

CONFIGURING WINDOWS FIREWALL WITH ADVANCED SECURITY IN WINDOWS 7

Windows Firewall with Advanced Security (WFAS)

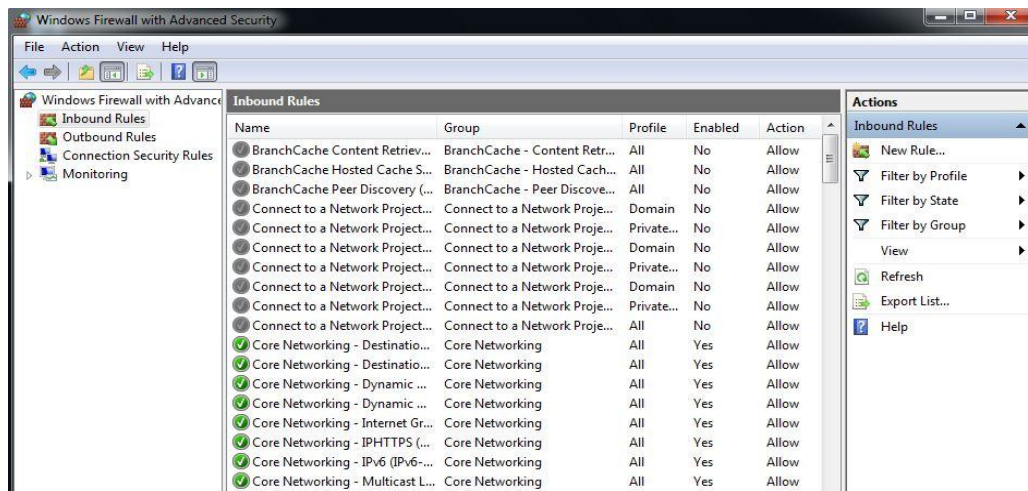
As you should know, with WFAS we have more granular control when compared to ordinary Windows Firewall which is also available in Windows 7. To open WFAS, simply start entering "windows firewall" in search and select "Windows Firewall with Advanced Security" option.



Open WFAS

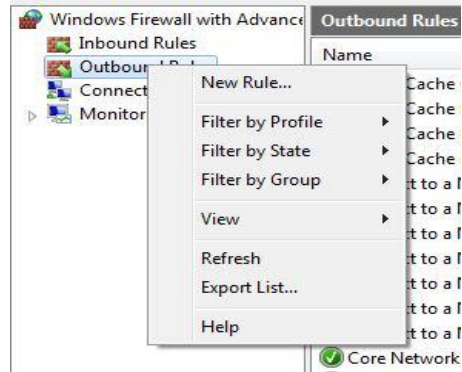
Once we open WFAS we will see a list of rules. Rules are divided to the Inbound, Outbound and Connection Security rules.

Notice that there is a lot of predefined rules that we can use. Some of them are enabled, and some of them are disabled. Each rule can be disabled/enabled for the different network profile (domain, private, public). We can also see the application that the rule relates to, the action, the protocol that is used, local and remote address, the local and remote port, allowed users and allowed computers.



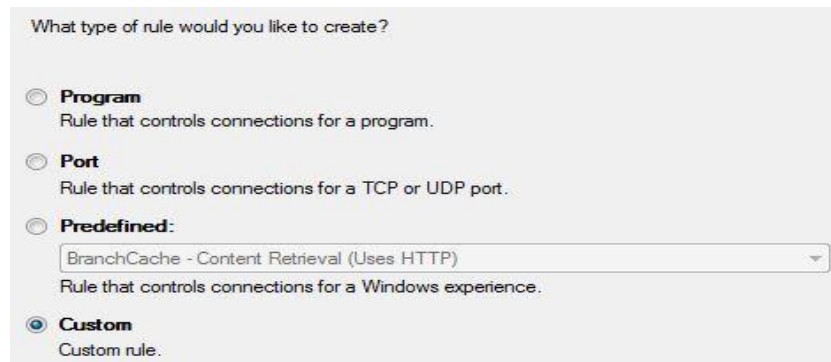
Rules

To restrict access to our computer we would edit the Inbound rules. To restrict users to access remote resources, we would go to the Outbound rules section. This is what we will do in this example. For the purpose of this demo we will block users on our local computer to access the www.utilizewindows.com site. So, to add a new rule, we can right-click on the Outbound rules section, all click on the New Rule option from the menu on the right side of the window.



New Rule Option

On the first screen we can choose to create rules based on programs, ports or use a predefined rule. We can also create a custom rule, which we will do in our example.



Custom Rule Option

On the next screen we can specify if this rule applies to all programs or only to a specific program. For example, here we could choose only specific Web Browsers. We could also apply this rule to specific services only. For the purpose of this demo we will choose the "All programs" option and click Next.

