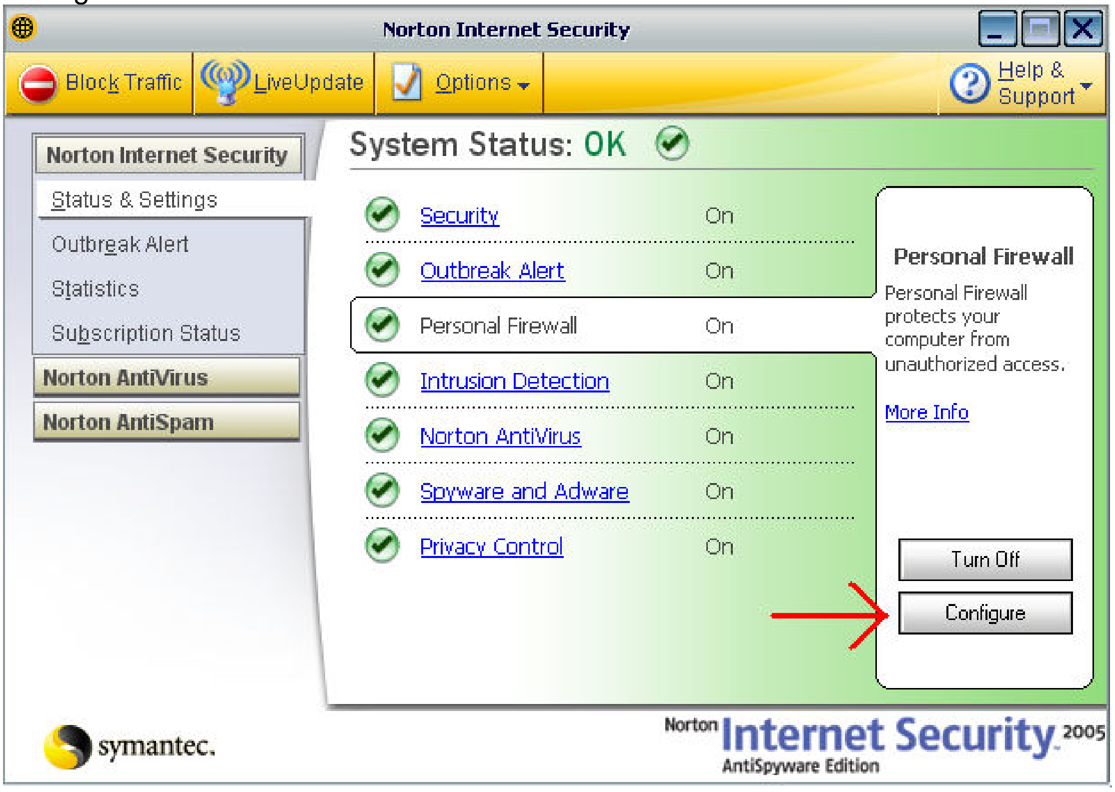
A Guide to blocking external connections to DC++ from on campus

1. Open the main Norton Screen and go to “Configure” in the Personal Firewall settings



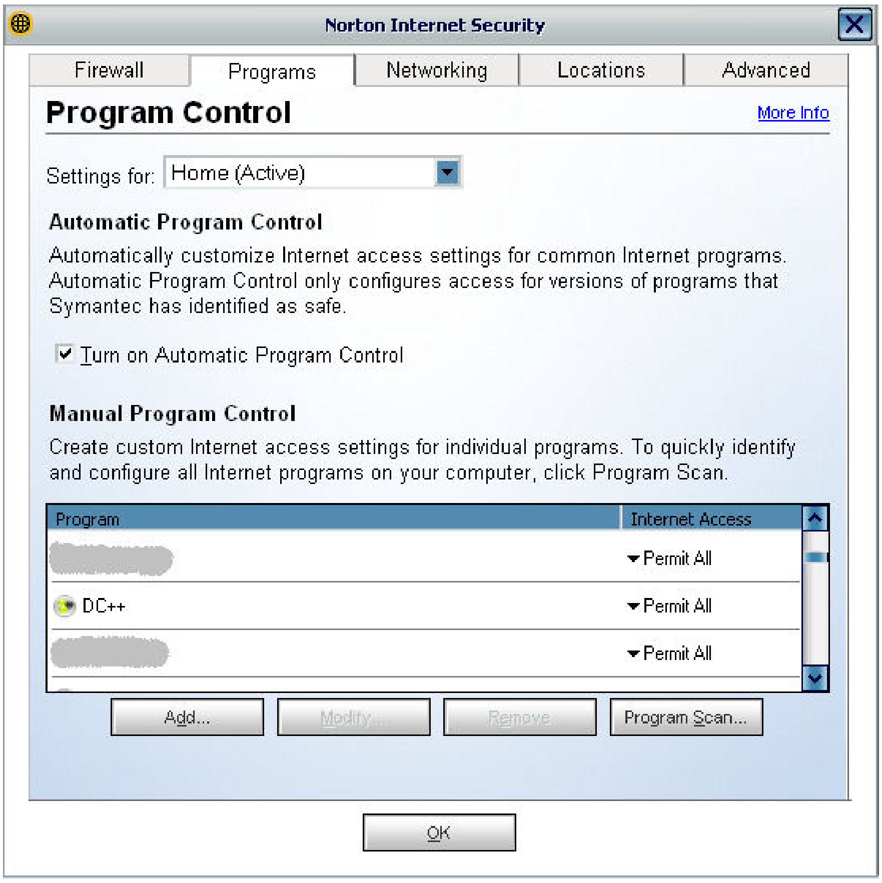
System Status: OK ✓

✓ Security	On
✓ Outbreak Alert	On
✓ Personal Firewall	On
✓ Intrusion Detection	On
✓ Norton AntiVirus	On
✓ Spyware and Adware	On
✓ Privacy Control	On

Personal Firewall

Personal Firewall protects your computer from unauthorized access.

2. Go to the Programs Tab at the top, and then scroll down to DC++ in the programs list



Program Control

Settings for: Home (Active)

Automatic Program Control

Automatically customize Internet access settings for common Internet programs. Automatic Program Control only configures access for versions of programs that Symantec has identified as safe.

