1 INTRODUCTION

This section provides an overview of Firewall security, and specifically of the Personal Firewall program. It also presents a summary of operations common to all Windows-based applications.

Computer Security

Computer security means protecting a computer's resources and data. In the days before networking and the Internet, security mechanisms usually relied on password protection. Using password protection, a system administrator made sure that only authorized persons could access certain directories, files or programs in a single user computer. Passwords also permit only specific users to log onto the computer.

In order to build even the simplest Password security system on a single user computer, the system administrator needs to know what to protect. More specifically, the system administrator should know the following information:

- The types of users who will try to access to the computer's files and resources.
- The types of operations that these users intend to perform.

Networking Issues

Once a computer connects to a network, and shares resources and files with other computers, password protection becomes less reliable. First of all, a network introduces unknown users who perform unpredictable operations. In addition, a network provides many points of entry into the computer due to operations like printing, file transfer and remote logins. It is almost impossible to protect every transaction with a password.

The Internet introduces an unmanageable number of users to a system. In 1981, approximately 500 hosts were detected on the Internet, and in 1995 the number approached 12 million. These are the number of **Hosts**, which are in turn connected to many users. Some sources estimate that there are as many as 50 million users on the Internet.

This means that if you use the Internet, there are millions of users who could potentially have access to your computer. Therefore, when a computer connects to the Internet, passwords cannot provide true security.

Although security and surveillance methods have become more sophisticated, there are many “hackers” on the Internet who are trying to damage innocent users’ data and resources.

A hacker's activities can cause damage to you and your computer beyond simple data loss, for example:

- Hackers have broken into computers and altered important data such as credit reports, telephone bills and bank account balances of unsuspecting individuals.
- Hackers have introduced computer viruses into the Internet that erase or damage programs, data or entire computers.
- Hackers have accessed internal technical documents from individual computers and posted them on public bulletin boards.

The best solution is to put a barrier at all points of entry into your network.

What is a Firewall?

A Firewall is a collection of components placed between two networks in order to prevent unwanted penetration of them. The Firewall, protects the networks because:

- The Firewall itself cannot be penetrated.
- All incoming and outgoing traffic must pass through the Firewall.

- Only authorized traffic, as defined locally, will be allowed to pass.

The Firewall is usually implemented in a gateway, which is a piece of hardware placed between networks in order to expand their scope. Since the gateway already filters traffic between networks, it can be used to provide computer security on the connected networks. A Firewall gateway is an effective solution for a large organization that has the financial resources to acquire the technology and the technical competence to manage it.

Personal Firewall Overview

For the single Internet user who wants to keep his system secure, a Firewall gateway is not, however, an affordable or practical solution. **Personal Firewall** provides such a solution. It implements much of the same logic as a Firewall gateway in an affordable, simple-to-use software package.

Basic Networking Concepts

In order to learn how Personal Firewall works you need to understand some basic networking concepts.

When data travels on a network, it is packaged in a form which can be "understood" by the various types of hardware and software components involved in the data transfer. This is called a data transfer **protocol**.

One type of data transfer protocol, **TCP/IP**, defines how data is divided into small units of information, or **packets**, that travel over the network, through computers, routers and gateways. Most of the applications used on the Internet to allow two people to transfer files between their computers use the TCP/IP protocol for data transfer.

The TCP/IP protocol provides the basis for packet delivery service as follows:

- **Standard Addresses:** Each data packet carries a standard Internet protocol address of both source and destination computers, called an **IP address**. A unique 32-bit IP address is assigned to each end user computer system, or host, that connects to a network in the Internet. The IP Address is divided into a portion that identifies the host and a portion that identifies the network.

- **Standard Port Numbers:** Each file process, or Internet service, such as e-mail or FTP, uses a standard **port** number on the computer. Each data packet specifies which port on the destination computer will receive the packet. There are two types of ports defined by TCP/IP, each providing different types of services: TCP and UDP.

Level of Protection

Personal Firewall provides TCP-level protection based on the source IP address and the destination port of any communication that reaches your computer.

