



Avaya Solution & Interoperability Test Lab

Configuring an IPSec Tunnel between a Cisco 3825 Router and the Cisco VPN Client to Support Avaya IP Softphone – Issue 1.0

Abstract

These Application Notes describe the steps to configure an IPSec tunnel between a Cisco 3825 Router and Cisco VPN Client to support Avaya IP Softphone. Cisco Security Device Manager (SDM) is used to configure the Cisco 3825 router as an EasyVPN Server.

1. Introduction

These Application Notes describe the steps to configure the Cisco 3825 Router and Cisco VPN client to support Avaya IP Softphones using IPsec tunnel. In these Application Notes, the Cisco router is configured as a VPN Server to establish a VPN tunnel with Cisco VPN client for remote access. Avaya IP Softphone that resides on the same PC with Cisco VPN client will utilize this VPN tunnel to connect to Avaya Communication Manager. Signaling and audio packets from the IP Softphone will be encrypted through this tunnel. Note: Network Address Translation (NAT) is not addressed in these Application Notes.

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 1**. The Corporate IP Network location contains the Cisco 3825 Router functioning as a VPN Server. The Avaya S8710 Server and Avaya G650 Media Gateway are also located at the Corporate IP Network location. The Corporate IP Network is mapped to **IP Network Region 1** in Avaya Communication Manager.

The Cisco VPN clients are located in the public network and configured to establish an IPsec tunnel to the Public IP address of the Cisco 3825 Router. The Cisco 3825 Router will assign IP addresses to the VPN clients. The assigned IP addresses, also known as the inner addresses, will be used by the Avaya IP Softphones when communicating inside the IPsec tunnel and in the corporate IP network to Avaya Communication Manager.

Avaya Communication Manager maps the Avaya IP Softphones to the appropriate IP Network Region using this inner IP address and applies the IP Network Region specific parameters to the IP Softphones. In these Application Notes, the G.729 codec with two voice samples per packet is assigned to the IP Softphones.

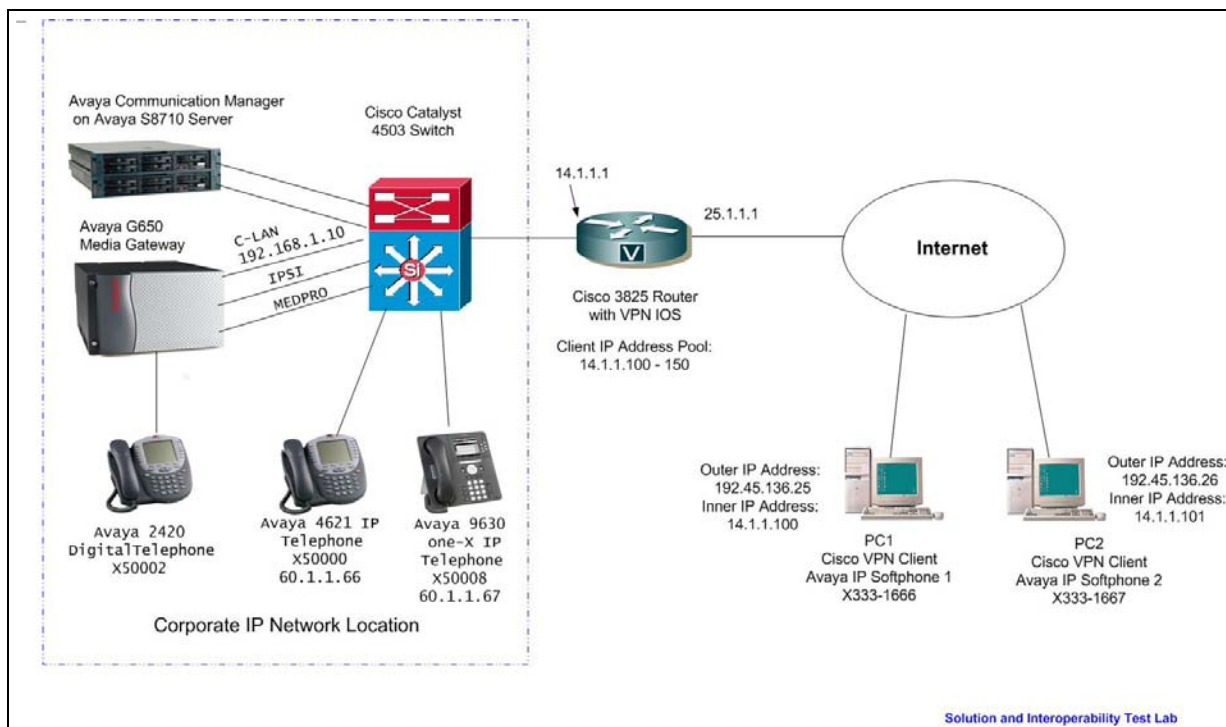


Figure 1: Network Diagram

3. Equipment and Software Validated

Table 1 lists the equipment and software/firmware versions used in the sample configuration provided.

Equipment	Software Version
Avaya S8710 Server with G650 Media Gateway	Avaya Communication Manager 4.0.1 (R014x.00.1.731.2)
Avaya IP Softphone	R6.0 with SP2
Avaya 9600 one-X IP Telephone	R1.5
Avaya 4621 IP Telephone	R2.8
Cisco 3825 Router	IOS 12.4-15 T1 SDM V2.2
Cisco VPN Client	V 5.0.02.0090

Table 1 – Equipment Version Information

4. Cisco 3825 VPN Router Configuration

These Application Notes assume that the Cisco 3825 Router has been configured with basic IP connectivity, is connected to the network, is running the VPN capable IOS and the Cisco Security Device Manager (SDM) software has been installed. For steps to install the SDM, refer to reference [1]. The Cisco 3825 VPN Router depicted in **Figure 1** has been configured with a corporate IP address 14.1.1.1 and a public IP address 25.1.1.1.

1. AAA must be enabled on the router before the Easy VPN Server configuration starts. To enable AAA, log into the router at configuration mode and execute command **AAA new-model**.

```
Cisco3825(config)# aaa new-model
```

2. From a web browser, enter the URL of the Cisco 3825 Router interface's corporate IP address <http://14.1.1.1> and log in using a user name with administrative privileges in the pop-up window (not shown here).The SDM will provide a second login window for user authentication as shown below. Enter user name and password and click **OK**



After successful login, the main menu is displayed as shown below.

Cisco Router and Security Device Manager (SDM): 14.1.1.1

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

About Your Router Host Name: C3825

Hardware [More ...](#)

Model Type: Cisco 3825

Available / Total Memory(MB): 353/512 MB

Total Flash Capacity: 61 MB

Software [More ...](#)

IOS Version: 12.4(15)T1

SDM Version: 2.2

Feature Availability: IP Firewall VPN IPS NAC

Configuration Overview [View Running Config](#)

Interfaces and Connections Up (4) Down (3)

Total Supported LAN: 4

Configured LAN Interface: 2

DHCP Server: Not Configured

Total Supported WAN: 1(Serial T1 CSU/DSU)

Total WAN Connections: 1(FR)

Firewall Policies Inactive Trusted (0) Untrusted (0) DMZ (0)

VPN Up (0)

