Topic: **I/Port I8800 Update: Microsoft Internet Connection Firewall**
Component(s) Affected: **I/Port I8800, XPe**
Date: **March 2, 2005**

OVERVIEW / ENVIRONMENT

A software firewall is a basic component of network security. A new update for the I8800 I/Port allows loading the Microsoft Internet Connection Firewall (ICF) onto the I/Port to provide added network security.

DETAILED DESCRIPTION

The Microsoft Internet Connection Firewall (ICF) provides baseline intrusion protection for systems using Windows XP. This functionality is now available for Windows XPe on the I8800 I/Port. ICF can be installed on I/Ports with a standalone installer, or with a Grid Center deployable installer.

ICF provides basic firewall security. It should not be relied on as the ultimate firewall for a large network or for a network requiring high security. This function should be provided by a dedicated system such as a hardware firewall or a PC controlling a single point of access between the network and the Internet.

ICF provides a stateful packet filtering policy that checks both a packet's state and its context. To accomplish this, ICF maintains a table of connection flows that follows these rules:

- Incoming packets that match established connection flows are forwarded. These are packets on the three open ports, as well as packets that are on the same ports as recently sent packets originating inside the firewall.
- A sent packet (sent from the ICF host, which is the I/Port) that does not match an established connection flow creates a new entry in the connection flow table and is then forwarded.
- Any received packet that does not match an established connection flow is dropped.

In addition, ICF performs limited structural checks on packets to prevent common packet-based attacks.

Two sets of files are provided for this I/Port update:

- The local installer files, in a folder named **Stand Alone**.
  - `Update.bat`
  - A folder named **IPORT-CLIENT**.
- The Grid Center remote installer files, in a folder named **GC Push**.
  - `GCUpdate.bat`
  - `IPORT-CLIENT.zip`

The local installer is run by physically carrying the files to the I/Port on a Mass Storage Device such as a key drive, and then executing it. The Grid Center remote installer is run from the Grid Center Console, in the Update View, and can be applied to multiple I/Ports or I/Port groups simultaneously.

While the files in the `IPORT-CLIENT.zip` file are the same as the files in the **IPORT-CLIENT** folder, the associated batch files are slightly different and cannot be interchanged.

ClearCube Technology 8834 Capital of Texas Hwy N Suite 140 Austin, Texas 78759 **voice 512 652 3500** **www.clearcube.com**

INSTALLING ICF LOCALLY

To install this update locally, do the following:

1. Load the update files onto a Mass Storage Device (MSD) such as a key drive.

2. At the I/Port, log in as administrator. Press and hold the Left Shift key and select **Logoff** from the Start menu. Keep the Shift key depressed until the Administrator Login dialog box is displayed. The factory default Administrator account is `administrator` and the default password is `clearcube`. These can be changed in the User Accounts control panel.

3. Insert the USB storage device into an available USB port.

4. Copy the installer files to C:\.

5. Double-click the `Update.bat` batch file. The update installs automatically and reboots the I/Port.

Note: Do not press any keys during the update. Allow it to run undisturbed. This update reboots the I/Port twice during the installation process.

INSTALLING ICF REMOTELY USING GRID CENTER

To install an update remotely with Grid Center, do the following:

1. Load the update files onto a volume accessible by the Grid Center Console.

2. Start Grid Center (if it is not already running).

3. From the Update View, select an individual I/Port or an I/Port Group to update.

4. In the I/Port Update View dialog box, enter the path and name of the Update file, including the .zip suffix (you can browse for this).

5. Enter the path and name of the Answer file, including the .bat suffix (you can browse for this).

6. Press the **Update** button.

7. A dialog box confirming the successful update is displayed at the Grid Center console when the update is complete. If any I/Ports did not update successfully, a dialog box containing the names of these I/Port is displayed. Write these names down and re-deploy the update to these I/Ports individually.

8. If an I/Port cannot be successfully updated via Grid Center, attempt to update the I/Port locally (using the first procedure) before contacting ClearCube technical support.

Note: At the I/Port, do not press any keys during the update. Allow it to run undisturbed. This update reboots the I/Port twice during the installation process. When pushing this update using Grid Center, allow approximately 10 minutes for the installation.

CONFIGURING ICF

To change settings locally on ICF, use the following procedures:

Note: You must be logged into the I/Port as an administrator to save configuration settings. These procedures work for both user and administrator account, but the administrator account has right-click functionality enabled.

1. Disable the Write Filter by double-clicking the **Write Filter Disable** icon on the desktop. The Write Filter is a special mechanism that prevents unauthorized writes to the I/Port's flash memory. The Write Filter status is always displayed in the toolbar by a green circle for Write Filter Enabled (flash memory cannot be written), or by a red circle for Write Filter Disabled (flash memory can be written).

