Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Introduction to the Microsoft Windows XP Firewall

Microsoft's Internet Connection Firewall was designed to work with personal firewall applications, not to compete with them. ICF is far from perfect as firewalls go. It doesn't block any outbound traffic; which won't protect you from Trojan application that have made it onto you computer by other means (email, downloads, etc). Its rules are rather basic compared to other personal firewalls. But on the other hand, ICF has no cost (other than the OS cost). It has little or no complexity, if the average home user uses the...

Copyright SANS Institute
Author Retains Full Rights

AD

Introduction to the Microsoft Windows XP firewall

SANS Security Essentials (GSEC) v1.2e

Matt Snitchler

© SANS Institute 2001, Author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Introduction to the Microsoft Windows XP firewall

Introduction

Here we go again with another version of Windows. Windows XP is the soon to be released version of Windows. Windows XP promises to be the OS that will appeal to Geeks and Power users as well as to beginners and users generally timid around computers. This new version of Windows signifies a convergence of its home and business operating systems. This product will replace Windows 2000 and Windows 9x (including Windows Millennium). Both home and business operating systems will be based off the same source. For the first time in Microsoft's history all of their Operating Systems will be built off of the Windows NT Kernel. This is thought to be a much more stable platform than the old DOS command.com platform. This is the platform Operating Systems like DOS and Windows 95 were built from. The home version will be called "Windows XP Home Edition" and the business version will be called "Windows XP Professional". Their server offerings will be based off of this same Kernel as well but are beyond the scope of this paper. This platform will bring together the strengths of Windows 2000, like security, manageability and reliability, and the strengths of Windows Millennium, like Plug-and-Play, easy-to-use user interface, etc. Windows XP will sport a new start menu as well as a new version of Internet Explorer. Windows XP introduces numerous security enhancements. These include controlled network access, software restriction policies, credential management, encrypted file system, and a basic firewall. This firewall is called the "Internet Connection Firewall" (IFC), and is the topic of this paper.

Internet Connection Firewall might be a tool used to protect a home computer or maybe a small home network. You also might find ICF protecting a small business network. Microsoft does also produce a full fledged firewall designed for a dedicated server and a LAN. This product, Internet Security and Acceleration Server is generally used for protecting large networks and is quite a bit more complex to configure.

Why do I need a firewall?

"Why do I need a firewall?" you are asking yourself. Well the Internet can be a hostile environment. You are susceptible to attacks whenever you are connected. Very fast always on internet connections are becoming very popular in the home. Fast connections make attacks on your system very efficient. An attacker can try many different attacks in a shot amount of time. The always on nature of high speed Internet access with technologies like DSL or Cable modems make you a very convenient target. A hacker doesn't need to coordinate his attacks because your computer is always available. Even when you connect to the Internet with a modem you can be vulnerable, although much slower and cumbersome. You may not think you have anything of interest on your computer. Attackers may have an interest in your personal information often stored on home computers. Do you store any passwords or credit card numbers on your computer? How about personal email or financial information, such as account numbers or electronic bank statements?

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Well, you seem pretty safe; you don't store any of this information on your computer. Not so, your computer itself can become the tool of interest to hackers. Computers are compromised on the Internet and used to launch attacks on other computers. This can prove to be advantageous to a hacker who would prefer to keep his identity hidden. Do you think it would look good if your computer, unbeknownst to you was attacking a government website? Aside form hiding the identity of an attacker, many of these so called "Drone" machines (yours being only one of thousands maybe) can be used in organized and distributed attacks on large sites. I hope I've got you convinced perhaps a firewall is good.

If all this isn't enough for you to feel a little afraid, there are malicious attacks as well. You computer may be able to be broken for an internet attack, requiring you to reboot to regain access. Your internet access can be affected with a Denial of Service (DOS) attack. This can be described as a whole bunch of invalid information being sent to your computer. Your computer is so busy handling this garbage, that it can no longer function correctly, effectively breaking your Internet connection.

General firewall overview

"So, what is this firewall thing?" you ask. One such definition comes from the Windows XP Help file:

> "A Firewall is a security system that acts as a protective boundary between a network and the outside world."

Firewalls are usually designed to prevent unauthorized access to your internal network. There are many types of firewalls. You can buy dedicated hardware firewalls whose only role in life is to keeps bad guys out, or there are software firewalls that are applications that run on dedicated computers or personal computers. All firewalls function off of a predefined set of rules and are only as good as their configuration.