IPSec (Site-to-Site): 0

Xauth Login Required: 0

No. of DMVPN Clients: 0

GRE over IPSec: 0

Easy VPN Remote: 0

No. of Active VPN Clients: 0

Routing

No. of Static Route: 0

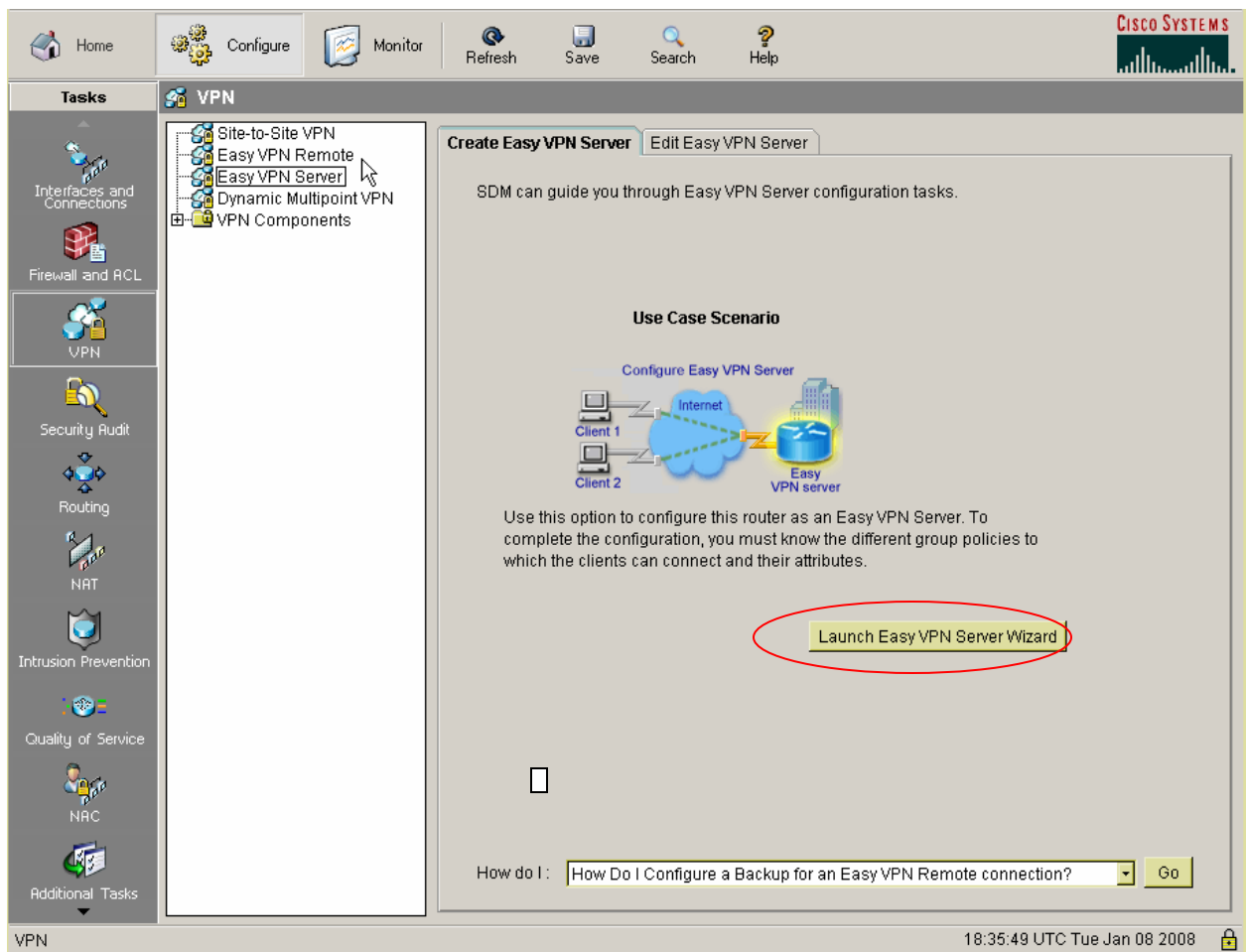
Dynamic Routing Protocols: EIGRP

Intrusion Prevention

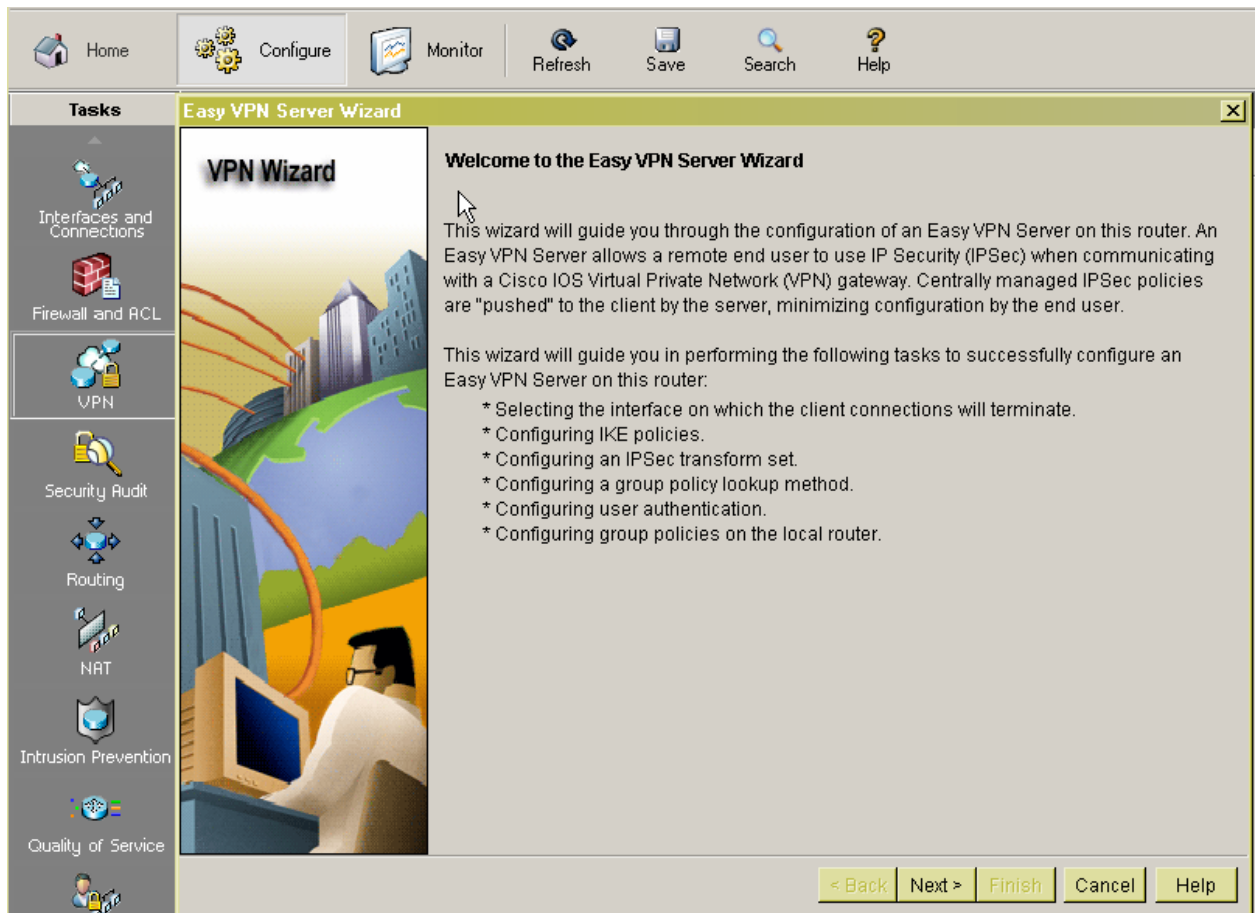
Active Signatures: 0

No. of IPS-enabled Interfaces: 0

3. Select **Configure** → **VPN** → **Easy VPN Server** from the Home window and the following Cisco Router screen appears. Click **Launch Easy VPN Server Wizard** as shown below.