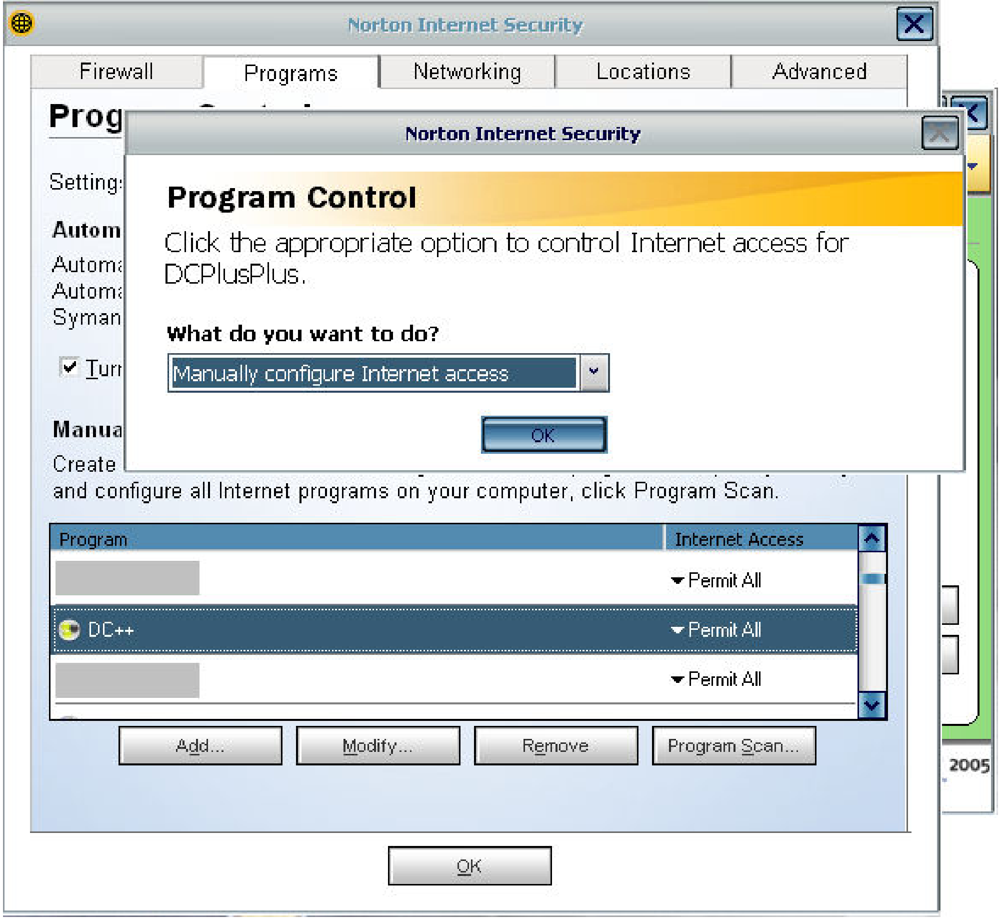
☑ Turn on Automatic Program Control

Manual Program Control

Create custom Internet access settings for individual programs. To quickly identify and configure all Internet programs on your computer, click Program Scan.

Program	Internet Access
[redacted]	Permit All
DC++	Permit All
[redacted]	Permit All

3. Select DC++ and click on Modify underneath it. A box should pop up in which you should choose Manually Configure Internet Access



Norton Internet Security

Firewall | Programs | Networking | Locations | Advanced

Program Control

Click the appropriate option to control Internet access for DCPlusPlus.

What do you want to do?

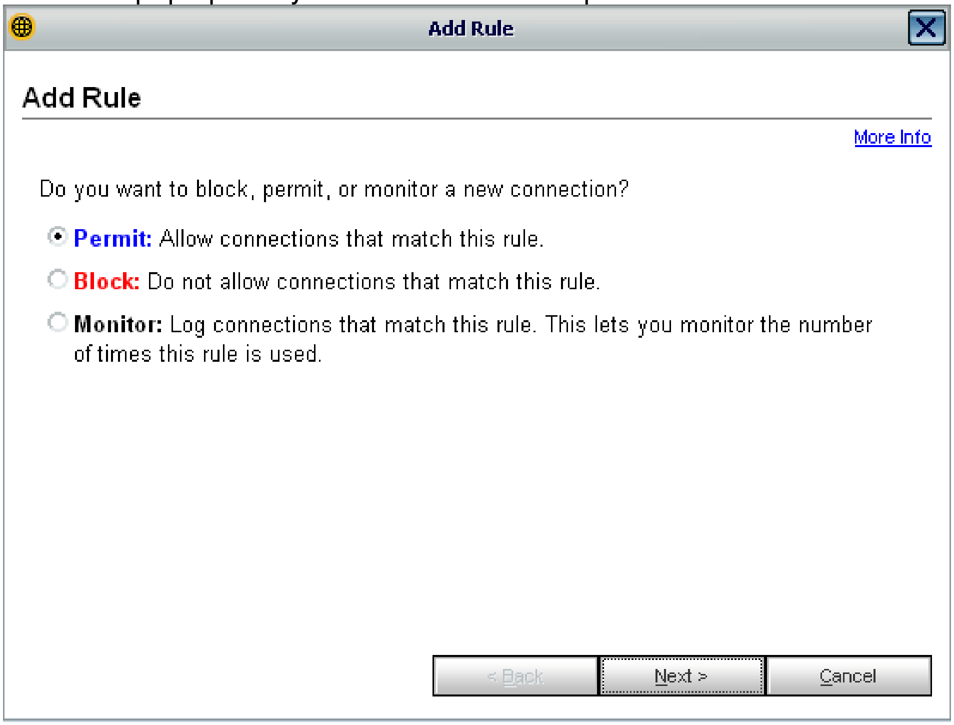
Manually configure Internet access

OK

and configure all Internet programs on your computer, click Program Scan.

