Configuring Check Point VPN-1/FireWall-1 and SecuRemote Client with Avaya™ IP Softphone via NAT - Issue 1.0

Abstract

Avaya™ IP Softphone R3 V2.1 now supports H.323 VoIP applications running over different Network Address Translation devices. These Application Notes provide the configuration information required to support the Avaya IP Softphone for customers utilizing Check Point VPN-1/Firewall-1 and SecuRemote client in a NAT environment. This work was requested by IP Softphone developers to verify NAT functionality.

1. Introduction

Check Point VPN-1/Firewall-1 has been widely deployed by companies to protect their private network from the public network. These companies also want their authorized remote users to access their internal network. These users will most likely have a public IP address that is not routable within the internal or private network. The IP Pool NAT feature on the Check Point VPN-1/Firewall-1 will replace an incoming packet's source IP address with a new source IP address selected from a configurable pool. By doing this, IP packets coming from the public domain become routable in the private domain. Since the H.323 protocol has embedded IP addresses that are not translated by NAT devices, this solution does not work for VoIP. A new version of Avaya™ Call Processing software solves this problem by sending back a virtual IP address to the Avaya™ IP Softphone client. The Avaya IP Softphone client will use this address for registration, call control signaling, and media transport. No new configuration is required in Avaya Call Processing software or the Avaya IP Softphone.

2. Network Configuration

This document provides the configuration information required to support Avaya's IP Softphone R3 V2.1 for customers utilizing VPN-1/Firewall-1 and SecuRemote Client in a NAT environment. **Figure 1** depicts the network setup for these Application Notes. In this case the IP Softphone uses a valid IP address. A VPN tunnel is established between the IPSec client and the Check Point VPN-1/Firewall-1 Gateway. Since 'IP Pool NAT' is configured on the Check Point VPN-1/Firewall-1, it assigns a new IP address from its pool (which is routable in the internal or private network) to the IP packets coming from the SecuRemote client on the Avaya IP Softphone.

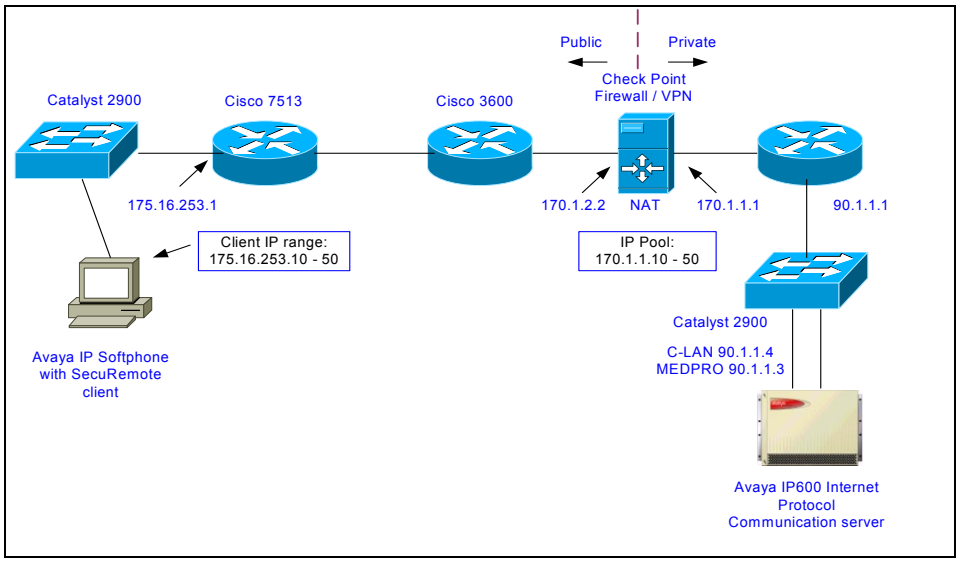

Figure 1: Network Topology

3. Software Validated

The following Avaya software is required:

- **Avaya™ IP Softphone R3 V2.1x**
- **Avaya™ IP Agent versions later than IP Agent V3**
- **Avaya Softconsole™ R1.0 (or later)**
- **Avaya™ Call Processing release R10 load 35 (or later), or release R11**

Software/Hardware used for verification:

- **Avaya IP Softphone R3 V2.1**
- **Avaya Call Processing release R10 load 35**
- **Avaya™ Communication Server**
- **Windows 2000 PC with Check Point VPN-1/Firewall-1 V4.1 SP-5**
- **Windows 2000 PC with SecuRemote Client V4.1 SP-5**
- **Cisco Router 7513 with IOS 12.2(2)T and 3640 with IOS 12.2(2)T**
- **Cisco Catalyst Switch 2900 with IOS 12.0(5.2)XU**

4. Configuration for VPN-1/Firewall-1

The following are VPN-1/Firewall-1 configuration steps:

1. **Creating a private network:** Start Programs → Check Point Management Clients → Policy Editor 4.1. Select from the main menu, Manager → Network Objects → New → Network and create the private network behind the Check Point. From the Network Properties Window, select below.
    - Name = pbx
    - IP Address = 90.1.1.0
    - Net Mask = 255.255.255.0
    - Comment = ip600
    - Location = Internal
    - Broadcast = Allowed
    - Select **OK**