- Click **Next** to start the Easy VPN Server Wizard.



4. Select the interface on which the client connections terminate and the authentication type. In these Application Notes, interface FastEthernet2/1 is used for the router's public interface and Pre-shared keys is chosen as Authentication type. Click **Next** when done.

The screenshot shows the 'Easy VPN Server Wizard - 10% Complete' window. The left sidebar contains a 'Tasks' menu with icons for Home, Configure, Monitor, Refresh, Save, Search, and Help. Below these are icons for various network features: Interfaces and Connections, Firewall and ACL, VPN, Security Audit, Routing, NAT, Intrusion Prevention, and Quality of Service. The main content area is titled 'VPN Wizard' and is divided into two sections: 'Interface and Authentication' and 'Authentication'. In the 'Interface and Authentication' section, there is a text box that says 'Please select the interface on which the Easy VPN Server should be configured. Easy VPN clients will connect to the server through this interface.' Below this, a dropdown menu is set to 'FastEthernet2/1', which is circled in red. To the right of the dropdown is a 'Details...' button. In the 'Authentication' section, there is a text box that says 'Select the method used for authenticating VPN clients connecting to this Easy VPN Server.' Below this, three radio buttons are present: 'Pre-shared keys' (which is selected and circled in red), 'Digital Certificates', and 'Both'. At the bottom of the window, there is a diagram of a router connected to the Internet. The diagram includes a blue router icon with four arrows pointing outwards, connected to a blue cloud labeled 'Internet'. A red lightning bolt symbol is between the router and the cloud. Text next to the router says 'Interface connected to Internet. This is the interface where the VPN connections from the VPN clients will terminate.' Text next to the cloud says 'You can select an interface which is participating in site to site VPN connection. But you cannot select an interface if it is participating in GRE over IPSec, DMVPN or Easy VPN client connection. For more information please click the help button.' At the bottom right of the window, there are five buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

Home Configure Monitor Refresh Save Search Help

Tasks Easy VPN Server Wizard - 10% Complete

VPN Wizard

Interface and Authentication

Interface

Please select the interface on which the Easy VPN Server should be configured. Easy VPN clients will connect to the server through this interface.

Interface for this Easy VPN Server: FastEthernet2/1 Details...

Authentication

Select the method used for authenticating VPN clients connecting to this Easy VPN Server.

☒ Pre-shared keys ☐ Digital Certificates ☐ Both

Interface connected to Internet. This is the interface where the VPN connections from the VPN clients will terminate.

You can select an interface which is participating in site to site VPN connection. But you cannot select an interface if it is participating in GRE over IPSec, DMVPN or Easy VPN client connection. For more information please click the help button.

Internet

< Back Next > Finish Cancel Help

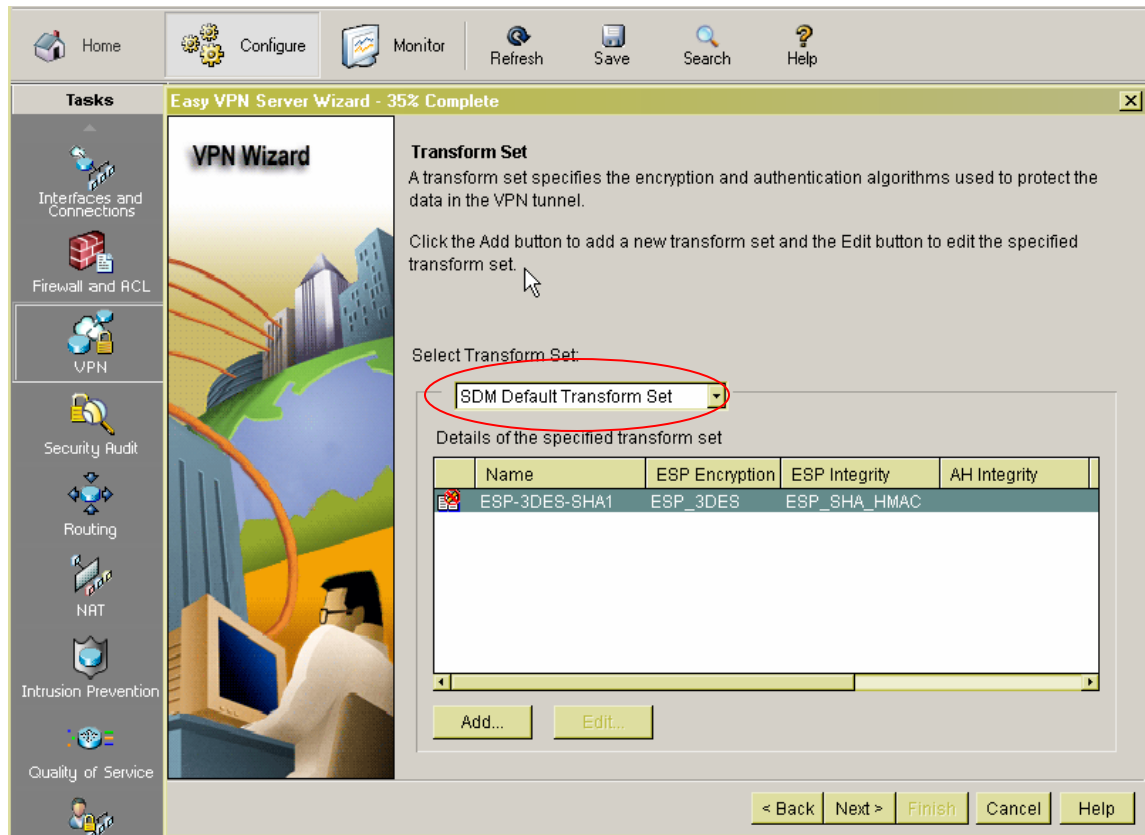
- At the next screen, configure the IKE Proposals. Note that there is a default IKE policy that exists in the router as shown below. These Application Notes use this default policy. Highlight the IKE policy and click **Next** to select the default Internet Key Exchange (IKE) policy.

The screenshot shows the 'Easy VPN Server Wizard - 20% Complete' window. The left sidebar contains a 'Tasks' menu with icons for Interfaces and Connections, Firewall and ACL, VPN, Security Audit, Routing, NAT, Intrusion Prevention, and Quality of Service. The main area is titled 'VPN Wizard' and features an illustration of a person at a computer. Below the illustration, the 'IKE Proposals' section explains that these proposals specify encryption, authentication, and key exchange algorithms. It includes instructions to click 'Add' or 'Edit' buttons. A table lists the existing proposals:

Priority	Encryption	Hash	D-H Group	Authentication	Type
1	3DES	SHA_1	group2	PRE_SHARE	User Defined

Below the table are 'Add...' and 'Edit...' buttons. At the bottom of the window are navigation buttons: '< Back', 'Next >', 'Finish', 'Cancel', and 'Help'.

6. The next screen shows the Transform Set configuration. There is a default Transform Set pre-defined on the router.
- Click **Next** to choose this default transform set or add a new one to specify the encryption and authentication algorithm. In this example, the default transform set is used.



7. Use this step to configure the Group Authorization and Group Policy.
- In this configuration, select **Local** under **Method List for Group Policy Lookup**.
 - Click **Next**.

