GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Windows Security Center and Window Firewall

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4c
Option 1 - Research on Topics in Information Security

Author - David Douglas
Submitted - January 24, 2005

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract

The explosive growth of the Internet, the dominance of Microsoft Windows in the computer world, and the dramatic increase in virus and worm activity has prompted Microsoft to greatly increase the attention they give to Windows security.

Microsoft Windows XP Service Pack 2 is the latest result of this new focus. The Service Pack was designed to greatly increase the security of the default configuration of Windows. The security highlights of this update are Windows Security Center and Window Firewall. This document explores the operation and configuration of these two products and how they effect Automatic Updates and Anti-Virus protection.

Windows Firewall is also useful in a corporate environment and can be managed via group policies in an Active Directory Domain. A brief overview of the settings available via group policy is provided. The usage of the netsh firewall command line to configure the firewall is also briefly covered.

Windows Firewall has been criticized for not blocking outgoing traffic and for providing an API that allows software to activate or deactivate it, but overall it provides for a more secure default installation of Microsoft Window than previously existed.

Introduction

The Internet connects the entire world in a global network of interconnected and interdependent computers. According to the International Telecommunications Union there were approximately 593 million personal computers and 687 million Internet users in the world in 2003. This is a 13 percent in the number of personal computers and a 39 percent increase in the number of Internet users from 2001 to 2003. These 687 million users are beginning to depend on the Internet for everything from checking the latest sports scores to interacting with their financial institutions to accepting customer orders. They need an Internet that is secure, stable and available.

Statistics complied by W3Schools, a web development tutorial site, suggest that nearly 90 percent of the web traffic comes from computers running a version of Microsoft Windows. Errors and vulnerabilities discovered in this operating system can cause considerable problems for Windows users and everyone else connected to the Internet, and over the last several years, Windows has had more than its fair share of problems.

2001 was a very busy year for large-scale worm/virus outbreaks. Viruses like

© SANS Institute 2000 - 2005 Author retains full rights.

Melissa and Love Bug (both spread by Outlook) caused considerable difficultly in 1999 and 2000, but 2001 brought about viruses like CodeRed, Nimda, Sircam, BadTrans. These viruses infected hundreds of thousands of systems, replicated through a variety of means, and spread exclusively to Windows systems.

The worm/virus outbreaks of 2001 seem to have sent a message to Microsoft. On January 15, 2002, Microsoft Chairman Bill Gates sent out an email to Microsoft and subsidiaries titled "Trustworthy Computing." In this email he declared, "Trustworthy Computing is the highest priority for all of the work we are doing" (qtd. in CNET News.com Staff.) Gates describes a system in which computing has the reliability and ubiquity of public utilities like electricity and telephony. He also added that Microsoft worked to always provide their customers with increased features, but that now, when faced with a decision between features and security, Microsoft must choose security.

The reaction to the "Trustworthy Computing" email was mixed. Many analysts called the email more of a public relations stunt than a change in policy, but Microsoft appeared to be making a serious commitment to security. The release of Windows Server 2003 was delayed on three separate occasions, delays attributed to security. When Microsoft Windows Server 2003 was finally released, it showed a marked improvement in security over its predecessors. One of the many signs of this improvement was the difference between the versions of Internet Information Services. Microsoft's web server product had previously installed with almost all of its capabilities active and running, regardless of environment, need, or security risk. The newest incarnation of the product now installed with nearly every feature disabled or in a high security mode. Now the end user only had to worry about activating the features they needed instead of securing those that they did not. The company also spent around $100 million retraining 8,500 developers in secure coding and then redoing large sections of the Windows code.

Microsoft didn't receive much acclaim for their security initiatives. In Jan 2003 the Slammer wormed caused havoc on the Internet, despite the fact that patches for the vulnerability in question had been available for six months. In August 2003 the MSBlast worm used a flaw in the Remote Procedure Call service of Windows to compromise 9.5 million Windows machines.

The effects of the blaster worm seemed to drive Microsoft to dedicate its focus towards security related fixes for both the desktop customer and the server customer. They announced that the upcoming Windows XP Service Pack 2 would be dedicated to improving the security of Windows. Microsoft shifted priority away from Windows 2003 Service Pack 1 and development of the next generation OS, Windows Longhorn. Many new security-related features being developed for Windows Longhorn would be incorporated into Windows XP with Service Pack 2.

© SANS Institute 2000 - 2005 Author retains full rights.

Service Pack 2 contains a variety of security related fixes, but the key improvements are the Security Center dashboard and the Windows Firewall. These two products work together to provide more security an simpler security for the average Windows user.

© SANS Institute 2000 - 2005, Author retains full rights.