Personal Firewall protects your computer from incoming connections. In addition, it optionally, keeps a record (log) of incoming connections and two types of outgoing connections that are related to the incoming connections, Listen and Send.

Working With Personal Firewall Applications

There are five applications provided with **Personal Firewall**.

Rules Base Manager
The first step to implementing a Firewall is to decide what type of access is permitted on your computer and what action should be taken when unacceptable behavior occurs. This set of limits is called a Rules Base.

The Rules Base Manager allows you to define or modify the **Personal Firewall** Rules Base. This application is described in Section 3 of this manual.

Log Viewer
The Log Viewer application allows you to view the log data and perform log file operations. This application is described in Section 5 of this manual.

Firewall Filter
The Firewall Filter application is the actual firewall, that decides to accept or reject any incoming communication based on the current rules. This application is described throughout this manual.

Configuration
The Configuration application allows you to define the program's operating parameters, including log file directory and active program icon placement. This application is described in Section 4 of this manual.

Firewall Setup
This Setup application is used to un-install or reinstall the Personal Firewall software. This application is described in Section 2 of this manual.

2 INSTALLATION AND PREPARATION

This section describes the basic system requirements and installation procedures for Personal Firewall.

System Requirements

In order to be able to install and run Personal Firewall, your system must meet the following minimum requirements:

Hardware

1. An IBM PC/AT 386 (or compatible) or higher.
2. At least 4 MB RAM.
3. 2 MB of free hard disk space.
4. A properly installed and configured means of communication with the Internet (for example, LAN connection or modem).

Software

5. Microsoft Windows version 3.1 or higher.
6. Any TCP/IP stack for Microsoft Windows (Winsock 1.1 compliant).

Installation Procedures

To install Personal Firewall, perform the following:

1. If Windows is not active, start Windows by typing *win* at the DOS prompt.
2. Insert the installation disk into the disk drive.
3. From the Program Manger File menu, select the Run option.
4. Either type *A:\SETUP* in the command line (if the disk is not in drive A, enter the appropriate drive letter) or press Browse to select SETUP.EXE from the installation disk.

The **Personal Firewall** setup program automatically performs the following:

- Creates a new directory called FIREWALL.
- Copies the program files to your hard disk.
- Creates a new program group containing five application icons.
- Makes the necessary changes to your **WIN.INI** file.

FW Setup Application

Once you have installed Personal Firewall, you can un-install or reinstall the program using the FW Setup application.

To open FW Setup, double-click on the application icon. 

Follow the instructions for un-installing the program and reinstalling the program..

Preparation

Before you begin working with Personal Firewall, you should prepare some information about the type of protection you require for your computer.

Source IP Address

Since Personal Firewall can block incoming communication, you must be able to identify who will and will not be allowed to access your computer. Identification is by IP address.

The IP address is 32-bit address written in the format xxx.xxx.xxx.xxx, where each xxx is eight bits. One portion of the address identifies the network and one portion identifies the host on that network.

The three high-order bits are used to determine one of the following three formats of an IP address:

- **Class A** addresses are used for networks that have more than 2^{16} (65,536) hosts. The first 7 bits are the netid and the last 24 bits are the hostid.
- **Class B** addresses are used for medium sized networks that have between 2^8 (64) and 2^{16} hosts. The first 14 bits are the netid and the last 16 bits are the hostid.
- **Class C** addresses are used for networks with less than 2^8 hosts. The first 21 bits are the netid and the last 8 bits are the hostid.

NOTE:
There are two more formats of IP addresses, one used for multicast addresses and one for future use. Neither is relevant for this application.

Destination Port

Identify which file transfer services can and cannot be accessed, and which of your computer's ports provide access to these services. The TCP/IP protocol defines standard TCP and UDP ports that provide Internet file transfer services. For example, TCP port number 21 provides the FTP service. A list of ports and the services they provide appears in the Rules Base Manager Ports dialog box, as described in Section 3 of this manual.

Tracking

Personal Firewall can keep track of all incoming connections by recording each connection activity (for example, Receive) in a file, called a log file. In addition, an alarm can sound when there is an incoming connection. Determine which activities should be recorded in a log file and which activities should cause an alarm to sound.