Home Configure Monitor Refresh Save Search Help

Tasks

Easy VPN Server Wizard - 50% Complete

VPN Wizard

Group Authorization and Group Policy Lookup

An ISAKMP client configuration group (or VPN group) is a group of VPN clients that share the same authentication and configuration information. Group policies can be configured locally on this router, an external server, or both. Easy VPN Server will use these group policies to authenticate VPN clients.

Method List for Group Policy Lookup

Select the servers on which group policies will be configured, or select an existing AAA policy that defines the servers used for configuring group policies.

☒ Local

☐ RADIUS

☐ RADIUS and local

☐ Select an existing AAA method list

-Select an entry

Add RADIUS Server...

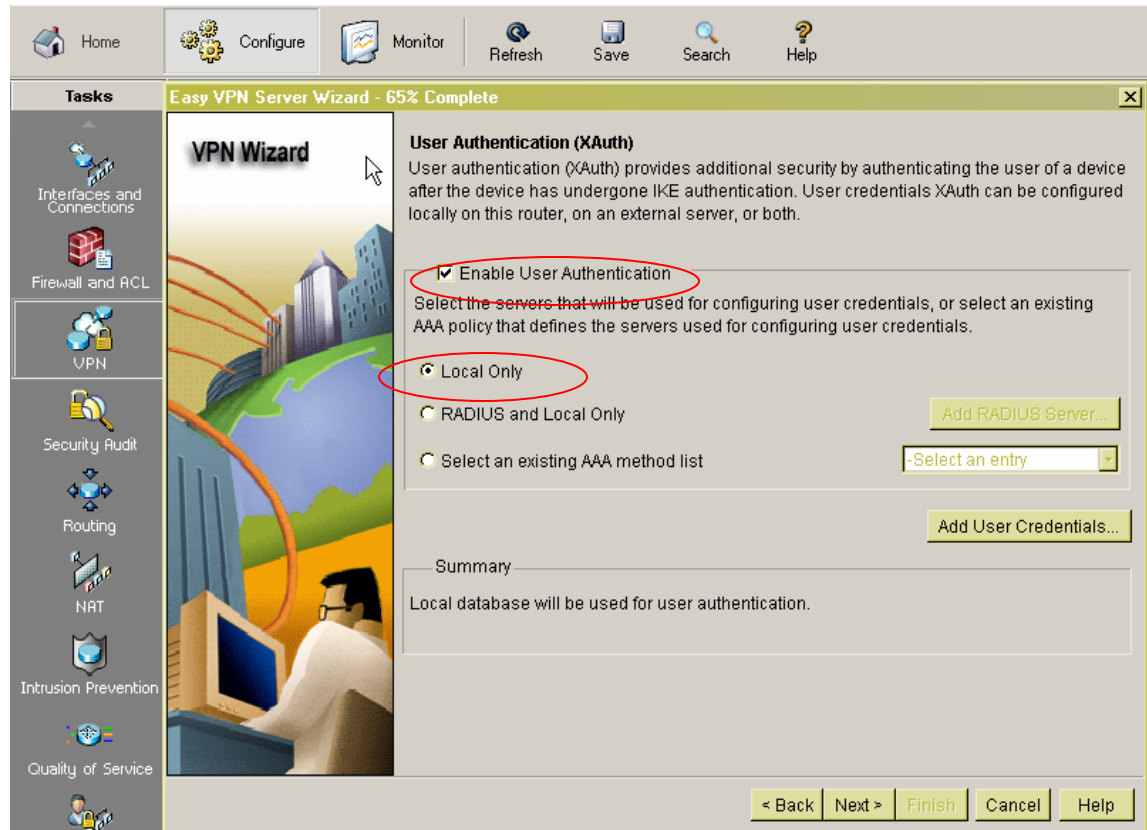
Summary

The local database will be used for group authorization. This option is recommended if you do not have a RADIUS or TACACS+ server in your network.

< Back Next > Finish Cancel Help

8. Configure user authentication on the Easy VPN server. User authentication details can be stored on an external server such as a RADIUS server or a local database or on both. An AAA login authentication method list is used to decide the order in which user authentication details should be searched. In this configuration,

- Check the box **Enable User Authentication** and select **Local Only** to authenticate users using the local database on the router.
- Click tab **Add User Credentials** to add a user



- Enter **user** and **password** for Username and password as shown
- Check box **Encrypt password using MD5 hash algorithm**
- Select **Privilege Level 1**. Note this privilege level only allow users to access VPN server, not to make any changes on the server.
- Click **OK** and bring the screen back to the previous **User Authentication** configuration
- Click **OK** to proceed to group configuration

Add an Account

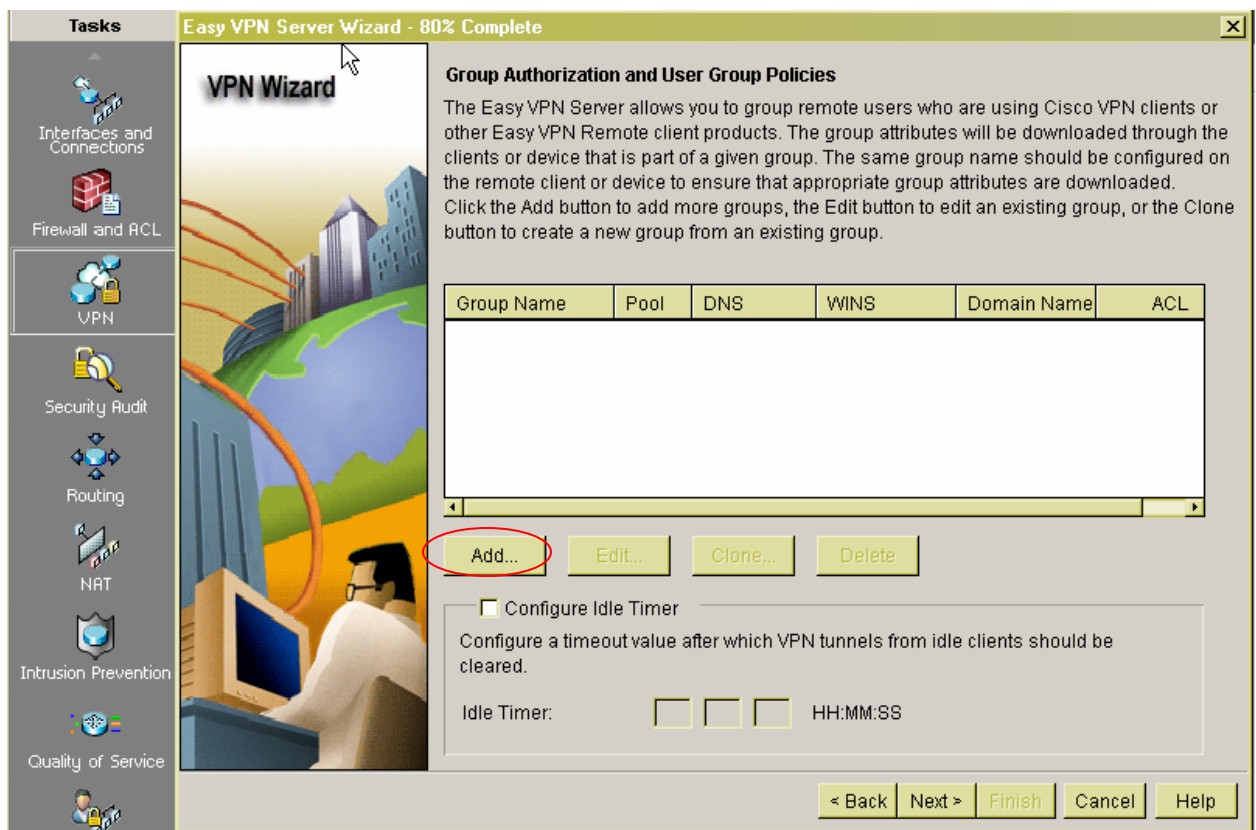
Enter the username and password

Username:

Password
 Password:
 New Password:
 Confirm New Password:
☒ Encrypt password using MD5 hash algorithm

Privilege Level:

9. Use the window below to add user group policies on the local database.
- Click **Add** to add a group policy for this VPN.
 - Click **Next**.



