Windows XP
OEM Preinstallation Kit
Design Notes

Microsoft® Windows® Family of Operating Systems

Using the Windows Firewall .Inf File in Microsoft® Windows® XP Service Pack 2

July 14, 2004

Abstract:

Microsoft Windows XP Service Pack 2 (SP2) includes significant enhancements to the Windows Firewall component (formerly known as the Internet Connection Firewall). Windows Firewall is a stateful host firewall that discards unsolicited incoming traffic, providing a level of protection for computers against malicious users or programs. To provide better protection for computers connected to any kind of network (such as the Internet, a home network, or an organization network), Windows XP SP2 enables Windows Firewall on all network connections by default. Network administrators can use the Windows Firewall .inf file (Netfw.inf) to modify default settings either before installation or after installation. This article describes the usage of the Windows Firewall .inf file.

Contents

Overview

Windows XP Service Pack 2 (SP2) includes significant enhancements to Windows Firewall, formerly known as the Internet Connection Firewall (ICF). Windows Firewall is a stateful, host-based firewall that drops all unsolicited, incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic). This behavior of Windows Firewall provides a level of protection from malicious users and programs that rely on unsolicited, incoming traffic to attack computers.

A new feature in Windows XP SP2 is the enabling of Windows Firewall by default during an installation of Windows XP or during an update to Windows XP SP2. Because Windows Firewall is enabled by default, network administrators need the flexibility to modify the default configuration of Windows Firewall during the installation of Windows XP SP2 and after its installation. Typical configuration modifications include adding programs to Windows Firewall's exception list or disabling Windows Firewall, for example, if a third-party, host-based firewall is already installed and enabled.

Windows Firewall can be preconfigured by modifying the Windows Firewall .inf file, named Netfw.inf, in which Windows Firewall's default configuration is stored. During an installation of or an update to Windows XP SP2, Windows Firewall imports its configuration from this .inf file. This means that any modifications made to the Windows Firewall .inf file before an installation of Windows will automatically be incorporated into the default configuration of Windows Firewall.

Scenarios for Modifying Default Windows Firewall Configuration

The following are common scenarios for modifying the default configuration of Windows Firewall.

Third-Party Firewall-Enabled

An original equipment manufacturer (OEM) may choose to provide its customers with a third-party, host-based firewall. If this firewall is enabled by default, then it is recommended that Windows Firewall be disabled. This can be done by modifying the Windows Firewall .inf file to disable Windows Firewall by default.

Preinstalled Programs

An OEM or enterprise may choose to install a suite of programs by default. Some of these programs may need to receive unsolicited, incoming traffic in order to function correctly. Windows Firewall can be configured to enable specific, unsolicited, incoming traffic by default by adding the programs to the Windows Firewall's exceptions list. This can be done by adding entries for the programs to the Windows Firewall .inf file. Only programs that require unsolicited, incoming traffic should be added to the exceptions list; programs that do not require unsolicited, incoming traffic should not be added to the exceptions list.

Pre-Opened Ports

An enterprise may choose to use various network services and want to ensure that the network traffic for those services is enabled by default through Windows Firewall. For example, an enterprise may use some of the remote management functionality included in Windows XP. You can configure Windows Firewall to open the necessary ports by default by adding them to the Windows Firewall's exceptions list. Specifically, you can add entries for the TCP or UDP ports to the Windows Firewall .inf file. Statically opening ports does potentially increase a computer's exposure to attack, so the number of ports opened in Windows Firewall by default should be at a minimum.

Location of Windows Firewall .Inf File

On a Windows XP CD image, the location of the Windows Firewall .inf file is:

Cd_drive:\I386\Netfw.in_

Note: On a Windows XP CD image, the file's name is Netfw.in_ (not Netfw.inf). This is for signing purposes. If an OEM modifies this file, the file must also be re-signed.

