Managing Windows XP® Firewall Through Command-line

By
Pavan Shah
Net-square Solutions
pavan@net-square.com

Overview

The purpose of this document is to introduce functionalities of Windows XP®'s native netsh command. In this document we will see how we can change certain firewall's configuration settings using netsh command.

Windows XP Firewall

Windows XP with Service Pack 2 includes a basic firewall that protects users from various attacks. Firewall feature in windows XP is designed for home and small business users. By default firewall is turned on in Windows XP.

For example, Windows XP with SP2 is installed on machine A (IP Address 192.168.7.113).Firewall is turned on.

netsh command

netsh command in Windows XP allows us to change most of configuration parameters through command line. It is a nice command line utility to perform most of the configuration tasks.

We will not go into details of netsh options and we will straight away jump to netsh firewall context.

Open command prompt and give netsh command.
C:\>netsh
netsh>

As show above this will change to netsh> prompt. This gives us an interactive shell to run commands.

To change to firewall context of netsh write firewall at the netsh> prompt as shown below:

netsh>firewall
netsh firewall>?
Commands in this context:

?	*- Displays a list of commands.*
add	*- Adds firewall configuration.*
delete	*- Deletes firewall configuration.*
dump	*- Displays a configuration script.*
help	*- Displays a list of commands.*
reset	*- Resets firewall configuration to default.*
set	*- Sets firewall configuration.*
show	*- Shows firewall configuration.*

As shown above ? command prints help for the commands available in netsh context.

Default settings of firewall prevents:

-ICMP ECHO requests to the machine running firewalls. Users can't ping that machine.
-File and print sharing is disabled. Users can't share folders with other users on the network.

Let us change default settings through command line.

Allowing incoming ICMP ECHO Requests

To allow Incoming ICMP ECHO requests give following command:

netsh firewall>set icmpsetting 8 ENABLE
Ok.

Now other users on the network should be able to ping 192.168.7.113.

To disable this feature give following command:

netsh firewall>set icmpsetting 8 DISABLE
Ok.

Enabling File and Printer sharing

netsh firewall>set service

This command will show help for set service command.

netsh firewall>set service FILEANDPRINT ENABLE
Ok.

This will let all users on the network to access shared resources on the host 192.168.7.113.

If I wish that only users on the subnet 192.168.7.0/24 should be able to access shared resources on 192.168.7.113 then I can specify that with:

netsh firewall>set service FILEANDPRINT ENABLE CUSTOM 192.168.7.0/24
Ok.

Turning Off Firewall
To turn off firewall through command line give following command in the netsh firewall context

netsh firewall>set opmode disable
Ok.

This will turn off firewall. You can verify the same through control panel. To enable firewall again give following command:

netsh firewall>set opmode enable
Ok.

Disabling Don't Allow Exceptions

In Windows XP Firewall we can specify exceptions that the firewall will allow.
If Don't allow exceptions check box is enabled then programs and ports mentioned in exceptions are not allowed by the firewall.

In default XP Firewall don't allow exceptions check box is not enabled.

Let us enable the check box through command line:

netsh firewall>set opmode enable disable
Ok.

Let us disable the check box.
netsh firewall>set opmode enable enable
Ok.

Allowing Specific programs

In firewall control panel in the exceptions tab we can add programs that should be allowed through firewall.

For example, I want to run netcat on my machine. netcat is called swiss army knife in the security field and is used for many purposes.

For example, I want netcat to listen on port TCP 5000 on my machine. For that I will issue following command:

C :> nc.exe –l –p 5000

Firewall will immediately prompt me and ask me whether I want to allow this program or not.

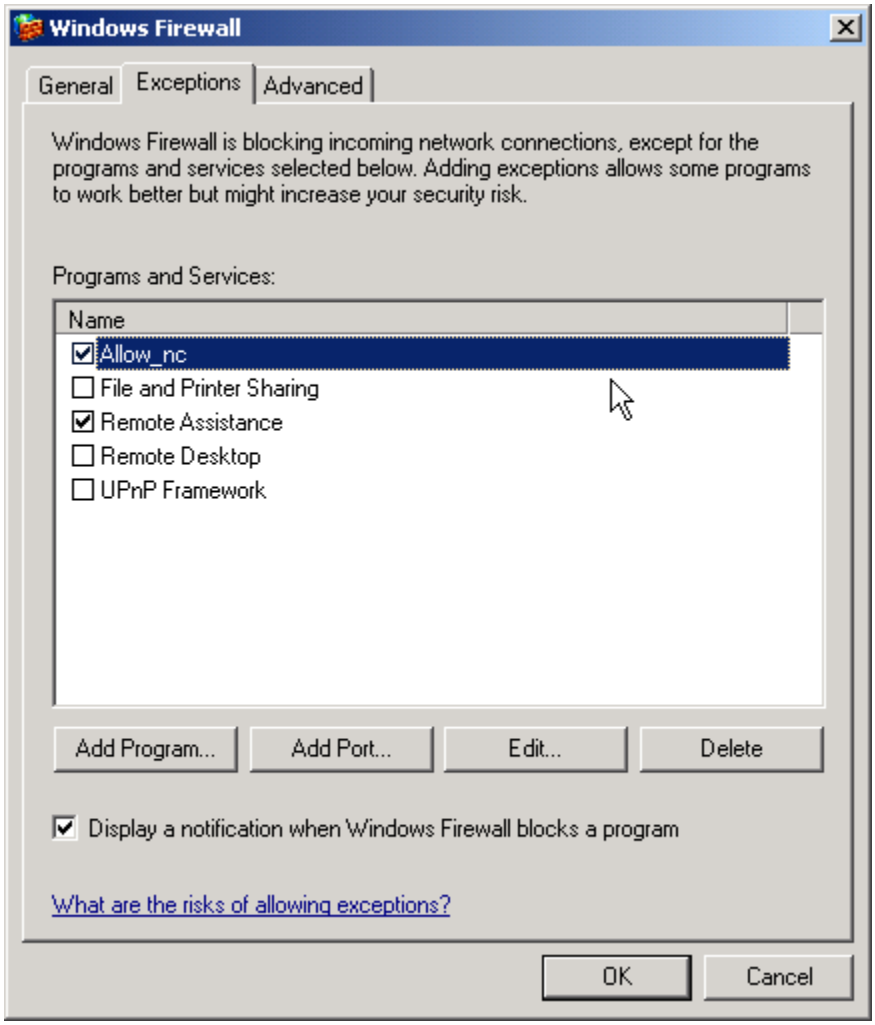
Let's click on the keep blocking button. This means that next time when we run nc.exe it will block nc.exe from running.

Now let us allow nc.exe through command line and add it to the exceptions list.

netsh firewall>set allowedprogram

This command will show you usage for set allowedprogram.

netsh firewall>set allowedprogram c:\nc.exe allow_nc ENABLE
Ok.



As shown above our command adds allow_nc to the list of exception programs.

Now try to connect to port 5000 from other machine. You should be able to connect.

Resetting Firewall to default settings

Now we have played enough with the firewall and let us change it to the default settings.

netsh firewall>reset
Ok.

This will change firewall to the default state. All our modifications will be gone.