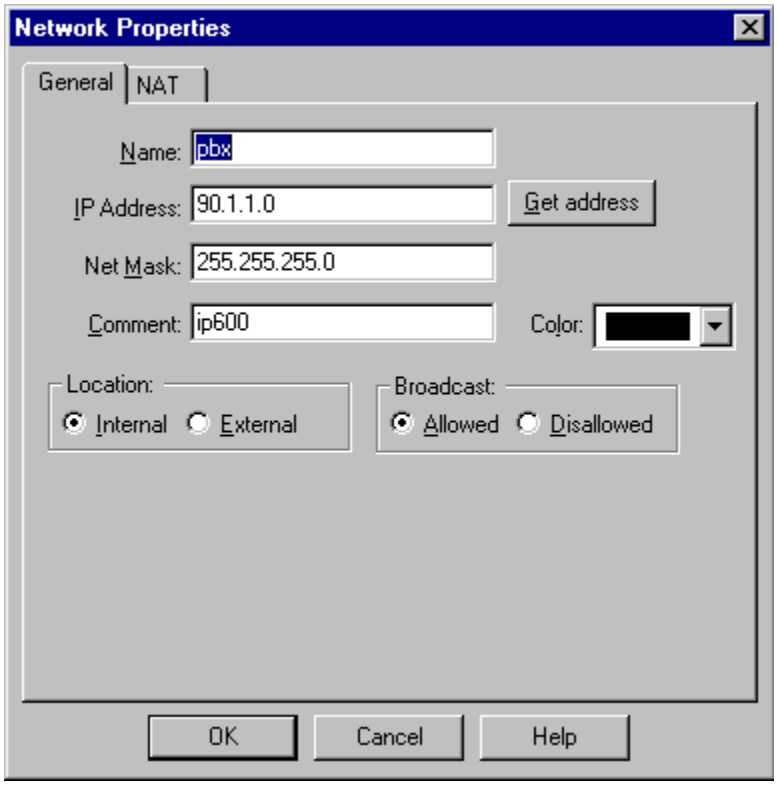

Figure 2: Creating a Private Network

2. **Creating an IP Pool:** Select from the main menu, Manager → Network Objects → New → Address Range and create an internal range of IP addresses. This internal address range will be used in the 'IP Pool NAT' function of the Firewall. Define an IP range from 170.1.1.10 to 170.1.1.50 for translation. Select **OK**.

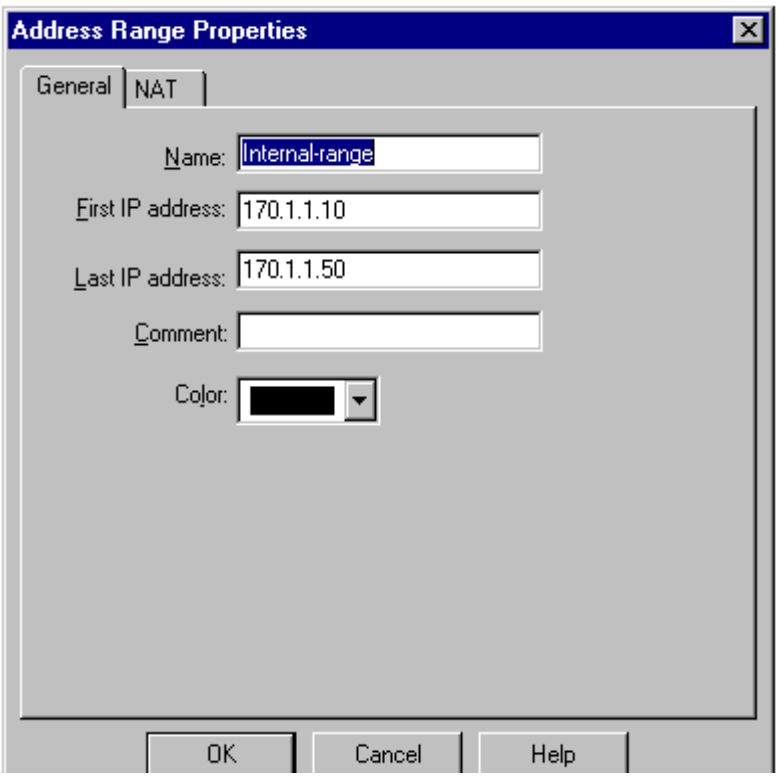

Figure 3: Creating an IP Pool

3. Creating a Check Point Object:

3a. From 'Policy Editor 4.1', select Manager → Network Objects → New → Workstation. In the General tab, add a name and IP address (170.1.2.2) of the interface connected to the public network.

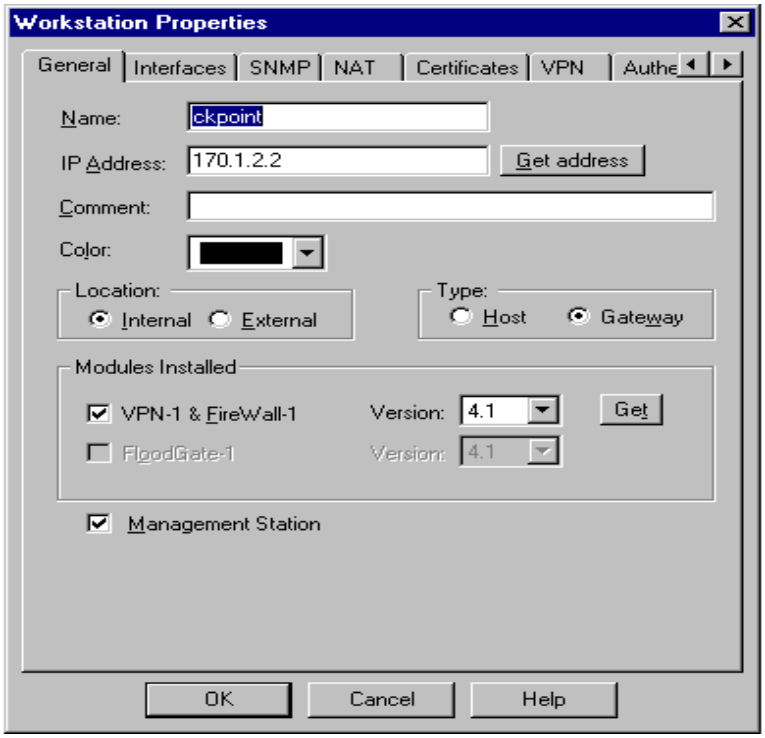

Figure 4: Creating Check Point Object

3b. In the Authentication Tab, select '**VPN-1 & Firewall-1 Password**'.

