Using Comodo Personal Firewall to block external connections to DC++

Comodo is a bit tricky to configure properly, as it had a nasty habit of removing old firewall rules when adding new ones. So you may need to repeat some of these steps if you find it is being a pain.

1. First close DC++. Configuring the rules with it open may mean they get over written when you do next close it.

2. Open the main Comodo window and go to "*Network Security Policy*" under 'Advanced tasks of the Firewall'.

😂 COMODO Firewall Pro 📃	
C·O·M·O·D·O Firewall Professional Summary Firewall	
Prewall Tasks Network Security Policy Common Tasks Define and Network Security Policy	dify
Advanced Predefined Firewall Policies Configure a Predefined Firewall Policy by creating a set of firewall rules which can be shared by more than or application.	ne
Attack Detection Settings This section allows you to configure the Firewall's Denial of Service (DoS) protection settings.	
Firewall Behavior Settings Access and configure various firewall options such as security level, alert frequency level and more.	
Image: All systems are active and running.	

This will bring up the '*Application Rules*'. Scroll down to any existing DC++ rules and remove them.

😻 Network Security Policy		
Application Rules Global Rules		
Application Name TreatAs		<u>A</u> dd
🖃 📩 %windir%\system32\svchost.exe Outgoing Only		
- Allow Outgoing TCP or UDP Requests		<u>E</u> dit
Block and Log All Unmatching Requests		Remove
System Outgoing Only		<u>V</u> eniove
— 🥪 Allow Outgoing TCP or UDP Requests		Move Up
Block and Log All Unmatching Requests		
C:\Program Files\MSN Messenger\msnmsgr.exe Custom		Move <u>D</u> own
Allow IP Out From IP Any To IP Any Where Protocol Is Any	≡	
🖃 🧐 C:\Program Files\Mozilla Firefox\firefox.exe Custom		Purge
Allow IP Out From IP Any To IP Any Where Protocol Is Any		
🖃 🕡 C:\Program Files\CA\CA Internet Security Suite\ccupdate\ccupd Custom		
Allow IP Out From IP Any To IP Any Where Protocol Is Any		
C:\Program Files\DC++\stunnel\stunnel.exe Custom		
Allow IP Out From IP Any To IP Any Where Protocol Is Any	-	
What do these settings do?	ply	Cancel

3. Click on '*Add*' and select the path to the DC++ application on your computer.

Application Notwork Ac	control		
S Application Network Ac	cess Control		
Application Path:			
C:\Program Files\DC++\DCPlusl	Plus.exe		Select 🔹
Mahuradi, Anna an Dadan			
INECWORK ACCESS RUles			
🔘 Use a Predefined Policy	Blocked Application	-	
(a) Ice a Custom Policy	Copy From		
	Copy from		

4. Now click '*Add*' to add a custom policy for this application. Configure it to Allow all TCP or UDP connections (In/Out) naming it as 'Localhost Allow'. Then leaving the Source Address, Source Port and Destination Port as is, set it to allow 127.0.0.1 under '*Destination Address*' and click Apply. (This is shown in the figure below)

😻 Network Contr	ol Rule			
General				
Action :	Allow 🔽	🔲 Log as a firewa	all event if this rule is fired	
Protocol :	TCP or UDP 🛛 🔽			
Direction :	In/Out 🗾 🔽			
Description :	Localhost Allow			
Source Address	Destination Addres	ss Source Port	Destination Port	
🔲 Éxclude (i.e.	NOT the choice below))		
O Any	IP:	127 . 0 .	0.1	
Single IP				
🔘 IP Range				
🔘 IP Mask				
🔘 Zone				
🔘 Host Name				
MAC Address				
What do these set	ettings do?		Apply Can	tel

5. Add another rule and configure it to Allow all TCP or UDP connections (In/Out) naming it as 'Resnet Allow'. Then leaving the Source Address, Source Port and Destination Port as is, set it to allow the range 137.205.0.0 - 137.205.140.0 under '*Destination Address*' and click Apply. (This is shown in the figure below)