There are four basic types of firewalls. Packet filtering, Circuit-level gateway, Application-level gateway, and Stateful inspection firewall.

- **Packet filtering**
  A packet filtering firewall accepts or denies traffic based on TCP and IP Headers. Generally it is the lowest cost firewall solution but will also offer the least protection. This type of firewall does not perform content checking. One good thing about a packet filtering firewall, other than cost, is the little or no network performance hit. A packet filtering firewall operates at the network layer of the OSI Model.
- **Circuit-level gateway**
  A circuit-level gateway monitors TCP handshaking between trusted clients or servers and untrusted hosts to determine the legitimacy of a requested session. A circuit-level gateway uses SYN & ACK flags as well as valid sequence

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

numbers to determine a requested session in logical. This type of firewall is usually implemented with application level gateways. A circuit-level gateway operates at the session layer of the OSI model (two levels up from packet filtering).

- **Application-level gateway**
  An application-level gateway is much like a circuit-level gateway with two major differences. Proxies are application specific and proxies filter at the application layer of the OSI model.
- **Stateful inspection firewall**
  A stateful inspection firewall includes aspects of a Packet filtering firewall, Circuit-level gateway & an Application-level gateway. It filters packets based on source and destination addresses as well as port numbers. A Stateful inspection firewall monitors SYN & ACK flags as well as valid sequence numbers like a circuit-level gateway. It evaluates the contents of packets at the application layer like an Application-level gateway. Generally offers better performance than a Circuit-level or Application-level gateway. A Stateful inspection firewall operates at the network layer of the OSI Model.

Most all firewalls offer some form of logging. This is useful for troubleshooting as well as learning about your attackers and the types of exploits that you are being exposed to.

Overview of Microsoft's "Internet Connection Firewall" (ICF)

Now you now know what a firewall is and why you need one. Let's take a look at Microsoft's Internet Connection Firewall (ICF). Internet Connection Firewall is considered to be a stateful inspection firewall. ICF is used to set restrictions on what connections can be made to your computer from the Internet. It is also used to define what types of connections are not allowed. It will disable all incoming traffic unless traffic is associated with an exchange that began from within your computer or private network (return traffic). Microsoft's Internet Connection Firewall is capable of protecting a standalone machine or an entire network. It is designed to function with Internet Connection Sharing (ICS), which a capability built into Windows XP to provide a shared Internet Connection.

ICF will protect Local Area Network (LAN), Point-to-Point Protocol over Ethernet (PPPoE), and Virtual Private Networks (VPN) or dial-up connections.

A Local Area Network is simply a group of machines connected together for the purpose of sharing resources. The resources may be files, printers or Internet access.

Point-to-Point Protocol over Ethernet is commonly used with broadband access (cable, wireless, dsl, etc.) to achieve access to high speed networks like the Intrenet.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

VPN are a way for two or more computers to connect over public media, like the Internet and control public access.

Dial up connections allow for home users with no broadband access to connect to other resources, like the Internet over a basic phone line.

Microsoft's Internet Connection Firewall can block ICMP traffic. ICMP, commonly know as "ping" is traditionally used to report errors and status information. Bad guys often use ICMP to 'map" out network services on computers.

How to Install Microsoft's Internet Connection Firewall

Windows XP is not configured out of the box with Internet Connection Firewall enabled. There are two ways to enable ICF.

Network Setup Wizard

You can run the Network Setup Wizard and it will enable the Internet Connection Firewall on all Internet connections it finds. This will enable ICF with default settings and will not ask you any customization questions. This may be a good option for a beginner user or for someone who will not be hosting any services, like a web server or a game server on their computer. ICF will block any attempt to ping your computer. Also by default ICF doesn't do any logging.

Manual Configuration

Manually configuring Internet Connection Firewall will expose you all the advanced options available. To manually configure Internet Connection Firewall:

- Open Control-Panel
- Click "Network and Internet Connections"
- Click "Network Connections"
- Right-click on your Internet Connection and select "Properties"
- Click the "Advanced" tab of your connection's dialog
- Under the "Internet Connection Firewall" section you can enable the firewall

You may want to configure specific unsolicited inbound traffic into your network. Say you want to run a web server to publish your children's pictures on the web, or maybe you want to host a game server. You can configure ICF to allow these types of services to function. From the "Advanced" tab described above you will find a "Settings" button. Behind this button you will see commonly used services predefined for you on the "Services" tab. Enabling things like a web server or a telnet server are just a checkbox away.