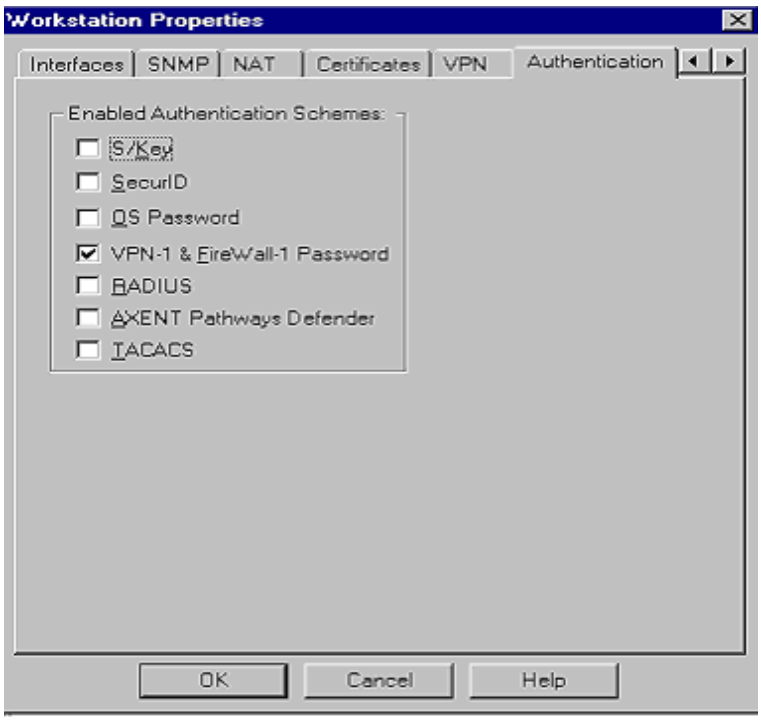

Figure 5: Set up Password

3c. In the VPN Tab, select **IKE** and click '**Edit**'.

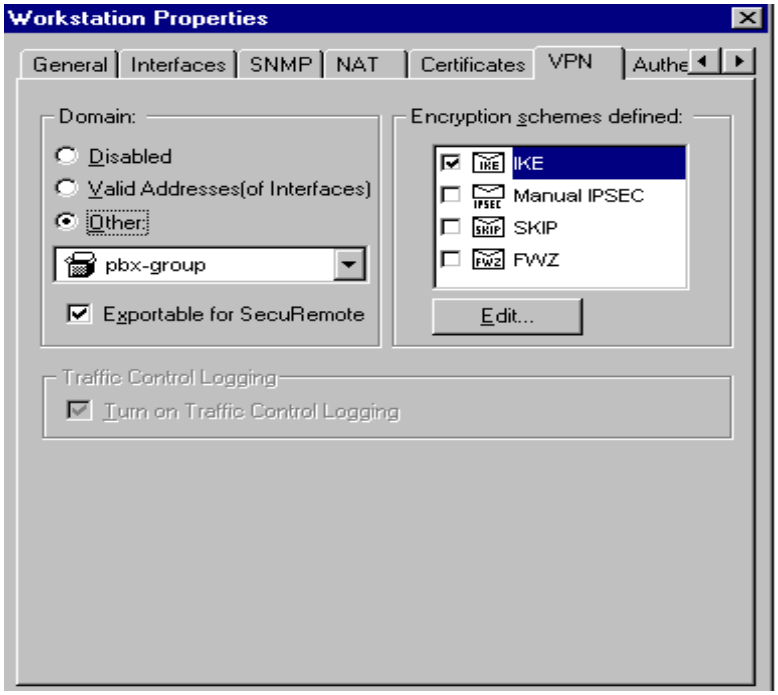

Figure 6: Configure IKE for VPN

3d. Select **3DES** as the key exchange encryption and **MD5** for data integrity. Select **OK**.

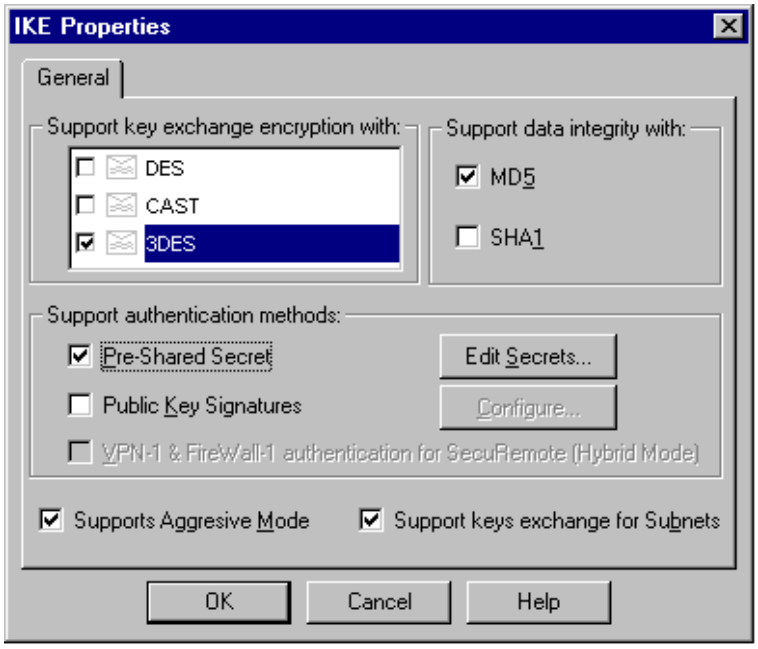

Figure 7: General Tab for IKE Properties

3e. In the NAT Tab, select '**Use IP Pool NAT for SecuRemote connections**'. Select **OK**.

