Windows 7 Firewall: How To Block Off Campus – Campus Connections

Windows 7 Firewall has the capability to block both inbound and outbound connections. The Scripts we used for Vista still work brilliantly in Win7. The Win7 firewall interface also lets us configure the firewall graphically, something Vista did not allow.

The firewall scripts are the easiest way to set up these rules, however if you wish to see exactly what is happening graphically this guide may help you.

Before you begin, please close DC++ to avoid any conflict with active applications.

Step 1

From the Control Panel, open the *Windows Firewall* settings and navigate to *Advanced Settings*. You should see the below page.

File Action View Help			
Windows Firewall with Advance	Windows Firewall with Advanced Security on Local Computer		Actions
Inbound Rules Outbound Rules Connection Security Rules Monitoring	Windows Firewall with Advanced Security provides network security for Windows computers.		Windows Firewall with Adv
	Overview		Restore Default Policy
	Domain Profile		Diagnose / Repair
	😵 Windows Firewall is off.	E	View
	Private Profile		Refresh
	😵 Windows Firewall is off.		Properties
	Public Profile is Active		[Help
	Windows Firewall is off.		
	Windows Firewall Properties		
	Getting Started	*	
	Authenticate communications between computers		
	Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).		
	Connection Security Rules	-	

Step 2

Navigate to the Outbound Rules, and select Add New Rule.

File Action View Help	l security	_	_		_			
Windows Firewall with Advance	Outbound Rules						Actions	
Inbound Rules	Name	Group	Profile	Enabled	Action	-	Outbound Rules	*
Connection Security Rules	BranchCache Content Retrieval (HTTP-O BranchCache Hosted Cache Client (HTT BranchCache Hosted Cache Server(HTTP BranchCache Peer Discovery (WSD-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (TCP-Out) Connect to a Network Projector (WSD Ev	BranchCache - Content Retr BranchCache - Hosted Cach BranchCache - Hosted Cach BranchCache - Peer Discove Connect to a Network Proje Connect to a Network Proje Connect to a Network Proje	All All All Domain Private	No No No No No No	Allow Allow Allow Allow Allow Allow		 New Rule Filter by Profile Filter by State Filter by Group View Refresh 	> > >
	Connect to a Network Projector (WSD Ev., Connect to a Network Projector (WSD Ev., Connect to a Network Projector (WSD Ev., Connect to a Network Projector (WSD-O.,	Connect to a Network Proje Connect to a Network Proje Connect to a Network Proje Connect to a Network Proje	Domain Private Domain All	No No No No	Allow Allow Allow Allow		Export List	

Select *Program* as the Rule Type.

P New Outbound Rule 1	Wizard
Rule Type Select the type of firewall rul	le to create.
Steps: Program Action Profile Name	What type of rule would you like to create?
	Leam more about rule types
	< Back Cancel

Step 4

Select the program path radio button and use the browse button to locate the DC++ executable file (usually C:\Program Files\DC++\DCPlusPlus.exe).

Program	
Specify the full program patl	h and executable name of the program that this rule matches.
Steps: Pule Type Program Action Profile Name	Does this rule apply to all programs or a specific program? All programs Rule applies to all connections on the computer that match other rule properties. This composes and the second secon
	Inis program path: //PmgramFiles*/\DC++\DCPlusPlus eye Bmwee
	Example: c:\path\program.exe %ProgramFiles%\browser\browser.exe
	Learn more about specifying programs

Now we need to create rules to allow Campus (ResNet) connections, and rules to block Off Campus connections. We will start with rules to allow campus connections. So for Action, select *Allow the connection*.

🔐 New Outbound Rule Wizar	a 🛁 🖊 🚽 🖉
Action Specify the action to be taken wh	en a connection matches the conditions specified in the rule.
Steps: Program Action Profile Name	What action should be taken when a connection matches the specified conditions? Image: Connection in the are protected with IPsec as well as those are not. Image: Connection in the secure Image: Connection in the secure in the

Step 6

I have selected all 3 profiles. There is probably another way of using the profiles to enhance these rules, however I have not tried them however.



Name the rule, I have used DC++ Allow here, the scripts use DC++1, DC++2 etc. You may use whatever is convenient for you. If you want you can also put a description for what the rule is doing.

New Outbound Rule W	izard
Name Specify the name and descrip	tion of this rule.
Steps:	
 Rule Type Program Action Profile 	Name:
Name	DC++ Allow
	Description (optional):
	Allow DC++ For Campus Connections
	< Back Finish Cancel

Step 8

Now right click on the rule you created, and select *Properties*. Navigate to the *Scope* tab, and under Remote IP address click *add*. Now enter the IP address as 137.205.0.0/16. You may also select from *137.205.0.0-137.205.255.255*. We now have the rule to allow ResNet connections configured!