2. From the Start menu, select **Settings —> Control Panel —>Networking**.

3. Double-click the **Local Network** icon and choose **Properties**.

4. The following tabs are displayed:
   - **General** – accesses settings for the network connection.
   - **Authentication** – accesses settings such as authentication protocols and certificates.
   - **Advanced** – accesses the most frequently used firewall settings.
5. Select the **Advanced** tab and then click its **Settings** button to access port controls, logging, and Internet Message Control Protocol (ICMP) settings.
6. Save your changes.
7. Re-enable the Write Filter to permanently keep the configuration changes. The I/Port must be rebooted.

Remember that if you made any changes besides ICF configuration changes, they will also be saved.

Configuration settings can be changed remotely by pushing out the IFC files with the `GCUpdate.bat` file edited to reflect the new configuration. For example, to add an open port, open the `GCUpdate.bat` file with a text editor. Locate the port configuration lines. Copy one or more lines and modify them to open the required ports, and save the batch file. Then push the update as described in this Technical Bulletin.

It should be noted that users can change their ICF settings for an individual session, but these settings cannot be saved unless the user has execute access to the Write Filters. This access should be granted conservatively, and controlled through established security policies.

The simplest way to give write access for ICF settings is to copy the two Write Filter shortcuts from the `C:\Documents and Settings\Administrator\Desktop\` folder and paste them in the `C:\Documents and Settings\All Users\Desktop\` folder. This causes two copies of the shortcuts to be displayed on the Administrator's desktop, which indicates to the Administrator that all users of this I/Port can access these filters.

DEFAULT SETTINGS

Logging:

- Logging is turned off.
- The default size for the log file is 4 MB.
- The default location for the log file is `C:\Windows\pfirewall.log`.

The size and the location of the log file can be changed by the Administrator. If the log file remains on C:\, the risk exists to write more data to the C:\ drive than there is available space. This may cause corruption of the I/Port operating system image, even when the Write Filter is turned on to prevent permanent writes.

As an alternative, the log file can be saved to an external storage device such as a USB key drive or a network share.

Open Ports:

- TCP 137 (NetBIOS)
- TCP 9000 (Grid Center)
- UDP 4001 (Grid Center)

Ports TCP 21 (FTP), TCP 389 (LDAP), TCP 1002 (not formally assigned), and TCP 1720 (H.323) are closed but scan as open from the I/Port itself, because the port scan communicates with the proxies for these services, and not with the ports themselves. A remote host, such as the I/Port on the next desk or the Grid Center console, accurately reports these ports as closed. Any attempts to connect through these ports when they are closed will appear to succeed, but nothing—such as TCP file transfers—can occur.

These limitations in ICF functionality should be noted:

- Each instance of ICF stores its own set of port mappings and ICMP configuration options. Network-based security policies such as those in SMS cannot be used, but configurations can be set by default at deployment time and later reset by pushing a new configuration set with Grid Center. Settings can also be individually configured at the I/Port.

- Applications that require a range of ports to be opened to enable return traffic on ports other than the outbound set will not work by default. Ports need to be opened in both directions from the Administrator account on the I/Port.
- Applications that run in user context where the user is not the Administrator cannot change port mappings.
- When the log file reaches its maximum capacity, it is flushed and restarted. Log files larger than the default should be saved to an external storage device such as a USB key drive or a network share.

Users can see whether ICF is operational by selecting **Start —> Control Panel —>Networking**. The icon for the local network has a yellow lock on it when ICF is activated, as shown in *Figure 1*.

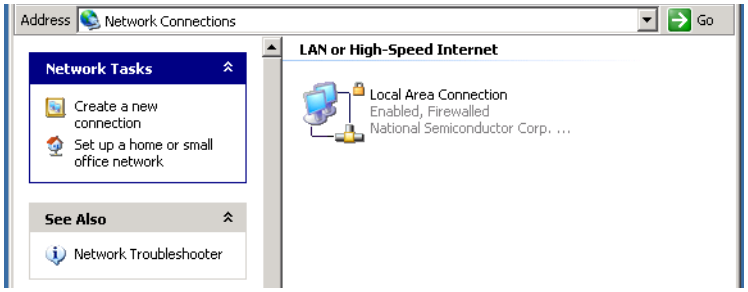

Figure 1 *ICF is Enabled*

These Microsoft documents provide more information on configuring and managing ICF.

http://www.microsoft.com/technet/prodtechnol/winxppro/plan/icf.mspx

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnxpesp1/html/icf_enable.asp

http://support.microsoft.com/?kbid=315846

For more information, please contact ClearCube technical support.

support@clearcube.com	Email address for ClearCube Technical Support
support.clearcube.com	ClearCube Support Website
(866) 652-3400	Direct line in the US
+1 (512) 652-3400	Direct line from outside the US