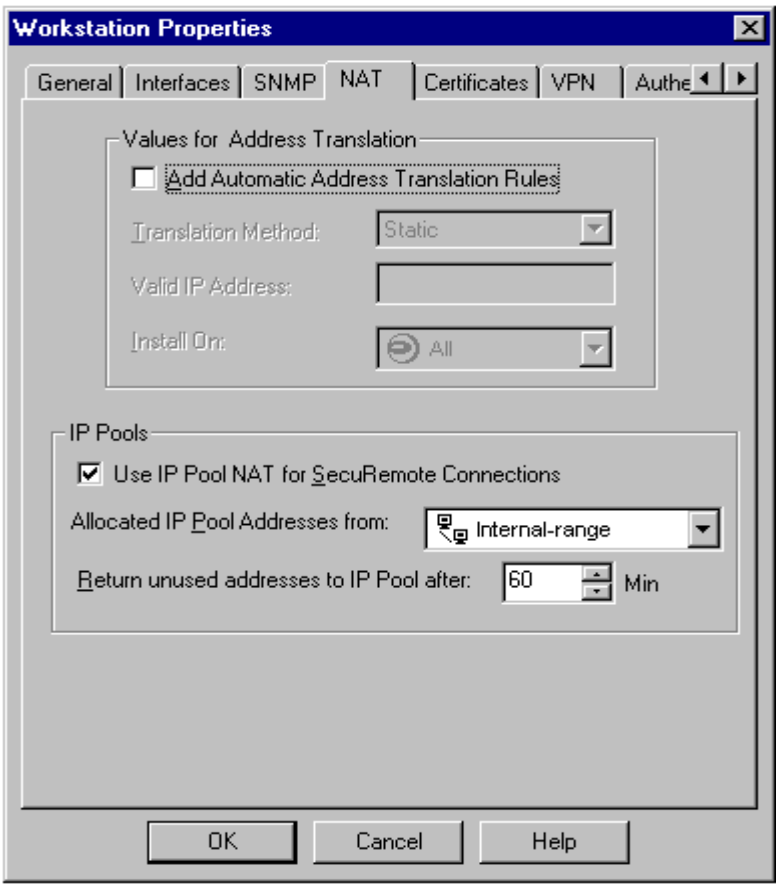

Figure 8: Configure IP Pool for Client

3f. Select from the Main menu, Policy → Properties and click on the '**IP Pool NAT**' Tab. Select '**Enable IP Pool NAT for SecuRemote connections**'. Select '**OK'**.

This enables the Check Point Firewall/VPN1 to use this pool for client address translation.

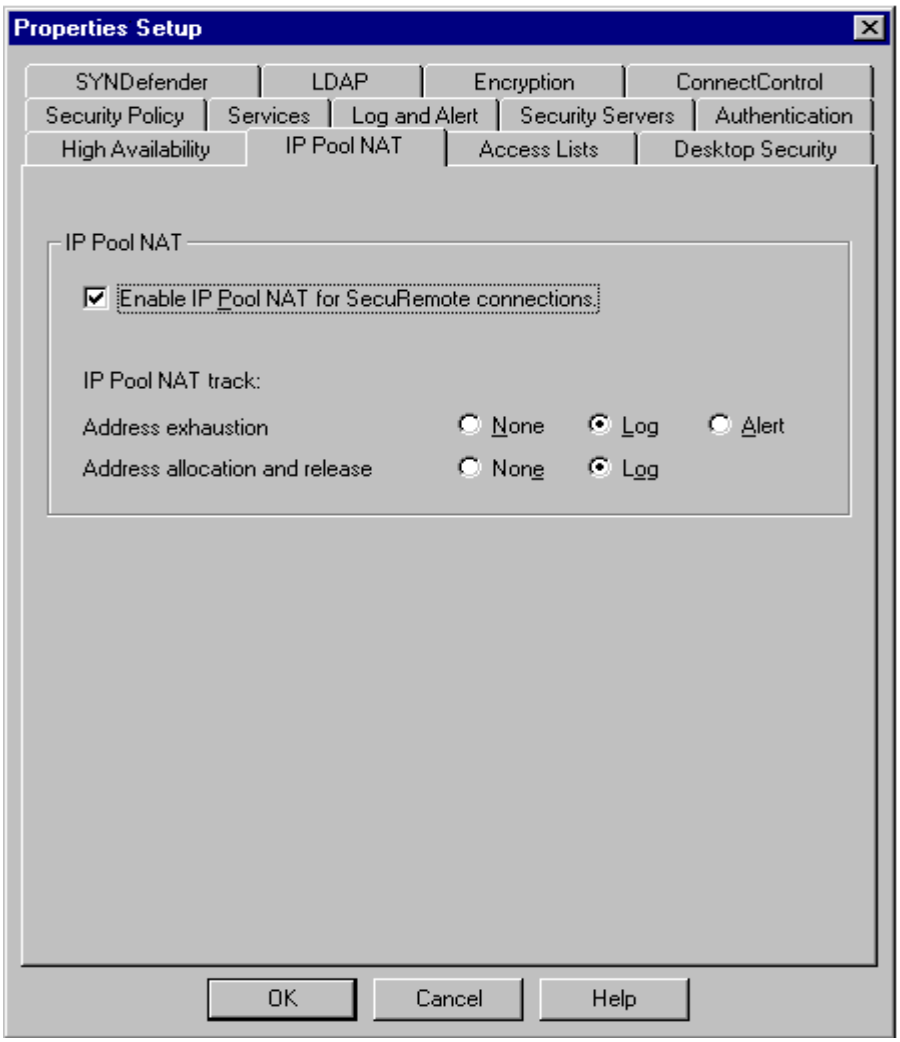

Figure 9: Enable IP Pool NAT on Policy

Note: Since the address range is created on the VPN-1/Firewall-1, be sure that the packets destined to these IP addresses can reach the gateway.

3g. On line 'Help' suggests that we need to create a file called 'local.arp' in the **C:\WINNT\FW1\4.1\STATE** directory. In the file local.arp, we have to link the addresses created in the internal-range 170.1.1.10 - 50 to the MAC address of the internal interface of the VPN-1/Firewall-1 gateway as shown below.

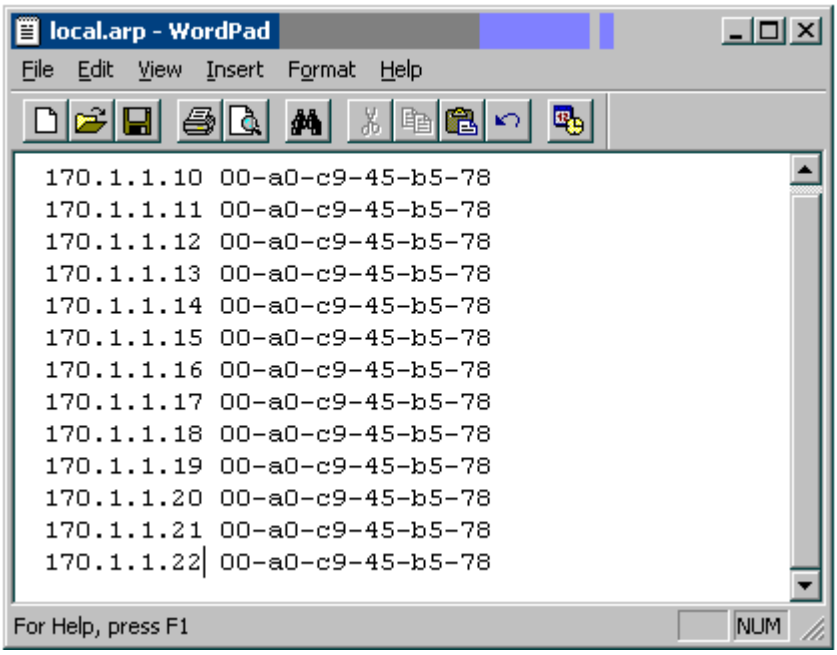

Figure 10: Creating local.arp File

4. Add new users for remote client on Check Point.

4a. Select from the main menu, Manager → Users → New → Group and create a group (for example group-1). Select **OK**.

