

Avaya Solution & Interoperability Test Lab

Sample Configuration for Microsoft Firewall and McAfee Desktop Firewall 8.5 to Support Avaya IP Softphone – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Microsoft Firewall and McAfee Desktop Firewall to interoperate with Avaya IP Softphone.

1. Introduction

These Application Notes describe a solution for configuring both Microsoft Firewall and McAfee Desktop Firewall to interoperate with Avaya IP Softphone. By default, both the Microsoft Firewall and the McAfee Desktop Firewall are enabled to automatically prompt the user to either Unblock/Allow or Block/Deny the necessary services needed for Avaya IP Softphone. Once the user selects to Unblock/Allow the needed service for Avaya IP Softphone, both firewalls will automatically configure the appropriate firewall policy to permit the operation of Avaya IP Softphone. Where applicable, these Application Notes will highlight areas where optimization can be made in either firewall policies for better intrusion prevention.

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All IP addresses are statically administered. The Avaya IP Telephone and Avaya IP Softphones are registered with Avaya Communication Manager shown in **Figure 1**. All telephone extensions belong to ipnetwork-region 1 in Avaya Communication Manager. Avaya IP Softphone version R5 and R6 are individually verified using the same sample network.



Figure 1: Sample Network Configuration

3. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration:

DEVICE DESCRIPTION	VERSION TESTED
Avaya S8500 Server with Avaya G650 Media	Avaya Communication
Gateway	Manager R4.0.1
	(R014x.00.1.731.2)
Avaya 4625SW IP Telephone	R2.8.3 (H.323)
Avaya IP Softphone	R5 SP3
Avaya IP Softphone	R6.0.0.25
Microsoft Windows	XP Professional with SP2
Microsoft Firewall	Built-in
McAfee Desktop Firewall	Product Version 8.5
	Build Number 260
	IDS Signature 101

4. Configure McAfee Desktop Firewall

This section describes the configuration for the McAfee Desktop Firewall in **Figure 1**. The configuration shown in this section assumes that McAfee Desktop Firewall is in the default initial configuration. The auto configuration mechanism of McAfee Desktop Firewall is used to create the initial policies and then manually edited to optimize security.

 Initiate McAfee Desktop Firewall via Start → Program → McAfee Desktop Firewall → McAfee Desktop Firewall, and verify that the McAfee Desktop Firewall is enabled (default).

Application Policy	Intruder Policy	Activity Log	1			
Description	Outgoing Enable Protocol	d	Service (R)	Address	Application	Truşted.
9 🐼 Fing and ICMP 🎝 Allow BOOTP 🎝 Allow DNS 🎝 Allow Net Time Protocol B 🔂 NetBIOS Group	IC I I DP I I I I I I I I I I I I I I I I I I I	bootpe (69) Any ntp (123)	bootps (67) dns (53) ntp (123)	Any Any Any		

2. Initiate Avaya IP Softphone via Start → Programs → Avaya IP Softphone → Avaya IP Softphone. This will cause the following three pop-up windows to appear. Click Allow on each of the pop-up Window.

Note: If this is the first time Avaya IP Softphone being initiated, there are parameters such as Extension, Password, Call Server Address, etc. that must be entered (not shown). Please refer to reference [1] and [4] for additional information.

McAfee Desktop Firewall	N 200
Application Information Connection	Information
Network Application attem Application attem Selecting Deny will cr	on Alert pting to access the Network. create a new permission rule for this application. reate a new block rule for this application.
Information Event Time : 11/29// Product Name : Avaya I Application Name : ipsoftph Application Path : C:VProg Vendor Name : Avaya I Version : 5, 2, 7,	2007 10:11:51 AM P Softphone R5 ione.exe gram Files\Avaya IP Softphone\ipsoftphone.exe nc. 0
Options Previous Next	
McAfee Desktop Firewall	McAfee Desktop Firewall
Application Information Connection Information	Application Information Connection Information
Network Application Alert Application attempting to access the Network. Selecting "Allow" will create a new permission rule for this application. Selecting Deny will create a new block rule for this application.	Network Application Alert Application attempting to access the Network. Selecting "Allow" will create a new permission rule for this application. Selecting Deny will create a new block rule for this application.
Information Information Event Time : 11/29/2007 10:12:07 AM Product Name : QosServM MFC Application Application Name : QosServM.EXE Application Path : C:\WINDOWS\system32\qosservm.exe Vendor Name : AVAYA Communication Version : 4, 0, 4, 1	Information Event Time : 11/29/2007 10:12:07 AM Product Name : Avaya IP Softphone R5 Application Name : ipsoftphone.exe Application Path : C:\Program Files\Avaya IP Softphone\ipsoftphone.exe Vendor Name : Avaya Inc. Version : 5, 2, 7, 0
Options Options Previous Next - 1	Options Previous Next

3. Three additional policies should now appear under the Firewall Policy tab in the McAfee Desktop Firewall. At this point, Avaya IP Softphone will be able to register with Avaya Communication Manager and will be able to function fully.