10. Configure Group Policy as follows:

- Enter **Softphone** for the Name of This Group and enter the **pre-shared key** used for authentication information.
- Check **Pool Information** and **Create a new pool** to allocate the IP addresses to be assigned to VPN Clients. In this configuration, IP addresses range **14.1.1.100 – 14.1.1.150** is used.
- Click **OK**.

The screenshot shows the 'Add Group Policy' dialog box with the 'General' tab selected. The 'Name of This Group' field is circled in red and contains the text 'Softphone'. Below this, the 'Pre-shared keys' section has a description: 'Specify the key that will be used to authenticate the clients associated with this group.' It includes fields for 'Current Key' (set to '<None>'), 'Enter new pre-shared key:' (with a masked input '*****'), and 'Reenter new pre-shared key:' (also with a masked input '*****'). The 'Pool Information' section is checked. It contains a description: 'Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.' There are two radio buttons: 'Create a new pool' (selected) and 'Select from an existing pool'. Under 'Create a new pool', there are fields for 'Starting IP address:' (14.1.1.100) and 'Ending IP address:' (14.1.1.150). To the right of these is a dropdown menu showing '-Select an entry' and a 'Details...' button. Below these is a field for 'Subnet Mask:' (255.255.255.0) with '(Optional)' next to it. At the bottom, there is a 'Maximum Connections Allowed:' field. The dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.

Add Group Policy

General | DNS/WINS | Split Tunneling | Client Settings | XAuth Options | Client Update

Name of This Group: **Softphone**

Pre-shared keys

Specify the key that will be used to authenticate the clients associated with this group.

Current Key: <None>

Enter new pre-shared key: *****

Reenter new pre-shared key: *****

☒ **Pool Information**

Specify a local pool containing a range of addresses that will be used to allocate an internal IP address to a client.

☒ **Create a new pool** ☐ **Select from an existing pool**

Starting IP address: 14.1.1.100

Ending IP address: 14.1.1.150

-Select an entry Details...

Enter the subnet mask that should be sent to the client along with the IP address.

Subnet Mask: 255.255.255.0 (Optional)

Maximum Connections Allowed:

OK Cancel Help

- Click Next

Easy VPN Server Wizard - 80% Complete

VPN Wizard

Group Authorization and User Group Policies

The Easy VPN Server allows you to group remote users who are using Cisco VPN clients or other EasyVPN Remote client products. The group attributes will be downloaded through the clients or device that is part of a given group. The same group name should be configured on the remote client or device to ensure that appropriate group attributes are downloaded. Click the Add button to add more groups, the Edit button to edit an existing group, or the Clone button to create a new group from an existing group.

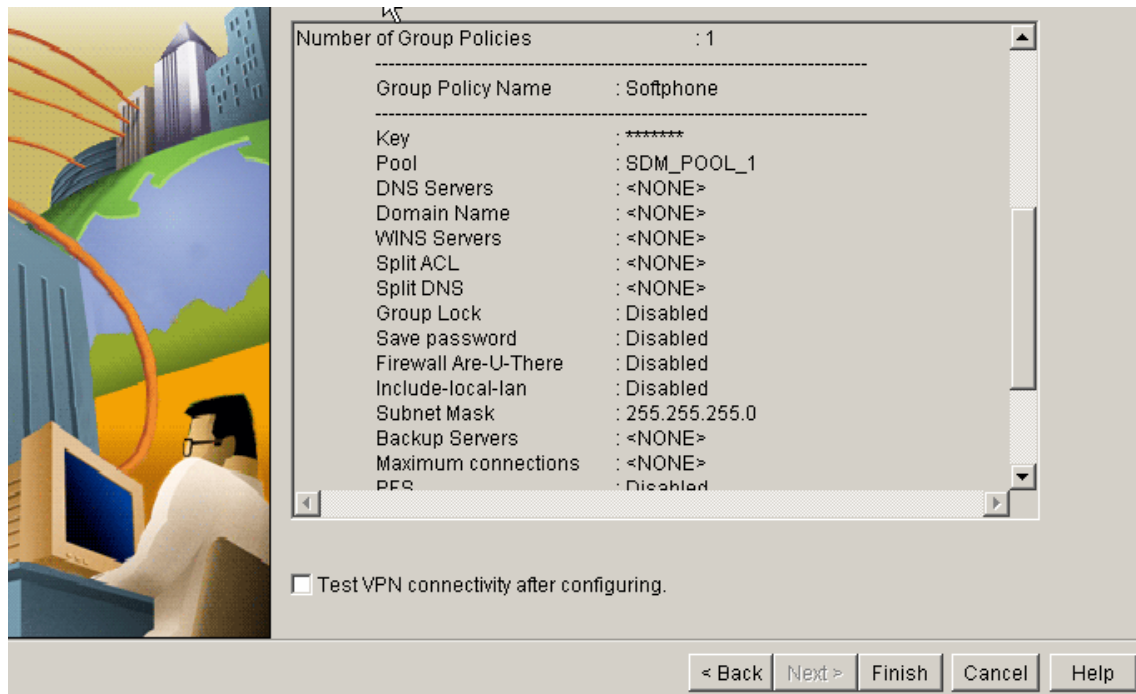
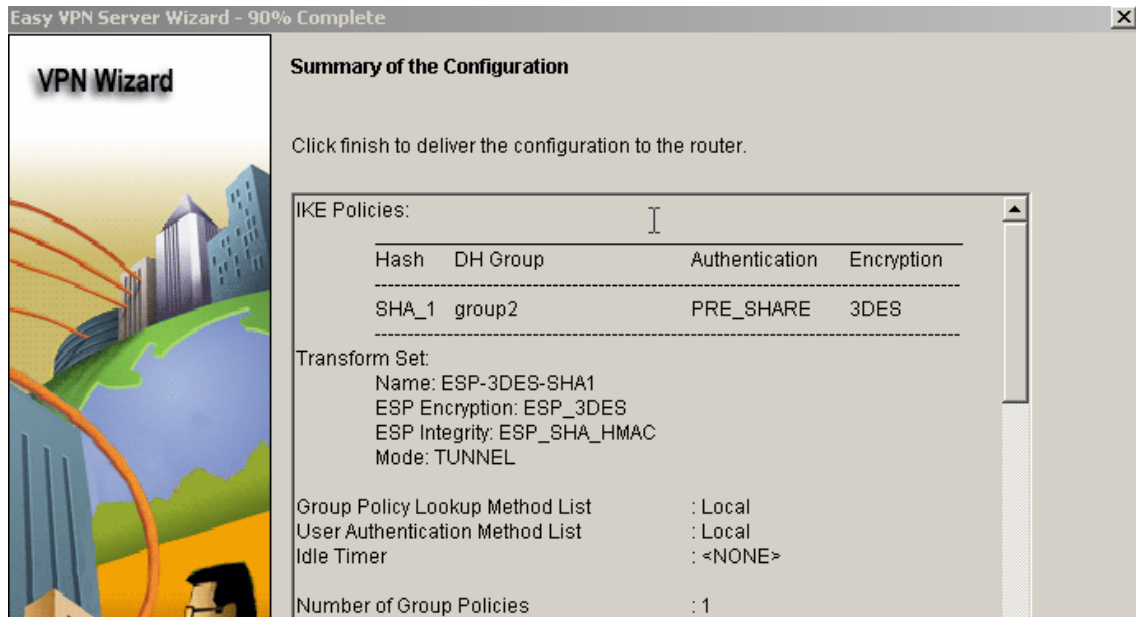
Group Name	Pool	DNS	WINS	Domain Name
Softphone	SDM_POOL_1			