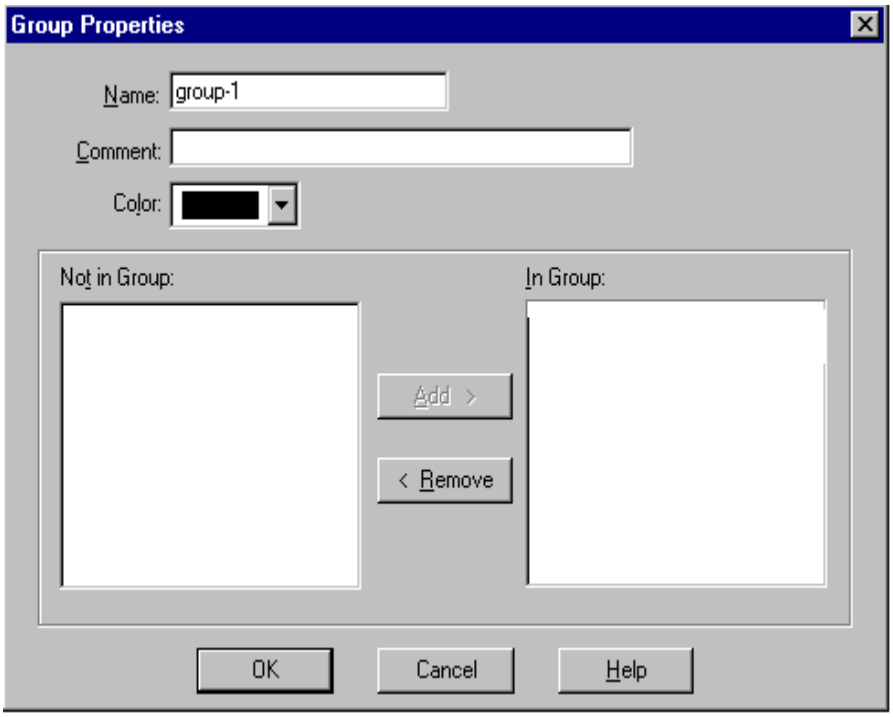

Figure 11: Creating Group

4b. Select from the main menu, Manager → Users → New → Default and create a user. Select **OK**.

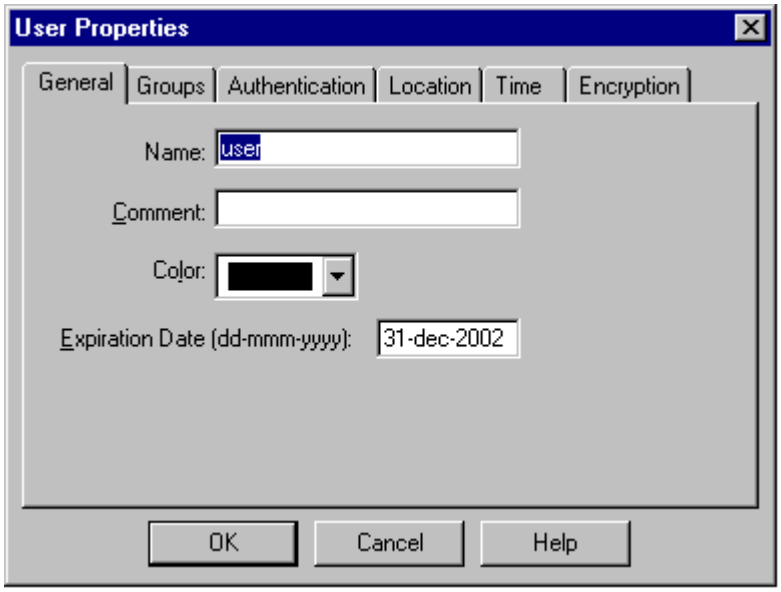

Figure 12: Creating User

4c. In the Groups Tab, add a user to group-1 by selecting group-1 and clicking '**Add**'.

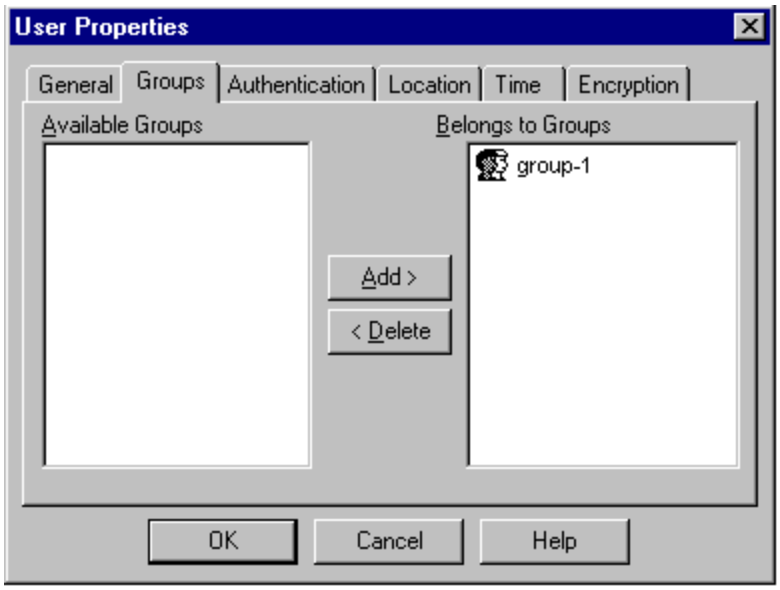

Figure 13: Add User to Group-1

4d. In the Authentication Tab, select **VPN-1 & FireWall-1 Password** and enter a password.

