

Firewall Settings for AVG 7.5

Document revision 75.2 (8.2.2007)

Copyright GRISOFT, s.r.o. All rights reserved.

This product uses RSA Data Security, Inc. MD5 Message-Digest Algorithm, Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. This product uses code from C-SaCzech library, Copyright (c) 1996-2001 Jaromir Dolecek <dolecek@ics.muni.cz>

This product uses compression library zlib, Copyright (C) 1995-2002 Jean-loup Gailly and Mark Adler

All other trademarks are the property of their respective owners.



Contents

1.	Introduction	. 3
2.	Windows XP built-in firewall (Security Center)	. 4
3.	Kerio Personal Firewall	. 8
	3.1. Run Kerio Personal Firewall	. 8
	3.2. Network Security	. 8
	3.3. System Security	10
4.	Zone Alarm Pro	13
5.	Microsoft ISA Server	16
6.	Agnitum Outpost Firewall	23
	6.1. Allowing Activities for an Application	23
	6.2. Configuring the Firewall at Once	23
7.	Sygate Personal Firewall	26
	7.1. Allowing Activities for an Application	26
	7.2. Configuring the Firewall at Once	26
8.	Kerio Winroute Firewall	30
9.	Technical Support	31





1. Introduction

In case you have installed **AVG** on your computer, and you are running a firewall at the same time, you might be experiencing problems while sending/receiving email messages and/or downloading **AVG** updates.

This documentation refers to the firewall settings required for proper **AVG** functionality and it covers the settings instructions and recommendations for the following firewalls:

- Windows XP built-in firewall (Security Center)
- Kerio Personal Firewall
- Zone Alarm Pro firewall
- Microsoft ISA Server
- Agnitum Outpost Firewall
- Sygate Personal Firewall
- Kerio Winroute Firewall



2. Windows XP built-in firewall (Security Center)

Typically, the *Windows XP built-in firewall* default settings correspond very well to **AVG** configuration. Most probably, no problems will occur at all. However, should you run up against problems, please follow these steps:

• Windows XP Firewall Settings

Open the Windows Firewall settings dialog window: *Start / Settings / Control Panels / Windows Firewall*. On the *General* tab make sure the *Do not allow exceptions* option is not selected.



Define Exceptions

Switch to the *Exceptions* tab with the list of applications that are blocked to access to the internet. You need to allow access to internet for all **AVG** applications. To do so, mark each check box related to an **AVG** application in the list of programs and services (see the following screenshot).







The AVG applications to be selected from the list and marked as allowed are as follows:

- AVG for Windows
- o AVG Control Center
- o avgemc.exe (only when the AVG EMS application is installed)
- o avginet.exe

If these applications are not listed in the list of exceptions, you need to add them manually. This can be done using the *Add Program* button (see the above screenshot).

Add a New Program

A new dialog window opens providing a list of programs that can be added to the previously seen *Windows Firewall* list of exceptions. Select the **AVG** applications from the list, and confirm adding them to the *Windows Firewall* list of exceptions by pressing the *OK* button (see the following screenshot).







In case you are not able to see any **AVG** application in the program list, you have to add them manually. Click the **Browse** button, and find the above listed files (*avgw.exe, avgcc.exe, avginet.exe* and *avgemc.exe*) in the **AVG7** program folder (by default *C:\Program Files\Grisoft\AVG7*):

Browse					?×
Look <u>i</u> n:	C AVG7		•	3 🕸 🖻 🖽-	
My Recent Documents Desktop My Documents My Computer	avg.exe avgamsvr.exe avgenc.exe avgenc.exe avgenc.exe avgenc.exe avgupet.exe avgupsvr.exe avgupsvr.exe avgupsvr.exe avguy.exe avgw.exe setup.exe				
My Network	, File <u>n</u> ame:			•	<u>O</u> pen
Places	Files of type:	Applications (*.exe;*.com;*.ic	cd)	•	Cancel

Confirm adding the selected files by pressing the *OK* button in the *Add a Program* dialog window.

AVG Remote Administration

In case the station you are working with is a part of the **AVG Remote Administration**, and it is:

- o running as an AVG client connected to the AVG DataCenter;
- o running AVGADMIN and AVG TCP Server at the same time;
- o running AVGADMIN;





it is necessary to specify ports to be opened through the *Windows XP builtin firewall*. To specify the ports numbers use the *Add a port* dialog that can be opened via the *Add a port* button in the *Exceptions* tab:

Add a Port	×
Use these settings number and protoc want to use.	to open a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you
<u>N</u> ame:	AVG Port 1
Port number:	4156
	⊙ <u>I</u> CP C <u>U</u> DP
What are the risks	of opening a port?
Change scope	OK Cancel

You need to add one by one the following ports:

0	4156
0	6051
0	6052
0	0052

- o 6053
- o 6150





3. Kerio Personal Firewall

With the *Kerio Personal Firewall* you will probably need to configure the settings to allow **AVG** (and its applications) to connect to the internet (send/receive data), and to launch other applications (to update). To configure the *Kerio Personal Firewall* settings, follow these steps:

3.1. Run Kerio Personal Firewall

You should see the *Kerio Personal Firewall* shield icon in your system tray – double-click on it to open the *Kerio Personal Firewall* configuration window.