Program	Internet Access
	Permit All
DC++	Permit All
	Permit All

4. First of all, remove any rules already in there. Next, you want to create a rule to always permit connections to DC from on campus. To do this, click add rule.
A box will pop up and you should leave the option set to Permit



Add Rule

Add Rule

More Info

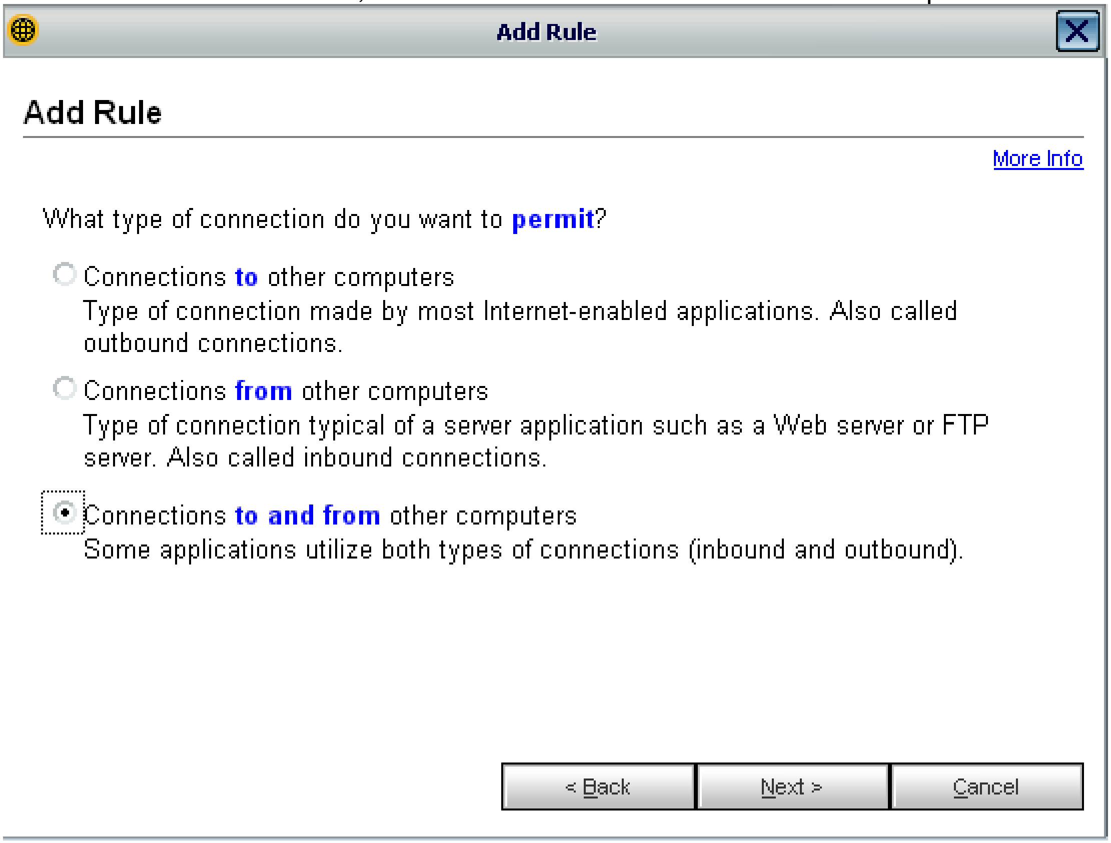
Do you want to block, permit, or monitor a new connection?

● **Permit:** Allow connections that match this rule.

○ **Block:** Do not allow connections that match this rule.

○ **Monitor:** Log connections that match this rule. This lets you monitor the number of times this rule is used.

5. On the next window, select “Connections to and from other computers”



Add Rule

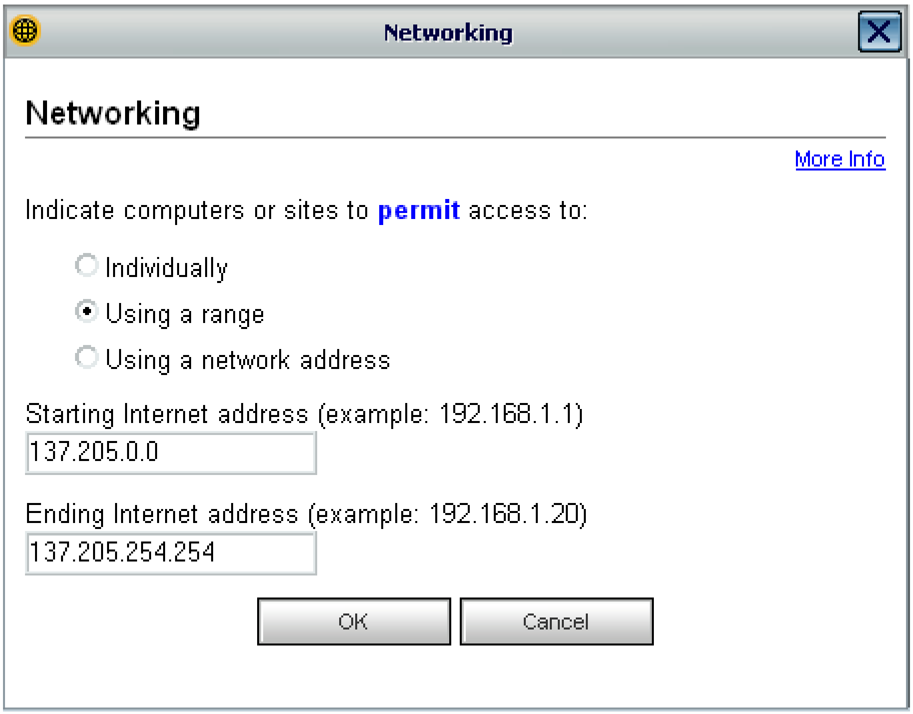
What type of connection do you want to **permit**?

○ Connections **to** other computers
Type of connection made by most Internet-enabled applications. Also called outbound connections.

○ Connections **from** other computers
Type of connection typical of a server application such as a Web server or FTP server. Also called inbound connections.

● Connections **to and from** other computers
Some applications utilize both types of connections (inbound and outbound).

6. On the next screen, select ‘Only the computers and sites listed below’, then click add. Select ‘Using a range’ and put in 137.205.0.0 as the starting address and 137.205.254.254 as the end address.