After the installation of Windows XP SP2, the location of the Windows Firewall .inf file is:

%WINDIR%\Inf\Netfw.inf

Methods for Replacing the Default Windows Firewall Configuration

Method 1: Pre-Installation

1. Copy the default Windows Firewall .inf file (Netfw.in_) from a Windows XP SP2 CD image.
2. Make the desired modifications to the .inf file. Directions for modifying the .inf file are provided in the "Configuration Options Provided in the Windows Firewall .Inf File" section of this article.
3. Save the modified .inf file as Netfw.in_.
4. Sign the modified Netfw.in_.
5. Replace the default Netfw.in_ with the modified Netfw.in_ in the Windows XP SP2 CD image.
6. Install Windows XP SP2 from the modified Windows XP SP2 CD image.

Method 2: Post-Installation

1. Copy the default Windows Firewall .inf file (Netfw.inf) from an installation of Windows XP SP2.
2. Make the desired modifications to the .inf file. Directions for modifying the .inf file are provided in the "Configuration Options Provided in the Windows Firewall .Inf File" section of this article.
3. Save the modified .inf file as Netfw.inf.
4. Replace the default Netfw.inf with the modified Netfw.inf in the installation of Windows XP SP2.
5. Run the **netsh firewall reset** command on the computer running Windows XP SP2. You can do this manually by typing the command at a command prompt or by including the command in a run-once script.

Default Windows Firewall .Inf File

The default contents of the Netfw.inf file are the following:

```
[Version]
Signature      = "$Windows NT$"
DriverVer      =07/01/2001,5.1.2600.2132

[DefaultInstall]
AddReg = ICF.AddReg.DomainProfile
AddReg = ICF.AddReg.StandardProfile

[ICF.AddReg.DomainProfile]
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\AuthorizedApplications\List","%WINDIR%\system32\
sessmgr.exe",0x00000000,"%WINDIR%\system32\
sessmgr.exe:*:enabled:@xpsp2res.dll.-22019"

[ICF.AddReg.StandardProfile]
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\AuthorizedApplications\List","%WINDIR%\
system32\sessmgr.exe",0x00000000,"%WINDIR%\system32\
sessmgr.exe:*:enabled:@xpsp2res.dll.-22019"
```

The first two sections of Netfw.inf contain versioning and configuration information, and do not need to be modified. The sections that are significant for modifying the default configuration for Windows Firewall are the following:

- **[ICF.AddReg.DomainProfile]** – Windows Firewall maintains two sets of configuration known as profiles. One profile is used when a computer is connected to the domain to which it is joined, while the other profile is used when the computer is not connected to its domain. This section is for defining changes to Windows Firewall's default configuration when a computer is connected to a network that contains its domain.
- **[ICF.AddReg.StandardProfile]** – This section is for defining changes to Windows Firewall's default configuration when a computer is not connected to a network that contains its domain. If a computer is not a member of a domain, then Windows Firewall will always enforce the configuration stored in the Standard Profile.

Configuration Options Provided in the Windows Firewall .Inf File

The majority of the default configurations for Windows Firewall can be defined in the Windows Firewall .inf file. This includes the following settings:

- Operational mode
- Disable notifications
- Block unicast responses to multicast and broadcast packets
- Enable Remote Administration
- Enable ICMP messages
- Open ports
- Enable programs

These settings are described in the next sections.

Notes: All of the settings made in the Windows Firewall .inf file will be applied to all of a computer's network interfaces.

You cannot open ports nor enable ICMP messages for individual interfaces through the Windows Firewall .inf file.

Logging settings cannot be defined through the Windows Firewall .inf file.