Security Center

The Security Center is designed to provide an easy to understand view into the status of three key system "security essentials": Windows Firewall, Automatic Updates, and Virus Protection. The Security Center shows each security essential and a color-coded status of that product. When a security essential is configured properly, the security essential shows a green light and is compacted down. Security essentials in a less acceptable state have a yellow light and show an expanded help explanation of the problem. Security essentials that are missing, disabled, or otherwise have a serious problem, display in red.

Windows Security Center

The picture above shows a computer where the Firewall is working properly. Its Automatic Updates are configured to download and install only after approved by the user. Since this is not the recommended setting the security essential displays in yellow. Finally, for Virus Protection, Security Center does not know how to interface with the installed version of Symantec AntiVirus, so this security essential displays in red.

When Windows detects any security essential that is in the red it notifies the user with a system tray icon and an audible alert. Clicking on the system tray icon opens the Security Center. Users have the option of disabling these alerts for security essentials in cases where a "red" condition is the desired one. The left side of the Security Center mostly contains links to related help resources, but the last link is "Change the way Security Center alerts me." The dialog that opens from this link shows each security essential, a brief description of the alert for that essential, and a check box. The Automatic Updates essential

© SANS Institute 2000 - 2005 Author retains full rights.

explains: “Alert me if my computer might be at risk because of my Automatic Updates settings.” If the system administrator of this machine didn’t want any updates downloaded or install until their impact could be properly judged, that essential may be unchecked to avoid pestering the user with undesired alerts.

Windows Security Center cannot obtain information from the installed version of Symantec AntiVirus in the picture above. Clicking on the “Recommendations…’ button opens a new dialog. This dialog explains the problem in general terms and suggests the user check on replace their anti-virus software. Down at the bottom of the dialog there is a check box that reads: “I have an antivirus program that I’ll monitor myself.” Checking this option and clicking OK changes the status of the Virus Protection security essential from red to yellow. The status changes to NOT MONITORED. Third party products released before Windows Security Center will likely not work with the product and a new, compatible version will have to be obtained to take advantage of Security Center.

The Security Center also provides shortcuts to open several security related tools. The Automatic Updates tool opens a configuration dialog for automatic updates. The dialog contains four update settings: “Automatic”, “Download updates for me, but let me choose when to install them”, “Notify me but don’t automatically download or install them”, and “Turn off Automatic Updates.” “Automatic” is the Recommended option. This is the only option will display green in the Security Center. The “Automatic” update option also allows the user to set the time of day that the updates will occur. “Download updates for me, but let me choose when to install them” and “Notify me but don’t automatically download or install them” display yellow statuses in the Security Center. The “Turn off Automatic Updates” option causes the Security Center to show red for this security essential. For environments where this is the desired setting, system administrator controlled updates is one example, the “Change the way Security Center alerts me” option on the left side of the Security Center can be used to disable the alert.

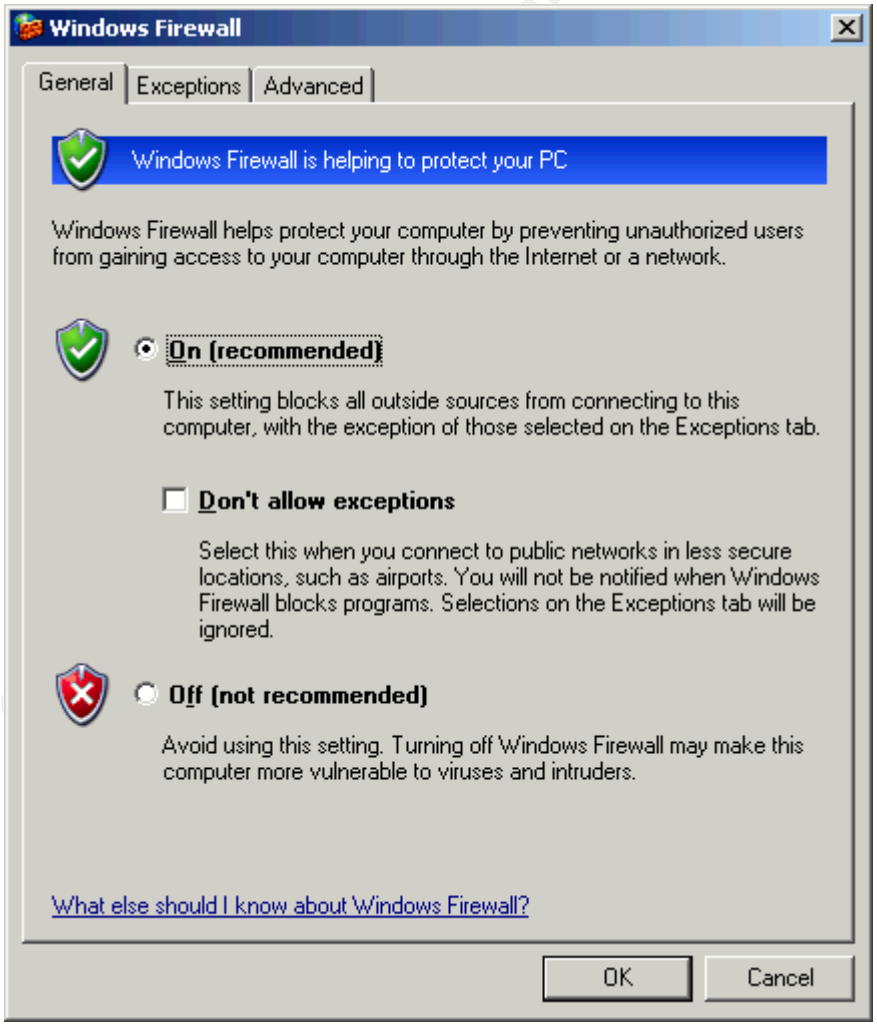
The last security tool shown in the display is “Windows Firewall.” This is a shortcut to the settings dialog for Windows Firewall.