If you find that the service you are interested in providing is not listed, you can add additional services. This is where you will need to go to host games over the Internet from behind your firewall. You will need to add a few pieces of information after clicking the 'Add" button found under the "Services" tab on the "Advanced Settings"

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

dialog. You will need a description of service, say "UT Server". This is just information, so anything will do. You will need the name or IP address of the internal computer hosting the server. This will most likely be an internal IP address, like 192.168.0.4. Then you will need an external port number for this service and an internal port number for this service. The external port number will be the port number that users on the Internet will connect to. The internal port number will be the actual port number on the computer hosting the service that we listed above. In most cases these port numbers will be the same; however you may have a need to make them different, maybe if your game server is using a specific port, than you can connect to the game server with another computer on your internal network. This would be a drag, you hosting a game server that you can't connect to. By configuring a different internal port number this problem could be avoided. The last thing that needs to be configured on this dialog is weather you are configuring TCP or UDP ports. You're application documentation can tell you this.

Also found on the "Advanced Settings" dialog, under the "Security Logging" tab you will find all the settings related to your logs. From this dialog you can choose to log dropped packets (incoming) and/or log successful connections (incoming and outgoing). You can also specify the name, size and location of the log file.

One more configuration dialog, "ICMP" configures, as you might expect ICMP settings. By default, Internet Connection Firewall is configured to not allow any ICMP traffic in. This dialog will give you the option to allow nine different types of ICMP traffic through. These are incoming echo request, incoming timestamp request, incoming mask request, incoming router request, outgoing destination unreachable, outgoing source quench, outgoing parameter problem, outgoing time exceeded and allow redirect.

Internet Connection Firewall log file overview

ICF maintains a log that can be rather useful in analyzing attempted connections to your computer. By default it is disabled, so be sure and enable logging. ICF will log all dropped packets. This means that every attempt by traffic to travel across the firewall will be logged. ICF will also log all outbound connections. This will give you a complete picture of every successful connection.

Logs are generated in World Wide Web Consortium (W3C) Extended Log Format. This is a standard format used by common log analysis tools. These logs have two sections, the header and the body. The header contains static information. Things like the version of the security log, the name of the log, time format and a list of fields used in the body. The body will include data entered from traffic attempting to cross firewall. This will include things like date/timestamp, action, protocol, src-ip, dest-ip, src-port, dest-port, size, tcpflags, tcpsyn, tcpack, tcpwin, icmptype, icmpcode, and/or info.

More information about the World Wide Web Consortium or about the Extended Log Format can be found at http://www.w3.org.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Conclusion

Microsoft's Internet Connection Firewall was designed to work with personal firewall applications, not to compete with them. ICF is far from perfect as firewalls go. It doesn't block any outbound traffic; which won't protect you from Trojan application that have made it onto you computer by other means (email, downloads, etc). Its rules are rather basic compared to other personal firewalls.

But on the other hand, ICF has no cost (other than the OS cost). It has little or no complexity, if the average home user uses the wizard to configure his Internet connection, he may not even know that ICF is in place. ICF is a tool designed for the average, not so knowledgeable home user with high speed Internet access and traditionally has little or no protections in place.

© SANS Institute 2001, Author retains full rights.

Sources

"Windows XP Technical Overview", May 18, 2001
http://www.microsoft.com/windowsxp/pro/techinfo/howitworks/overview/default.asp
http://www.microsoft.com/windowsxp/pro/techinfo/howitworks/overview/09security.asp

"What New in Security for Windows XP", July 3, 2001
http://www.microsoft.com/windowsxp/pro/techinfo/howitworks/security/01section01.asp

"Why you need a firewall"
http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch2.htm

"What is a firewall and why do I need one?"
http://www.simonzone.com/software/guarddog/manual/why-need-firewall.html

Choosing The Best Firewall, Gerhard Cronje, April 10, 2001
http://www.sans.org/infosecFAQ/firewall/best.htm

'What is a firewall?"
http://www.fishnetsecurity.com/secinfo/overview.html

Getting up to speed with Windows XP, Scot Finnie, Serdar Yegulalp, Neil Randall, and Dave Methvin, May 3, 2001
http://computers.lycos.com/software/xp.asp

"What is PPPoE?", July 23, 2001
http://www.carricksolutions.com/pppoe.htm

© SANS Institute 2001, Author retains full rights

Last Updated: May 19th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**