If you cannot see such an icon, you have to launch the *Firewall Engine* from the *All Programs / Kerio / Personal Firewall X* folder of the Windows Start menu. The X stands for the version of your product (for example 4). The *Kerio Personal Firewall* icon in the system tray will be present then.

3.2. Network Security

In the *Network Security* item (left menu), *Applications* tab (top menu) you are able to overview a list of programs with the information on whether these are allowed to connect to the internet. In the list, verify that all **AVG** applications are labeled as permit in all fields present (Trusted In/Out and internet In/Out).

Here is the list of all **AVG** applications that must always be allowed to connect to the internet:

- avginet.exe application for performing AVG online updates (located in the *Program Files/Grisoft/Avg7* directory by default)
- **avgemc.exe AVG E-mail Scanner** for anti-virus scanning of e-mail (located in the *Program Files/Grisoft/Avg7* directory by default)

Following two applications must be allowed to access the network when the workstation is a part of **AVG Remote Administration**:

- avgmsvr.exe AVG Alert Manager component (located in the Program Files/Grisoft/Avg7 directory by default)
- **avgcc.exe AVG Control Center** (located in the *Program Files/Grisoft/Avg7* directory by default)

And finally, when there are installed the control components of **AVG Remote Administration** on the workstation, the following applications must be also allowed to communicate over the network:

- avgadmin.exe the main control application of AVG Remote Administration, AVGADMIN (if the product is installed on your computer, it is located in the *Program Files/Grisoft/AvgAdmin7* by default)
- avgtcpsv.exe AVG TCP Server application for AVG Remote Administration (if the product is installed on your computer, it is located in the *Program Files/Grisoft/AVG TCP Server* by default)
- **avginetI.exe AVG InetLite** application (if installed, it is located in the *Program Files/Grisoft/Avg TCP Server* by default)



If any **AVG** application you need to be allowed to access the network is not permitted, you have to change its status. To do so, right click on every item and select the Permit option from the context menu:

🌆 Kerio Personal Firewall					
♦ KERIO	Applications	Predefined	Trusted area	Advanced	
(Overview	Enable Network security mode	ıle			
Network Security	Description	Trusted In Out	Internet In Out	Log Alert	
System Security Intrusions Image: System Security Image: Stop all traffic	LSA Shell (Export Version) Windows NT Logon App Userinit Logon Application Generic Host Process for AVG E-Mail Scanner AVG Update downloader Microsoft File and Printer AVG Control Center AVG Control Center AVG Alert Manager Any other application	 ask. permit ask. permit ask. permit ask. permit permit permit permit permit permit ask. permit ask. permit ask. permit ask. ask 	? ask ? ask ? ask ? ask ? ask ? ask ? ask ? permit ? permit ? permit ? f Permit ? ? f Permit smit ? ask ? ask ? ask ? ask ? ask ? ask	· · · · · · · · · · · · · · · · · · · · · · · · · · · · · · · ·	
	Edit Remove		Pa	oket filter Refres	sh
		Register	Help OK	Cancel	Apply

Press the *Apply* button in the *Kerio Personal Firewall / Network Security* window after finishing the network security configuration to confirm the changes performed (you will be asked for it otherwise).

If some application is missing on the list, it will be added when you attempt to launch it and/or when the application will try to connect to the network. *Kerio Personal Firewall* warning related to the particular **AVG** application will be displayed then:





KerioPersonal Firewall 4
An application is trying to communicate with a remote computer. Please decide if you want to permit such communication or deny it.
Outgoing Connection Alert (Internet)
📕 AVG Update downloader
Remote point: 212.67.88.66, port http [80]
Create a rule for this communication and don't ask me again.
✓ Permit X Deny
Details
[2.2.2005 12:07:53] Direction: outgoing Local Point: 0.0.0, port 1638 Adapter: Intel(R) PR0/100 VE Network Connection - Packet Scheduler Minip Remote Point: 212.67.88.66, port http [80] Protocol: TCP
Create an advanced filter rule Advanced filter rule

Press the *Permit* button there and refresh the list in the *Kerio Personal Firewall* / *Network Security configuration* window then (by pressing the Refresh button in the right-down corner). After doing this, you can label the application as permitted in all fields present as described in the beginning of this section.

