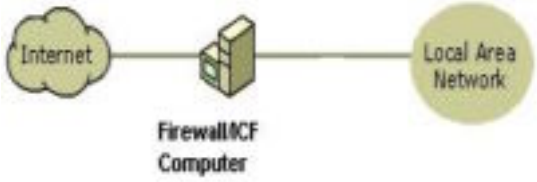
Global Information Assurance Certification Paper

XPerience Home and Small Office Security
Larry Graft
Version 1.2f
December 1, 2001

With Microsoft's latest operating system (Windows XP) released on October 25, 2001, one of the major features highlighted throughout the country that day was a new feature called the Internet Connection Firewall (ICF).

While attending one of the XP launch events, I was amazed at how the product was demonstrated as just a point and click feature. I was hearing from others around me at the event on how nice it was to only have to put a check in the box and my home or office network is secure. By writing this paper, I hope to expand more on what Windows XP's ICF is and the more detailed configurations available with it.

Let's first take a look at what a firewall and the ICF are.



A firewall acts as a boundary between a network and the outside world. ICF is firewall software that is used to set restrictions on what information is sent to and from the internet to your home or small office network.

ICF also can protect a single computer connected to the Internet. If you have a single computer connected to the internet with a cable, DSL, or dial-up modem, ICF protects your internet connection.

How ICF Works

To prevent unwanted traffic from the internet side of the connection from entering the private side, ICF keeps a table of all communications originated from the ICF enabled computer.

All inbound traffic from the internet is compared against the entries in the table. Inbound internet traffic is only allowed to reach the computers in your network when there is a matching entry in the table that shows that the communication exchange began from within your computer or private network.

Communications that originate from a source outside an ICF computer, such as the internet, are dropped by the firewall unless an entry in the services tab of ICF is set to allow it through. Rather than notifying you about the activity, ICF silently discards unsolicited communications, stopping common hacking attempts such as port scanning. Such notifications could be sent

frequently enough to annoy you. Instead, ICF can create a security log so that you can view the activity that is tracked by the firewall.

You also may have certain services on your network that you want to be configured to allow unsolicited traffic from the internet to be forwarded by the ICF computer to the private network.

For example, if you are hosting a web server and have enabled the HTTP service on your ICF computer, unsolicited HTTP traffic will be forwarded by the ICF computer to the web server.

Let's take a look at how to enable ICF.

Enabling ICF

1. You must be an administrator for the system in order to enable.

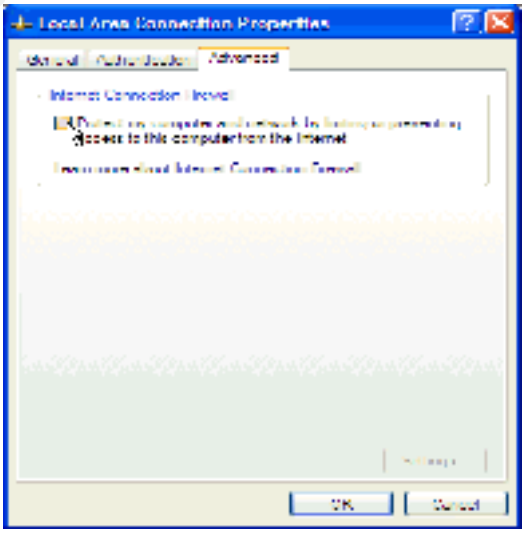
2. Click **Start**, click **Control Panel**, and then double–click **Network Connections**.

3. Click the Dial–up, LAN or High–Speed Internet connection that you want to protect, and then, under **Network Tasks**, click **Change settings of this connection**.

4. On the **Advanced** tab, under **Internet Connection Firewall**, select one of the following:

    - To enable Internet Connection Firewall (ICF), select the **Protect my computer and network by limiting or preventing access to this computer from the Internet** check box.

