

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:

- AvayaTM IP Softphone R3 V2.1x
- AvayaTM 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
- AvayaTM 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

Network Properties	×
General NAT	,
Name: Dist IP Address: 90.1.1.0 Net Mask: 255.255.255.0 Comment: ip600 Location: • Internal •	<u>G</u> et address Color: ▼ Broadcast: ● <u>Allowed</u> ○ <u>D</u> isallowed
OK	Cancel Help

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.

Address Range Prope	rties		×
General NAT			
<u>N</u> ame:	ternal-range		
Eirst IP address: 1	70.1.1.10		
Last IP address: 1	70.1.1.50		
<u>C</u> omment:			
Cojor:	•		
OK	Cancel	Help	

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.

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
Name: ckpoint
IP Address: 170.1.2.2 Get address
Comment:
Cojor:
Location: Type: ● Internal ○ External ○ Host ○ Gateway
Modules Installed
VPN-1 & EireWall-1 Version: 4.1 Cet
ElgodGrate-1 Version: 4.1
✓ <u>M</u> anagement Station
OK Cancel Help



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'.

Workstati	on Propert	ies			×
General	Interfaces	SNMP NAT	Certificates	VPN	Authe 🔹 🕨
Domai C <u>D</u> is C Val C <u>Dit</u> E	n: abled id Addresses ner: bx-group sportable for	(of Interfaces) SecuRemote	Encryption so File Inte File SH Edit	chemes d anual IPS (IP VZ	SEC
Traffic	: Control Log um on Traffic	ging : Control Loggin	g		



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

IKE Properties	×	
General		
Support key exchange encryption with:	-Support data integrity with:	
DES DES	✓ MD <u>5</u>	
	<u>, , , , , , , , , , , , , , , , , , , </u>	
Support authentication methods:		
Pre-Shared Secret	Edit <u>S</u> ecrets	
Public Key Signatures	<u>C</u> onfigure	
□ ⊻PN-1 & FireWall-1 authentication fo	r SecuRemote (Hybrid Mode)	
Supports Aggresive Mode Support keys exchange for Subnets		
OK Cancel	Help	

Figure 7: General Tab for IKE Properties

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

Workstation Properties
General Interfaces SNMP NAT Certificates VPN Authe
Values for Address Translation
Add Automatic Address Translation Rules
Iranslation Method: Static
Valid IP Address:
Install On:
IP Pools
Use IP Pool NAT for SecuRemote Connections
Allocated IP Pool Addresses from:
Return unused addresses to IP Pool after: 60 Min
OK Cancel Help

Figure 8: Configure IP Pool for Client

3f. Select from the Main menu, Policy \rightarrow 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.

Properties Setup
SYNDefender LDAP Encryption ConnectControl Security Policy Services Log and Alert Security Servers Authentication High Availability IP Pool NAT Access Lists Desktop Security
IP Pool NAT
IP Pool NAT track:
Address exhaustion O None O Log O Alert
Address allocation and release O None O Log
OK Cancel Help

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.

🗒 local.arp - WordPad	_ 🗆 ×
<u>File E</u> dit <u>V</u> iew Insert F <u>o</u> rmat <u>H</u> elp	
D 🖆 🖬 🚨 🛤 🐰 🖻 🛍 🗠 🖳	
170.1.1.10 00-a0-c9-45-b5-78 170.1.1.11 00-a0-c9-45-b5-78 170.1.1.12 00-a0-c9-45-b5-78 170.1.1.13 00-a0-c9-45-b5-78 170.1.1.14 00-a0-c9-45-b5-78 170.1.1.15 00-a0-c9-45-b5-78 170.1.1.16 00-a0-c9-45-b5-78 170.1.1.17 00-a0-c9-45-b5-78 170.1.1.18 00-a0-c9-45-b5-78	
170.1.1.19 00-a0-c9-45-b5-78 170.1.1.20 00-a0-c9-45-b5-78 170.1.1.21 00-a0-c9-45-b5-78 170.1.1.22 00-a0-c9-45-b5-78	
For Help, press F1	NUM //

Figure 10: Creating local.arp File

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

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

Group Properties	x
<u>N</u> ame: group-1	
Comment:	
Color:	
Not in Group:	In Group:
	Add > < <u>R</u> emove
	OK Cancel <u>H</u> elp

Figure 11: Creating Group

Solution & Interoperability Test Lab Application Notes © 2002 Avaya Inc. All Rights Reserved. 4b. Select from the main menu, Manager \rightarrow Users \rightarrow New \rightarrow Default and create a user. Select **OK**.