3.3. System Security

In the *System Security* item (left menu), *Applications* tab (top menu) you are able to overview a list of programs with the information on whether these are allowed to launch other application. Again, you need to make sure all **AVG** applications listed are labeled as permit to launch other applications (e.g. updates).

If not, you need to change the **AVG** applications' status. To do so, right click on every field present (*Starting*, *Modifying* and *Launching* others) and select the *Permit* option from the context menu.





Overview	Enable System security module	•				
Network Security	Application	Starting	Modifying	Launching ot	Log Alert	
<u> </u>	Windows NT Logon Applia	v permit	y dSK	v permit		
System Security	Windows I ogon III	. V permit	2 ask	v permit		
	Client Server Buntime Proc.	🖌 🗸 permit	2 ask	V permit		
Intrusions	Windows NT Session Man	. 🧹 permit	🤉 ask	V permit		
2	Userinit Logon Application	🖌 permit	🤶 ask	🗸 permit		
W/eb	🛜 Průzkumník Windows	🖌 permit	💡 ask	🖌 permit		
,	Generic Host Process for	🖌 permit	💡 ask	🖌 permit		
Logo & Alorto	📑 Net Command	🖌 permit	💡 ask	💡 ask		
	🔲 🛄 Net Command	ᢦ permit	💡 ask	💡 ask		
	📥 Logon Screen Saver	🖌 permit	💡 ask	💡 ask		
	AVG Control Center	🖌 permit	💡 ask	🗸 permit		
	AVGADMIN Application	🧹 permit	ask 🦉	🖉 🖌 Permit	· ·	
	AVG Update downloader	🗸 permit	2 ask	🕺 🗙 Deny		
oing: 0.00 KB/s	AVG 7.0	V permit	y ask	🕺 🥐 Ask		
ming. 0.12 (675	AVG Advanced Interface	v permit	y dSK	2 ack		
Stop all traffic	AVG TCP Server Monitor	🖌 permit	2 ask	j don Diank		
		🖌 permit	2 ask	2 ask		
	Edit Remove		-	-	I	Refresh

Press the *Apply* button in the *Kerio Personal Firewall / System Security* window after finishing the network security configuration to confirm the changes performed (you will be asked for it otherwise).

If some application is missing on the list, it will be added for example when it attempts to launch another application. *Kerio Personal Firewall* warning related to the particular **AVG** application will be displayed then:

KerioPersonal
'AVG Control Center' is trying to execute 'AVG Update downloader'. Permit the event if it is expected and intended. Deny this event if it is undesirable (can be caused by a virus, trojan horse or an application breaching this computer's security).
Application is launching other application
AVG Update downloader Launched by: AVG Control Center
Create a rule for this event and don't ask me again.
<u> </u>
Details
Application path: c:\Program Files\Grisoft\AVG7\avginet.exe Description: AVG Update downloader File version: 7.0.0,304 Product name: AVG Anti-Virus system Product version: 7.0.0,304 Created: 2005/2/1, 12:52:07 Modified: 2005/2/1, 12:52:07 Accessed: 2005/2/2, 09:46:25





Press the *Permit* button there and refresh the list in the *Kerio Personal Firewall* / *System Security configuration* window then (by pressing the *Refresh* button in the right-down corner). Then you can label the application as permitted in all fields present as described in the beginning of this section.





4. Zone Alarm Pro

With the *Zone Alarm Pro* you will probably need to configure the settings so that it is allowed for the **AVG** (and its applications) to connect to the internet (send/receive data), and to launch other applications (to update). To configure the *Zone Alarm Pro* settings, follow these steps:

Run Zone Alarm Pro

You should see the *ZoneAlarm Pro* icon in your system tray – double-click on it to open the *ZoneAlarm Pro configuration* window.

If you cannot see such an icon, you have to launch the *Zone Labs Security* application from the *All Programs / Zone Labs* folder of the Windows Start menu. The *ZoneAlarm Pro* icon in the system tray will be present then.

Program Control

In the *Program Control* section (left menu), *Programs* tab (top menu) you are able to overview a list of programs with the information on whether these are allowed to connect to the internet. In the list, verify that all **AVG** applications are labeled as allowed (green confirmation mark).