Changing Windows Firewall's Default Operational Mode

- Windows Firewall can be placed in one of three operational modes:
- **On** – This is the default operational mode for Windows Firewall. In this mode, Windows Firewall drops all unsolicited, incoming traffic, except those matching enabled entries in Windows Firewall's exceptions lists. Because this is the default operational mode, no entries need to be included in the Windows Firewall .inf file.
    - The assumed entries for the Domain Profile in the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file are:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile","DoNotAllowExceptions",0x00010001,0

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile","EnableFirewall",0x00010001,1
```

    - The assumed entries for the Standard Profile in the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file are:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile","DoNotAllowExceptions",0x00010001,0

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile","EnableFirewall",0x00010001,0x00000001
```

- **On with No Exceptions** – In this mode, Windows Firewall blocks all unsolicited, incoming traffic, even those matching enabled entries in Windows Firewall's exceptions lists.

    - To make this the default operational mode for the Domain Profile, add the following entries to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile","DoNotAllowExceptions",0x00010001,1

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile","EnableFirewall",0x00010001,1
```

    - To make this the default operational mode for the Standard Profile, add the following entries to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile","DoNotAllowExceptions",0x00010001,1

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile","EnableFirewall",0x00010001,1
```

- **Off** – In this mode, Windows Firewall is disabled and does not do any filtering of unsolicited, incoming traffic. All unsolicited, incoming traffic is enabled, and Windows Firewall does not help to protect the computer from network attacks.

    - To make this the default operational mode for the Domain Profile, add the following entries to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile","DoNotAllowExceptions",0x00010001,0

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile","EnableFirewall",0x00010001,0
```

    - To make this the default operational mode for the Standard Profile, add the following entries to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile","DoNotAllowExceptions",0x00010001,0

HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile","EnableFirewall",0x00010001,0
```

Disabling Windows Firewall's Notifications

By default, Windows Firewall displays a notification to users when a program not already included in the Windows Firewall exceptions list uses the new Windows Firewall APIs to add itself or its traffic to an exceptions list. By adding the appropriate entries to the Windows Firewall .inf file, these notifications can be disabled in either or both of Windows Firewall's profiles.

- To disable notifications by default in the Domain Profile, add the following entry to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile","DisableNotifications",0x00010001,1
```

- To disable notifications by default in the Standard Profile, add the following entry to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile","DisableNotifications",0x00010001,1
```

Blocking Unicast Responses to Multicast and Broadcast Packets

By default, Windows Firewall enables incoming, unicast-response packets to a port for three seconds after a multicast or broadcast packet is sent from the port. By adding the appropriate entries to the Windows Firewall .inf file, this behavior can be disabled in either or both of Windows Firewall's profiles.

- To block unicast responses to multicast and broadcast packets by default in the Domain Profile, add the following entry to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\
DomainProfile","DisableUnicastResponsesToMulticastBroadcast",0x00010001,1
```

- To block unicast responses to multicast and broadcast packets by default in the Standard Profile, add the following entry to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\
StandardProfile","DisableUnicastResponsesToMulticastBroadcast",0x00010001,1
```

Enabling Remote Administration

Windows Firewall includes a Remote Administration option that alters its configuration to enable Remote Procedure Call (RPC) and Distributed Component Object Model (DCOM) communication. Enabling this option statically opens TCP 135 and TCP 445 to unsolicited, incoming traffic. Additionally, communication over named pipes is permitted, and ports are dynamically opened as needed by Windows services using RPC. By adding the appropriate entries to the Windows Firewall .inf file, you can enable the Remote Administration option in either or both of Windows Firewall's profiles.

- To enable Remote Administration by default in the Domain Profile, add the following entry to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\RemoteAdminSettings","Enabled",0x00010001,1
```

- To enable Remote Administration by default in the Standard Profile, add the following entry to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\RemoteAdminSettings","Enabled",0x00010001,1
```

When enabling Remote Administration, the set of IP addresses from which unsolicited, incoming traffic is accepted can also be specified through an additional entry in the appropriate section of the Windows Firewall .inf file.