© SANS Institute 2000 - 2005 Author retains full rights.

Windows Firewall

The security centerpiece of Microsoft Windows XP Service Pack 2 is the new and improved Windows Firewall. Windows Firewall is a stateful host firewall that blocks incoming traffic that isn't in response to an earlier connection made by the host computer. This behavior is designed to help protect against viruses, worms and malicious users that are attempting to connect to unused open ports, or ports running little known services and protocols. Windows Firewall replaces the Internet Connection Firewall that was included in Windows XP and Windows XP Service Pack 1.

Windows Firewall's single greatest feature is that it is active by default. While the product is a substantial improvement over the older ICF, ICF also would have provided some protection if most users didn't leave it un-configured and inactive. Now the scores of Windows users in the world that know nothing about their computer or computer security are protected by a personnel firewall (at least those users running Windows XP Service Pack 2).



© SANS Institute 2000 - 2005 Author retains full rights.

Windows Firewall – General tab

The configuration dialog for Windows firewall contains three tabs: General, Exceptions, and Advanced. The General tab is the default tab displayed when the Windows Firewall dialog is opened. This tab controls the run mode of the firewall. Windows Firewall contains three different run modes. The first mode, "On," runs the firewall with the currently configured exceptions. This is the recommended option and shows a green status in the Windows Security Center.

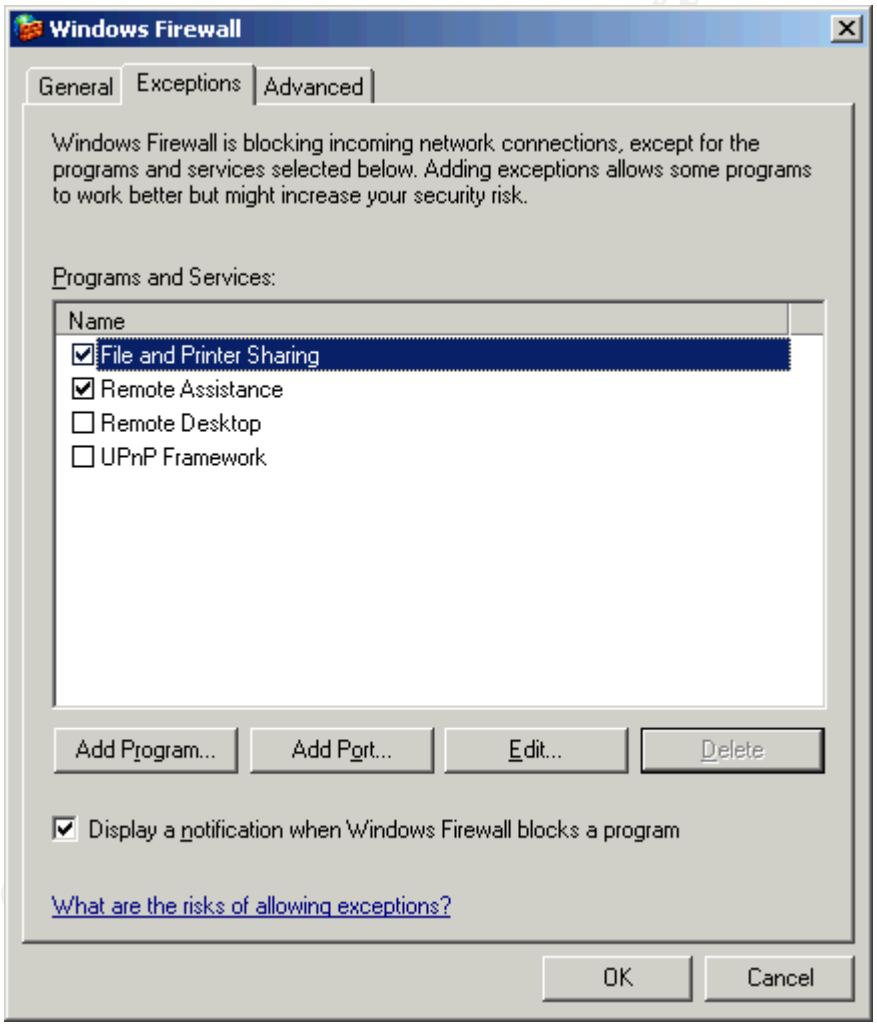
The second run mode is controlled by the checkbox located below the "On" mode. "Don't allow exceptions" is a feature particularly useful for laptops. When this mode is activated, the firewall stops all exceptions, blocking all incoming traffic requests regardless of other configuration settings. This mode is intended for use in unsecure / untrusted networks like wireless hotspots in airports and coffee shops. This is a more secure subset of the "On" mode and shows a green status in the Windows Security Center.