McAfee Desktop Firewall k Edit Yew Help	······································						
ewall Policy Application Policy	Intruder Policy	Ac	tivity Log	1			Ũ
Egable Firewal Learn Mode I Incoming Enabled	✓ Outgoing Enabled	ł				Trugte	d
Description	Protocol 😣	0	Service (L)	Service (R)	Address	Application	
By VPN Ping and ICMP Allow BOOTP Allow DNS Allow Net Time Protocol	(C) c⇔ UDP (C) c⇔ UDP (C) c⇔ UDP		boolpc (68) Any No (123)	bootps (67) dns (53) ntp (123)	Any Any Any		
Action of the second seco	n () () UDP n () () () UDP n () () () TCP		1024 - 65535 1024 - 65535 1024 - 65535	1024 - 65535 1024 - 65535 1024 - 65535	Ary Ary Ary	國 Avaya IP Softphone R5 (pso 戦 GosServM MFC Application (國 Avaya IP Softphone R5 (pso	
					Propertie	s Duplicate Berrove Add	
is: On	Firewall is active						

4. Double click on the newly defined firewall Rule 1 in **Step 3** to display the Firewall Rule pop-up window. Change the **Local Service** and **Remote Service** port range to fall within the values set in the ip-network-region form in Avaya Communication Manager shown in **Section 6**, **Step 1**. The sample configuration uses port range of 2048 to 3229. (This step is to close down un-used ports, and is optional.)

Firewall Rule	? 🛛			
Description:	Dynamically Created Via Learn Mode			
Action:	Permit			
Protocol:				
Direction:	Either			
Application:	🌃 Avaya IP Softphone R5 (ipsoftphone.exe) 📃			
	Browse			
Local Service	Range			
From:	2048 To: 3229			
- <u>R</u> emote Service—	Range			
From:	2048 To: 3229			
	Anu			
Options				
I reat rule match as intrusion Restrict rule to currently defined time interval Time				
Log matching traffic				
I Active				
	0 <u>K</u> Cancel			

5. Double click on the newly defined firewall Rule 3 in **Step 3** to display the Firewall Rule pop-up window. Change the Remote Service field to **Single** for the value of **1720** port, and Address to **Single** with IP address of the CLAN, **172.28.10.7**. (This step is to close down un-used ports and IP addresses, and is optional.)

Firewall Rule				
Description: Dynamically Created Via Learn Mode				
Action: Permit				
Protocol: • IP TCP C Non-IP Appletalk				
Direction: Outgoing				
Application: 🛛 🗰 Avaya IP Softphone R5 (ipsoftphone.exe) 🔍 💌				
Browse				
Local Service Range 💌				
From: 1024 To: 65535				
_ <u>R</u> emote ServiceSingle				
1720				
Address				
Address: 172 28 10 7				
Options Treat rule match as intrusion Restrict rule to currently defined time interval Time				
✓ Active				
0 <u>K</u>				

6. The final firewall policy should look as follow.

Ber Stor Geb						
wall Policy Application Policy	Intruder Policy	Activity Log				
Enable Firewall						
Learn Mode		7				
M Incoming Enabled	V Uutgoing Enabled					rugrea.
Description	Protocol 🔒	() Service (L)	Service (R)	Address	Application	
Allow BOOTP	C 🗘 🗘 UDP	bootpc (68)	bootps [67]	Any		
Allow DNS	🚱 🛟 UDP	Any	dns (53)	Any		
Allow Net Time Protocol	60 🚓 UDP	ntp [123]	ntp [123]	Any		_
Dynamically Created Via Learn.	🙆 👄 UDP	2048 - 3229	2048 - 3229	Anu	Avava IP Softphone B5 (ipso	
Dynamically Created Via Learn.	. 👸 ⇔ UDP	1024 - 65535	1024 - 65535	Any	QosServM MFC Application (
🕁 Dynamically Created Via Learn.	👩 🌩 ТСР	1024 - 65535	1720	172.28.10.7	Avaya IP Softphone R5 (ipso	
		S)	/			-
				Ourseller	Duning Damage	Add

5. Configure Microsoft Firewall

This section shows the steps for configuring the Microsoft Firewall.

 Open the Windows Firewall window by clicking on Start → Control Panel → Windows Firewall and turn on Windows Firewall by selecting the On radio button.