ZA ZoneAlarm P	Pro								
		•					📕 PR All Sys	OGRAM tems A	S
	Program Control			N	lain	Pr	ograms	C	(?) Help omponents
Overview	These are programs that have tried to access the	Active	Programs A	Acce Trusted	ess Internet	Ser Trusted	ver Internet	Send Mail	Ê
Firewall	Internet or local network.		AVG E-Mail Scanner	1	1	1	1	1	
Program	Access and Server columns show the	•	Generic Host Process for W	J	J	J	Ĵ	?	
Control	has for each Zone.		Internet Explorer Internet Explorer ILSA Shell (Export Version)	J	1 2	?	?	?	
Monitoring E-mail	Change a program's permissions by		Outlook Express	Ĵ	j	?	?	?	
Protection	left-clicking the icons in the Access or Server		Spooler SubSystem App	4	?	?	?	?	
Privacy	column.		Windows NT Logon Applica	?	?	?	?	?	
ID Lock			ZA Zone Labs Client	?	?	?	?	?	
Alerts & Logs									
	∢ Hide Text	Entry Produc File na Policy Last p Versio	Detail t name AVG Anti-Virus S; me F:VProgram Files/G Manually configure lolicy update Not applicable n 7,0,0,288 d date 2,9,2004,7:58:00	vstem risoft\AV ed	G Freek	avgemc.(exe	•	Add Options

If not, you have to change the **AVG** applications' status. To do so, right click on every item and select the confirmation mark from the context menu.

Here is the list of all **AVG** applications that must always be allowed to connect to the internet:

- *avginet.exe* application for performing AVG online updates (located in the *Program Files/Grisoft/Avg7* directory by default)
- **avgemc.exe AVG E-mail Scanner** for anti-virus scanning of e-mail (located in the *Program Files/Grisoft/Avg7* directory by default)





Following two applications must be allowed to access the network when the workstation is a part of **AVG Remote Administration**:

- avgmsvr.exe AVG Alert Manager component (located in the Program Files/Grisoft/Avg7 directory by default)
- **avgcc.exe AVG Control Center** (located in the *Program Files/Grisoft/Avg7* directory by default)

And finally, when there are installed the control components of **AVG Remote Administration** on the workstation, the following applications must be also allowed to communicate over the network:

- avgadmin.exe the main control application of AVG Remote Administration, AVGADMIN (if the product is installed on your computer, it is located in the *Program Files/Grisoft/AvgAdmin7* by default)
- avgtcpsv.exe AVG TCP Server application for AVG Remote Administration (if the product is installed on your computer, it is located in the *Program Files/Grisoft/Avg TCP Server* by default)
- **avginetI.exe AVG InetLite** application (if installed, it is located in the *Program Files/Grisoft/Avg TCP Server* by default)
- Add a Program

If any of the needed applications described in the list above is missing in the **Programs** tab of the **ZoneAlarm Pro / Program Control** window, you have to add it manually. Press the **Add** button in the right-down corner of the window:

ZA ZoneAlarm F	Pro								
	TERNET OUT						All Sys	OGRAM tems A	S ctive
	Program Control			I	Aain	Pr	ograms	s C	(?) Help omponents
Overview	These are programs that have tried to access the	Active	Programs 🛦	Acc Trusted	ess Internet	Ser Trusted	r ver Internet	Send Mail	û
Firewall	Internet or local network.		AVG E-Mail Scanner	J	<u> </u>	J		J	
Program	columns show the	•	Generic Host Process for W	J	Ĵ	Ĵ	Ĵ	?	
Antivirus	has for each Zone.	•	Internet Explorer ILSA Shell (Export Version)	J	7	?	?	?	
Monitoring E-mail	Change a program's permissions by		Outlook Express	1	1	?	?	?	
Protection	the Access or Server		VNC Server for Win32	J	5	i i	Ĵ	?	
Privacy	column.		Windows NT Logon Applica	?	?	?	?	?	
ID Lock									
Alerts & Logs									
	. (Hide Text	File na Policy Last po Versio Create	Detail AVG Anti-Virus S; me F:VProgram Files/G Manually configure blcy update Not applicable n 7,0,0,268 d date 2,9,2004,7:58:00	vstem risoft\A∨ ed	'G Free's	avgemc.	exe	•	Add Options





? X rowse Look in: 💼 AVG7 💽 🔇 🤌 📂 🖽-🗂 avg 2 🗂 avgamsvr 🛃 avgcc avgemc avginet R 🛅 avgscan avgupdln 🔤 avgupsvc avgw My Documents E File name: -Open -Cancel Files of type: Applications (*.exe;*.com;*.icd)

Choose the desired application in the following dialog:

By default, the files are located in the Grisoft program folder (*Program Files/Grisoft/AVG7*, *Program Files/Grisoft/AvgAdmin7* or *Program Files/Grisoft/Avg TCP Server*), as described in the list in previous section.

E-mail Protection

In the *E-mail Protection* item (left menu), *Main* tab (top menu) you need to disable the built-in inbound/outbound email protection provided by the *Zone Alarm Pro*. By switching the *Zone Alarm Pro* implemented email verification off you will enable the more comprehensive **AVG** email control.

