.2.100 and 100.2.2.232 (user= ehope) has been created.
Group = VPNPHONE, Username = ehope, IP = 100.2.2.232, **PHASE 2 COMPLETED** (msgid=51c8b207)

7.4.2. QTest Attempts

The Avaya VPNremote Phone **Quality Test** feature is used to test the quality of the network between the VPNremote Phone and VPN Head-end through the IPSec tunnel. The VPNremote Phone runs a short QTest sanity test against the VPN Head-end in quiet mode just after the IPSec tunnel has been established. If this QTest sanity test is executed successfully (i.e., if the VPN Head-end responded to the QTest packets), the QTest soft button is made available to the VPNremote Phone user. If this QTest sanity test does not complete successfully, the QTest soft button is not presented to the VPNremote Phone user.

The ASA characterizes the QTest packets sent by the VPNremote phone as a “Land Attack” type of Denial of Service attack due to the makeup of the QTest packets. **The ASA drops these QTest packets without responding, resulting in the QTest feature being disabled** on the VPNremote Phone. The ASA log entries shown below are the QTest packets being denied.

Src IP	Dest IP	Message Text
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4
10.10.9.4	10.10.9.4	Deny IP due to Land Attack from 10.10.9.4 to 10.10.9.4

7.4.3. TFTP Server Access

The following events are logged as the VPNremote Phone accesses the TFTP server on the enterprise network.

Src IP	Dest IP	Message Text
10.10.9.1	192.168.1.30	Built inbound UDP connection 928 for outside:10.10.9.1/1026 (10.10.9.1/1026) to inside:192.168.1.30/1297 (192.168.1.30/1297)
10.10.9.1	192.168.1.30	Built inbound UDP connection 927 for outside:10.10.9.1/1026 (10.10.9.1/1026) to inside:192.168.1.30/69 (192.168.1.30/69) (ehope)
10.10.9.1	192.168.1.30	Built inbound UDP connection 926 for outside:10.10.9.1/1025 (10.10.9.1/1025) to inside:192.168.1.30/1296 (192.168.1.30/1296)
10.10.9.1	192.168.1.30	Built inbound UDP connection 925 for outside:10.10.9.1/1025 (10.10.9.1/1025) to inside:192.168.1.30/69 (192.168.1.30/69) (ehope)
10.10.9.1	192.168.1.30	Built inbound UDP connection 923 for outside:10.10.9.1/1024 (10.10.9.1/1024) to **inside:192.168.1.30/1295 (192.168.1.30/1295)**
10.10.9.1	192.168.1.30	Built inbound UDP connection 922 for outside:10.10.9.1/1024 (10.10.9.1/1024) to **inside:192.168.1.30/69 (192.168.1.30/69) (ehope)**

7.4.4. DNS Server Access

The following events are logged as the VPNremote Phone accesses the DNS server on the enterprise network.

Src IP	Dest IP	Message Text
10.10.9.1	192.168.1.30	Teardown UDP connection 934 for outside:10.10.9.1/1032 to inside:192.168.1.30/53 duration 0:00:00 bytes 131 (ehope)
10.10.9.1	192.168.1.30	Teardown UDP connection 933 for outside:10.10.9.1/1031 to inside:192.168.1.30/53 duration 0:00:00 bytes 131 (ehope)
10.10.9.1	192.168.1.30	Teardown UDP connection 932 for outside:10.10.9.1/1030 to inside:192.168.1.30/53 duration 0:00:00 bytes 131 (ehope)
10.10.9.1	192.168.1.30	Teardown UDP connection 931 for outside:10.10.9.1/1029 to inside:192.168.1.30/53 duration 0:00:00 bytes 131 (ehope)
10.10.9.1	192.168.1.30	Teardown UDP connection 930 for outside:10.10.9.1/1028 to inside:192.168.1.30/53 duration 0:00:00 bytes 133 (ehope)
10.10.9.1	192.168.1.30	Teardown UDP connection 929 for **outside:10.10.9.1/1027 to inside:192.168.1.30/53** duration 0:00:00 bytes 133 **(ehope)**

7.4.5. H.323 Registration with Avaya Communication Manager

The following events are logged as the VPNremote Phone registers with Avaya Communication Manager via the CLAN interface of the G650 Media Gateway.