To define the default scope for Remote Administration in the Domain Profile, add the following entry to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\
RemoteAdminSettings","RemoteAddresses",0x00000000,scope
```

To define the default scope for Remote Administration in the Standard Profile, add the following entry to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\
RemoteAdminSettings","RemoteAddresses",0x00000000,scope
```

Permitted values for *scope* are defined in the “Defining the Scope for an Entry in the Windows Firewall .Inf File" section of this article.

Allowing ICMP Messages through Windows Firewall

While the default configuration for Windows Firewall blocks all ICMP message types, you can modify this behavior by adding entries to the Windows Firewall .inf file that enable certain ICMP message types by default.

To enable an ICMP message type by default in the Domain Profile, add the following entry to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\IcmpSettings","ICMP Message Type",0x00010001,1
```

To enable an ICMP message type by default in the Standard Profile, add the following entry to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\IcmpSettings","ICMP Message Type",0x00010001,1
```

Both of these entries require an *ICMP Message Type* to be specified. The permitted values for *ICMP Message Type* are listed in Table 1.

Table 1. ICMP Message Types

ICMP Message Type	Number	Description
AllowOutboundPacketTooBig	2	When an Internet Protocol version 6 (IPv6) packet is too large to be forwarded, data is dropped and a computer replies to the sender with a Packet Too Big message.
AllowOutboundDestinationUnreachable	3	Sent data that fails to reach this computer due to an error is discarded and reported with a Destination Unreachable message explaining the failure.
AllowOutboundSourceQuench	4	When a computer’s ability to process incoming data cannot keep up with the rate of a transmission,

		data is dropped and the sender is asked to transmit more slowly.
AllowRedirect	5	Data sent from a computer is rerouted.
AllowInboundEchoRequest	8	Messages sent to a computer are repeated back to the sender. This is commonly used for troubleshooting (for example, to ping a computer).
AllowInboundRouterRequest	10	A computer responds to router discovery messages.
AllowOutboundTimeExceeded	11	When a computer discards a packet because its hop count was exceeded or it ran out of time to assemble fragments of a packet, it replies to the sender with a Time Exceeded message.
AllowOutboundParameterProblem	12	When a computer discards data that it has received because of a problematic header, it replies to the sender with a Parameter Problem error message.
AllowInboundTimestampRequest	13	A confirmation message is sent, indicating the time that the data was received at a computer.
AllowInboundMaskRequest	17	A computer listens for and responds to requests for a network subnet mask.

Adding Static Ports to Windows Firewall's Default Exceptions List

In Windows XP SP2, Windows Firewall maintains an exceptions list for each of its two profiles. When in normal operation, Windows Firewall statically opens ports that are included in its current profile's exceptions list. It is generally recommended that programs be added to the exceptions list, instead of statically opening ports. This enables Windows Firewall to open and close ports dynamically and to minimize the number of ports open at any one time. It is recognized, however, that there are scenarios in which ports need to be statically opened. For example, a static port may need to be opened in order for a Windows service to receive unsolicited, incoming traffic. To support such scenarios, OEMs have the ability to add static ports to either or both of Windows Firewall's default exceptions lists through the Windows Firewall .inf file.

To add a static port to the Domain Profile's exceptions list, an entry in the following format should be added to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\GloballyOpenPorts\List","port
number:protocol",0x00000000, "port number:protocol:scope:mode:port's friendly
name"
```

To add a static port to the Standard Profile's exceptions list, an entry in the following format should be added to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\GloballyOpenPorts\List","port
number:protocol",0x00000000, "port number:protocol:scope:mode:port's friendly
name"
```

In the two entries above, the following elements must be defined, based upon the port added to Windows Firewall's default exceptions lists and the desired behavior:

- *port number* – A port is specified by the combination of a protocol and a port number. The port number must be between 1 and 65535 inclusive.
- *protocol* – A port is specified by the combination of a protocol and a port number. The protocol must be either **TCP** or **UDP**.
- *scope* – Permitted values for *scope* are defined in the "Defining the Scope for an Entry in the Windows Firewall .Inf File" section of this article.
- *mode* – An entry can be added to Windows Firewall's default exceptions lists as either enabled or disabled. The two permitted values for this element are **Enabled** and **Disabled**. If a port's entry is enabled, the port will be statically opened in Windows Firewall. If a port's entry is disabled, the port will not be statically opened in Windows Firewall.
- *port's friendly name* – This is the description that will be used to represent the entry for Windows Firewall in Control Panel. It should provide an indication of why the port is statically opened, such as "Web Server (TCP 80)" or "Telnet Server (TCP 23)".

As an example for opening a port, two entries are required to enable the static port used by the Internet Key Exchange (IKE) protocol, which uses UDP 500, for a scope of all IP addresses in the default exceptions lists for both of Windows Firewall's profiles.

This entry is added to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\GloballyOpenPorts\
List","500:UDP",0x00000000,"500:UDP:*:enabled:IKE (UDP 500)"
```

This entry is added to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\GloballyOpenPorts\List","500:UDP",0x00000000,
"500:UDP:*:enabled:IKE (UDP 500)"
```

Adding Programs to Windows Firewall's Default Exceptions List

In Windows XP SP2, Windows Firewall maintains an exceptions list for each of its two profiles. When in normal operation, Windows Firewall dynamically opens the ports used

by programs in its current profile's exceptions list. The Windows Firewall .inf file can be used to add programs to either or both of Windows Firewall's default exceptions lists. Only programs that actually require unsolicited, incoming traffic should be added to the exceptions lists; there is no benefit to adding programs that use only outgoing connections to the exceptions lists.

To add a program to the Domain Profile's exceptions list, an entry in the following format should be added to the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\AuthorizedApplications\List","program's image
path",0x00000000,"program's image path:scope:mode:program's friendly name"
```

To add a program to the Standard Profile's Exceptions List, an entry in the following format should be added to the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\AuthorizedApplications\List","program's image
path",0x00000000,"program's image path:scope:mode:program's friendly name"
```

In the two entries above, the following elements must be defined, based upon the program added to Windows Firewall's default exceptions lists and the desired behavior:

- *program's image path* – This is the fully qualified path for the file to be added to Windows Firewall's default exceptions lists. It may include environmental variables, such as %ProgramFiles%.
- *scope* – Permitted values for *scope* are defined in the "Defining the Scope for an Entry in the Windows Firewall .Inf File" section of this article.
- *mode* – An entry can be added to Windows Firewall's default exceptions lists as either enabled or disabled. The two permitted values for this element are **Enabled** and **Disabled**. If a program's entry is enabled, ports are dynamically opened in Windows Firewall for the program when it opens ports. If a program's entry is disabled, ports will not be dynamically opened in Windows Firewall for the program.
- *program's friendly name* – This is the name that is used to represent the entry in the Windows Firewall user interface. It should include the product name and publisher, such as **MSN Messenger v6.1** or **AOL Instant Messenger v5.5**.

As an example of enabling programs, two entries are included in the Windows Firewall .inf file to enable Remote Assistance with a scope of all IP addresses in the default exceptions lists for both Windows Firewall profiles.

This entry is included in the **[ICF.AddReg.DomainProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\DomainProfile\AuthorizedApplications\List","%WINDIR%\system32\
sessmgr.exe",0x00000000,"%WINDIR%\system32\
sessmgr.exe:*:enabled:@xpsp2res.dll,-22019"
```

This entry is included in the **[ICF.AddReg.StandardProfile]** section of the Windows Firewall .inf file:

```
HKLM,"SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\
FirewallPolicy\StandardProfile\AuthorizedApplications\List","%WINDIR%\
system32\sessmgr.exe",0x00000000,"%WINDIR%\system32\
sessmgr.exe:*:enabled:@xpsp2res.dll,-22019"
```

Defining the Scope for an Entry in the Windows Firewall .Inf File

When enabling Remote Assistance, opening a port, or enabling a program, the set of IP addresses from which the unsolicited, incoming traffic is enabled can be defined. This set of IP addresses from which unsolicited, incoming traffic is enabled is the scope of the exception. There are three options for defining the scope for a Windows Firewall exception.

- **All IP addresses** – This is the default scope for a Windows Firewall exception, and it enables unsolicited, incoming traffic that matches the exception from any computer. In the Windows Firewall .inf file, making an entry's scope element an asterisk ("*****") results in a scope of all IP addresses for the entry.
- **Local subnet only** – This scope enables unsolicited, incoming traffic that matches the exception from any computer on the same subnet as the network connection on which the traffic was received through Windows Firewall, while dropping unsolicited, incoming traffic from all other computers. When a computer's subnet changes, the set of enabled IP addresses dynamically changes to match the new subnet. In the Windows Firewall .inf file, making an entry's scope element **LocalSubnet** results in a local subnet-only scope for the entry.
- **Custom** – The final option is to define a custom scope, which is a list of IPv4 addresses and address ranges that typically correspond to subnets. Unsolicited, incoming traffic that matches the exception and originates from a computer with an IPv4 address in the defined list is enabled through Windows Firewall. Unsolicited, incoming traffic from computers with IPv4 addresses that are not in the list is dropped. A custom scope can include the local subnet (using the "LocalSubnet" string), IPv4 addresses, and IPv4 address ranges, but cannot include IPv6 addresses and IPv6 address ranges. For IPv4 address ranges, you can specify the range using a dotted decimal subnet mask notation or a prefix length (*w.x.y.z/n*). When you use a dotted decimal subnet mask, you can specify the range as an IPv4 network ID (such as 10.47.81.0/255.255.255.0) or by using an IPv4 address within the range (such as 10.47.81.231/255.255.255.0). When you use a network prefix length, you can specify the range as an IPv4 network ID (such as 10.47.81.0/24) or by using an IPv4 address within the range (such as 10.47.81.231/24). Some examples of custom scope elements include the following:
  - 192.168.0.5
  - 192.168.0.0/255.255.255.0
  - 192.168.0.5,LocalSubnet
  - 157.54.0.1,172.16.0.0/12,10.0.0.0/255.0.0.0,LocalSubnet
  - 10.91.12.56,10.7.14.9/255.255.255.0,10.116.45.0/255.255.255.0,172.16.31.11/24,172.16.111.0/24

Note: You cannot have any spaces between the entries in the list of sources, or the entire list is ignored and Windows Firewall uses the default scope of any source IPv4 address. This can create an unintended vulnerability. Please double-check your scope syntax before saving changes to the Windows Firewall .inf file.

Summary

To install Windows XP SP2 with customized default settings for the new Windows Firewall or to change settings after installation, use the Windows Firewall .inf file (Netfw.inf). The Windows Firewall .inf file contains two main sections: **[ICF.AddReg.DomainProfile]** for modifying Windows Firewall settings for the domain profile, **[ICF.AddReg.StandardProfile]** for modifying settings for the standard profile, and **[Strings]** for defining strings for some settings. Typical uses of the Windows Firewall .inf file include disabling the Windows Firewall (if a third-party .inf file is already installed and enabled) and adding either programs or ports to the Windows Firewall exceptions lists (one list for each profile).

Related Links

See the following resources for more information:

- Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2 at http://www.microsoft.com/downloads/details.aspx?familyid=4454e0e1-61fa-447a-bdcd-499f73a637d1&displaylang=en
- Manually Configuring Windows Firewall in Windows XP Service Pack 2 at http://www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx
- Windows XP Service Pack 2: Resources for IT Professionals at http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.mspx

For the latest information about Windows XP, see the Windows XP Web site at http://www.microsoft.com/windowsxp.