    - To disable Internet Connection Firewall, clear the **Protect my computer and network by limiting or preventing access to this computer from the Internet.** (Microsoft)



Enabling ICF as you can see is just a point and click feature but configuring it properly is the key. So now let's take a look at adding services and configuring our event logging options.

Adding services

Services run to support programs on your computer. An example of a service is a Web server that supports hosting Web pages from your home or small office network. If you have the Web server service enabled for your network, you can use that service to supply your own Web pages to the Internet.

To permit the traffic to flow from the Internet to the computer hosting the service, you must add the service to the **Services** list by entering information about the services "operational" settings on the **Services** tab of the ICF host computer. The settings provide the rules that are required for ICF to allow traffic to travel from the Internet to the network.

The "operational" settings are known as a "service definition," because they define that required service. The information that you must enter to add a service definition includes: the description of the service, the name or IP address of the computer hosting the service, and the TCP or UDP port number of the service.

Some services are predefined for ICF. FTP Server (Port 21), Internet Mail Server (Port 25), Secure Web Server (Port 443), Telnet Server (Port 23), and Web Server (Port 80) are examples of built-in services. These services can run on the ICF host computer.

You can add a new service to your network by installing the service software on one of your network computers and then adding the service definition so that ICF will allow the service to be accessed from the Internet. Services that are preconfigured require only the name or IP address of the computer hosting the service for the service definition.

By default all unsolicited inbound connections to ICF are dropped. This is a problem if there are services running behind ICF that you want people on the Internet to access. Port mappings are a way for services and applications to create rules in the firewall for how to handle inbound connections. By creating a port mapping (for example, opening port 80 for a Web server), ICF allows requests from users on the Internet to reach your Web site and be serviced by the Web server.

If you are having trouble getting to your web server or other programs and services on your Windows XP machine and ICF is enabled, you may need to add the program or service in the ICF services tab. To do so, follow these steps:

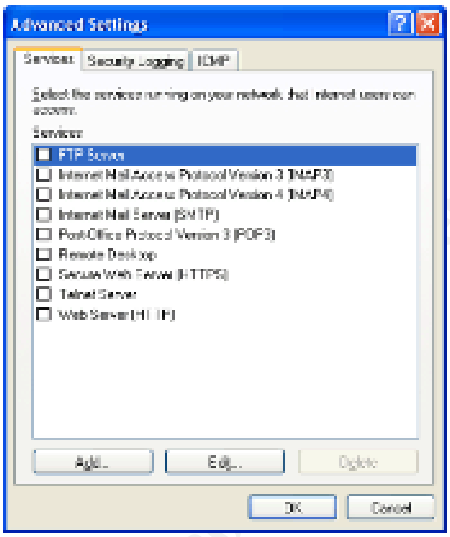
1. Click **Start**, click **Control Panel**, click **Network and Internet Connections**, and then click **Network Connections**.

2. Right-click your Internet connection and then click **Properties**.

3. Click the **Advanced** tab in the Properties dialog box.

4. Click **Settings**, and the Advanced Settings dialog box opens.

5. From there you can enable most common services just by clicking them, or add your own by clicking the **Add** button. (Moreno)



Another new feature in XP is the Remote Desktop. If you use ICF and wish to use this new feature be sure to enable the Remote Desktop (Port 3389) on the services tab.

Editing and changing log file options

If you want to examine incoming connection attempts, you can turn on logging from the ICF **Advanced Settings** tab as well as specify the size of a log file.

ICF has four basic logging options. By default all logging options are disabled.

1. Log all dropped packets. This option logs all dropped packets from both inbound and outbound connections.

2. Log all successful connections. This option will log successful outbound connections and successful inbound connections.

3. Log filename and location. The default name of the log file is pfirewall.log. The default location of the log file is %windir%. The user has the ability to set both the log file name and location.

4. Log file size. The default file size is 4096 kilobytes (KB). The maximum file size is 32767 KB.

To enable the security logging options:

1. Click **Start**, click **Control Panel**, click **Network and Internet Connections**, and then click **Network Connections**.