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 program path:

 Example: c:\path\program.exe
 %ProgramFiles%\browser\browser.exe

Services
Specify which services this rule applies to.

Programs

On the next screen we have to choose the right protocols and ports. For this, you have to know about different networking protocols and their specific ports. For example, to access web sites our Web Browsers use HTTP protocol. HTTP protocol uses TCP transport layer protocol, on port 80 by default. When configuring the Outbound rule, it is more important to configure the Remote port. The local port is actually auto-generated when the connection gets established, and it is used as a return path. Because of that, we don't have to enter it here. The remote port is the port we are connecting to. For the remote port we will use the specific port 80.

To which ports and protocols does this rule apply?

Protocol type:

Protocol number:

Local port:

 Example: 80, 443, 5000-5010

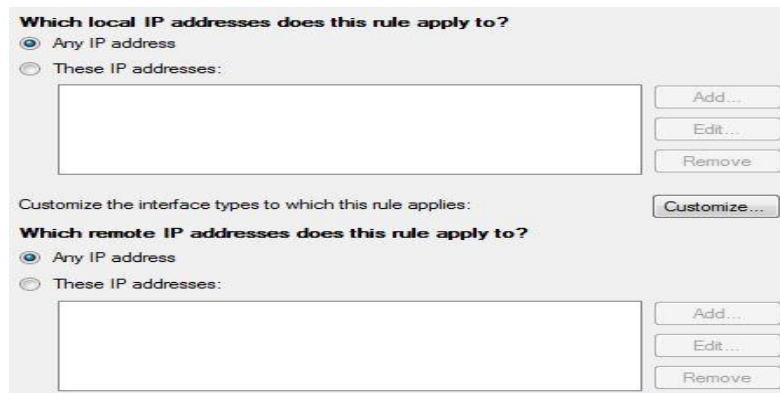
Remote port:

 Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings:

Protocols

On the next screen we have to choose the IP addresses that this rule applies to. For the local IP address we can choose the "Any IP address" option or choose to enter specific IP address. In this case this is not important since this rule will only be applied to the local machine. However, if we were to configure this rule through Group Policy and push it down to our machines, we would then have to specify the specific IP addresses that this rule should be applied to.



IP Address

If we click on the Customize button we can also select which interfaces this rule applies to. By default it will be applied to all interfaces, but we can choose to only apply it to wired or wireless interfaces, or to remote access sessions.



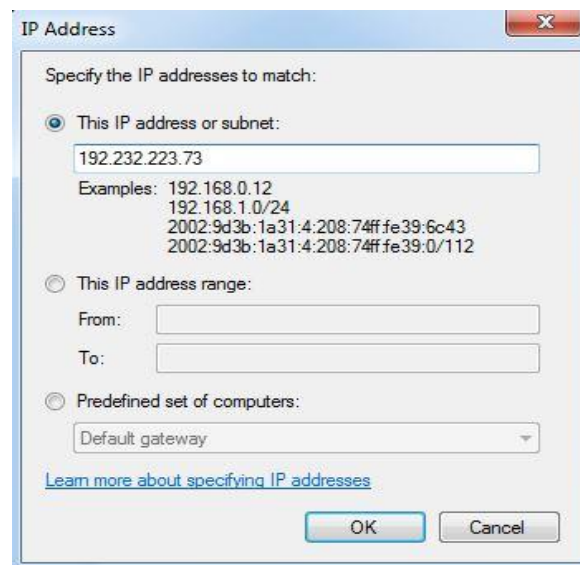
Interface Types

The important thing to configure is the remote IP addresses to which this rule applies to. So, we have to know the IP address of the www.utilizewindows.com site. To get the IP address we will try and PING it in the command line.

```
C:\Users\ivancic.INTRANET>ping www.utilizewindows.com
Pinging utilizewindows.com [192.232.223.73] with 32 bytes of data:
Reply from 192.232.223.73: bytes=32 time=166ms TTL=46
Reply from 192.232.223.73: bytes=32 time=166ms TTL=46
Reply from 192.232.223.73: bytes=32 time=165ms TTL=46
Reply from 192.232.223.73: bytes=32 time=166ms TTL=46
Ping statistics for 192.232.223.73:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 165ms, Maximum = 166ms, Average = 165ms
```