Src IP	Dest IP	Message Text
10.10.9.4	192.168.1.10	Built inbound UDP connection 366 for Outside:10.10.9.4/49300 (10.10.9.4/49300) to **Inside:192.168.1.10/1719 (192.168.1.10/1719) (ehope)**
10.10.9.4	192.168.1.10	Built inbound TCP connection 370 for Outside:10.10.9.4/5387 (10.10.9.4/5387) to **Inside:192.168.1.10/1720 (192.168.1.10/1720) (ehope)**

7.4.6. Call Between Two VPNremote Phones

The following events are logged as the VPNremote Phone of user “ehope” calls VPNremote Phone of user “jburlew” with IP-IP Direct Audio set to “yes” on Avaya Communication Manager for the IP Network Region to which the VPNremote Phones are assigned. The log shows the following:

- A connection between ehope VPNremote Phone (10.10.9.4) to the G650 MedPro (192.168.1.11) for dial tone RTP packets.
- A connection between jburlew VPNremote Phone (10.10.9.2) to the G650 MedPro (192.168.1.11) while the phone is alerting.
- A connection between ehope VPNremote Phone (10.10.9.4) and jburlew VPNremote Phone (10.10.9.2) for IP to IP Direct Audio RTP packets.

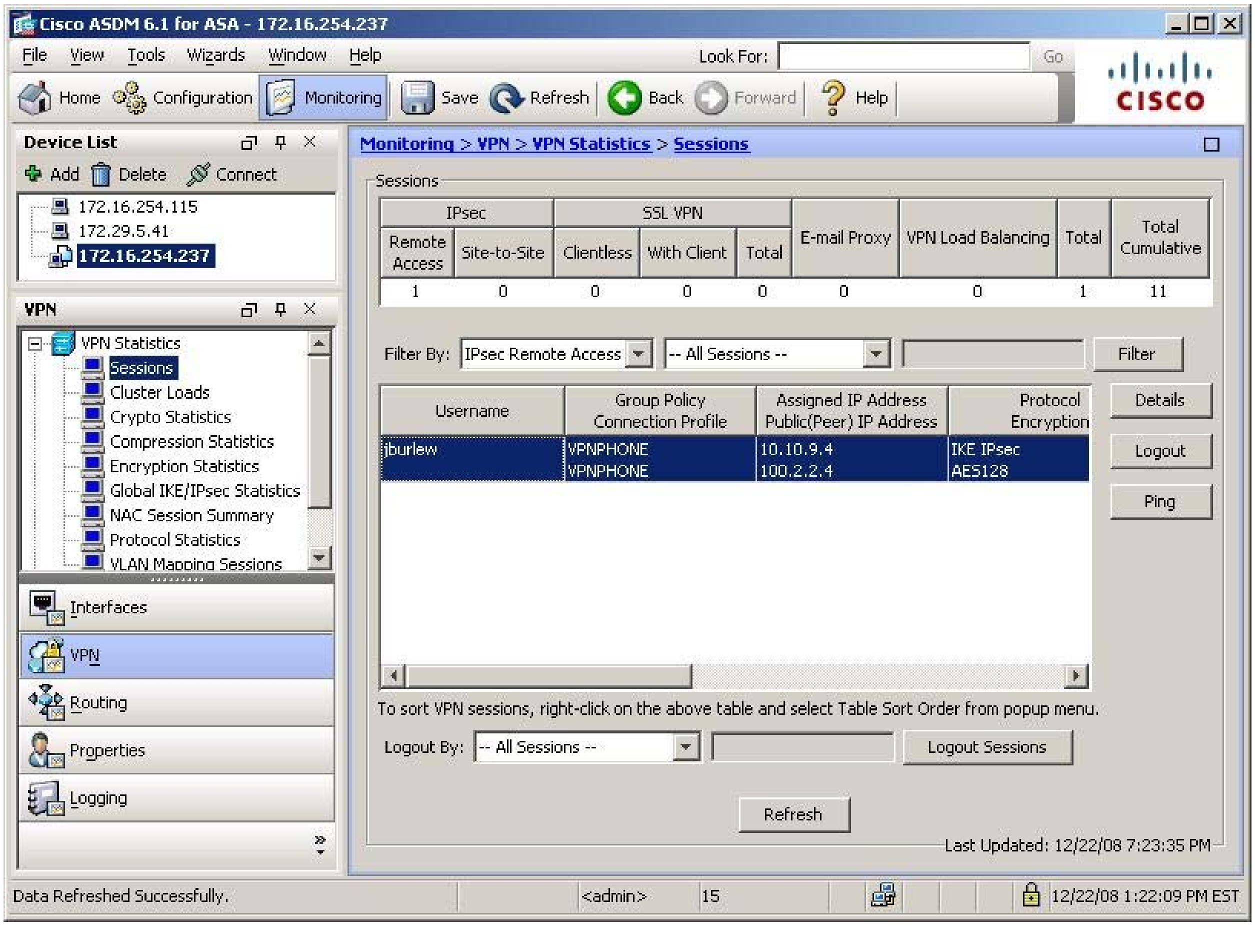
Src IP	Dest IP	Message Text
10.10.9.4	10.10.9.2	Built inbound UDP connection 7043 for **outside:10.10.9.4/2625 (10.10.9.4/2625) to outside:10.10.9.2/2903 (10.10.9.2/2903) (ehope)**
10.10.9.2	10.10.9.4	Built inbound UDP connection 7041 for **outside:10.10.9.2/2902 (10.10.9.2/2902) to outside:10.10.9.4/2624 (10.10.9.4/2624) (jburlew)**
10.10.9.4	192.168.1.25	Built inbound UDP connection 7048 for outside:10.10.9.4/2627 (10.10.9.4/2627) to inside:192.168.1.25/5005 (192.168.1.25/5005) (ehope)
10.10.9.2	192.168.1.25	Built inbound UDP connection 7047 for outside:10.10.9.2/2905 (10.10.9.2/2905) to inside:192.168.1.25/5005 (192.168.1.25/5005) (jburlew)