☐ Configure Idle Timer

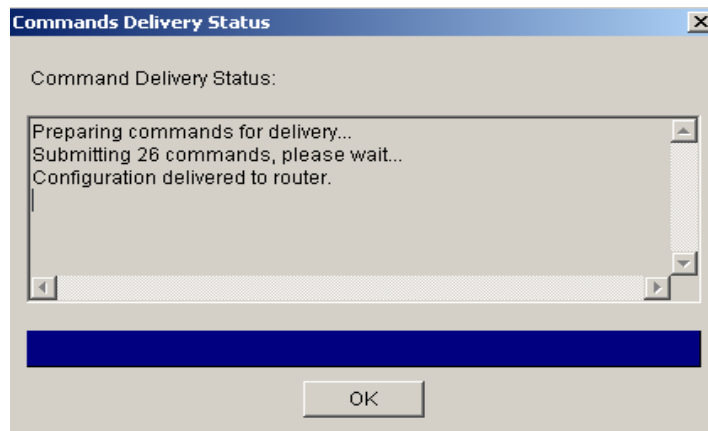
Configure a timeout value after which VPN tunnels from idle clients should be cleared.

Idle Timer: HH:MM:SS

11. The next window shows a summary of the completed configuration. Click **Finish** after reviewing the configuration.



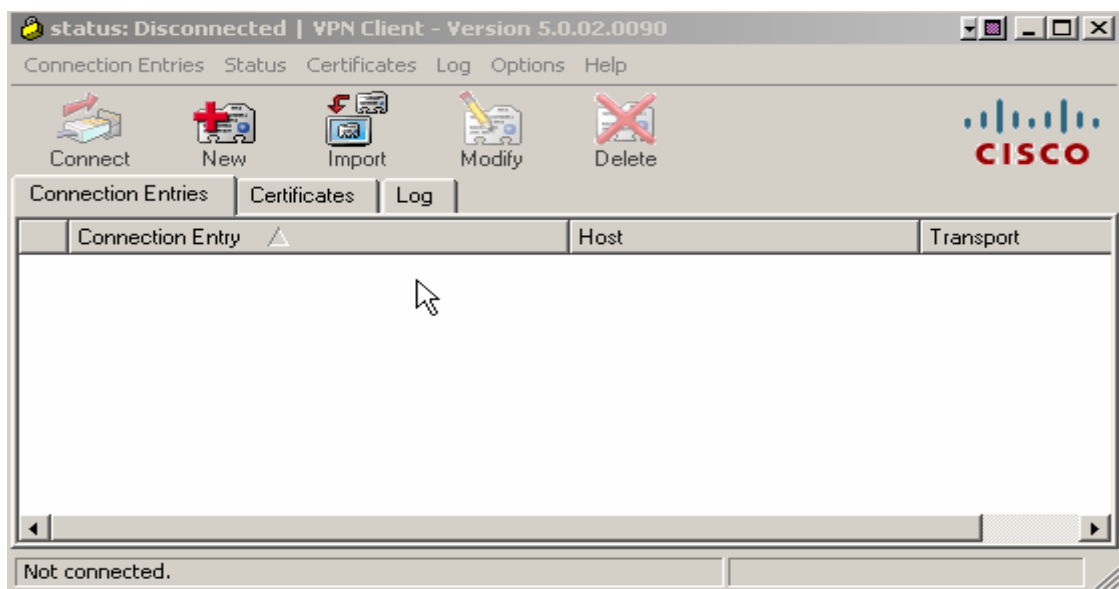
12. After the Finish button is clicked, the SDM sends the configuration to the router to update the running configuration. Click **OK**.



5. Cisco VPN Client Configuration

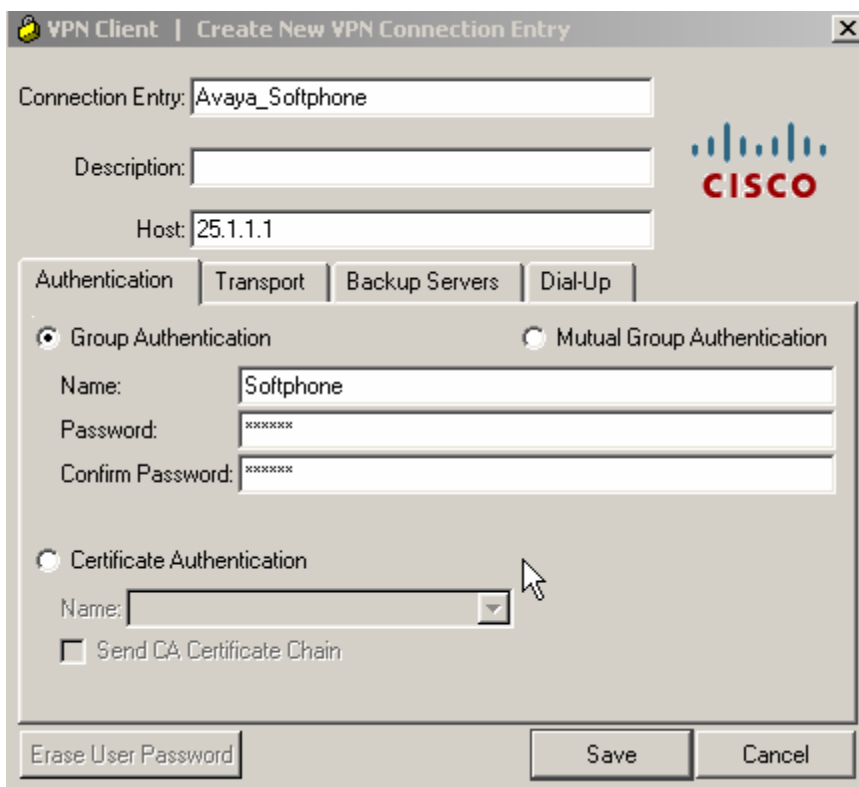
These Application Notes assume that the Cisco VPN client software has been installed on a computer and the computer has connectivity to the Cisco 3825 router via its Internet connection. For Cisco VPN software installation, refer to the reference [2].

1. Launch the VPN client application:
 - Select **Start → Programs → Cisco Systems VPN Client → VPN Client Programs**. The Cisco VPN Client application window appears as shown below.
 - Click **Connection Entries → New**



2. Enter connection information

- For **Connection Entry**, enter the name **Avaya_Softphone** in this example
- Enter the router's public interface IP address **25.1.1.1** in the **Host** field.
- Click **Group Authentication**
- Enter **Softphone** for group name and password created in Step 10, Section 4.
- Click **Save**.