The final run mode available is "Off." The "Off" mode stops all firewall operations, allowing all incoming traffic to connect. According to Microsoft this setting should only be used when another personal firewall product is running on the machine. All of the Windows documentation recommends running a personal firewall product on every machine, regardless of any external firewalls or proxies that exist. Microsoft is now promoting a defense in depth philosophy with multiple firewall usage.

© SANS Institute 2000 - 2005 Author retains full rights.

Windows Firewall – Exception Tab

The second tab in the Windows Firewall configuration tool is the Exceptions tab. This tab is used to configure which programs and ports are allowed to accept incoming traffic. Exceptions can be configured by program name or by port number. They are also configured to allow a specific network scope. Creating an exception for a specific program allows that executable to listen on any port and accept connections from any IP address inside the defined scope. Port exceptions allow any executable to listen on that specific port and accept connections from any IP address with in the defined scope. Program exceptions tend to be more secure than port settings because the firewall only allows the traffic when a program is actually listening on a port.



Windows Firewall – Exception tab

There are four exceptions configured by default. These entries can be enabled or disabled as needed, but they cannot be deleted from the list. These exceptions are more complicated than those that can be created via the dialog.

© SANS Institute 2000 - 2005 Author retains full rights.

Some of the exceptions define multiple ports within one exception. These preconfigured exceptions may or may not be active by default. Their configuration depends on whether or not that Program or Service was active when the firewall was installed.

File and Printer Sharing provides exceptions for accessing resources via Microsoft networking. Activating this exception is required for viewing shared folders and printers on other computers. This exception opens UDP 137, UDP 138, TCP 139, and TCP 445. The scope for each of these ports is defined to be the local subnet.

Remote Assistance creates an exception for the executable %systemRoot%\sessmgr.exe. This exception has a global scope, so any IP address is allowed to connect. The sessmgr.exe program only starts when the user has requested assistance using the Remote Assistance tool. Remote Assistance provides its own security, but it can be a fairly significant security risk since it allows a remote user to take control of the system.

Remote Desktop opens TCP port 3389 to the entire Internet. Remote Desktop can be another significant security risk when running because it allows for a remote login to the machine.

UPnP Framework is for the Universal Plug and Play technology. Some network devices exist that use UPnP to make themselves available to computers. This exception should only be activated when needed for one of these UPnP devices. This exception opens TCP 2869 and UDP 1900 to the local subnet.

The “Add a Program” button opens a dialog to create a program exception. This dialog displays a list of all programs registered on the system. It also has a Browse button that allows the user to enter the path for the executable. Once the proper executable has been selected, the user can either select the OK button to activate the exception or use the “Change scope…” button to modify the allowed scope for the program. The default scope for program exceptions is the global “Any computer” scope.

The “Change scope” dialog offers the user three radio buttons to select a scope. The available options are “Any computer”, “My network (subnet) only”, and “Custom list.” “Any computer” does not place any IP address restrictions on the exception. This is the option to use when it is not practical to determine the IP addresses of the connecting computers, like an Instant Messaging client.

“My network (subnet) only” creates a scope based on the current computer settings. The IPv4 routing table determines this scope. In general this will only include computers located on the local subnet, but depending on the routing options, it may include a greater range of computers. If a route exists that bridges two subnets, than both subnets are part of the local subnet.

SANS Institute 2000 - 2005, Author retains full rights.