10.10.9.2	192.168.1.11	Built inbound UDP connection 7040 for **outside:10.10.9.2/2903 (10.10.9.2/2903) to inside:192.168.1.11/2993 (192.168.1.11/2993) (jburlew)**
10.10.9.4	192.168.1.11	Pre-allocate **H323 UDP** backconnection for faddr **10.10.9.4 to laddr 192.168.1.11/2989**
10.10.9.4	192.168.1.11	Pre-allocate **H323 UDP** backconnection for faddr **10.10.9.4 to laddr 192.168.1.11/2988**
10.10.9.2	10.10.9.4	Pre-allocate **H323 UDP** backconnection for faddr

		10.10.9.2 to laddr 10.10.9.4/2625
10.10.9.2	10.10.9.4	Pre-allocate **H323 UDP** backconnection for faddr **10.10.9.2 to laddr 10.10.9.4/2624**
10.10.9.2	192.168.1.11	Pre-allocate H323 UDP backconnection for faddr 10.10.9.2 to laddr 192.168.1.11/2993
10.10.9.2	192.168.1.11	Pre-allocate H323 UDP backconnection for faddr 10.10.9.2 to laddr 192.168.1.11/2992
10.10.9.4	192.168.1.11	Built inbound UDP connection 7034 for outside:10.10.9.4/2624 (10.10.9.4/2624) to inside:192.168.1.11/2988 (192.168.1.11/2988)
10.10.9.4	192.168.1.11	Built inbound UDP connection 7035 for outside:10.10.9.4/2625 (10.10.9.4/2625) to inside:192.168.1.11/2989 (192.168.1.11/2989)
10.10.9.4	192.168.1.11	Pre-allocate H323 UDP backconnection for faddr 10.10.9.4 to laddr 192.168.1.11/2989
10.10.9.4	192.168.1.11	Pre-allocate H323 UDP backconnection for faddr **10.10.9.4 to laddr 192.168.1.11/2988**

7.5. ASA Active VPN Sessions

7.5.1. VPN Session Statistics

The active VPN sessions to the ASA can be viewed by selecting **Monitoring > VPN > VPN Statistics > Sessions**. The screen shot below shows sessions of two VPNremote Phones with active tunnels to the ASA.



