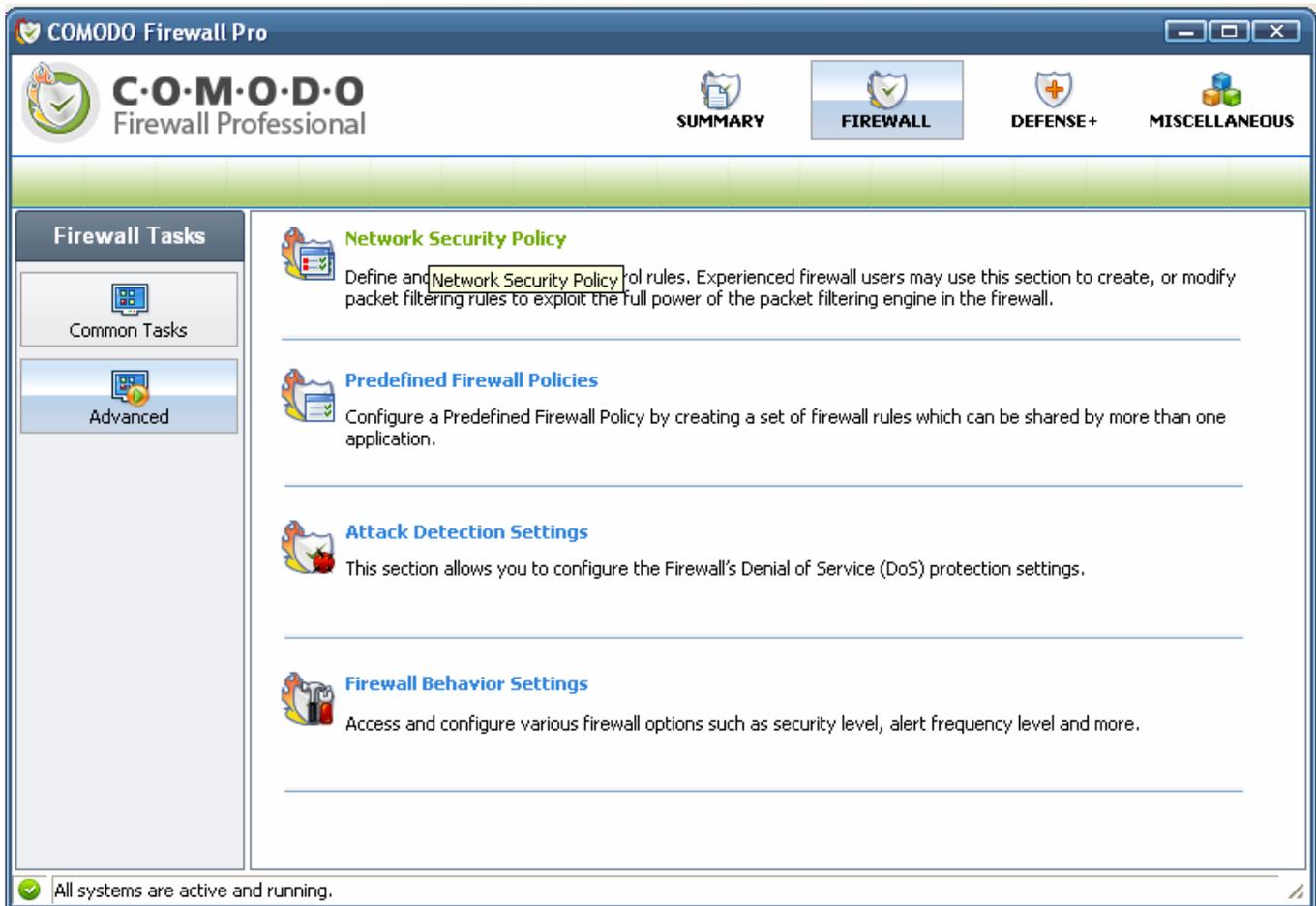


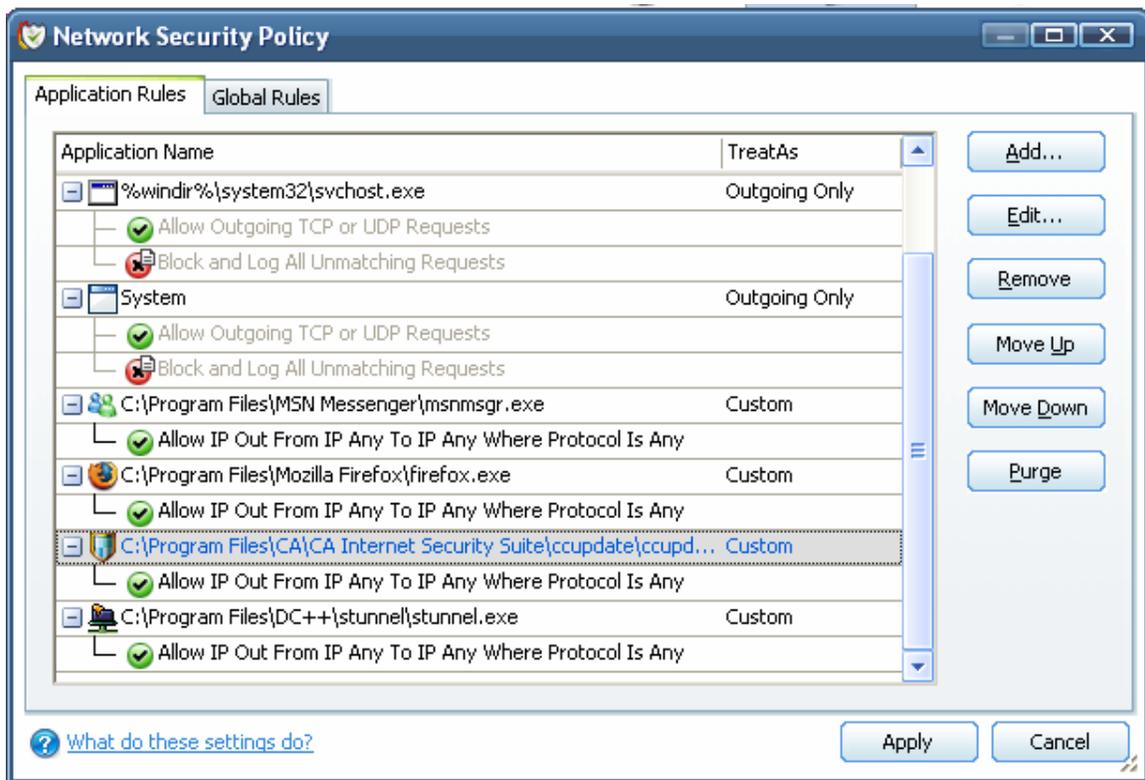
## Using Comodo Personal Firewall to block external connections to DC++

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.

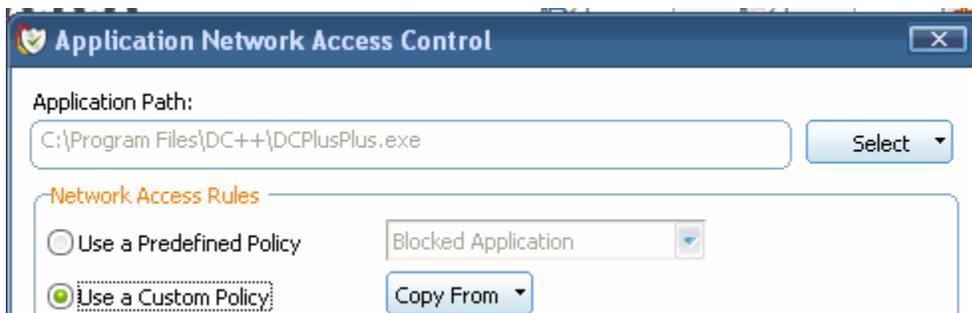
1. First close DC++. Configuring the rules with it open may mean they get over written when you do next close it.
2. Open the main Comodo window and go to “*Network Security Policy*” under ‘Advanced tasks of the Firewall’.



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



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



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)

The screenshot shows a 'Network Control Rule' dialog box with the following configuration:

- General** tab is selected.
- Action**: Allow (dropdown menu)
- Log as a firewall event if this rule is fired**:
- Protocol**: TCP or UDP (dropdown menu)
- Direction**: In/Out (dropdown menu)
- Description**: Localhost Allow (text field)

Below the General tab, the **Destination Address** sub-tab is selected:

- Exclude (i.e. NOT the choice below)
- Any
- Single IP (Selected)
- IP Range
- IP Mask
- Zone
- Host Name
- MAC Address

The **IP** field is set to 127 . 0 . 0 . 1.

At the bottom, there is a help link: [? What do these settings do?](#) and two buttons: **Apply** and **Cancel**.

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 Control Rule**

**General**

Action :   Log as a firewall event if this rule is fired

Protocol :

Direction :

Description :

**Destination Address**

Exclude (i.e. NOT the choice below)

Any

Single IP

IP Range

IP Mask

Zone

Host Name

MAC Address

Start IP:

End IP:

[? What do these settings do?](#)

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 Rule**

**General**

Action :   Log as a firewall event if this rule is fired

Protocol :

Direction :

Description :

**Destination Address**

Exclude (i.e. NOT the choice below)

Any

Single IP

IP Range

IP Mask

Zone

Host Name

MAC Address

Start IP:

End IP:

[? What do these settings do?](#)

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 127.0.0.2 – 137.205.0.0 under 'Destination Address' and click Apply. (This is shown in the figure below)

**Network Control Rule**

**General**

Action :   Log as a firewall event if this rule is fired

Protocol :

Direction :

Description :

Source Address | **Destination Address** | Source Port | Destination Port

Exclude (i.e. NOT the choice below)

Any

Single IP

IP Range

IP Mask

Zone

Host Name

MAC Address

Start IP:

End IP:

[? What do these settings do?](#)

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)

The screenshot shows the 'Network Control Rule' configuration window. The 'General' tab is active, displaying the following settings:

- Action: Block
- Protocol: TCP or UDP
- Direction: In/Out
- Description: Block 3

The 'Destination Address' tab is selected, showing the following options:

- Exclude (i.e. NOT the choice below)
- Any
- Single IP
- IP Range
- IP Mask
- Zone
- Host Name
- MAC Address

The 'IP Range' section shows the following IP addresses:

- Start IP: 137 . 205 . 140 . 0
- End IP: 255 . 255 . 255 . 255

At the bottom of the window, there is a link for 'What do these settings do?' and buttons for 'Apply' and 'Cancel'.

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.\*\***