Yy Connection: Trusted Internet	Personal Firewall 2005 Professional Build: 6.5.126					PTEN		
Applications My Applications Applications	sta Ne	etwork Security	🥵 Jilan St	1ah@2CDXT1J	J			
Control	🔄 Show Details	Show Extended Details	- Add New Account Specific - Add New Rule Rule	🍓 Global Edit	🙀 Integrity Check			
INetwork Protection	Descript	ion	Time Users					
touted Rules Cones IAT/ICS Settings Protocols and Ports Prodefined ID	High Priority Rules ^ No rule is available							
addresses	Allows all	TCP/UDP traffic for Inst		- 🗐 🗞 🎐	×			
File Protection	Allows all	TCP/UDP traffic for Use			×			
	Low Priority Rules							
	Allows all outbound TCP connections for Internet Explorer				仓 🐚 🎐	×		
DS & IPS	Allows all	TCP/UDP traffic for Tru:		🕆 📭 🎐	×			
iettings	Allows int	oound NetBIOS TCP con		û 📭 📑	x			
eports	Allows int	oound Terminal Service	connections for TrustedServices group		û 🔁 🌗	×		

You need to access "Local Rules" under the "Network Protection" tab and go to "Add New Rule"

C TF6 Administration Ce	enter			
My Connection: Trusted Internet			⇒TINY	
		🗿 Add Firewall R		
Applications My Applications	<u>s</u> žg		Add Firewall Rule	In Shah@2CDXT1J 👤
Application Start Control	Show	General	-Description	al 🙀 Integrity Check
Network Protection Local Rules Routed Rules Zones NAT/ICS Settings Protocols and Ports Predefined IP addresses	Desc High Pri No rule i: Account	Protocol My Computer Remote Computer(s)	 − Priority • High C Low □ Is Preferred − Status ✓ Enabled 	Users
■ File Protection	🔽 Allow	Restriction		🕫 🐚 🖳 🗙
System Protection (Advanced)	<i>Low Pric</i> I✓ Allow I✓ Allow	Summary		☆ 📭 🚽 🗙 수 📭 🚽 🗙
∃ Settings	🔽 Allow		Add Cancel	🕆 🐚 🚽 🗙
Reports Events	Allows	inbound Terminal	Service connections for TrustedServices group	

Put the "*Description*" as **DC++** # and move on to the "*Protocol*" tab.



For the "*Protocol*" select "**TCP UDP ALL**" and on the "*Access*" option select "**Prevent**" to block connections or the appropriate as needed move on the "*My Computer*" tab.



Now select "DCPlusPlus(DC++)" under "Application: By ID".



You need to set up 3 IP range blocks to completely block external connections and still allow connections from on campus and your connection to the hub itself

For "*Remote Computer(s)*", under "*Remote IP Address*" select ">> > Specify Directly ..." and in the box opened select "Range" followed by the beginning IP address and ending IP address and click update.

Your first IP range should start at "1.0.0.0" and end at "127.0.0.0", as above.



You then need to set up another block, using the same steps as before, for the 2nd Range from "127.0.0.2" to "137.205.0.0"



And the same for the final range from "137.206.0.0" to "255.255.255.255"

YOU ARE NOW DONE!