2. Click the connection on which Internet Connection Firewall (ICF) is enabled, and then, under **Network Tasks**, click **Change settings of this connection**.

3. On the **Advanced** tab, click **Settings**.

4. On the **Security Logging** tab, under **Logging Options**, select one or both of the following options:

    - To enable logging of unsuccessful inbound connection attempts, select the **Log dropped packets** check box.

    - To enable logging of successful outbound connections, select the **Log successful connections** check box. (Help and Support)

(Bowman)

If you wish to later disable the logging features, remove the check in boxes as stated above to do.

To view your log files click on the browse button shown above and scroll to pfirewall.log, then right click the file and select open. Here is an example from a log file:

#Verson: 1.0
#Software: Microsoft Internet Connection Firewall
#Time Format: Local

#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack tcpwin icmptype icmpcode info

2001-11-28 10:04:07 DROP ICMP 10.1.2.3 10.1.2.4 - - 60 - - - - 8 0 –

2001-11-28 10:04:08 DROP ICMP 10.1.2.3 10.1.2.4 - - 60 - - - - 8 0 –

2001-11-28 10:04:09 DROP ICMP 10.1.2.3 10.1.2.4 - - 60 - - - - 8 0 –

2001-11-28 10:04:10 DROP ICMP 10.1.2.3 10.1.2.4 - - 60 - - - - 8 0 –

2001-11-28 10:04:18 DROP ICMP 10.1.2.3 10.1.2.4 - - 60 - - - - 8 0 –

2001-11-28 10:04:19 DROP ICMP 10.1.2.3 10.1.2.4 - - 60 - - - - 8 0 –

2001-11-28 10:04:20 DROP ICMP 10.1.2.3 10.1.2.4 - - 60 - - - - 8 0 –

2001-11-28 10:04:21 DROP ICMP 10.1.2.3 10.1.2.4 - - 60 - - - - 8 0 -

ICF Considerations

As you can see there is a little more to the ICF than just clicking a box. As well there are also some considerations you should take before enabling and configuring ICF.

You should not enable ICF on any connection that does not directly connect to the internet. If the firewall is enabled on the network adapter of another client computer, it could interfere with some communications between that computer and all other computers on the network.

ICF is not needed if your network already has a firewall or proxy server such as Microsoft's Internet Security and Acceleration server (ISA) setup.

If your network has only one shared internet connection, you should protect it by enabling ICF.

Individual client computers may also have adapters, such as a dial up modem, that provide individual connections to the internet and are vulnerable without ICF protection. ICF can only check the communications that cross the internet connection on which it is enabled. Because of this, you need to enable it on all computers with direct connections to the internet to ensure protection for your entire network. Don't leave any back doors open.

Summary

While the ICF feature is a good start for the home user to protect their home computers it will never replace a dedicated hardware or software firewall product such as Microsoft's ISA server, CISCO, Checkpoint, and 3Com products for the office network.

Another consideration is that ICF will help HIDE your computers and not find/prevent viruses from entering your network. Consider ICF as your first line of defense and your virus protection as the necessary second line of defense.

References:

1. Microsoft, Use the Internet Connection Firewall to Secure Your Small Network, August 24, 2001 http://www.microsoft.com/windowsxp/pro/using/howto/netorking/icf.asp
2. Moreno, Alfred, Enable Services to Work Through Internet Connection Firewall, November 12, 2001 http://www.microsoft.com/windowsxp/expertzone/tips/november/moreno1.asp
3. Bowman, Barb, Don't Let the Defense Rest, November 12, 2001 http://www.microsoft.com/windowsxp/expertzone/columns/bowman/november12.asp
4. Help and Support, Windows XP, Internet Connection Firewall Overview
5. Help and Support, Windows XP, Services Definitions Overview
6. Help and Support, Windows XP, Security Logging

Last Updated: July 27th, 2017

Upcoming Training

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
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event