3 RULES BASE MANAGER

The Rules Base defines the limits of acceptable behavior in your system. **Personal Firewall** relies on these rules in keeping the system secure. This section provides instructions for using the Rules Base manager application.

To open the Rules Base Manager, double-click on the icon.

The initial screen appears with a list of existing rules files.

Each rules file contains the list of rules for Firewall operation.

File Operations

1. To create a new file: Press **New File** and type the file name at the prompt.

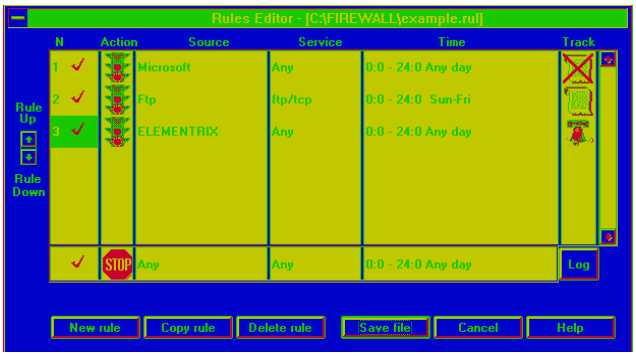
2. To delete a file: Highlight the file and press **Delete File**.

3. To create a new file based on an existing file: Highlight the file and press **Copy File**. A prompt appears. Type the name of the new file.

The Rules List

If you chose to create a new file or the modify an existing file, the rules definition screen appears.

This screen contains the list of rules that determine whether incoming communication can reach the computer.



Each rule appears on a separate line in the table and consists of the following fields:

N
The rule number, followed by a check mark if the rule is activated.

Action
The action that Personal Firewall should take (accept or reject) if the incoming communication matches all of the other conditions in the rule.

Source IP address
IP address which should match the incoming packet's source IP address.

Service
The service port which should match the port that the incoming packet is trying to reach.

Time
Time when the rule should apply.

Track
The type of tracking for this rule: No Logging, Log, Alert. There are six types of communication operations that can be logged: Listen, Accept, Connect, Send, Receive and Close. Alert will sound an audible alarm whenever an activity is recorded in the log file.

Sample Rules

This rules list contains three examples of typical rules:

1. Accept all incoming connections from host Microsoft, any time of the day and do not log the activities.

2. Accept all incoming connections from host FTP, to port number 21, from 0:00 to 24:00 Monday through Friday. Log these activities.

3. Accept all incoming connections from host Elementrix, log the activities and sound an alarm for each incoming connection.

Modifying Lines in the Rules List

4. Use the **New Rule** button to add a new line with initial rule values to the rules list.

5. Use the **Copy Rule** button to copy a rule to a new line in the list.

6. Use the **Delete Rule** button to delete a selected rule.

7. Use the **Rule Up** or **Rule Down** arrow buttons on the left side of the list to change the order of the rules.

Modifying Individual Rules

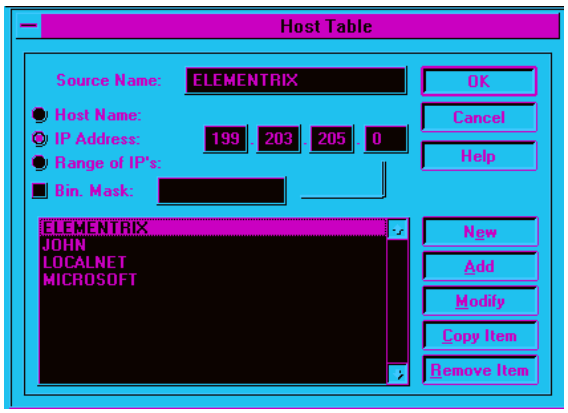
To modify specific information for an individual rule, double-click on the desired value to open a dialog box.

The **Action** dialog box contains two options: Accept or Reject.

The **Track** dialog box contains three options: No logging, Log, Alert.