Monitoring > VPN > VPN Statistics > Sessions

Sessions

IPsec		SSL VPN			E-mail Proxy	VPN Load Balancing	Total	Total Cumulative
Remote Access	Site-to-Site	Clientless	With Client	Total				
1	0	0	0	0	0	0	1	11

Filter By: IPsec Remote Access   -- All Sessions --

Username	Group Policy Connection Profile	Assigned IP Address Public(Peer) IP Address	Protocol Encryption
jburlew	VPNPHONE VPNPHONE	10.10.9.4 100.2.2.4	IKE IPsec AES128

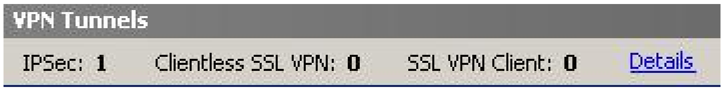
To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions --

Last Updated: 12/22/08 7:23:35 PM

Data Refreshed Successfully.   <admin>   15   12/22/08 1:22:09 PM EST

The ASDM Home page also provides some basic VPN Tunnel statistics as shown below.

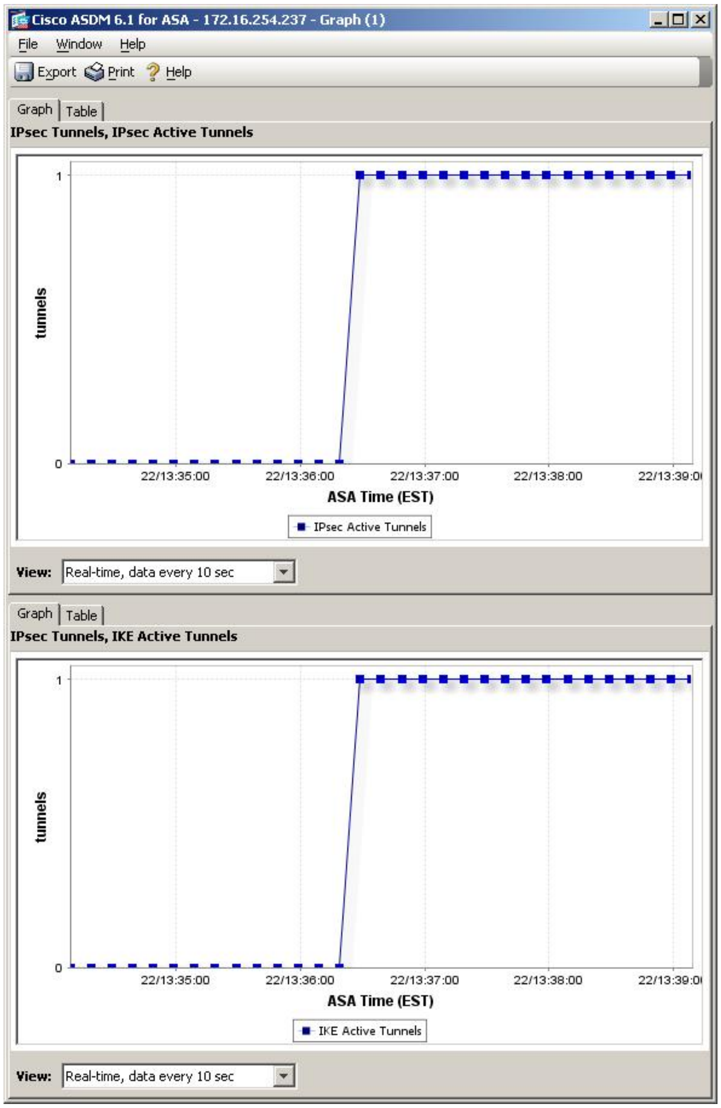


VPN Tunnels

IPSec: 1   Clientless SSL VPN: 0   SSL VPN Client: 0   Details

7.5.2. VPN Session Graph

The active VPN sessions to the ASA can be shown in a graph by selecting **Monitoring > VPN > VPN Connection Graphs > IPSec Tunnels**. Add **IPSec Active Tunnels** and **IKE Active Tunnels** to the Selected Graphs list and click the **Show Graphs** button to display the graph. The screen shot below shows the IPSec and IKE sessions of two VPNremote Phones with active tunnels to the ASA.