<mark>ZA</mark> ZoneAlarm F	Pro	
	TERNET OUT	TRUSTED All Systems Active
	E-mail Protection	(3) Help Main Attachments
Overview Firewall Program Control	MailSafe is an important supplement to antivirus software because it protects you from known as well as unknown viruses delivered via e-mail.	Inbound MailSafe Protection ○ On ⓒ Off File attachment protection is disabled
Antivirus Monitoring	MailSafe protects your computers from incoming e-mail attachments that	Outbound MailSafe Protection
E-mail Protection	may contain malicious	C On Off
Privacy ID Lock	code or viruses. MailSafe quarantines these attachments, preventing them from running	Outbound e-mail protection is disabled
Alerts & Logs	without your permission. Outbound MailSafe Protection halts outgoing e-mail for virus-like activity before it can do damage.	Advanced
	∢ Hide Text	



5. Microsoft ISA Server

Any network traffic is blocked by default after installation of *ISA Server*. If you want to allow **AVG** applications to connect to the network, you must create at least one rule in the *ISA Server* environment.

To create a rule, follow the steps below:

- Open the Microsoft ISA Server Main Configuration Window
- Launch the New Access Rule Wizard

Choose the *Microsoft Internet Security and Acceleration Server 2004* item in the main navigation tree located in the left side of the window. The name of your computer should be displayed here. Unpack it (for example by double-clicking on the computer's icon in the navigation tree) and choose the *Firewall Policy* item:



Go to the *Tasks* tab in the right side of the window then and choose the *Create New Access Rule* action. The wizard's window displays then.

• Proceed with the New Access Rule Wizard

Fill in the name of the new rule (e. g. AVG):





New Access Rule Wizard Microsoft Internet Security & Acceleration Server 2004	Welcome to the New Access Rule Wizard This wizard helps you create a new access rule. Access rules define the action that is taken, and the protocols that may be used, when specified clients from one network attempt to access specific destinations or content on
	Access rule name:
	To continue, click Next.
	< Back Next > Cancel

Choose the *Allow* option in the next window (the rule's purpose is to allow the **AVG** applications to communicate over the network):

New Access Rule Wizard		×
Rule Action Select how client requests for content from if the conditions specified in the rule are me	the specified destination are dealt with at.	
Action to take when rule conditions are met:		
 Allow 		
C Deny		
		-
	< <u>Back N</u> ext >	Cancel

In the following *Protocols* window choose the *Selected protocols* option in the This rule applies to field:





w Access Rule Wizard			
Protocols Select the protocols this rule applies to.			
This rule applies to:			
Selected protocols			•
<u>P</u> rotocols:			
			<u>A</u> dd
		_	<u>E</u> dit
			Remo <u>v</u> e
			Po <u>r</u> ts
		1	-
	< <u>B</u> ack	<u>N</u> ext >	Cancel

Use the *Add* button to open the tree menu with protocols available to add:

<u>N</u> ew -	Edit Delete	
₽ 20	Common Protocols DNS HTTP HTTPS HTTPS Server MAPS Server MSN Messenger Ping POP3 POP3 Server POP3S Server SMTP SMTP Server SMTPS Server Telnet Telnet Server Infrastructure	<u></u>

Choose the HTTP and *HTTPS* protocols in the *Add Protocols* window using the *Add* button.





When the station is a part of **AVG Remote Administration**, or when there are the **AVGADMIN** and/or the **AVG TCP Server** applications running on the station, you have to add also the TCP protocol as well.

However, any station may be in need of use of the TCP protocol under some circumstances (for example when performing an update from a local web server), so it is always recommended to add the TCP protocol connection!

The protocol is not in the list, so you must create a new protocol connection using the *New* button in the upper area of the *Add Protocols* window.

A *New Protocol Definition Wizard* launches then. Choose a name for the new protocol connection (e.g. **AVGADMIN**). Press the *New* button then. A *New/Edit Protocol Connection* window appears:

New/Edit Protoco	ol Connection		<u>?×</u>
Protocol type:	ТСР 💌	Protocol <u>N</u> umb	er: 6
Direction:	Outbound 💌		
Port Range	4156	<u>T</u> o:	4156
ICMP Properties		ICMP Type:	
	ОК	Cancel]

Choose the following values for the fields present:

- TCP Protocol type
- Outbound Direction
- Port Range from 4156 to 4156

Press the **OK** button to confirm the changes.

Do the same procedure of creating a new protocol connection once more then. All values remain the same except for the *Port Range*, which will be from *6051* to *6053* now.