Networking

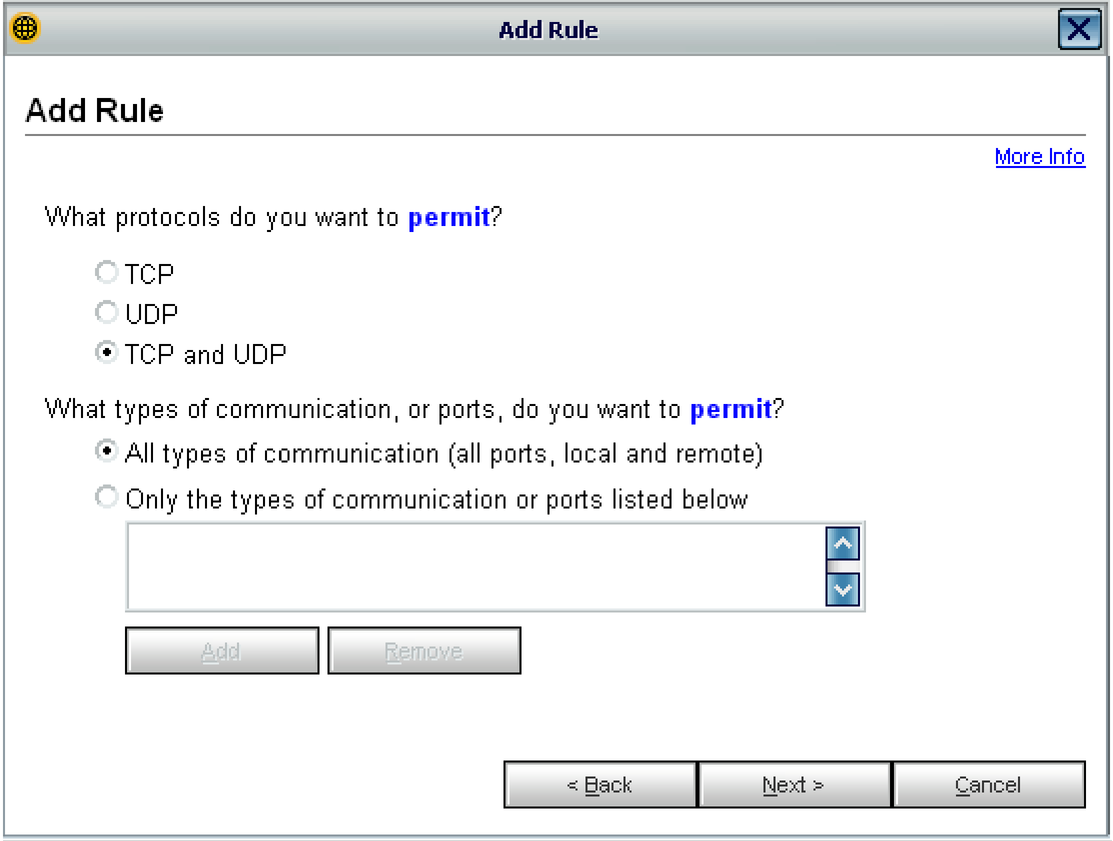
Indicate computers or sites to **permit** access to:

○ Individually
● Using a range
○ Using a network address

Starting Internet address (example: 192.168.1.1)
137.205.0.0

Ending Internet address (example: 192.168.1.20)
137.205.254.254

7.The next few sections can be left as they were originally mostly. You only need to choose a name for this rule and what Location/Zone the rule is for (Home, Work, Away etc)



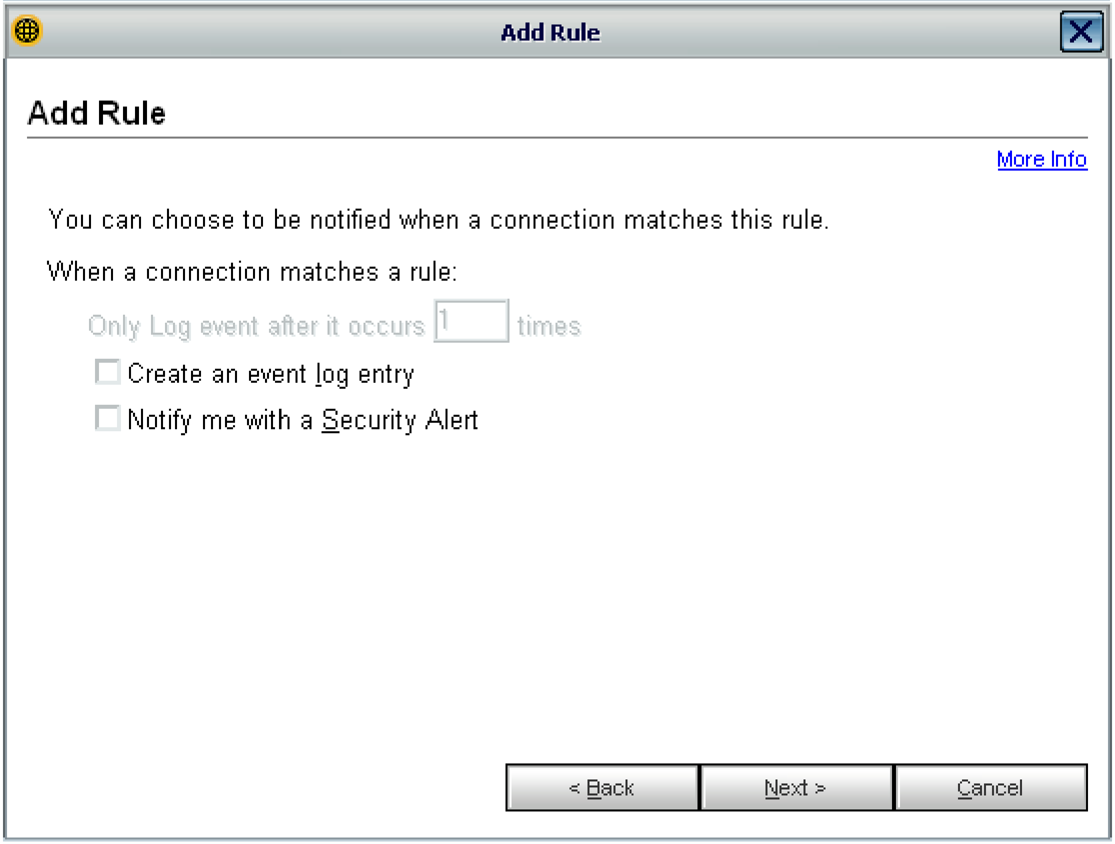
Add Rule

What protocols do you want to **permit**?