User Properties
General Groups Authentication Location Time Encryption
Name: user
Comment:
Cojor:
Expiration Date (dd-mmm-yyyy): 31-dec-2002
OK Cancel Help



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

User Properties	E	×
General Groups	Authentication Location Time Encryption	
<u>Available</u> Groups	Belongs to Groups	L
	€dd >	
	< <u>D</u> elete	
	TK Cancel Help]

Figure 13: Add User to Group-1

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

User Properties	×
General Groups Authentication Location Time Encryption	
Authentication Scheme: VPN-1 & FireWall-1 Password	
C Settings:	
Password (up to 8 characters): ************	
OK Cancel Help	

Figure 14: Add User Authentication Password

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

User Properties	×
General Groups Authentication Location Time Encryption	
Client Encryption Methods	
KE	
E FWZ	
Successful Authentication Track:	
O None O Log O Alert	
OK Cancel Help	

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'.

IKE Properties
Authentication Encryption
Select authentication schemes used:
Public Key
OK Cancel Help

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'.

IKE Properties	×
Authentication Encryption	
Transform: © Encryption + Data Integr © Data Integrity Only (AH)	ity (ESP)
Data Integrity: O SHA1 O MD5	Encryption Algorithm: 3DES
ОК	Cancel Help

Figure 17: Configure IKE Encryption

Solution & Interoperability Test Lab Application Notes © 2002 Avaya Inc. All Rights Reserved.

5. Edit 'Services'.

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

Serv	Services X				
	Services:				
	Show: All			-	
	TACACS				
	😰 TACACSplus				
	😳 top-high-ports	;			
	🗐 telnet				
	पुर्वे tftp				
	🗃 time				
	TCP Ports 1024-65	535			
	<u>N</u> ew	<u>R</u> emove	<u>E</u> dit		
	<u>C</u> lose		<u>H</u> elp		

Figure 18: Edit tcp-high-ports

TCP Service Properties				
General				
Name: tcp-high-ports				
Comment: TCP Ports 1024-65535				
Cojor:				
<u>P</u> ort: >1023 <u>G</u> et				
Source port range: 40000 to 40100				
Protocol Type: None				
East Mode				
J				
OK Cancel Help				

Figure 19: Set TCP Port Range

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

UDP Service Properties
General
Name: udp-high-ports
Comment: UDP Ports 1024-65535
Port: >1024 <u>G</u> et
Source port range: 40000 to 40100
OK Cancel Help

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.

T 17	0.1.2	.2 - Check Poin	t Policy Editor					_ 🗆 ×
<u>F</u> ile	<u>E</u> dit	⊻iew <u>M</u> anage <u>I</u>	<u>Policy W</u> indow <u>H</u>	elp				
	E # C.) % & C. & S. & V. (? 🕸 12 12 12 12 12 12 12 12 12 12 12 12 12							
🚔 S	iecurity	y Policy - policy 🛛 🖁	📩 Address Translatio	on - policy				
No) .	Source	Destination	Service	Action	Track	Install On	Time
1	2	🙀 group-1@Any	🛱 pbx	ഈ tcp-high-ports 亚 udp-high-ports	Client Encrypt	Long	GW Gateways	🧿 Any
2	€	Any	ව Any	🧿 Any	drop	Long	GW Gateways	🧿 Any
								Þ
For He	lp, pre	ss F1				170.1.2.2	Read/Write	

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 \rightarrow Advanced and enter the port range of 40000 – 40100 as shown below.

Login Settings
Login Server Audio Call Control Emergency Advanced
Local IP Address Information
Use this option only if you experience problems logging in while using a VPN client. Consult on-line help for more information.
Use the following IP address (as displayed by the VPN client):
0.0.0
Local Port Range Information
Choose from the following port range to communicate with the server:
Lowest port number: 40000
Highest port number: 40100
OK Cancel <u>H</u> elp



6. Configuration for IP Softphone on PC

These Application Notes provide the configuration information required to support the AvayaTM IP Softphone for customers utilizing Check Point VPN-1/Firewall-1 and SecuRemote client in a NAT environment. AvayaTM 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 AvayaTM IP Softphone provides an enterprise.

© 2002 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by \mathbb{R} and \mathbb{T} 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 <u>interoplabnotes@list.avaya.com</u>