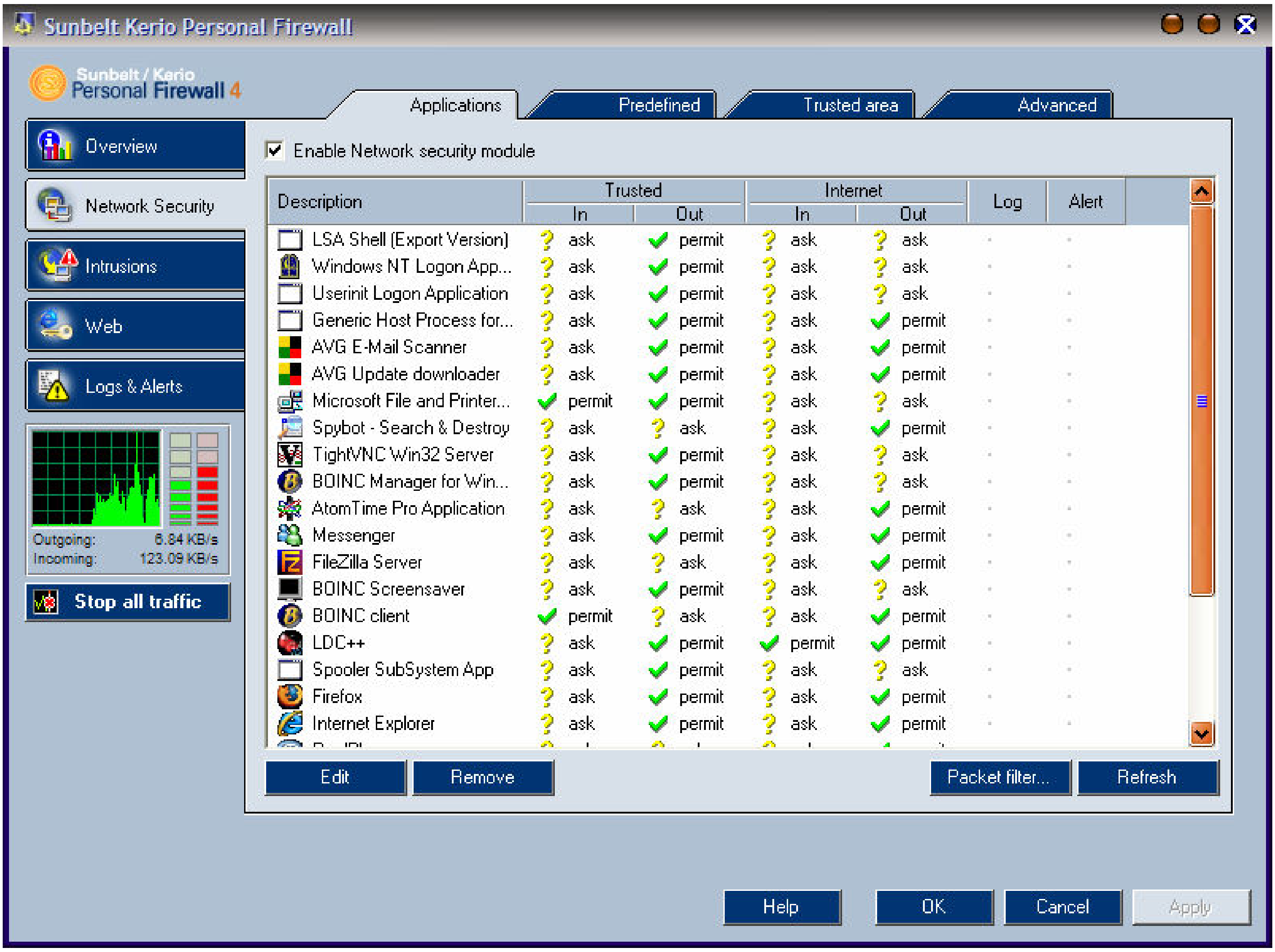
Instructions for Blocking external connections to DC++ using the Kerio Personal Firewall (v4.2.3)