○ TCP
○ UDP
● TCP and UDP

What types of communication, or ports, do you want to **permit**?

● All types of communication (all ports, local and remote)
○ Only the types of communication or ports listed below



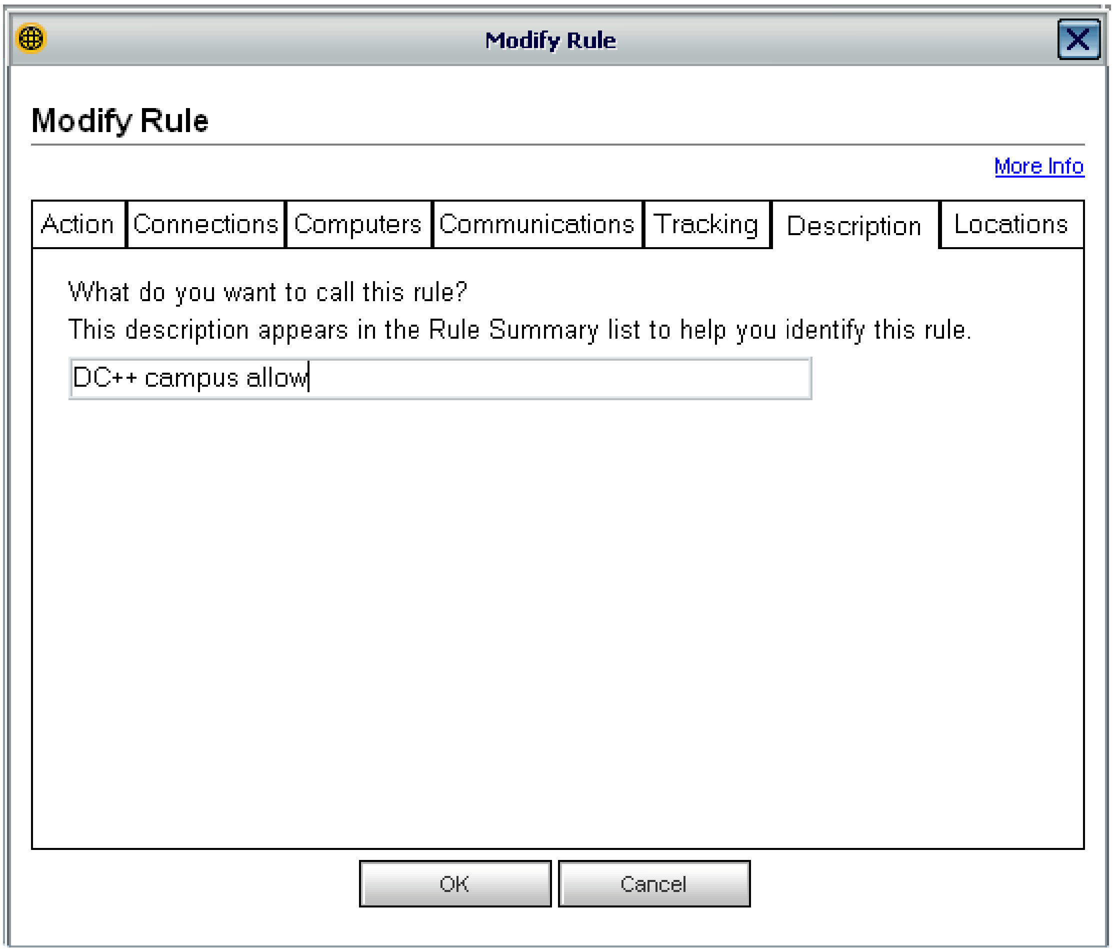
Add Rule

You can choose to be notified when a connection matches this rule.

When a connection matches a rule:

Only Log event after it occurs 1 times

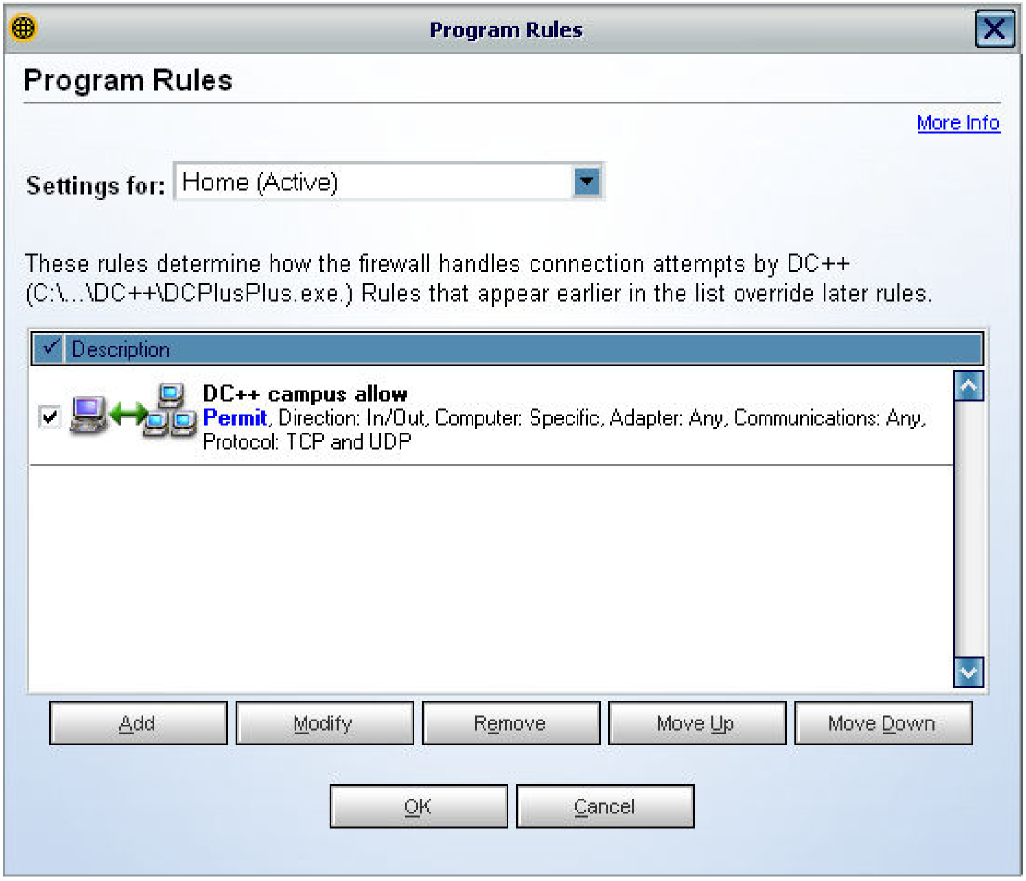
□ Create an event log entry
□ Notify me with a Security Alert



What do you want to call this rule?
This description appears in the Rule Summary list to help you identify this rule.