"Custom list" limits the connection to a specific list of computers. The list is a comma separate list of IP address and IP address ranges. The simplest form is an IPv4 address (e.g.: 10.47.81.23). The list can also support ranges based on network id (e.g. 10.47.81.0/255.255.255.0 or 10.47.81.0/24) or IP address (e.g. 10.47.81.231/255.255.255.0 or 10.47.81.231/24). Only IP addresses are allowed, hostnames or DNS names cannot be used.

Once the scope has been selected, clicking the OK button in the scope dialog and then in the "Add a Program" dialog activates the new exception.

The new program exception will appear in the list of exceptions. Removing the checkmark from the checkbox next to the exception will disable it. The Delete button can be used to completely remove an exception. The Edit button opens a dialog to edit the exception. In the Edit dialog the path for the program cannot be changed, but the "Change scope…" button can be used to edit the scope for the exception.

The "Add Port…" button is used to create a port based exception. The "Add a Port" dialog has a Name box and a Port number box. The name box is used to provide an identifier for this exception. The port number box accepts a port number between 1 and 65535. There are also two radio buttons for TCP or UDP. The "Change scope…" button can be used to determine a scope for the connection. Once the port is properly configured, the OK button will activate the exception. Removing the checkmark from the checkbox next to the exception will disable it. The Delete button can be used to completely remove an exception. The Edit button opens a dialog to edit the exception. The Edit dialog is functionally the same as the "Add a Port" dialog.

The Exceptions tab also has a checkbox for "Display a notification when Windows Firewall blocks a program." When this box is checked and a program attempts to start a listener on a port then a Windows Security Alert will display to the user. This dialog displays a friendly name for the program, lists the publisher of the program and offers three buttons: "Keep Blocking", "Unblock", and "Ask Me Later."

© SANS Institute 2000 - 2005 Author retains full rights.

Windows Security Alert

"Keep Blocking" creates an exception entry for the program but disables the exception. The firewall will continue to block the program, but a Windows Security Alert will not open the next time the program attempts to start a listener.

"Unblock" creates an exception for that program with a global scope and activates that exception to allow the program to create the listener now and in the future.

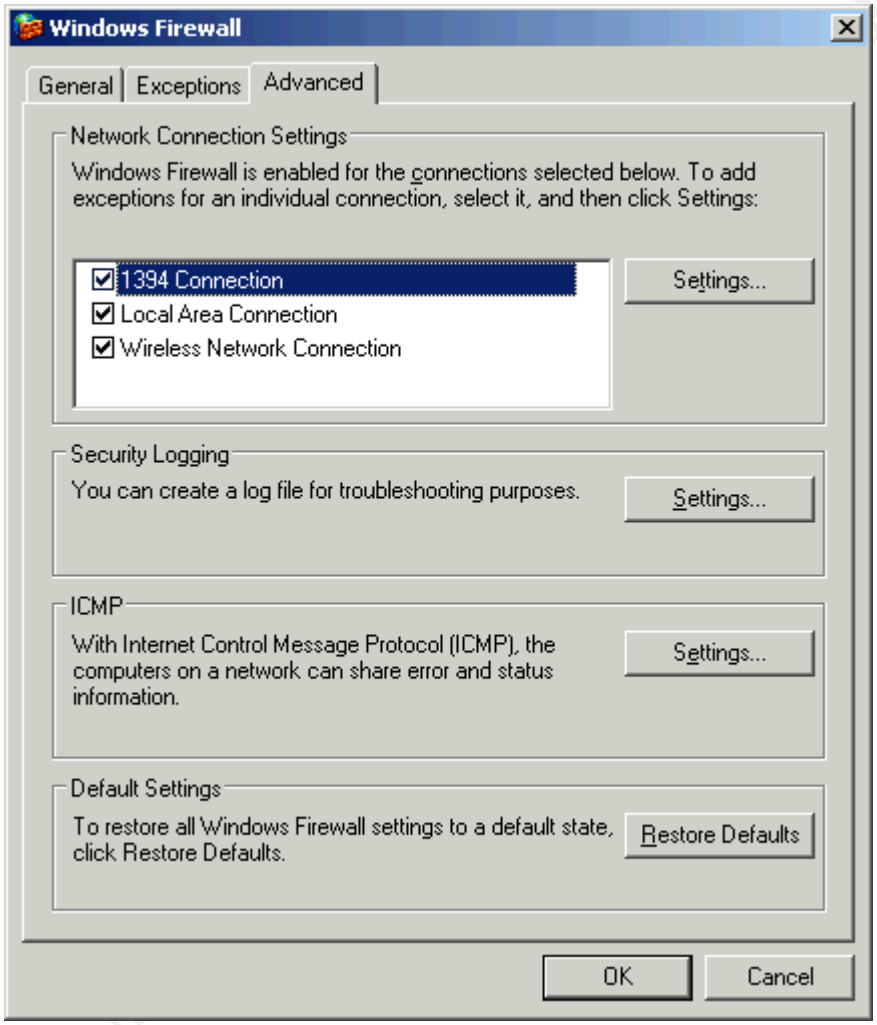
"Ask Me Later" continues to block the program but doesn't modify the exceptions list so that the user is informed the next time the program attempts to start a listener.