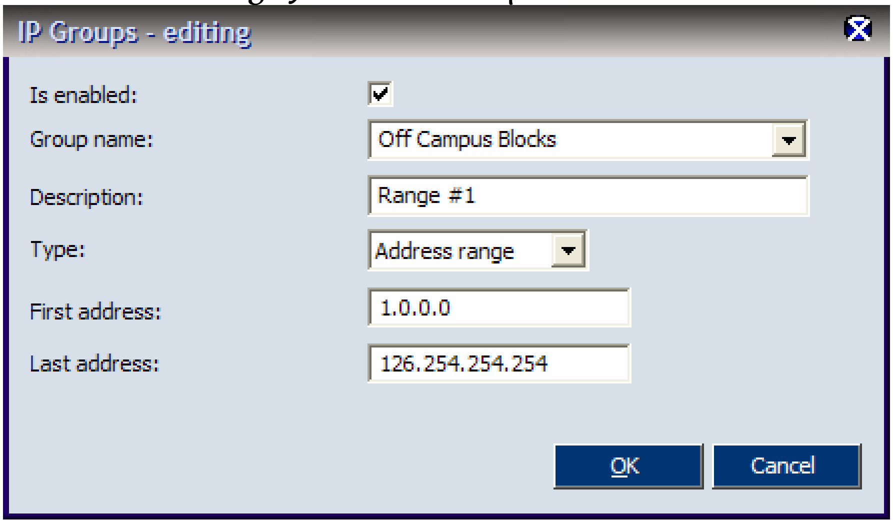
1. Open up the main Kerio Firewall window and go to the Network Security section on the left. Make sure the Applications tab is selected and click on 'Packet Filter' underneath the list of programs



☑ Enable Network security module

Description	Trusted		Internet		Log	Alert
	In	Out	In	Out		
LSA Shell (Export Version)	? ask	✓ permit	? ask	? ask	·	·
Windows NT Logon App...	? ask	✓ permit	? ask	? ask	·	·
Userinit Logon Application	? ask	✓ permit	? ask	? ask	·	·
Generic Host Process for...	? ask	✓ permit	? ask	✓ permit	·	·
AVG E-Mail Scanner	? ask	✓ permit	? ask	✓ permit	·	·
AVG Update downloader	? ask	✓ permit	? ask	✓ permit	·	·
Microsoft File and Printer...	✓ permit	✓ permit	? ask	? ask	·	·
Spybot - Search & Destroy	? ask	? ask	? ask	✓ permit	·	·
TightVNC Win32 Server	? ask	✓ permit	? ask	? ask	·	·
BOINC Manager for Win...	? ask	✓ permit	? ask	? ask	·	·
AtomTime Pro Application	? ask	? ask	? ask	✓ permit	·	·
Messenger	? ask	✓ permit	? ask	✓ permit	·	·
FileZilla Server	? ask	? ask	? ask	✓ permit	·	·
BOINC Screensaver	? ask	✓ permit	? ask	? ask	·	·
BOINC client	✓ permit	? ask	? ask	✓ permit	·	·
LDC++	? ask	✓ permit	✓ permit	✓ permit	·	·
Spooler SubSystem App	? ask	✓ permit	? ask	? ask	·	·
Firefox	? ask	✓ permit	? ask	✓ permit	·	·
Internet Explorer	? ask	✓ permit	? ask	✓ permit	·	·

2. In the window that opens up, select the IP Groups tab at the top, and then click Add. In the box that shows up, choose a name and description for the IP range (completely arbitrary so choose what you like). In the drop down box for 'Type', choose Address Range
Next add the starting and ending addresses.
The first range you want to input is 1.0.0.0 - 126.254.254.254 as below