DC++ campus allow

7. Once those are done, the rules window should look like below.

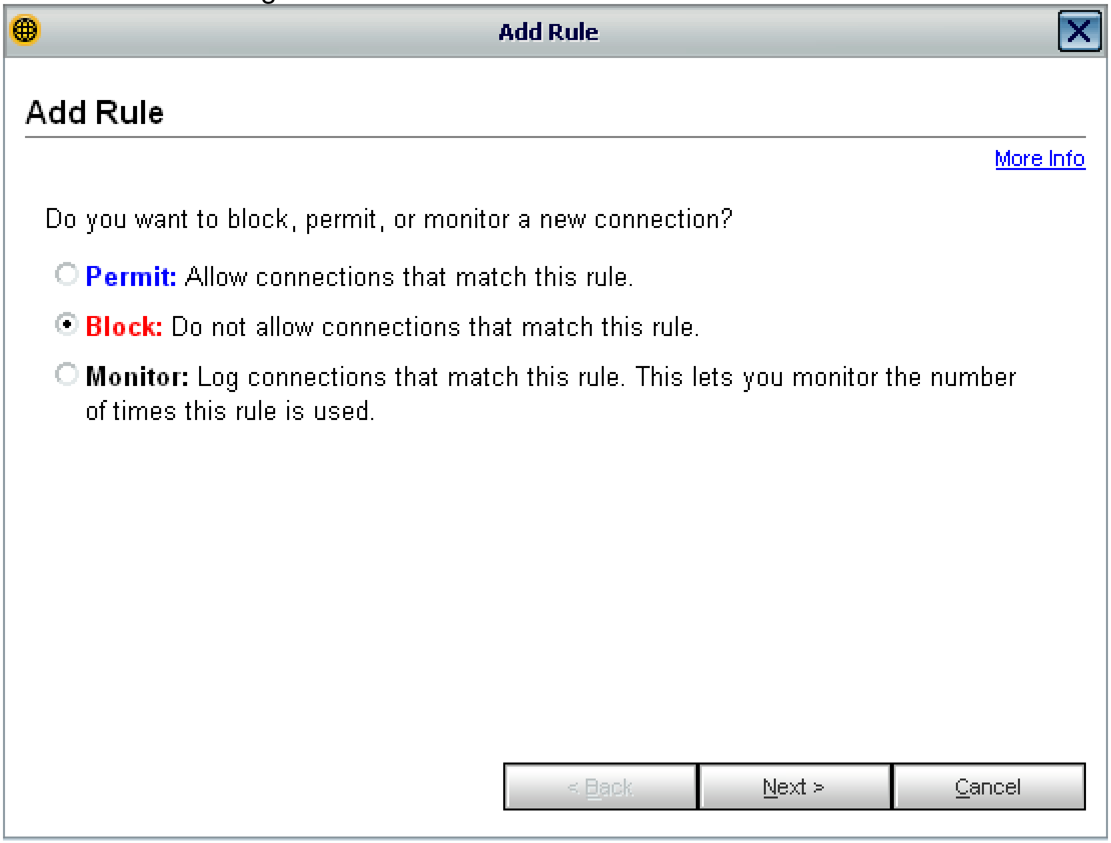


Settings for: Home (Active)

These rules determine how the firewall handles connection attempts by DC++ (C:\...\DC++\DCPlusPlus.exe.) Rules that appear earlier in the list override later rules.

✓ Description
☑ **DC++ campus allow** **Permit**, Direction: In/Out, Computer: Specific, Adapter: Any, Communications: Any, Protocol: TCP and UDP

8. Next you need to create a rule to block connections from everywhere else. Click ‘Add’ again. Then choose block from the list



Add Rule

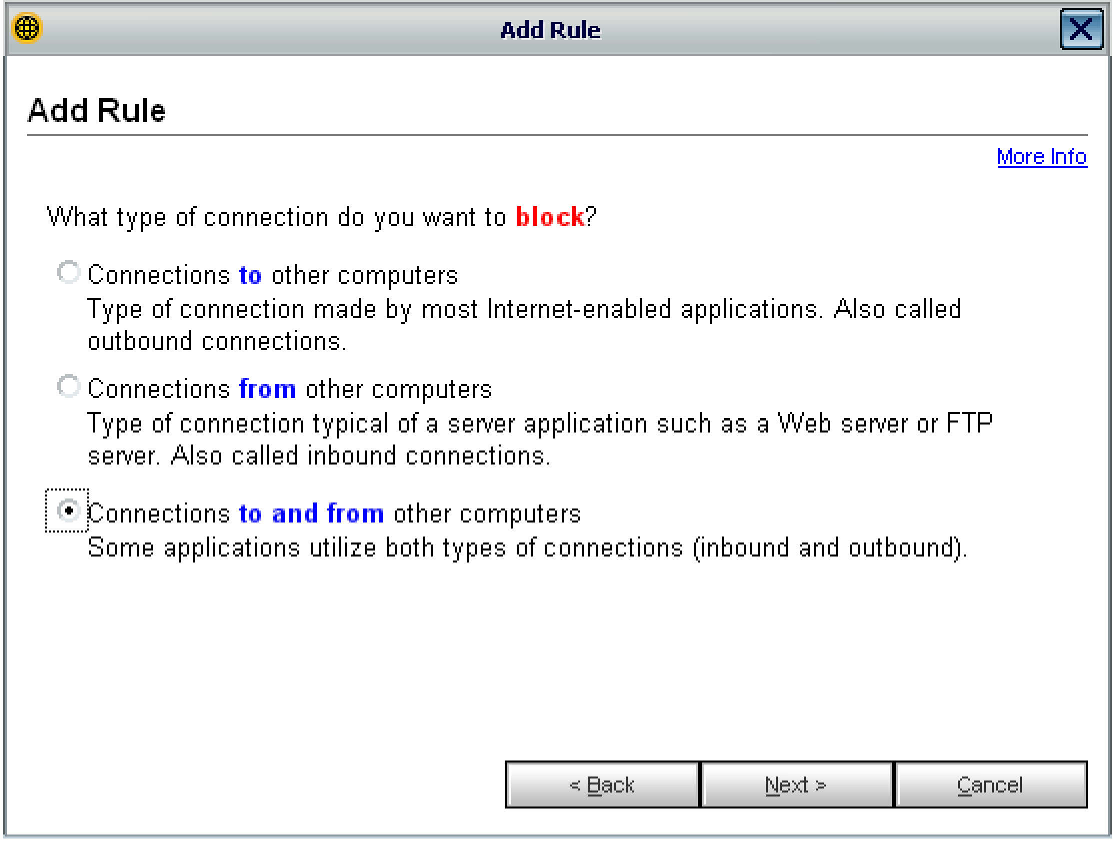
Do you want to block, permit, or monitor a new connection?