Windows Firewall does not notify the user if another computer attempts to connect to a blocked port. The firewall also does not display an alert when a service attempts to open a port, but the service will still not be able to receive any traffic on that port.

© SANS Institute 2000 - 2005 Author retains full rights.

Windows Firewall – Advanced Tab

The final tab in the Windows Firewall configuration tool is the “Advanced” tab. There are four different categories of options available under this tab: “Network Connection Settings”, “Security Logging”, “ICMP”, and “Default Settings.”



Windows Firewall – Advanced tab

“Network Connection Settings” allows for manipulation of the firewall rules on an interface-by-interface basis. Each interface, or connection, is shown with a checkbox next to it. Removing the checkmark from the checkbox next to a connection will disable Windows Firewall protection from that particular interface. By default, Windows Firewall runs on all connections on the computer, whether they are active or not.

Clicking on the “Settings…” button opens a dialog to select services that are allowed to run on this interface. The “Advanced Settings” dialog that opens is nearly identical to the interface from the original Internet Connection Firewall

© SANS Institute 2000 - 2005 Author retains full rights.

that was included in Windows XP and Windows XP Service Pack 1. This dialog can be used to add port exceptions that only apply to a specific interface. These exceptions are not visible in the Windows Firewall exceptions tab. Exceptions activated or created from this dialog always have a global scope. In general, it is better to create an appropriately scoped rule from the exceptions tab then to configure individual interfaces. The "Advanced Setting" dialog has a second tab for ICMP. This tab offers the same options as the ICMP settings discussed below, but only applies to the selected interface.

"Security Logging" is used to setup logging for Windows Firewall. The "Log Settings" dialog offers two logging options: "Log dropped packets" and "Log successful connections." Logging is disabled by default, but checking one or both logging options activates the logging. The dialog also has a field to specify where the log file is kept and a setting for the maximum size allowed for the log. Log entries record: date, time, action, protocol, source IP, destination IP, source port, destination port, packet size, TCP flags, TCP sync flag, TCP ack flag, TCP window, ICMP type, ICMP code, an info field, and a path field. When the log reaches its maximum size, the new log file has ".old" appended to its name and a new log file is started. This means the logs are of limited use for forensic analysis since old log entries are clobbered by the new log entries. Repeated requests to a blocked port could be used to conceal a successful connection on another port.

"ICMP" settings control which Internet Control Message Protocol requests are serviced and which are blocked. The dialog consists of a list of the various ICMP message and checkboxes to enable or disable that message. When TCP port 445 is in the exception list than the echo request message is automatically allowed and cannot be disabled.

The last option under the "Advanced" tab is the "Restore Defaults" button. This button will undo all customizations and restore Windows Firewall to its default settings. This button removes all custom exceptions. Unless the default configuration is modified all of the built in exceptions are disabled except for Remote Assistance.

© SANS Institute 2000 - 2005 Author retains full rights.

Windows Firewall and the Domain

Windows Firewall is an excellent tool for the home or small office user, but it can also be used to provide additional protection in a larger corporate network. Microsoft advices that all computers run a personal firewall product of some type, even if they are part of a corporate network with external security measures.

Windows Firewall maintains two separate configuration profiles. When the computer is a member of a domain and connected to the network that contains the domain controllers, Windows Firewall loads the "Domain" profile. When the computer is connected as such, a note is displayed at the bottom of the General tab: "Windows Firewall is using your domain settings." This configuration can be very useful for a laptop that is connected to the domain in some cases, but connected to a home network in other situations.

Configuring Windows Firewall using Group Policies

The recommended method for configuring computers connected to an Active Directory domain with Windows 2000 or Windows 2003 domain controllers is by using Group Policies. Group Policies can enforce certain firewall policies across the entire domain while leaving some settings up to the local machine administrator. When a group policy is in effect, the Windows Firewall configuration tool displays a message at the top of the General tab: "For your security, some settings are controlled by Group Policy."