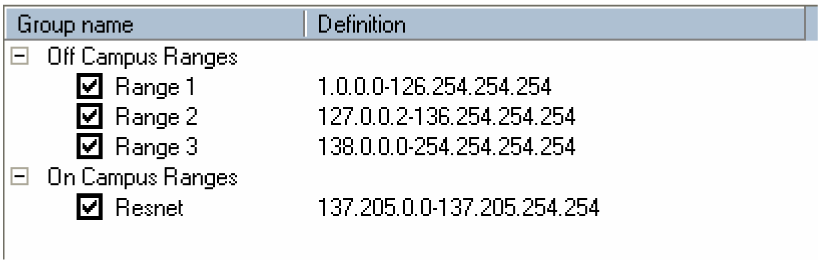


IP Groups - editing

Is enabled:	☑
Group name:	Off Campus Blocks
Description:	Range #1
Type:	Address range
First address:	1.0.0.0
Last address:	126.254.254.254

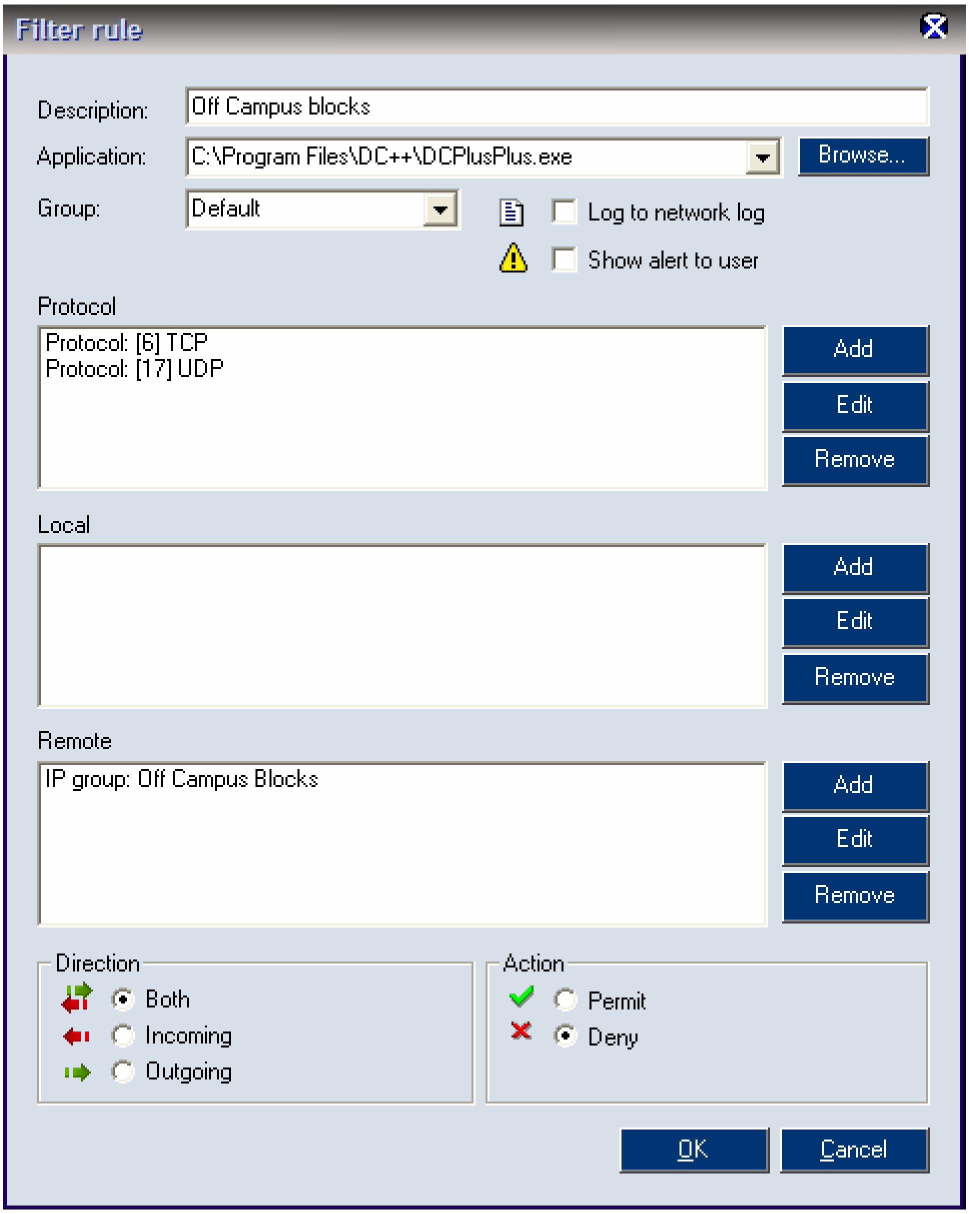
Once this is added, click on Add again to add the next range of IPs. First select the Group Name you chose before and then choose a name for this block. Again, choose Address Range as the Type. The range this time should be 127.0.0.2 - 136.254.254.254
Repeat this process one more time and add the final range as 138.0.0.0 - 254.254.254.254.
If you click on the '+' next to the Group you just created, the window you get ought to look something like this:

You also need to add a group for the Resnet itself to allow you to search/download whilst on the hub. Once again, click on Add, and now choose a different Group Name (something obvious). Again set it to Address Range and set the First Address as 137.0.0.0 and the Last Address as 137.205.254.254



Group name	Definition
⊟ Off Campus Ranges	
☑ Range 1	1.0.0.0-126.254.254.254
☑ Range 2	127.0.0.2-136.254.254.254
☑ Range 3	138.0.0.0-254.254.254.254
⊟ On Campus Ranges	
☑ Resnet	137.205.0.0-137.205.254.254

3. Next, go back to the Filter rules tab (You will be prompted to save the previous rules, do so) and click on Add to the lower left.
   Again, choose a description for the rule (doesn't need to be the same as before). Next, click on browse next to the Application box and navigate to and select the DC++ executable.
   In the Protocol Section, click 'Add' and select TCP from the drop down list. Do this again and select UDP.
   Next, in the Remote section, click 'Add' and select 'Add IP group' and choose the IP Group you created in part 2 of this guide for Off Campus people.
   Make sure that 'Both' is selected in the Direction box at the bottom and that Deny is selected in the Action section
   You should end up with it looking something like:



Filter rule

Description: Off Campus blocks

Application: C:\Program Files\DC++\DCPlusPlus.exe

Group: Default

□ Log to network log

□ Show alert to user

Protocol

Protocol: [6] TCP
Protocol: [17] UDP

Local

Remote

IP group: Off Campus Blocks

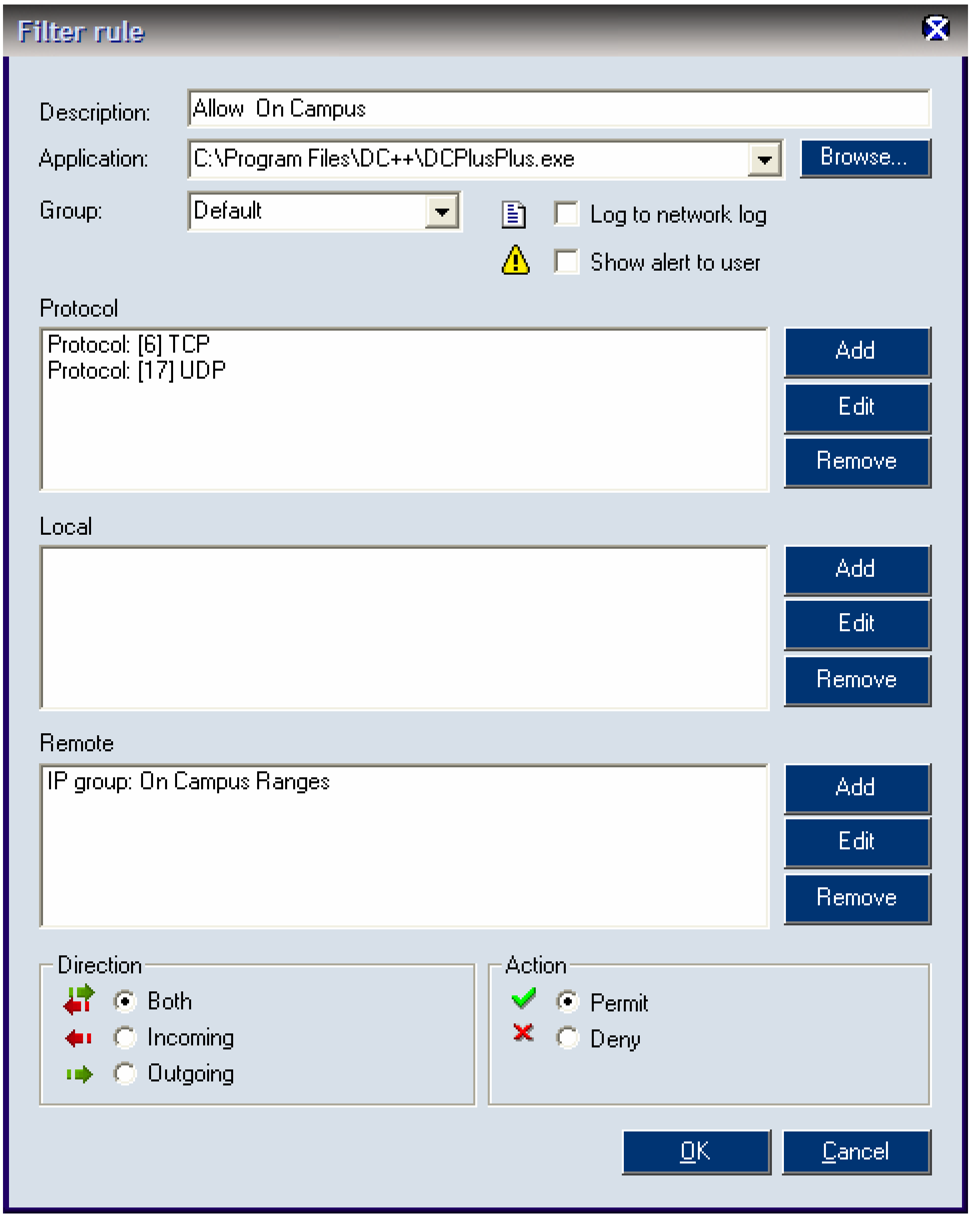
Direction

● Both
○ Incoming
○ Outgoing

Action

○ Permit
● Deny

4. To allow DC to download from on campus people, you need to create a new rule for DC++. In Filter Rules, click Add again. Again, choose another Description (technically arbitrary, but it might be an idea to make it somewhat useful). Select DC++ as the application and add in TCP and UDP as protocols as before.
This time however, in the Remote section, click Add and choose your IP group for On Campus IPs.
The boxes at the bottom should be set to Both and Permit giving you something as below



Filter rule

Description: Allow On Campus

Application: C:\Program Files\DC++\DCPlusPlus.exe

Group: Default

☐ Log to network log

☐ Show alert to user

Protocol

Protocol: [6] TCP
Protocol: [17] UDP

Local

Remote

IP group: On Campus Ranges

Direction

● Both
○ Incoming
○ Outgoing

Action

● Permit
○ Deny

Make sure all the rules are saved and leave the firewall settings

Congratulations, your DC++ client ought to no longer accept connections from anybody off campus and let you download freely on campus