The *New Protocol Definition Wizard* window with the protocol listing will now look like this:



		725	
Port Range	Protocol Type	Direction	N <u>e</u> w
4156	TCP	Outbound	
6051-6053	TCP	Outbound	Edi <u>t</u>

Press the *Next* button to continue.

In the next window with secondary connections prompt choose *No* and continue pressing the *Next* button. Complete the *New Protocol Definition Wizard* by clicking on the Finish button.

Now you can add the newly created protocol connection in the *Add Protocols* window:





<u>N</u> ew - Edit <u>D</u> elete	
🖃 🦾 Common Protocols	_
🖳 DNS	
Щ НТТР	
HTTPS	
HTTPS Server	
IMAPS Server	
MSN Messenger	
Ping	
POP3	
POP3 Server	
POP3S Server	
SMTP	
SMTP Server	
SMTPS Server	
Telnet	
Telnet Server	
🗄 🦲 Infrastructure	-

Your protocol is in the *User-Defined* folder of the tree menu here. Use the *Add* button to add it.

The *Protocols* window of the *New Access Rule Wizard* should look like this now:

w Access Rule Wizard			
Protocols Select the protocols this rule applies to.			
<u>This rule applies to:</u>			
Selected protocols			•
Protocols:			
Admin		Add	
HTTPS		<u>E</u> dit.	
		Remo	ve
		Po <u>t</u> ts	
	< Back	Next > 0	ancel
			ancer





Press the *Next* button to continue.

Choose the sources and destinations of data on selected ports in the next two windows. Use the *Add* button and select the *External*, *Localhost* and *Internal* (in case your *ISA Server* acts as gate for internet connection of other computers in your network) in the tree menu again.

Both of the sources and destinations windows should look like this then:

Access Rule Wizard		
Access Rule Destinations This rule will apply to traffic sent in this page.	from the rule sources to the destinations	specified
his rule applies to traffic sent to the External Internal Local Host	se destinations:	<u>A</u> dd <u>E</u> dit <u>R</u> emove
	< <u>B</u> ack <u>N</u> ext >	Cancel

Press the *Next* button to continue and complete the wizard by clicking on the *Finish* button.

Save the changes in the *Firewall policy* by clicking on the *Apply* button that is located above the rule list.

Microsoft ISA Server should be configured properly in order to allow all AVG applications to communicate over the network now.





6. Agnitum Outpost Firewall

You may be asked to allow network connection for some applications during their start up after installation of the product. This is related to **AVG** products as well.

You can set up the firewall so that it will permanently allow network communication for all **AVG** applications. Doing this you will definitely not decrease the level of protection of your system. On the contrary, **AVG** will be enabled to fully employ all of its functions then, bringing the reliability of your anti-virus protection to maximum.

6.1. Allowing Activities for an Application

The firewall will react whenever an unknown application is trying to make a network connection. This holds even for **AVG** applications before setting them up manually. The following window is displayed (for **AVG Control Center** in this example):

Ireate	rule for AVGCC.EXE
	AVG Control Center Application is requesting an outbound connection
	Remote Service: TCP:4156
	Remote Address: 192.168.104.237
	Allow all activities for this application
	C Stop all activities for this application
	C Create rules using preset Custom
	Create rules using preset
A	llow Once Block Once OK

Choose the *Allow all activities for this application* option and press the *OK* button. Perform the same action whenever a similar **AVG** related window appears.

6.2. Configuring the Firewall at Once

However, you should allow the **AVG** applications to access the network even before they try to open a connection. If you want to allow the network communication for **AVG** applications (recommended!) at once, open the **Agnitum Outpost Firewall** main window:







Add the allowed applications by right-clicking on the *Plugins* item in the main navigation tree. Choose the *Options* menu item then. A new window will open then. Go to the *Applications* tab in the window:

General Applicatio	n System Policy	Plug-Ins	
<u>S</u> ettings:			
MOBSYN	NC.EXE		<u>A</u> dd
MSIMN.E	EXE		
)K.EXE		<u>R</u> emove
	ST.EXE		1
REGWIZ	.EXE		<u>E</u> dit ▼
	.32.EXE		
	I.EXE		
	LT.EXE		
Trusted ap	plications (6)		
AVGADN	IIN.EXE		
🔄 🛅 AVGAMS	SVR.EXE		
AVGCC.	EXE		
AVGEM0	C.EXE		Hidden Proc
AVGINE	T.EXE		<u> </u>
AVGTCF	SV.EXE	_	Lomponents

Add all AVG applications currently installed on your computer using the Add button.