View: Real-time, data every 10 sec

View: Real-time, data every 10 sec

8. Conclusion

The Avaya VPNremote Phone combined with the Cisco ASA Security Appliance 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 ASA Security Appliance.

9. Additional References

Avaya Application Notes and additional resources can be found at the following web address http://www.avaya.com/gcm/master-usa/en-us/resource/. Avaya Product Support web site can be found at the following web address http://support.avaya.com/.

[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 VPN Concentrator to Support Avaya VPNremote™ Phones – Issue 1.0,*** Avaya Application Note

[5] ***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

[6] ***Configuring Cisco PIX Security Appliance with Microsoft Internet Authentication Service and Active Directory using RADIUS to Support Avaya VPNremote Phones – Issue 1.0,*** Avaya Application Note

[7] ***Cisco Security Appliance Command Line Configuration Guide***, Software Version 8.0, Part Number: OL-12172-03**,** www.cisco.com

[8] ***Cisco ASDM User Guide***, Version 6.1, Part Number: OL-16647-01**,** www.cisco.com

10. Appendix A: ASA Command Line Configuration

The complete command line configuration of the ASA for the sample configuration is provided below. Please note that the below configuration contains entry that is above what is necessary for the solution described in these Application Notes.0

```
ASA Version 8.0(3)
!
hostname ciscoasa
domain-name avaya.com
enable password 8Ry2YjIyt7RRXU24 encrypted
names
dns-guard
!
interface GigabitEthernet0/0
 description Public ISP connection
 nameif Outside
 security-level 0
 ip address 195.2.2.100 255.255.255.0
!
interface GigabitEthernet0/1
 description Corporate Network connection
 nameif Inside
 security-level 100
 ip address 192.168.1.195 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
 no ip address
!
interface Management0/0
 nameif management
 security-level 100
 ip address 172.16.254.237 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa803-k8.bin
boot system disk0:/asa723-k8.bin
ftp mode passive
clock timezone EST -5
clock summer-time EDT recurring
dns server-group DefaultDNS
 domain-name avaya.com
same-security-traffic permit intra-interface
access-list Inside_nat0_outbound extended permit ip any 10.10.9.0
255.255.255.0
```

```
pager lines 24
logging enable
logging asdm informational
mtu Outside 1500
mtu Inside 1500
mtu management 1500
ip local pool vpnphone-ip-pool 10.10.9.1-10.10.9.254 mask 255.255.255.0
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp permit any Outside
icmp permit any management
asdm image disk0:/asdm-615.bin
no asdm history enable
arp timeout 14400
nat (Inside) 0 access-list Inside_nat0_outbound
route Outside 0.0.0.0 0.0.0.0 195.2.2.1 1
route Inside 10.10.5.0 255.255.255.0 192.168.1.198 1
route Inside 10.10.8.0 255.255.255.0 192.168.1.197 1
route Inside 50.50.100.0 255.255.255.0 192.168.1.199 1
route Inside 60.1.1.0 255.255.255.0 192.168.1.1 1
route management 135.0.0.0 255.0.0.0 172.16.254.4 1
route management 148.147.0.0 255.255.0.0 172.16.254.4 1
route management 198.152.0.0 255.255.0.0 172.16.254.4 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 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy
nac-policy DfltGrpPolicy-nac-framework-create nac-framework
 default-acl  unused
 reval-period 36000
 sq-period 300
http server enable
http 60.1.1.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 management
http 172.16.254.0 255.255.255.0 management
http 135.0.0.0 255.0.0.0 management
http 148.147.0.0 255.255.0.0 management
http 198.152.0.0 255.255.0.0 management