To use group policies to administer Windows Firewall, the enterprise group policies must be updated to include the new settings available for Windows Firewall. This can be done by logging into a Windows XP SP2 machine, opening the appropriate group policy using the mmc.exe tool and browsing to the Windows Firewall section. This section is located at Computer Configuration → Administrative Templates → Network → Network Connections → Windows Firewall. After this has been done on all group policies that will be used to maintain Windows Firewall, then the policy settings for the firewall can be configured as needed. Once the group policy includes Windows Firewall settings a Windows XP SP2 machine must be used to administer the policy. Microsoft is developing tools to allow for administration from other versions of Windows.

The Window Firewall section of the group policy has entries for the Domain Profile and the Standard Profile. The policy has the following entries: "Protect all network connections", "Do not allow exceptions", "Define program exceptions", "Allow local program exceptions", "Allow remote administration exception", "Allow file and printer sharing exception", "Allow ICMP exceptions", "Allow Remote Desktop exception", "Allow UPnP framework exception",

© SANS Institute 2000 - 2005 Author retains full rights.

"Prohibit notifications", "Allow logging", "Prohibit unicast response to multicast or broadcast requests", "Define port exceptions", and "Allow local port exceptions."

Appropriate use of these setting can allow or prohibit a great deal of activity on the network. Setting the "Do not allow exceptions" option for the Standard profile would automatically provide a higher level of protection for laptops that were not connected to the corporate network. Creating program exceptions for the domain profile could be used to insure that a third party management application would not be blocked when it attempted to administer domain machines, but would also insure that those ports wouldn't be misused when the computer was out in the wild.

The "Allow remote administration exception" is necessary for the Microsoft Management Console administration tools to work with machine running Windows Firewall. Setting this exception with a custom scope limited only to the system administrators IP addresses would provide the desired remote management but with an enhanced level of security.

Configuring an enterprise for Windows Firewall by using group policies is complex topic. All key business applications need be examined in a test bed environment to determine the appropriate settings and prevent outages. "Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2" contains a great deal of information about configuring Windows Firewall using group polices and is an excellent resource for planning an enterprise deployment of Service Pack 2.

Windows Firewall group policies can be tested in a limited but safe fashion by modifying the Local Computer Group Policy. The Local Computer Group Policy can be edited by running the "gpedit.msc" MMC plug-in from the Run command. Browse to the Window Firewall section: Local Computer Policy → Computer Configuration → Administrative Templates → Network → Network Connections → Windows Firewall. Editing the local group policy and then examining the results in the Windows Firewall configuration tool is an easy way to discover the effects of settings on the local administrator.

Using netsh to configure Windows Firewall

The netsh tool is a command line utility used to modify networking parameters from the command line. Service Pack 2 has added a new "netsh firewall" context to allow for firewall administration from the command line or batch file scripts.

Any of the configuration settings available in the Windows Firewall configuration tool are also available using netsh. Running "netsh firewall" will start the netsh tool in the firewall context. The "help" command will list all of the options

© SANS Institute 2000 - 2005 Author retains full rights.

available for use in the current context. The commands available are: add, delete, dump, help, reset, set, and show. For example the command “netsh firewall show config” will display all of the configuration information for both the Domain and the Standard configuration profiles.

The following command could be used to create an exception for an FTP server:

```
netsh firewall add portopening protocol = TCP port = 21
name = "FTP Server"
```

© SANS Institute 2000 - 2005, Author retains full rights.

Limitations of Windows Firewall

There has been a fair amount of criticism directed at Windows Firewall on two fronts. Windows Firewall only blocks incoming traffic while many of the other Windows personal firewall programs block both incoming and outgoing traffic. If the computer becomes infected with some type of malware, then Windows Firewall will do nothing to block its undesired outgoing traffic. In the case of worm, Windows Firewall may help prevent the computer from getting infected in the first place, but once it is infected, there is nothing to hinder the worm from creating outgoing traffic to infect other computers. ZoneLab's ZoneAlarm is one of the more popular personal firewall products currently available and it blocks both incoming and outgoing traffic.

The other charge leveled against Windows Firewall is that it provides APIs that can be used to disable the firewall once it is infected with some type of malware. Programs like ZoneAlarm are being modified to automatically disable Windows Firewall on installation and then re-enable Windows Firewall when they are uninstalled, but if these programs can do this, clever malware programs could simply disable Windows Firewall before they open a port to listen for additional instructions/updates.

Microsoft has stated that it isn't the role of a firewall to protect the PC once it has been infected. That role is better suited for Anti-Virus software or corporate network perimeter appliances that examine outbound traffic. They have also stated that asking users about all outgoing traffic backfires when users start agreeing to every dialog that is displayed.