VPN Client | Create New VPN Connection Entry

Connection Entry: Avaya_Softphone

Description:

Host: 25.1.1.1

Authentication | Transport | Backup Servers | Dial-Up

☒ Group Authentication ☐ Mutual Group Authentication

Name: Softphone

Password: XXXXXXXX

Confirm Password: XXXXXXXX

☐ Certificate Authentication

Name: [Dropdown]

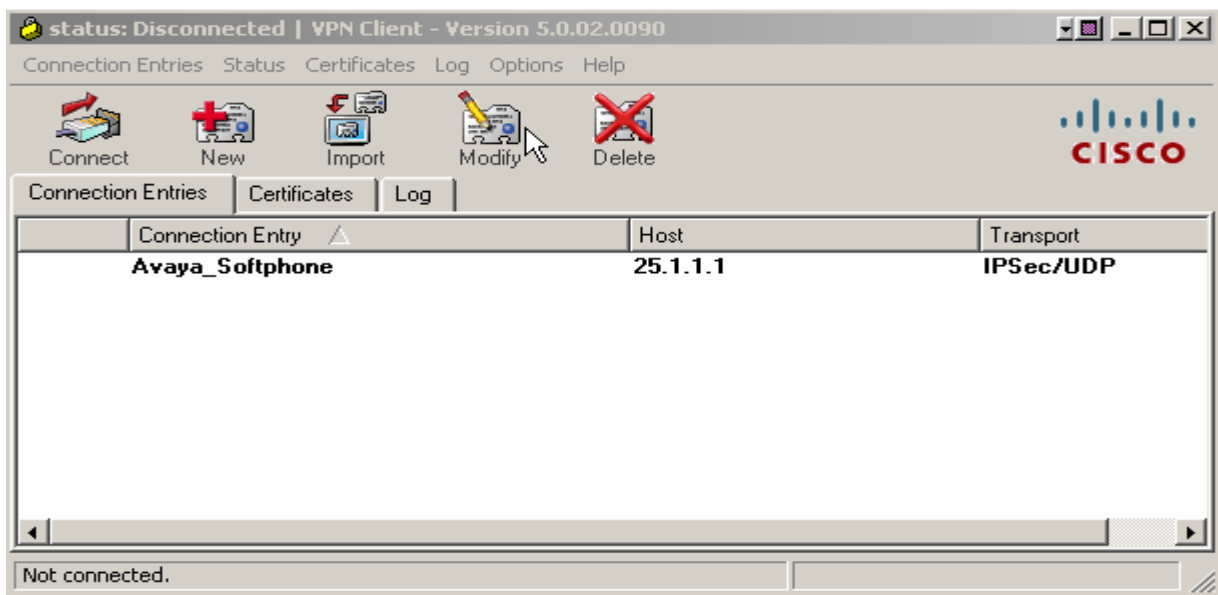
☐ Send CA Certificate Chain

Erase User Password Save Cancel

The following screen shows the **Avaya_Softphone** connection entry and the default Transport is **IPSec/UDP**. Click **Modify** to change the connection property if needed.

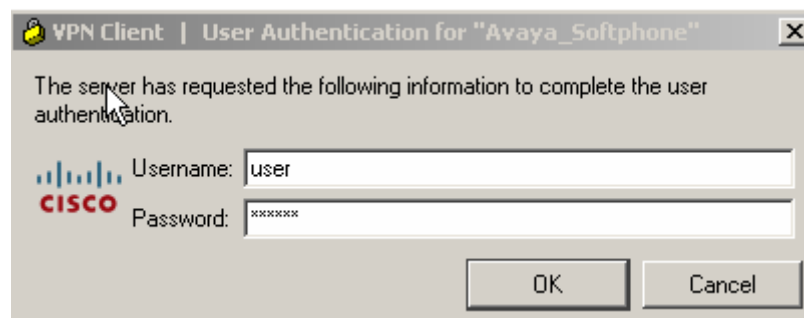
3. Connect to VPN server

- Click the **Connect** button to connect to the VPN Server (3825 Router).



At the login screen,

- Enter the user **name** and **password** as defined in Step 8, Section 4.
- Click **OK**.



These Application Notes do not cover the Avaya IP Softphone configuration and usage. Refer to reference [4] for detail.

6. Avaya Communication Manager Configuration

All the commands discussed in this section are executed on Avaya Communication Manager using the System Access Terminal (SAT). This section assumes that basic configuration on Avaya Communication Manager has already been completed.

The Avaya IP Softphones are assigned to IP Network Region 2 using the IP address range of the VPN Client IP Address Pool. G729 codec is assigned to IP Network Region 2 for calls within this region and between the IP Network Region 1.

6.1. IP Softphone Administration

An Avaya IP Softphone is administered similar to other IP telephones within Avaya Communication Manager. The following screens show IP Softphone extension 333-1666 being added to Avaya Communication Manager. For additional information regarding the administration of Avaya Communication Manager, refer to reference [3].

- Enter **4620** for phone Type
- Enter **y** for IP Softphone

add station 3331666		Page	1 of	5
STATION				
Extension: 333-1666	Lock Messages? n	BCC: 0		
Type: 4621	Security Code: *	TN: 1		
Port: IP	Coverage Path 1:	COR: 1		
Name: IP-Softphone	Coverage Path 2:	COS: 1		
	Hunt-to Station:			
STATION OPTIONS				
Loss Group: 19	Time of Day Lock Table:			
	Personalized Ringing Pattern: 1			
	Message Lamp Ext: 333-1666			
Speakerphone: 2-way	Mute Button Enabled? y			
Display Language: english	Expansion Module? n			
Survivable GK Node Name:	Media Complex Ext:			
Survivable COR: internal	IP SoftPhone? y			
Survivable Trunk Dest? y				
	IP Video Softphone? N			

- Enter **y** for Direct IP-IP Audio Connections?

add station 3331666		Page 2 of 5
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		
	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	
	Multimedia Early Answer? n	
Remote Softphone Emergency Calls: as-on-local	Direct IP-IP Audio Connections? y	
Emergency Location Ext: 333-1888	Always Use? n IP Audio Hairpinning? N	

6.2. IP Codec Sets Configuration

Use the **change ip-codec-set n** command to configure IP Codec Set parameters where n is the IP Codec Set number. Use the **change ip-codec-set 2** command to define a codec set for the G.729 codec with no media encryption as shown below. Since the call is going through the VPN tunnel, the media encryption is not necessary. Note the ip-codec-set 1 is configured to use G.711mulaw and the configuration is not shown here since it's similar to ip-codec-set 2 configuration.

change ip-codec-set 2		Page 1 of 2
IP Codec Set		
Codec Set: 1		
Audio	Silence	Frames
Codec	Suppression	Per Pkt
1: G.729	n	2
2:		20
Media Encryption		
1: none		
2:		

6.3. 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. Below is the display for ip-network-region 2 configuration. Configure the highlighted fields shown below. All remaining fields can be left at their default values.