_			
()	Network Cont	rol Rule	×
6	-General		
	Action :	Allow 📃 🔲 Log as a firewall event if this rule is fired	
	Protocol :	TCP or UDP	
	Direction :	In/Out 🗾	
	Description :	Resnet Allow	
	Source Address	Destination Address Source Port Destination Port	
	🔲 Exclude (i.e.	NOT the choice below)	
	O Any	Start IP: 137 . 205 . 0 . 0	
	🔘 Single IP		
	🧿 IP Range	End IP: 137 . 205 . 140 . 0	
	🔘 IP Mask		
	🔘 Zone		
	🔘 Host Name		
	MAC Address	s	
	What do these s	settings do? Cancel	

6. Add another rule and configure it to Block all TCP or UDP connections (In/Out) naming it as Block 1. Then leaving the Source Address, Source Port and Destination Port as is, set it to allow the range 0.0.0.1 - 127.0.0.0 under '*Destination Address*' and click Apply. (This is shown in the figure below)

😻 Network Control F	Rule			X
General				
Action : Bloc	:k 🔽 🛙	Log as a firewall	event if this rule is	fired
Protocol : TCP	or UDP 🔽			
Direction : In/C	Dut 🔽			
Description : Blo	ck 1			
Source Address D	estination Address	Source Port	Destination Port	
🔲 Exclude (i.e. NOT	the choice below)			
O Any	Start IP:	0.0.0), 1	
Single IP				
IP Range	End IP:	127 . 0 . 0).0	
🔘 IP Mask				
Zone				
O Host Name				
MAC Address				
What do these settin	i <u>qs do?</u>	[Apply	Cancel

7. Add another rule and configure it to Block all TCP or UDP connections (In/Out) naming it as Block 1. Then leaving the Source Address, Source Port and Destination Port as is, set it to allow the range 127.0.02 - 137.205.0.0 under '*Destination Address*' and click Apply. (This is shown in the figure below)

		10 M M	A CONTRACT OF A	
😻 Network Conti	rol Rule			X
-General				
Action :	Block 🗾	🔲 Log as a firewall	event if this rule is fire	d
Protocol :	TCP or UDP 🗾			
Direction :	In/Out 🗾			
Description :	Block 2			
Source Address	Destination Addre	ess Source Port	Destination Port	
🔲 Exclude (i.e.	NOT the choice below	∾)		
O Any	Start IP:	127 . 0 . 0	0.2	
Single IP				
🧿 IP Range	End IP:	137 . 205 .	. 0	
🔘 IP Mask				
Zone				
🔘 Host Name				
O MAC Address	;			
What do these s	ettings do?		Apply Ca	ncel

8. Add another rule and configure it to Block all TCP or UDP connections (In/Out) naming it as Block 1. Then leaving the Source Address, Source Port and Destination Port as is, set it to allow the range 137.205.140.0 – 255.255.255.255 under '*Destination Address*' and click Apply. (This is shown in the figure below)

		and the second sec		
😻 Network Conti	rol Rule			X
-General				
Action :	Block 🗾	🔲 Log as a firewall	event if this rule is fired	
Protocol :	TCP or UDP			
Direction :	In/Out 🗾 🔽			
Description :	Block 3			
Source Address	Destination Addre	ss Source Port	Destination Port	
🔲 Exclude (i.e.	NOT the choice below	ı)		
O Any	Start IP:	137 . 205 . 14	1 0.0	
Single IP				
😐 IP Range	End IP:	255 . 255 . 25	55 . 255	
🔘 IP Mask				
Zone				
🔘 Host Name				
MAC Address	;			
What do these s	ettings do?		Apply Cano	:el

Now Click apply and you are done! You can now start DC++.



One thing I noticed while configuring Comodo was its Global rules setup. This will override all Application rules. Now you may not have to do this, but in case you can not download for any reason, do check the Global Rules. If you see something you are not familiar with do ask the Ops for assistance. But if you see something along the lines of "Block IP In From IP Any To IP Any Where Protocol Is Any" or "Block TCP In From IP Any To IP Any Where Protocol Is Any" then select and delete this rule.