General	Programs and Services	Computers	General P	rograms and Services	Computers
Protocols and	Ports Scope	Advanced	Protocols and Ports	Scope	Advanced
Protocols and ocal IP address Specify the This IF 137.21 Examp This IF From: To: Predef Defau	I Ports Scope I Ports Scope I Paddresses to match: address or subnet: I5.0.0/16 Ies: 192.168.0.12 192.168.1.0/24 2002.9d3b:1a31:4:208:74ff fe39: 2002.9d3b:1a31:4:208:74ff fe39: address range: address r	Advanced	Protocols and Ports Local IP address These IP add Remote IP address These	ss scope	Advanced Add Edit Edit Edit Remove
	OK	Cancel			

We will now make a rule to allow DC++ to connect to stunnel. Please repeat *Steps 2-7* naming the rule appropriately. Navigate to the *Properties* of the new rule, go to the *Scope* tab and enter the IP address as *127.0.0.1*.

Ge	eneral Programs and Services Computers
P	rotocols and Ports Scope Advanced
loca	I IP address
[IP	Address
F	
	Specify the IP addresses to match:
	This IP address or subnet:
	127.0.0.1
R	Examples: 192.168.0.12 192.168.1.0/24 2002:9d3b:1a31:4:208:74ff.fe39:6c43 2002:9d3b:1a31:4:208:74ff.fe39:0/112
1	This IP address range:
	From:
L	То:
L	Predefined set of computers:
L	Default gateway
1	Learn more shout energiting IP addresses
	OK Cancel
L	

Step 10

We will now make a rule to block Off Campus connections. Please repeat *Steps 2-4* naming the rule appropriately. In *Step 5*, we selected *Allow the connection*, however in this case please select *Block the connection*. Continue with *Steps 6-7*, to create the rule. Navigate to the *Properties* of the new rule, go to the *Scope* tab and enter the IP address range *0.0.0.1-127.0.0.0*.

pec	ify the l	P addresses to match:
D T	This IP a	address or subnet:
E	Example	es: 192.168.0.12 192.168.1.0/24 2002:9d3b:1a31:4:208:74fffe39:6c43 2002:9d3b:1a31:4:208:74fffe39:0/112
F	From:	0.0.0.1
1	To:	127.0.0.0
DF	redefin	ed set of computers:
G	Default	gateway 👻

We will now make another rule to block Off Campus connections. Please repeat *Steps 2-4* naming the rule appropriately. In *Step 5*, we selected *Allow the connection*, however in this case please select *Block the connection*. Continue with *Steps 6-7*, to create the rule. Navigate to the *Properties* of the new rule, go to the *Scope* tab and enter the IP address range *127.0.0.2-137.205.0.0*.

Spec	ify the	IP addresses to match:
© T	his IP a	address or subnet:
E	Example	IN: 192.168.0.12 192.168.1.0/24 2002.9d3b:1a31:4:208:74fffe39:6c43 2002:9d3b:1a31:4:208:74fffe39:0/112
F	inis ir d	127.0.0.2
	To:	137.205.0.0
- 21	Nores	ed set of computers:
© P	redefin	
י P © [נ	' redefin Default	gateway *
© P	redefin Default 1 more i	gateway *

Step 12

We will now make a rule to block Off Campus connections. Please repeat *Steps 2-4* naming the rule appropriately. In *Step 5*, we selected *Allow the connection*, however in this case please select *Block the connection*. Continue with *Steps 6-7*, to create the rule. Navigate to the *Properties* of the new rule, go to the *Scope* tab and enter the IP address range *0.0.0.1-127.0.0.0*.

Aut	11622	
Spe	cify the	IP addresses to match:
O	This IP :	address or subnet:
ĺ		
	Example	es: 192.168.0.12 192.168.1.0/24
		2002.9d3b:1a31:4:208:74ff fe39:6c43
		2002.3030.1831.4.200.74111633.0/112
۲	This IP a	address range:
	From:	137.205.255.255
	To:	255.255.255
Ø	Predefin	ed set of computers:
(Default	gateway 👻
Lear	m more	about specifying IP addresses
		OK Cancel

Step 13

With these steps all the outgoing rules are complete. Please repeat Steps 2-12, for Inbound Rules naming the rules appropriately.

Congratulations! You are all done now. Please contact an operator on the hub to test your configuration.