The **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** fields determine the flow of RTP audio packets. Setting these fields to **yes** enable the most efficient audio path to be taken. Codec Set 2 is used for IP Network Region 2.

change ip-network-region 2		Page 1 of 19
IP NETWORK REGION		
Region: 2		
Location:	Authoritative Domain: avaya.com	
Name:		
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: 65535		
DIFFSERV/TOS PARAMETERS	RTCP Reporting Enabled? y	
Call Control PHB Value: 26	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: 3		
Audio 802.1p Priority: 5		
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	IP NETWORK REGION	

Page 3 of the IP-Network-Region form, shown below, defines the codec set to use for intra-region and inter-region calls. Since only ip-network-region 1 is defined in this configuration, Avaya IP Softphones are in Region 1 and use codec set 1 for audio.

change ip-network-region 2		Page 3 of 19									
Inter Network Region Connection Management											
src rgn	dst rgn	codec set	direct	WAN Units	WAN-BW-limits	Video				Dyn	
2	1	2	y	NoLimit							n
2	2	2									
2	3										

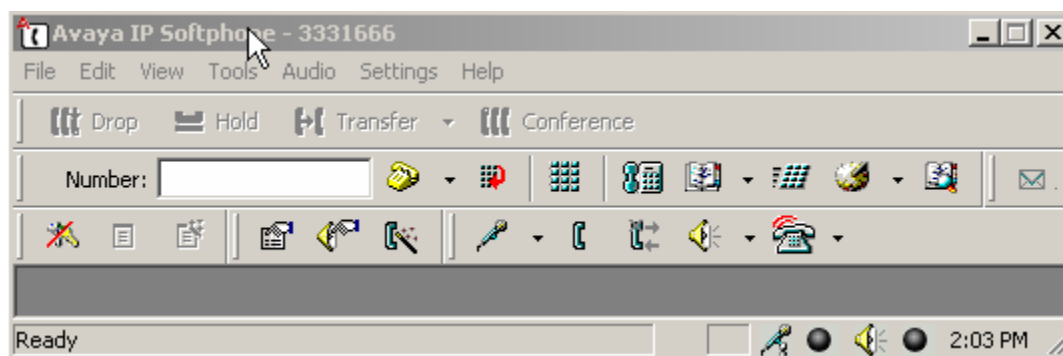
Use the **change ip-network-map** command to map all IP Softphones to IP Network Region 2, which is using G.729 codec.

change ip-network-map						Page 1
IP ADDRESS MAPPING						
		Subnet		Emergency		
From IP Address		(To IP Address	or Mask)	Region	VLAN	Location
192.168.1 .1		192 .168.1 .254	24	1	n	Extension
14 .1 .1 .100		14 .1 .1 .150	24	2	n	

7. Verification

7.1. Avaya IP Softphone Statistics

On client PC, ping the Cisco 3825 router's public interface IP address to verify the connectivity before launching the VPN client. Once the Cisco VPN Client establishes an IPsec tunnel with VPN Server, launch a ping from the client PC to C-LAN and verify that the ping is successful. Start the Avaya IP Softphone from the client PC 1 and verify that the IP Softphone is registered with Avaya Communication Manager and becomes functional. The screen capture below shows the status of the IP Softphone station 3331666.



Also, from the Avaya Communication Manager SAT terminal, use the command **list registered-ip-stations** to show both IP Softphones are registered with Avaya Communication Manager with their inner IP addresses assigned from the address pool on Cisco 3825 VPN router.

list registered-ip-stations								
REGISTERED IP STATIONS								
Station Ext/ Orig Port	Set Type	Product ID	Prod Rel	Station IP Address	Net Rgn	Gatekeeper IP Address	TCP Skt	
50000	4621	IP_Phone	2.800	60.1.1.66	1	192.168.1.10	y	
50008	4620	IP_Phone	1.500	60.1.1.67	1	192.168.1.10	y	
333-1666	4621	IP_Soft	5.620	14.1.1.100	2	192.168.1.10	y	
333-1667	4621	IP_Soft	5.242	14.1.1.101	2	192.168.1.10	y	

Make a call from the IP Softphone 1 (x333-1666) to the IP softphone 2 (x333-1667). Use the command **status station x** (x represent the extension #) to verify the status of the IP Softphone 1 as shown below. Notice on **Page 1**, the IP Softphone Service State is **in-service/off-hook**.

status station 3331666		Page 1 of 7	
GENERAL STATUS			
Administered Type: 4620		Service State: in-service/off-hook	
Connected Type: N/A		TCP Signal Status: connected	
Extension: 333-1666			
Port: S00002		Parameter Download: complete	
Call Parked? no		SAC Activated? no	
Ring Cut Off Act? no			
Active Coverage Option: 1			
EC500 Status: N/A		Off-PBX Service State: N/A	
Message Waiting:			
Connected Ports: S00020			

On **Page 3**, the IP Softphone uses IP address **14.1.1.100**, which is assigned from the IP address pool defined on the Router. Note the IP address **192.168.1.10** is C-LAN IP address and is in Region 1 as shown below.

status station 3331666			Page 3 of 7		
CALL CONTROL SIGNALING					
Port: S00002		Switch-End IP Signaling Loc: 01A0217		H.245 Port:	
IP Address		Port		Node Name Rgn	
Switch-End: 192.168. 1. 10		1720		c-lan 1	
Set End: 14. 1. 1.100		31244		2	
H.245 Near:					
H.245 Set:					

Page 4 shows that the audio is between the two IP Softphones and the **Audio Connection Type** is **ip-direct**.

status station 3331666					Page	4 of	7
AUDIO CHANNEL Port: S00002							
G.729A		Switch-End Audio Location:					
	IP Address			Port	Node Name		Rgn
Other-End:	14.	1.	1.101	2048			2
Set-End:	14.	1.	1.100	2048			2
Audio Connection Type: ip-direct							

Page 6 shows the g729a codec is used for this call.

status station 3331666		Page	6 of	7
SRC PORT TO DEST PORT TALKPATH				
src port: S00002				
S00002:TX:14.1.1.100:2048/g729a/20ms				
S00085:RX:14.1.1.101:2048/g729a/20ms				

7.2. Cisco 3825 VPN Router Logging

The Cisco VPN Router **VPN Status** displays the current client login status. To access to the VPN Status, select **VPN Status** → **Easy VPN Server** from the main web management interface.

The detailed client connection information is shown below. Note that the VPN client's Public IP address is 192.45.136.25 and the Assigned IP address is 14.1.1.100.

The screenshot shows the 'VPN Status' page with the 'Easy VPN Server' tab selected. It displays the 'Total number of active clients: 1' and a table of client connections for the 'Softphone' group.

Group Name	Number of Client Connections
Softphone	1

Public IP address	Assigned IP address	Encrypted Pkts	Decrypted Pkts	Dropped Outbound Pkts	Dropped Inbound
192.45.136.25	14.1.1.100	10820	11261	0	0

Click **IPSec Tunnels** tab to show the IPSec tunnel status. Note that the Local IP address **25.1.1.1** is the router's public interface and the Remote IP address **192.45.136.25** is the Cisco VPN client's (PC1) outer IP address. The **Tunnel Status** column shows Up.

The screenshot shows the 'VPN Status' page with the 'IPSec Tunnels' tab selected. It displays a table of IPSec tunnel status for a single tunnel.

Local IP	Remote IP	Peer	Tunnel Status	Encapsulation F	Decapsulation F	Send Error Pack	Received Error P
25.1.1.1	192.45.136.25	192.45.136.25:3	Up	13159	13634	0	0

8. Conclusion

The Avaya IP Softphones can utilize the IPSec tunnel established between Cisco VPN Router and VPN Client to provide a secure solution for remote worker telephony over any broadband Internet connection. These Application Notes verify that Avaya IP Softphone can successfully interoperate with the Cisco 3825 VPN Router using the Cisco VPN client application.

9. References

- [1] *Cisco Router as a Remote VPN Server using SDM Configuration Example*, Doc ID: 70374 at <http://www.cisco.com/>
- [2] *Downloading and Installing Cisco Router and Security Device Manager* at <http://www.cisco.com/>
- [3] *Administrator Guide for Avaya Communication Manager*, Doc ID: 03-300509, Issue 3.0, February 2007 at <http://www.support.avaya.com/>
- [4] *Avaya IP Softphone Release 6.0 User Reference*, Issue 1, May 20007 at <http://www.support.avaya.com>

©2008 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