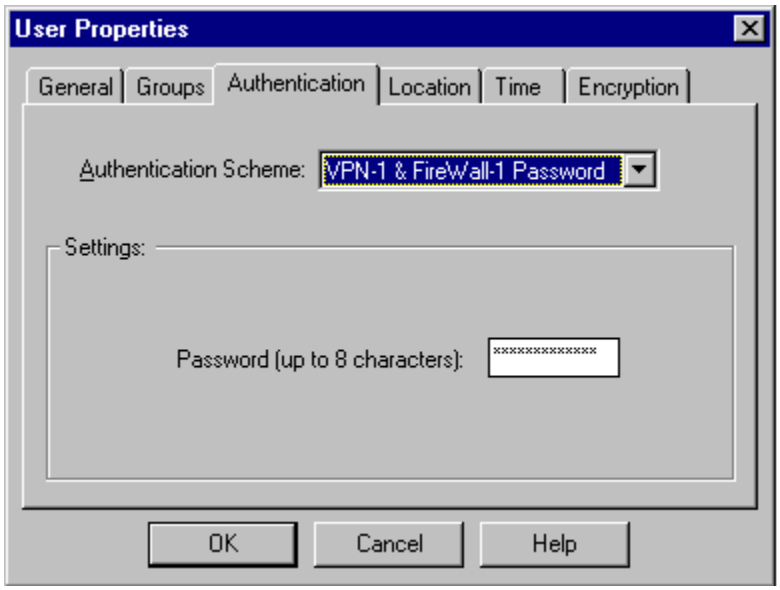

Figure 14: Add User Authentication Password

4e. In the Encryption Tab, check the box **IKE.**

Figure 15: Configure IKE for User

4f. Click on '**Edit**' and in the authentication tab select '**password**' and enter the password selected above. Select '**OK**'.

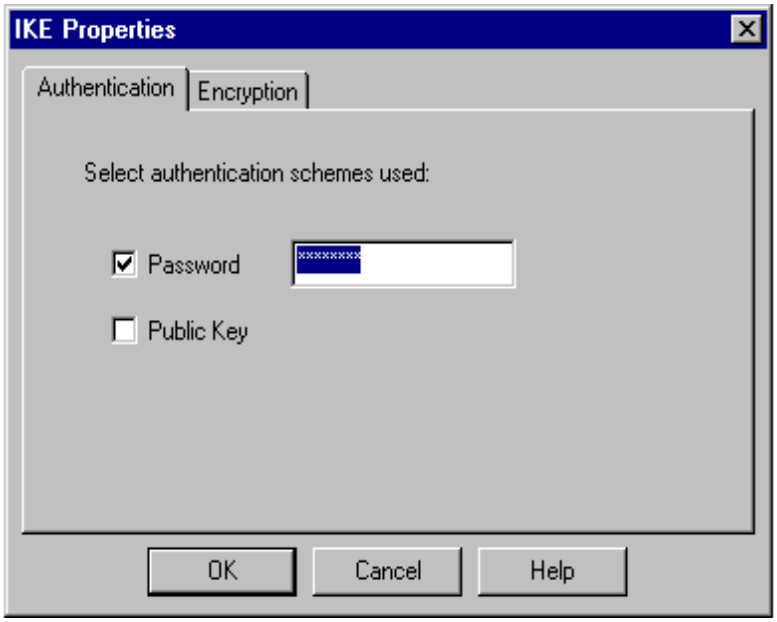

Figure 16: Enter Password

4g. Click on the '**Encryption**' Tab and select **ESP** as Transform, **MD5** as Data Integrity and **3DES** as Encryption Algorithm. Select '**OK**'.

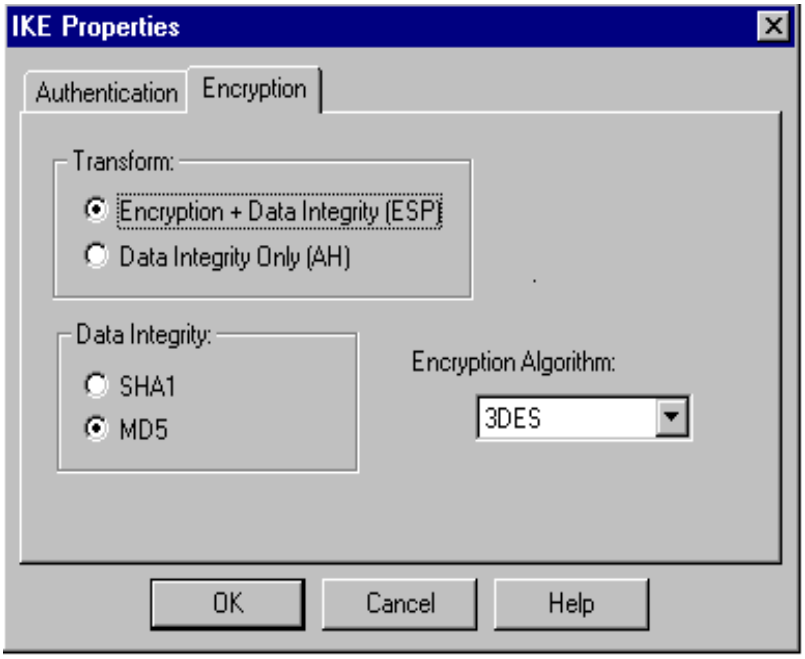

Figure 17: Configure IKE Encryption

5. **Edit 'Services'.**

From the main menu go to Manager → Services and select '**tcp-high-ports**' and enter the port range 40000 to 40100 as shown below.