Initiate Avaya IP Softphone via Start → Programs → Avaya IP Softphone → Avaya IP Softphone. This will cause the following three pop-up windows to appear. Click Unblock on the pop-up Window.

Note: If this is the first time Avaya IP Softphone being initiated, there are parameters such as Extension, Password, Call Server Address, etc. that must be enter (not shown). Please refer to reference [1] and [4] for additional information.



3. Avaya IP Softphone will be able to register with Avaya Communication Manager upon the completion of **Step 2**. Avaya IP Softphone should be automatically added under the exceptions tab as shown below.

🐱 Windows Firewall 🛛 🛛 🔀				
General Exceptions Advanced				
Windows Firewall is blocking incoming network connections, except for the programs and services selected below. Adding exceptions allows some programs to work better but might increase your security risk.				
Programs and Services:				
Name				
Avaya IP Softphone R5 File and Plinter Sharing Remote Assistance Remote Desktop UPnP Framework				
Add Program Add Port Edit Delete				
What are the risks of allowing exceptions?				
OK Cancel				

6. Configure Avaya Communication Manager

The following shows the configuration of Avaya Communication Manager relevant to the firewall configuration. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please consult references [1], [2], [3] and [4].

 Use the "display ip-network-region" command to display the UDP Port Min and UDP Port Max values used for ip-network-region 1 using the System Access Terminal (SAT). These values are used to defined the firewall policy in Section 4, Step 4.

dignlaw in-notwork-region 1		Dago 1 of 10
display ip-network-region i		Page I OI IS
1	IP NETWORK REGION	
Region: 1		
Location: 1 Authoritative	Domain:	
Name:		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio	: ves
Codec Set: 1	Inter-region IP-IP Direct Audio	: ves
UDP Port Min: 2048	IP Audio Hairpinning	? n
UDP Port Max: 3229		
DIFFSERV/TOS PARAMETERS	RTCP Reporting Enabled	? v
Call Control DHP Value: 16		. 1
Call CONCLOI PHB Value: 40	RICP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46	Use Default Server Parameters	? У
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6	5	
Audio 802.1p Priority: 6	5	
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATIO	N PARAMETERS
H.323 IP ENDPOINTS	RSVP E	nabled? n
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20)	
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

7. Verification Steps

The following steps may be used to verify the configuration:

- Place and receive a call using Avaya IP Softphone, verify whether the call can be established successfully and the call has two-way audio. For McAfee, if a call failed to establish, verify that Rule 3 in **Section 4**, **Step 3** is defined. If a call can be established but fails to provide two-way audio, verify that Rule 1 in **Section 4**, **Step 3** is defined.
- The following is the version of Microsoft Windows used in the sample network.



• The following shows the version of McAfee Desktop Firewall used in the sample network.



• The following shows the versions of Avaya IP Softphone used in the sample network.

	About Avaya IP Softphone 🛛 🔀
	Avaya IP Softphone OK Version: 6.0.0.25 More
About Avaya IP Softphone Image: Control of the softphone Avaya IP Softphone Image: Control of the softphone Version: R5.2 SP3 More	Avaya Inc. Copyright © 2007 Avaya Inc.
Avaya Inc. Copyright © 2007 Avaya Inc. Product Version: 5.27.2 Configuration: Road Warrior Station Type: 4620 Station Extension: 11011 Call Server Version: 11011 Call Server Version: R014x.00.1.731.2 Avaya IP Service Provider Version: 5.24.5.0 (5.2.5.1) Avaya iClarity Version: 5.2.6.0	Product Version: 6.00.54 Configuration: Road Warrior Station Type: 4620 Station Extension: 11011 Call Server Version: R014x.00.1.731.2 Avaya IP Service Provider Version: 6.0.0.6 (6.0.0.13) Avaya iClarity Version: 6.0.0.14

8. Conclusion

These Application Notes have described the administration steps required to configure McAfee Desktop Firewall and Microsoft Firewall to support Avaya IP Softphone R5 and Avaya IP Softphone R6.

9. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com

- [1] Administrator Guide for Avaya Communication Manager, Doc # 03-300509, Issue 3.1, February 2007
- [2] Avaya Communication Manager Advanced Administration Quick Reference, Doc # 03-300364, Issue 3, February 2007
- [3] Administration for Network Connectivity for Avaya Communication Manager, Doc # 555-233-504, Issue 12, February 2007
- [4] Avaya IP Softphone Release 6.0 User Reference, Issue 1, May 2007

Product documentation for Microsoft Networks products may be found at <u>http://www.microsoft.com</u>

Product documentation for McAfee products may be found at http://www.mcafee.com

©2008 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by B and TM 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>