○ **Permit:** Allow connections that match this rule.

● **Block:** Do not allow connections that match this rule.

○ **Monitor:** Log connections that match this rule. This lets you monitor the number of times this rule is used.

9. Next screen, again you have to select “Connections to and from other computers”



Add Rule

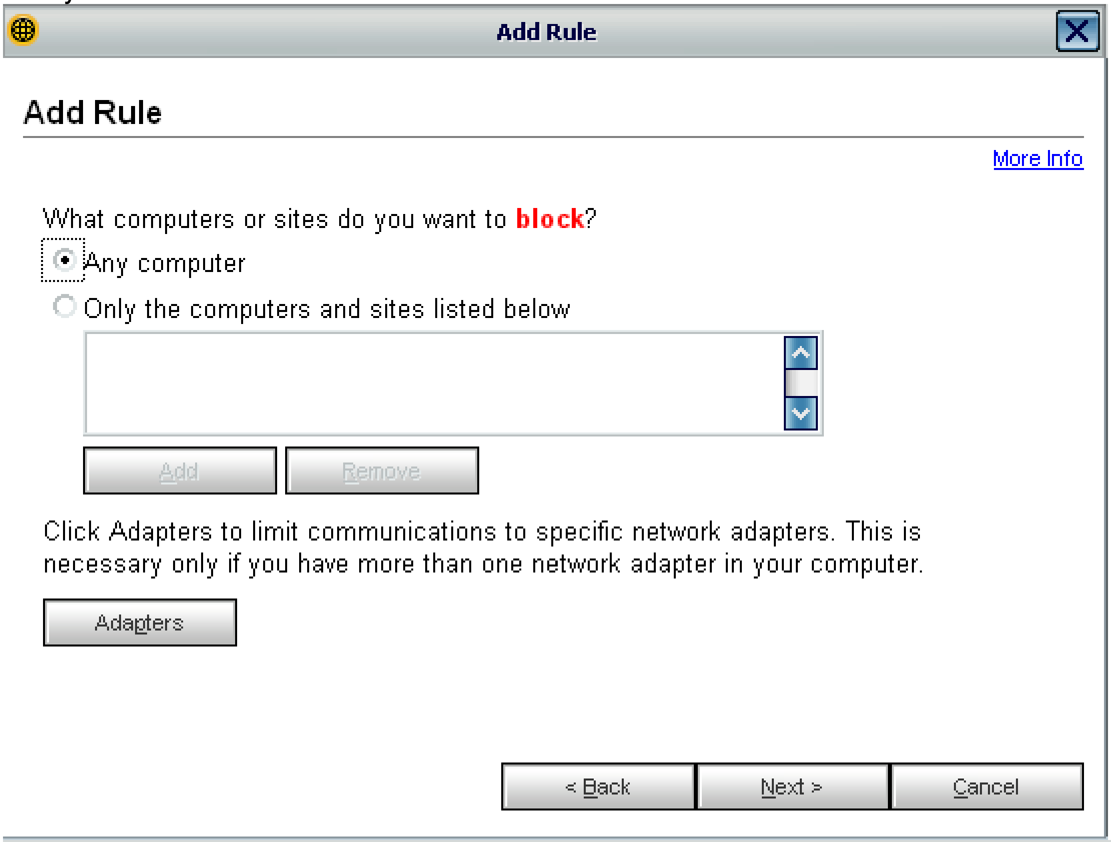
What type of connection do you want to **block**?

○ Connections **to** other computers
Type of connection made by most Internet-enabled applications. Also called outbound connections.

○ Connections **from** other computers
Type of connection typical of a server application such as a Web server or FTP server. Also called inbound connections.

● Connections **to and from** other computers
Some applications utilize both types of connections (inbound and outbound).

10. Again, from this point on, the options can be left mostly as what they are by default. Ie. Block connections from any computer, All types of communication etc. And you need to choose a name for this rule.