Here is the list of all **AVG** applications that must always be allowed to connect to the internet:





- avginet.exe application for performing AVG online updates (located in the *Program Files/Grisoft/Avg7* directory by default)
- **avgemc.exe E-mail Scanner** for anti-virus scanning of e-mail (located in the *Program Files/Grisoft/Avg7* directory by default)

Following two applications must be allowed to access the network when the workstation is a part of **AVG Remote Administration**:

- avgmsvr.exe AVG Alert Manager component (located in the Program Files/Grisoft/Avg7 directory by default)
- **avgcc.exe AVG Control Center** (located in the *Program Files/Grisoft/Avg7* directory by default)

And finally, when there are installed the control components of **AVG Remote Administration** on the workstation, the following applications must be also allowed to communicate over the network:

- avgadmin.exe the main control application of AVG Remote Administration, AVGADMIN (if the product is installed on your computer, it is located in the *Program Files/Grisoft/AvgAdmin7* by default)
- avgtcpsv.exe AVG TCP Server application for AVG Remote Administration (if the product is installed on your computer, it is located in the *Program Files/Grisoft/Avg TCP Server* by default)
- **avginetI.exe AVG InetLite** application (if installed, it is located in the *Program Files/Grisoft/Avg TCP Server* by default)

Commit your selection by pressing the *OK* button. All **AVG** applications requiring the network communication should be fully operational then.





7. Sygate Personal Firewall

You may be asked to allow network connection for some applications during their start up also after installation of the *Sygate Personal Firewall* product. This is related to **AVG** products as well.

You can set up the firewall so that it will permanently allow network communication for all **AVG** applications. Doing this you will definitely not decrease the level of protection of your system. On the contrary, **AVG** will be enabled to fully employ all of its functions then.

7.1. Allowing Activities for an Application

The firewall will react whenever an unknown application is trying to make a network connection. This holds even for **AVG** applications. The following window is displayed (for **AVG Control Center** in this example):

Sygate Per	sonal Firewall 02/02/2005 10:27:49			×
	AVG Control Center (avgcc.exe) is trying to Do you want to allow this program to acce	o connect to [192.168.] ss the network?"	104.237] using remote	e port 4156.
I	ember my answer, and do not ask me n for this application.	Yes	No	<u>D</u> etail >>

Check the *Remember my answer*... field and press the *Yes* button. Repeat the action for any **AVG** application that tries to connect the network.

7.2. Configuring the Firewall at Once

If you want to allow the network communication for **AVG** applications at once (recommended!), open the *Sygate Personal Firewall* main window:





Sygate Pe	ersonal Firewa	all Pro				
ile <u>S</u> ecurity	<u>I</u> ools <u>V</u> iew	<u>H</u> elp				
) Block All	Applications	Logs	Security Test	3 Help		
Incoming OB OB	100B	Incoming Tra	Affic History	10	Attack History Graph	
Outgoing OB OB	100B	Outgoing Tra	Iffic History	0		
Running App	plications :			Hide <u>W</u> indows	s Services 🗹 Hide <u>B</u> roadcas	t Traffic
[₩Základr [₩AVG Alı	ní součást jádra ert Manager	Win32	<mark>או</mark> AVG Contro או WIN32 Netנ	l Center work Interface	Service Process	
ecurity Status	: Normal		Show <u>M</u> essage Co	nsole		

Select the *Advanced Rules* menu item in the *Tools* folder of the main application menu. A new window will open then:

💋 Advanced Rules 👘				
Description	Host	Ports and Protocols		
✓ AVG Internet Traffic A	All hosts		All ports and protocols	
•			•	
Add <u>R</u> emov	/e <u>E</u> dit	Remove	All 1	
		OK	Cancel	

You can create a new rule for the **AVG** applications using the **Add** button in the **Advanced Rules Settings** window. Go to the **Applications** tab first:





Distributed COM Serv	4.71.2900	c:\windows	\system\rpc	ss.exe	
WIN32 Network Inter	4.10.1998	c:\windows	\system\mpi	rexe.exe	
🗖 🛅 Spooler Sub System	4.10.1998	c:\windows	\system\spa	ol32.exe	
AVG TCP Server	7.1.0.295	C:\Program	Files\Grisoft	VAVG TCP S	erve
🗹 🎞 AVG Update downloa	7.0.0.298	c:\Program	Files\Grisoft	\AVG7\avgin	iet.e:
🗹 🗂 AVG Alert Manager	7.0.0.297	c:\Program Files\Grisoft\AVG7\avgamsvr.			
🗹 🗂 AVG Control Center	7.0.0.298	c:\Program Files\Grisoft\AVG7\avgcc.exe			
AVGADMIN Application	7.1.0.296	c:\Program	Files\Grisoft	\AvgAdmin7\	avg
•					►
<u>S</u> elect All	<u>C</u> lear /	All	B	rowse	
Rule Summary: This rule will allow both incoming protocols. This rule will be applic recorded in the 'Packet Log'. Ti TCP Server AVG Update downli	g and outgoing tr ed to all network he following app oader,AVG Alert	raffic from/to a interface car lications will b Manager,AV(all hosts on a ds. This tra affected in & Control	II ports and ffic will be a this rule: AVI	G

Add all **AVG** applications currently installed on your system using the *Browse* button.