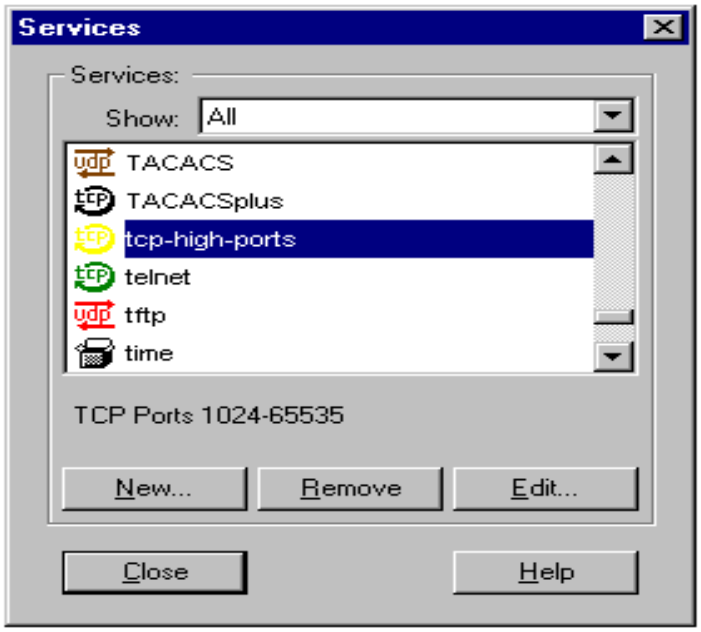

Figure 18: Edit tcp-high-ports

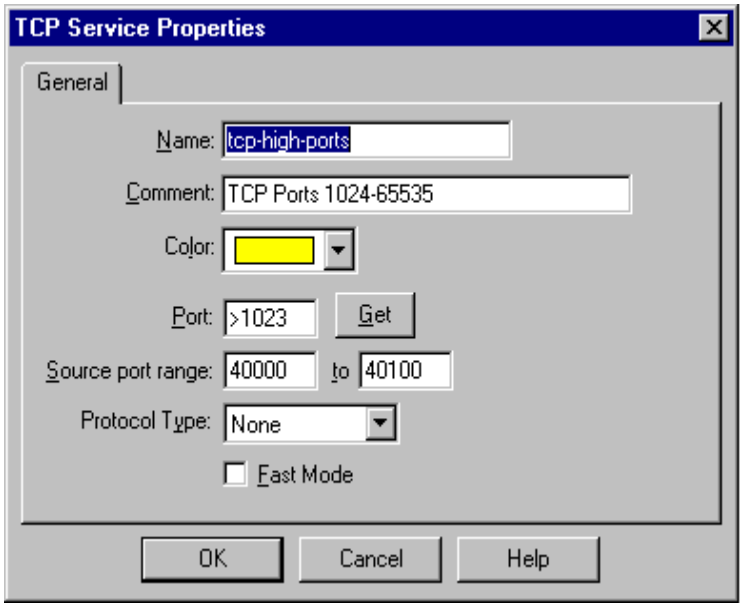

Figure 19: Set TCP Port Range

Similarly select udp-high-ports service and enter the same range as entered for tcp-high-ports.

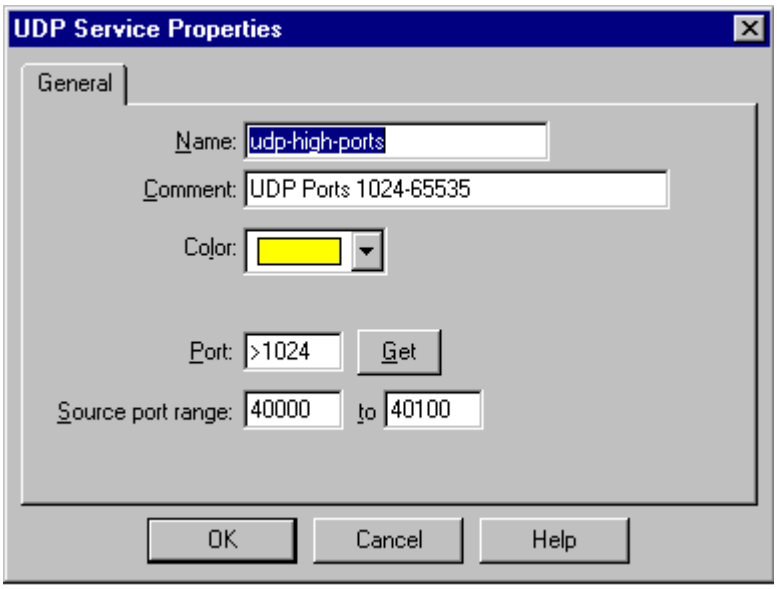

Figure 20: Set Udp Port Range

Note: Check Point takes all TCP/UDP ports which are greater than 1024 as high ports. In order to pass VoIP packets using high UDP ports, a policy has to be created to accept these packets. Customers also have the option to set the port range to use. In this example, we set the port range from 40000 to 40100. The range configured for tcp-high-ports as well as udp-high-ports should be entered in the IP Softphone login screen by the users. Only then, will users be able to register with Avaya IP600 Server, because the Firewall will only allow those sessions that use the defined TCP/UDP port range.

6. Create Policy for Remote Client

- Open '**Policy Edit**' and create the following policy for the remote client.