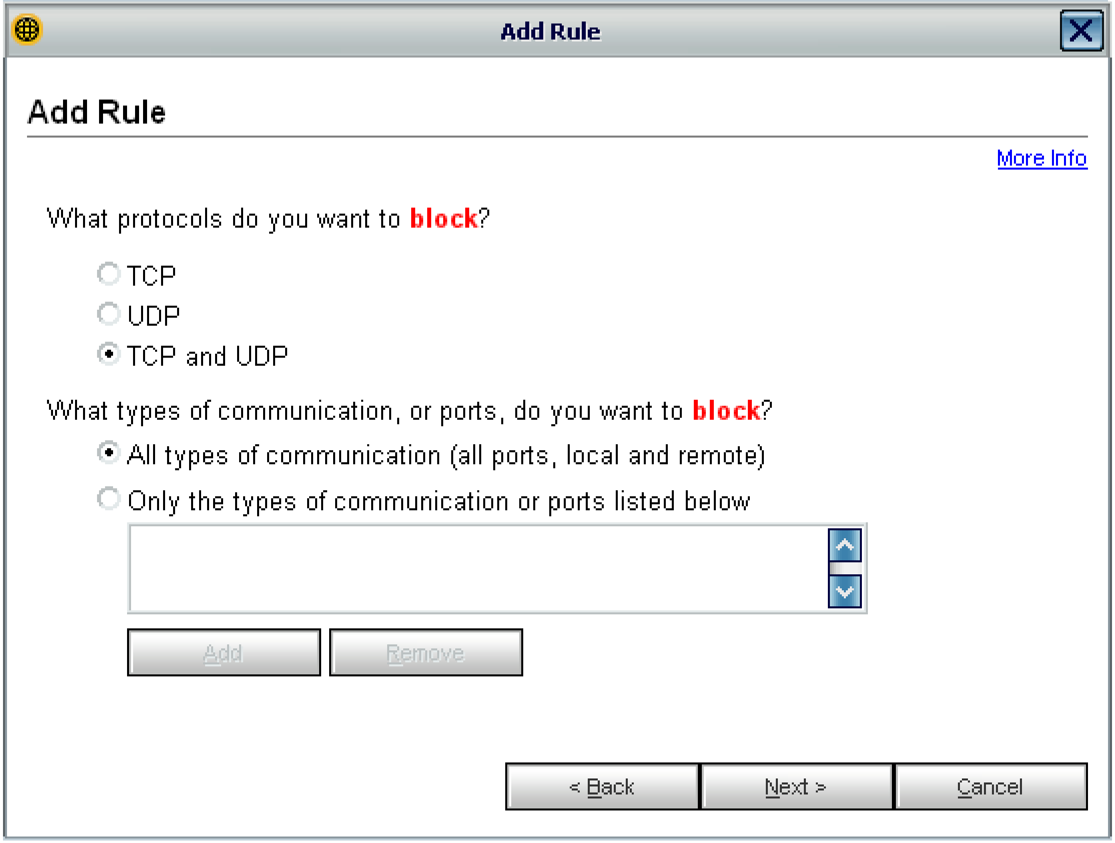
Add Rule

What computers or sites do you want to **block**?

● Any computer

○ Only the computers and sites listed below

Click Adapters to limit communications to specific network adapters. This is necessary only if you have more than one network adapter in your computer.



Add Rule

What protocols do you want to **block**?

○ TCP

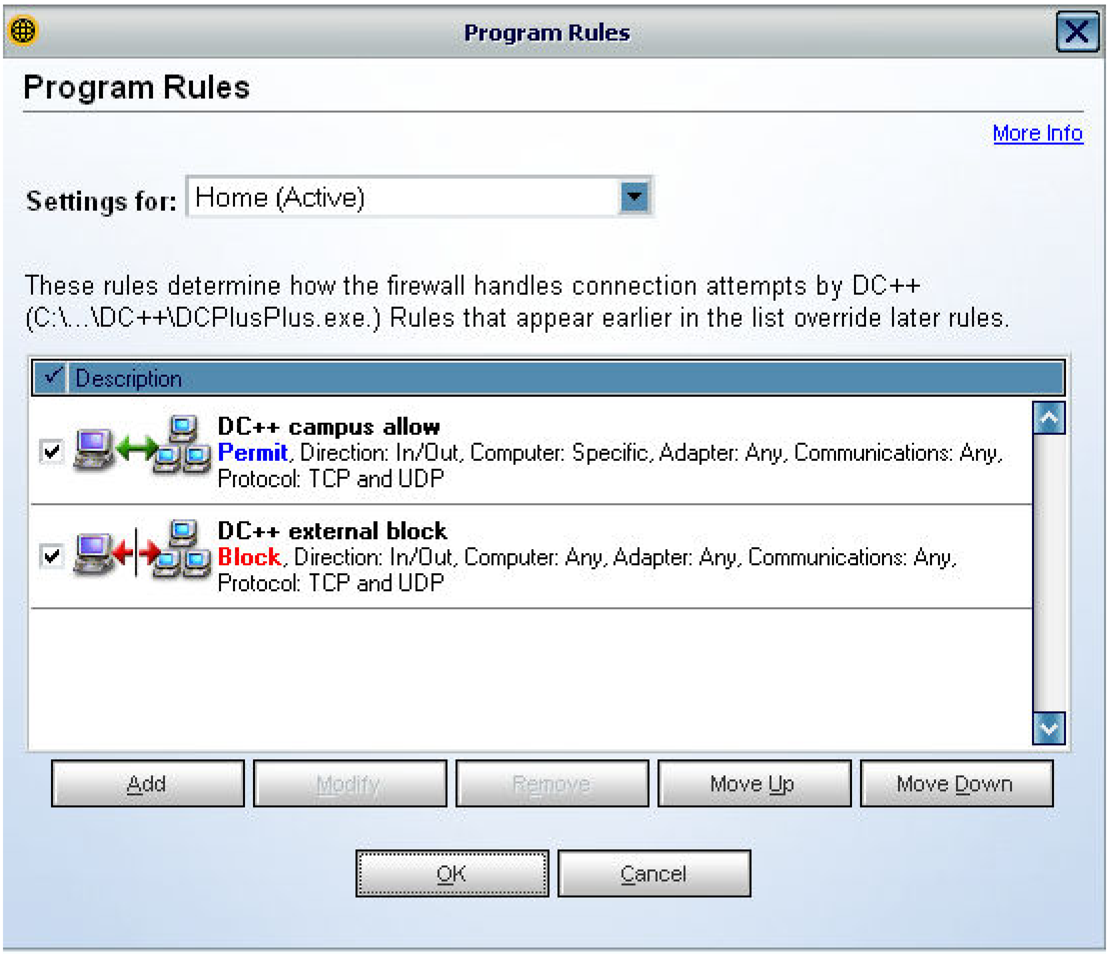
○ UDP

● TCP and UDP

What types of communication, or ports, do you want to **block**?

● All types of communication (all ports, local and remote)

○ Only the types of communication or ports listed below



Program Rules

Settings for: Home (Active)

These rules determine how the firewall handles connection attempts by DC++ (C:\...\DC++\DCPlusPlus.exe.) Rules that appear earlier in the list override later rules.

✓	Description
☑	**DC++ campus allow** **Permit**, Direction: In/Out, Computer: Specific, Adapter: Any, Communications: Any, Protocol: TCP and UDP
☑	**DC++ external block** **Block**, Direction: In/Out, Computer: Any, Adapter: Any, Communications: Any, Protocol: TCP and UDP

You should now be set up to only allow connections to dc from on campus people.