Blocking external connections to DC++ using the Kaspersky Firewall

1. Open up the main Kaspersky window. In the list of items under Protection on the left, click on "Firewall". Then in the window that has appeared on the right, click on configure.



2. In the window that shows up, click on Settings in the "Filtration System" section as shown.

K Settings: Kaspersky Internet	Security
 Protection File Anti-Virus Mail Anti-Virus Web Anti-Virus Proactive Defense Firewall Privacy Control Anti-Spam Parental control Scan Critical areas My Computer Startup objects Rootkit scan Threats and exclusions Update Proxy server Traffic monitoring Reports and data files Service Appearance 	Firewall ✓ Enable Firewall - Filtration system ✓ Enable filtration system - Low Security - Allow the network activity of all applications - except those explicitly prohibited by - except those except those explicitly prohibited by - except those except th
🔞 <u>Help</u>	OK Close Apply

3. If you can find DC++ on the list of Applications, then click on it and remove it from the list. Then click Add to the right. Otherwise, just click Add straight away, Choose Browse navigate to the DC++ program (normally in C:\Program Files\DC++)

K	Settings: Firewa	au -			
٢	Rules for applications	Rules for packet	filtering Zones	Additio	nal
	Group rules by app	lication			
	Application	Numbe	e Folder	<u></u>	Add
	vchost.exe	19	C:\WINDOWS		Browse
	🗹 🛅 alg.exe	3	C:\WINDOWS	\ [−]	
	🗹 🛅 dwwin.exe	2	C:\WINDOWS		Applications
	🗹 🛅 regwiz.exe	2	C:\WINDOWS		
	🔽 🛅 rdpclip.exe	3	C:\WINDOWS\		
	🔽 🔦 mstsc.exe	3	C:\WINDOWS\		
	🔽 🛅 sessmgr.exe	2	C:\WINDOWS	1	
	🔽 🥘 mobsync.exe	2	C:\WINDOWS		
	🗹 🛅 wuauclt.exe	2	C:\WINDOWS		
	🗹 📄 rundll32.exe	6	C:\WINDOWS		
	🔽 📩 spoolsv.exe	2	C:\WINDOWS		
	🔽 🛐 msimn.exe	8	C:\Program File	ε	
	🔽 🧕 explorer.exe	5	C:\WINDOWS		
	🔽 🎽 iexplore.exe	11	C:\Program File	e	
	🔽 🧕 firefox.exe	8	C:\Program File	e r	Export
	🔽 🥅 ftp.exe	3	C:\WINDOWS		Export
	<	_	>	i l	Import
	🕑 <u>Help</u>		ОК		Cancel

4. Click on DCPlusPlus.exe and click Open

📕 Se	ettings: Kaspersl	ky Internet Secu	rity					
	Protect 🔀 Settin	gs: Firewall						block
	File Rules for	applications Rules	for packet filtering Zones	Additio	nal			
	Please specify	the executable r	module				?	\mathbf{X}
	Look in:	🗁 DC++		~	0) 📂 🗉]-	
	Recent	FileLists CJCPlusPlus.exe						
	Desktop	uninstall.exe						
	My Documents							
 	My Computer							
		File name:	DCPlusPlus.exe			~	Open	
0	My Network	Files of type:	Executable files (*.exe)			~	Cancel	<u>.</u> .

5. A new window should appear in which you can specify the rules for DC++ itself. First give the rule a name (this can be anything you like). Next tick the box for Remote IP Address **ONLY**.

📕 New rule	×
Rule name: Properties:	DC++ Block Remote IP address Remote port Local port Time range
Additional action: Rule description (clict	Notify user
Allow Inbound & Ou Remote IP addres	itbound TCP connections, where: is: Enter IP address.
lep Help	OK Cancel

Next, click on where it says "Enter IP Address" in bold.

6. Select "Range of IP addresses" at the top, and enter the 3 ranges one at a time, clicking add after each one to add it to the list at the bottom. 0.0.0-126.254.254.254, 127.0.0.2-136.254.254.254 and

	138.0.0.	.0-254.254.254	The order y	you add them	in is	unimportant
--	----------	----------------	-------------	--------------	-------	-------------

📕 Specify address	×
Address type: IP address Range of IP addresses Subnet address Address: Begins at: Ends on: 138 , 0 , 0 , 0 	4
List of addresses: 138.0.0.0-254.254.254.254 Add 127.0.0.2-136.254.254.254 Delet 0.0.0.0-126.254.254.254 Delet	e
Canc	el

Then click OK to close the window

7. Finally you should be presented with a summary of the rule you just created. By default this is an "Allow" rule, so to change it to a block rule, just click on where it says "Allow" in blue underlined in the Rule description section. The text should change to Block and the icon next to the rule should change to an exclamation mark on a red circle as shown below.

K Edit rules for DCPlusP	lus.exe	\mathbf{X}
DC++ Block		Add Edit Delete
		Move up Move down
Rule description (click underline Block Inbound & Outbound TC Remote IP address: <u>138.0.0</u> <u>136.254.254.254</u> , 0.0.0.0-120	parameters to edit): connections, where: .0-254.254.254.254, 127.0. 5.254.254.254.	<u>0.2-</u>
Command line	ОК	Cancel

8. Finally Click on Template, and click "Allow All" to allow everything except the blocked ranges you have just inputted.

Now just OK out of all of the settings, and everything should be set up.