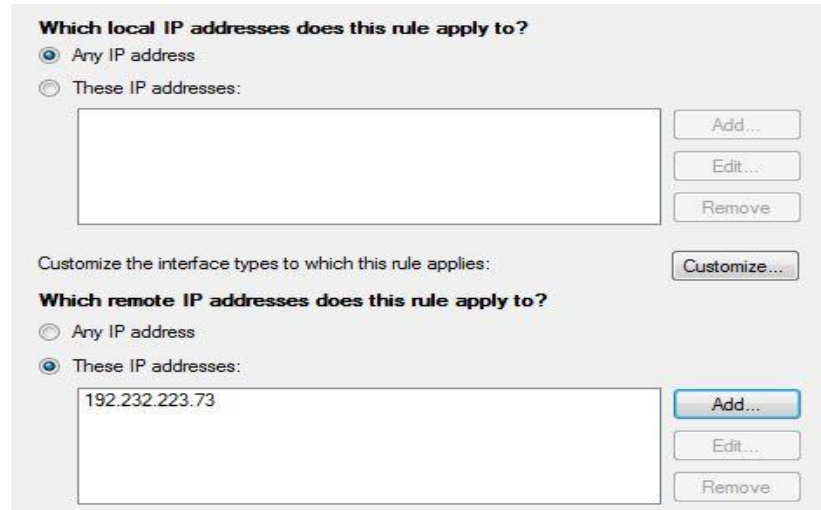
Ping

We got the reply and now we know that the IP address is 192.232.223.73. Let's click on the Add button and enter the IP address.



IP Address Specified

Notice that in this window we can also enter the whole subnet, the range of IP addresses, or some predefined set of computers (WINS servers, DHCP servers, DNS servers, or local subnet computers. When we click OK, our screen now looks like this.



The screenshot shows a configuration window titled "Which local IP addresses does this rule apply to?". It has two radio button options: "Any IP address" (selected) and "These IP addresses:". Below the second option is an empty text box and three buttons: "Add...", "Edit...", and "Remove".

Below this section is a label "Customize the interface types to which this rule applies:" followed by a "Customize..." button.

The second section is titled "Which remote IP addresses does this rule apply to?". It has two radio button options: "Any IP address" and "These IP addresses:" (selected). Below the second option is a text box containing "192.232.223.73" and three buttons: "Add..." (highlighted in blue), "Edit...", and "Remove".

IP Address Entered

On the next screen we choose the action we want to be performed for this rule. In our case we will block the connection.



The screenshot shows a configuration window titled "What action should be taken when a connection matches the specified conditions?". It has three radio button options:

- Allow the connection**
This includes connections that are protected with IPsec as well as those are not.
- Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.
A "Customize..." button is located below this option.
- Block the connection**

Action

On the next screen we have to choose the network profile that this rule applies to.

The default is all profiles.

When does this rule apply?

- Domain**
Applies when a computer is connected to its corporate domain.
- Private**
Applies when a computer is connected to a private network location.
- Public**
Applies when a computer is connected to a public network location.

Profile








On the next screen we enter the name of our rule and a brief description.

Name:

Description (optional):

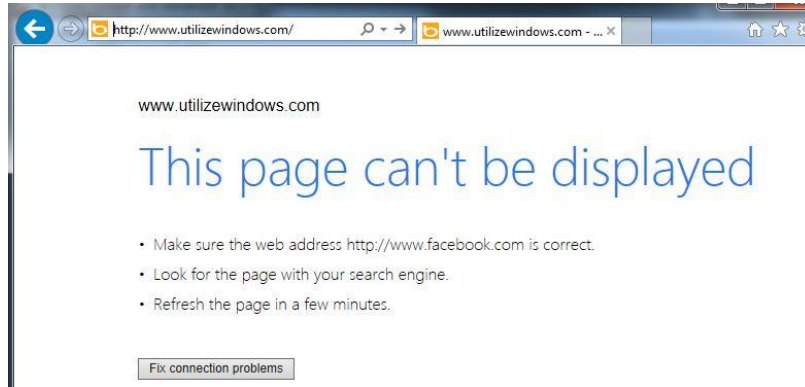
Name

When we click Finish, we will see our new rule in the list.

Outbound Rules	
Name	Group
 Block UtilizeWindows	
 BranchCache Content Retrieval (HTTP-O...	BranchCache -
 BranchCache Hosted Cache Client (HTT...	BranchCache -
 BranchCache Hosted Cache Server(HTTP...	BranchCache -
 BranchCache Peer Discovery (WSD-Out)	BranchCache -
 Connect to a Network Projector (TCP-Out)	Connect to a N
 Connect to a Network Projector (TCP-Out)	Connect to a N

Rule Created

When we try to browse to the www.utilizewindows.com now, we will see something like this.



Site Blocked

Bigger organizations often use multiple IP addresses assigned to multiple servers which all serve the same web site. For example, facebook.com uses several ranges of IP addresses, and in order to block facebook.com we have to enter all those IP addresses (or ranges) in our outbound firewall rule in order to block access to Facebook.

Source: <http://www.utilizewindows.com/7/networking/462-configuring-windows-firewall-with-advanced-security>