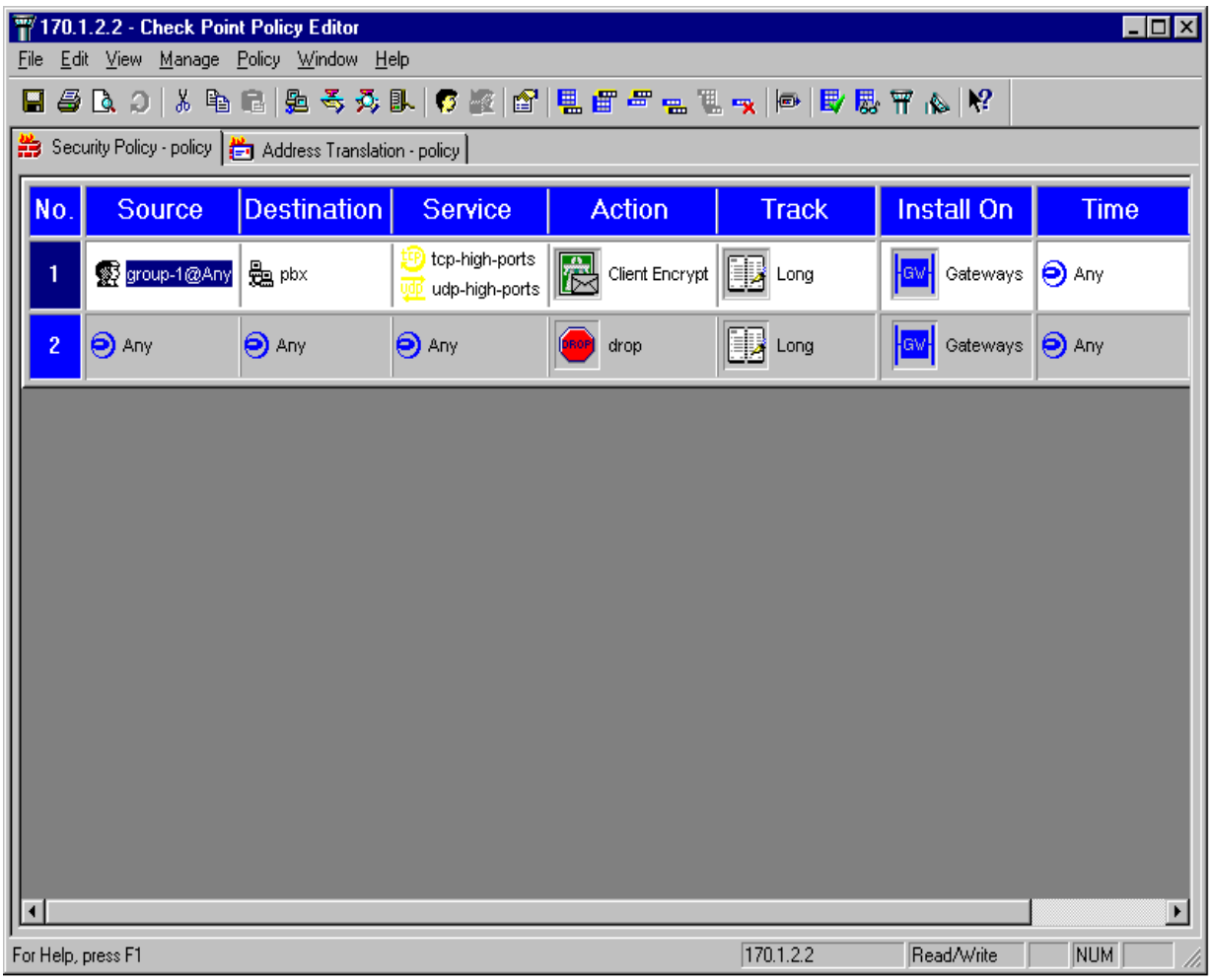

Figure 21: Configure Policy

Note: This is the minimal policy required to support IP Softphones. Applications like ICMP pings, FTP, Telnet will not work with this policy. Additional policies need to be added for them.

To check the status of the tunnel:
Start the Program and select **log viewer 4.1.** A detailed session log will be displayed on the screen.

4. Configuration for Remote Client Software on PC

- Follow these instructions to install SecuRemote client software on a PC.
- Open the VPN-1 SecuRemote Icon and

  In the Certificates Tab check '**Don't use Entrust Intelligence in the future'.**

  In the Tool Tab, open **Encryption Scheme** and Check the box **IKE.**

5. Configuration for IP Softphone on PC

Since the firewall allows only those sessions that use TCP/UDP port 40000 to 40100, IP Softphones should be configured to use ports within this range. In the login screen of the IP Softphone go to Setting → Advanced and enter the port range of 40000 – 40100 as shown below.

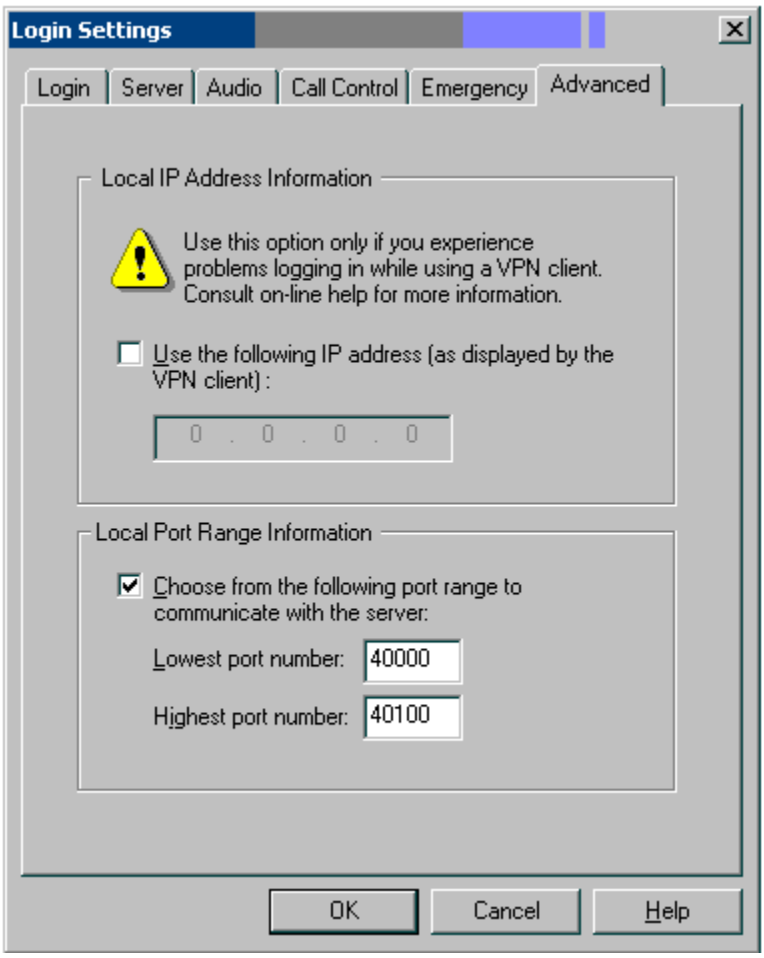

Figure 22: Set Port Range for IP Softphone

6. Configuration for IP Softphone on PC

These Application Notes provide the configuration information required to support the Avaya™ IP Softphone for customers utilizing Check Point VPN-1/Firewall-1 and SecuRemote client in a NAT environment. Avaya™ IP Softphone R3 V2.1 now supports H.323 VoIP applications running over different Network Address Translation devices. Check the implementation guides or application notes for the proper utilization of those network address translation tools. The configurations described in this document facilitate the full range of mobility benefits that the Avaya™ IP Softphone provides an enterprise.

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