Here is the list of all **AVG** applications that must always be allowed to connect to the internet:

- *avginet.exe* application for performing AVG online updates (located in the *Program Files/Grisoft/Avg7* directory by default)
- **avgemc.exe AVG E-mail Scanner** for anti-virus scanning of e-mail (located in the *Program Files/Grisoft/Avg7* directory by default)

Following two applications must be allowed to access the network when the workstation is a part of **AVG Remote Administration**:

- avgmsvr.exe AVG Alert Manager component (located in the Program Files/Grisoft/Avg7 directory by default)
- avgcc.exe AVG Control Center (located in the Program Files/Grisoft/Avg7 directory by default)

And finally, when there are installed the control components of **AVG Remote Administration** on the workstation, the following applications must be also allowed to communicate over the network:

 avgadmin.exe – the main control application of AVG Remote Administration, AVGADMIN (if the product is installed on your computer, it is located in the *Program Files/Grisoft/AvgAdmin7* by default)





- avgtcpsv.exe AVG TCP Server application for AVG Remote Administration (if the product is installed on your computer, it is located in the *Program Files/Grisoft/Avg TCP Server* by default)
- avginetl.exe AVG InetLite application (if installed, it is located in the Program Files/Grisoft/Avg TCP Server by default)

Go to the *General* tab then:

😥 Advanced Rule Settings	×
General Hosts Ports and Protocols Scheduling Applications	
AVG Internet Traffic Allowance	
Action :	
C Block this traffic C Allow this traffic	
Advanced Settings :	
Apply Rule to Network Interface	
All network interface cards	
Apply this rule during Screensaver Mode Both on and off	
Record this traffic in "Packet Log"	
Rule Summary: This rule will allow both incoming and outgoing traffic from/to all hosts on all ports and protocols. This rule will be applied to all network interface cards. This traffic will be recorded in the 'Packet Log'. The following applications will be affected in this rule: AVG TCP Server,AVG Update downloader,AVG Alert Manager,AVG Control Center,AVGADMIN Application.	
OK Storno	

You have to allow any network communication for the selected **AVG** applications by selecting the *Allow this traffic* option.

Commit the rule creation by pressing the *OK* button. All **AVG** applications requiring the network communication should be fully operational then.



8. Kerio Winroute Firewall

AVG update downloading and email scanning is working properly with the default settings of *Kerio Winroute Firewall*.

However, if the station is incorporated into **AVG Remote Administration** or if **AVGADMIN** with **AVG TCP Server** are running on the computer, it is necessary to create a new rule of traffic policy then:

🚳 localhost - Administration Conso	le for Kerio WinRoute Firewall				(
File Help						
🐏 Kerio WinRoute Firewall 🖃 🧊 Configuration	Traffic Polic	;y				
📷 Interfaces 🐌 Traffic Policy 💯 DHCP Server 🚓 DNS Forwarder	Name	Source	Destination	Service	Action	
⊕ 😋 Content Filtering ⊜ ∰ Definitions — 😭 Address Groups		-		*** TCP 6051 *** TCP 6052 *** TCP 6053		
@ Time Ranges 	ICMP traffic Image: Compare the second sec	 Firewall Firewall 	💠 Any 💠 Any	も Ping 아 HTTPS 같 TCP 6000	✓ ✓	
Bouting Table Acgs & Alerts Advanced Options Status Constant Groups Constant Groups Constant Groups Constant Groups	🗹 Firewall Traffic 🔎	🚯 Firewall	📇 Local Area Connection	DNS FTP HTTP HTTPS MAP POP3 SMTP Telnet	-	
	Add Bemove	I ocal área Connection	Firewall	stent	₩izard	¥
				Apply		Reset
🧞 Kerio WinRoute Firewall / Configuration / Traffic Policy 🛛 📑 localhost:44333 🛛 🤱 Admin 🛛 📇 Ready 👘						

For full functionality of **AVG Remote Administration** you have to allow any source and destination for the following ports: *4156*, *6051*, *6052*, *6053*.





9. Technical Support

Should you have any further problems with your **AVG** product, please refer to the *FAQ section* of the *Grisoft* website at <u>http://www.grisoft.com</u>.

If you do not succeed in finding help this way, contact the technical support department at technicalsupport@grisoft.com. Be sure to include your **AVG** license number in the body of the e-mail.