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto dynamic-map Outside_dyn_map 20 set pfs
crypto dynamic-map Outside_dyn_map 20 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 40 set pfs
crypto dynamic-map Outside_dyn_map 40 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 60 set pfs
crypto dynamic-map Outside_dyn_map 60 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 80 set pfs
crypto dynamic-map Outside_dyn_map 80 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 100 set pfs
crypto dynamic-map Outside_dyn_map 100 set transform-set ESP-3DES-SHA
crypto dynamic-map Outside_dyn_map 120 set pfs
crypto dynamic-map Outside_dyn_map 120 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 140 set pfs
crypto dynamic-map Outside_dyn_map 140 set transform-set ESP-AES-128-SHA
crypto dynamic-map Outside_dyn_map 160 set pfs
crypto dynamic-map Outside_dyn_map 160 set transform-set ESP-AES-128-SHA
crypto map Outside_map 65535 ipsec-isakmp dynamic Outside_dyn_map
crypto map Outside_map interface Outside
crypto ca trustpoint MS-CA02-AV-EST
 enrollment url http://192.168.1.30:80/certsrv/mscep/mscep.dll
 password *
 keypair keypair01
 crl configure
  no protocol http
  no protocol ldap
crypto ca certificate map VPNphone_rule 10
 subject-name attr cn co 00-04-0d
crypto ca certificate chain MS-CA02-AV-EST
 certificate ca 3267928f467534b749f33b1819648b30
    30820369 308202d2 a0030201 02021032 67928f46 7534b749 f33b1819 648b3030
    -------------cut----------------------
    a30b8ba6 e61876c8 b9075898 de
  quit
 certificate 18e46bac000100000019
    308204d1 3082043a a0030201 02020a18 e46bac00 01000000 19300d06 092a8648
    -------------cut----------------------
    c388c84a 6ab35c0b b3a62478 03ff4a0a b4024288 7a
  quit
crypto isakmp enable Outside
crypto isakmp policy 1
 authentication rsa-sig
 encryption 3des
 hash md5
 group 2
 lifetime 86400
crypto isakmp policy 30
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 50
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400
crypto isakmp policy 70
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
no crypto isakmp nat-traversal
telnet 192.168.1.0 255.255.255.0 Inside
telnet 60.1.1.0 255.255.255.0 Inside
telnet timeout 5
ssh timeout 5
console timeout 0
management-access management
threat-detection basic-threat
threat-detection statistics access-list
group-policy DfltGrpPolicy attributes
 vpn-idle-timeout 3
 nac-settings value DfltGrpPolicy-nac-framework-create
 webvpn
  svc keepalive none
  svc dpd-interval client none
  svc dpd-interval gateway none
  customization value DfltCustomization
group-policy VPNPHONE internal
group-policy VPNPHONE attributes
 vpn-tunnel-protocol IPSec
username test password 0AKWGtPSEgAcPI9K encrypted privilege 0
username test attributes
 vpn-group-policy VPNPHONE
username user password TTNKHqfM6YyTcEzA encrypted
username jburlew password jQRXFM.1zeziD8g7 encrypted
username jburlew attributes
 vpn-group-policy VPNPHONE
username ehope password 0SvLxMEfKe7LGJKH encrypted
username ehope attributes
 vpn-group-policy VPNPHONE
tunnel-group DefaultRAGroup general-attributes
 address-pool (Inside) vpnphone-ip-pool
 address-pool vpnphone-ip-pool
tunnel-group DefaultRAGroup ipsec-attributes
 pre-shared-key *
 isakmp ikev1-user-authentication (Outside) none
tunnel-group VPNPHONE type remote-access
tunnel-group VPNPHONE general-attributes
 address-pool vpnphone-ip-pool
 default-group-policy VPNPHONE
tunnel-group VPNPHONE ipsec-attributes
 pre-shared-key *
tunnel-group-map enable rules
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
!
!
prompt hostname context
Cryptochecksum:f716b8a8ed24c275b0ac9575b20e66df
```

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