There is also the issue of a recent critical update relating to the firewall. According to the Knowledge Base article for patch 886185, some dial-up configuration set the routing tables to include an address of 0.0.0.0 and a net mask of 0.0.0.0. Before the patch, released December 14, 2004, Windows Firewall would interpret this as part of the local subnet. In many cases, resources made available via file and print share would be available to the entire Internet.

© SANS Institute 2000 - 2005, Author retains full rights.

Conclusion

Despite criticisms that Windows Firewall doesn't do enough, it does block most outgoing traffic, and provides scoping that hides File and Print Sharing and other frequently attacked Microsoft Windows technologies. With Windows Firewall and Automatic Updates activated by default many Internet users now have a far greater level of protection then they have ever had before.

Windows Firewall is an easy to configure application that can work well in both the home and office environments and is a good step forward for Microsoft's Trustworthy Computer initiative. Its philosophy of providing a secure operating environment as the default configuration will help protect both home users and inexperienced administrators.

This new technology may go a long way towards slowing or stopping the next generation of virus and worms and help users keep their computer part of a secure, stable and available Internet.

© SANS Institute 2000 - 2005, Author retains full rights.

Sources

Broersma, Matthew. "Is Microsoft's Firewall Secure?" PCWorld. 13 Aug 2004. 23 Jan 2005. <http://www.pcworld.com/news/article/0,aid,117380,00.asp>

Browser Statistics. Jan 2005. W3Schools. Refsnes Data. 20 Jan 2005. <http://www.w3schools.com/browsers/browsers_stats.asp>

CNET News.com Staff. "Gates memo: 'We can and must do better'." CNET News.com. 17 Jan 2002. 20 Jan 2005. <http://news.com.com/2009-1001-817210.html>

"Computer Virus Timeline." Infoplease. 2000–2004 Pearson Education, publishing as Infoplease. 20 Jan. 2005 <http://www.infoplease.com/ipa/A0872842.html>.

Davies, Joseph. "Manually Configuring Windows Firewall in Windows XP Service Pack 2." Microsoft TechNet. 17 Dec 2004. 23 Jan 2005. <http://www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx>

Description of the critical update for Windows Firewall "My Network (subnet) only" scoping in Windows XP Service Pack 2. 23 Dec 2004. Microsoft Help and Support. Microsoft Corporation. 23 Jan 2005. <http://support.microsoft.com/kb/886185>

ICT - Free Statistics Home Page. 30 Jul 2004. International Telecommunication Union. 20 Jan 2005. <http://www.itu.int/ITU-D/ict/statistics/>

Lemos, Robert. "Microsoft's blast from the past." CNET News.com. 12 Aug 2004. 20 Jan 2005. <http://news.com.com/2100-1002_3-5306235.html>

Lemos, Robert. "One year on, is Microsoft 'trustworthy'?" CNET News.com. 16 Jan 2003. 20 Jan 2006. <http://news.com.com/2100-1001-981015.html>

Microsoft Corporation. Deploying Windows Firewall Settings for Microsoft Windows XP with Service Pack 2. Microsoft Corporation, Oct 2004. 21 Jan 2005. <http://www.microsoft.com/downloads/details.aspx?FamilyID=4454e0e1-61fa-447a-bdcd-499f73a637d1&DisplayLang=en>

Microsoft Corporation. Microsoft Windows XP Professional Service Pack 2. Microsoft Corporation, 2004.

© SANS Institute 2000 - 2005 Author retains full rights.

Naraine, Ryan. "'Critical' XP SP2 Update Fixes Windows Firewall Bug." EWeek. 17 Dec 2004. 23 Jan 2005. <http://www.eweek.com/article2/0,1759,1743114,00.asp>

Team Flexbeta. "How Secure is Windows Firewall?" Flexbeta. 14 Aug 2004. 23 Jan 2005. <http://www.flexbeta.net/main/articles.php?action=show&id=76>

"Timeline of notable computer viruses and worms." Wikipedia. 29 Dec 2004. 20 Jan 2005. <http://en.wikipedia.org/wiki/Timeline_of_notable_computer_viruses_and_worms>

Thurrott, Paul. "Windows XP Service Pack 2 with Advanced Security Technologies Review." SuperSite for Windows. 30 Aug 2004. 20 Jan 2005 <http://www.winsupersite.com/reviews/windowsxp_sp2.asp>

Tulloch, Mitch. "Customizing Windows Firewall." Windows Security.com. 18 Nov 2004. 23 Jan 2005. <http://www.windowsecurity.com/articles/Customizing-Windows-Firewall.html>

Understanding Windows Firewall. 4 Aug 2004. Microsoft Corporation. 23 Jan 2005. <http://www.microsoft.com/windowsxp/using/security/internet/sp2_wfintro.mspx>

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 29th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event