Defining a Source

The Source dialog box allows you to define a list of sources and to select the source for the current rule in the rules list.



There are three ways to define a source. In each case, define the source as described below and use the **New**, **Add** or **Modify** buttons to update the list of sources.

- To define a source by its **Host Name**, click the **Host Name** button , type the source name and type the host name in the space provided.

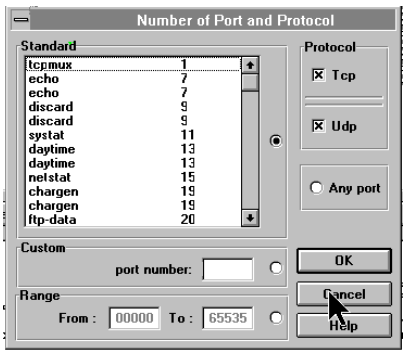
- To define a source by its **IP Address**, click the **IP Address** button, type the source name and type the IP address in the space provided.
- To define a source by a **range of IP Addresses**, click the **Range of IPs** button, type the source name and type the From and To IP Addresses in the spaces provided.

To select a source for the current rule:

- Highlight a source in the source list or enter the source definition in the source definition fields, in the same manner as used for defining a new source.
- Press **OK** to close the dialog box and select the source. The source appears in the rules list.

Defining a Service Port

The Service dialog box allows you to select a standard UDP or FTP port or to define a specific port.



You can display a list of standard TCP ports, UDP ports or both. Many of the ports are used for the same operation in both TCP and UDP.

- To display a list of standard TCP ports, click the TCP checkbox and select the button to the right of the list.
- To display a list of standard UDP ports, click the UDP checkbox and select the button to the right of the list.

To select a port:

- Highlight a port in the list or click the **Custom** or **Range** button and type a custom port number or range of ports.
- Press **OK** to close the dialog box and select the port.

Defining a Time Frame

The Time dialog box contains command buttons for defining a period of dates and times. The default is Any Day, where all of the days and hours are selected.

Use the checkboxes to select or deselect the days and resize the hour bar to select a time from 00:00 to 24:00.

Applying and Saving Rules

Each individual rule can be activated by clicking next to the rule number until a check appears. Only rules which are activated will be considered by **Personal Firewall**.

Once the rules list is complete and you want Personal Firewall to begin using the rules, press the **Apply Rules** button.

Use the **Save File** button to save the list of rules.

How the Firewall Filter Applies the Rules

When the Firewall Filter detects incoming communication packet it goes through each activated rule in the list as follows:

1. If the current time corresponds to the time frame defined in the Time field, it compares the source IP address of the TCP/IP packet with the value in the Source field.

2. It also compares the service requested by the TCP/IP packet with the port in the Service field.

3. If the Source and Service match, it takes the necessary action (rejects or accepts communication).

If the Track field contains Log or Alarm, then communication is recorded in the log file and an alarm is sounded, if so defined.

IMPORTANT:
The last rule is the same for all rules list. This rule says the Firewall Filter automatically rejects any incoming communication packet that does not comply with any other rule in the list.

Multiple Rules Files

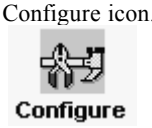
You can define many rules files and switch between them when necessary.

For example, if you work with a laptop computer, you may want one set of rules for the office connection, that allows all office LAN users to access your computer and one set of rules for home connection, that blocks all access attempts.

4 CONFIGURATION

This section describes the Configuration application, which is used for defining the location of the log files and the operating modes of **Personal Firewall**.

To start the Configuration application, double-click on the Configure icon.



The configuration screen appears.

Operating Modes

The following options define the **Personal Firewall** operating modes. These definitions are used whenever Windows is restarted. Click each checkbox to turn an option on or off. A check indicates that the option is selected and an empty checkbox indicates that the option is off:

Load on startup
This option causes the Firewall Filter to automatically begin operation as soon as Windows opens.

Show Logo
If the Firewall Filter is loaded at Windows startup, this option displays a Personal Firewall logo screen during Windows initialization.

Output Log
These options define where the output log should be stored, **To file** or **To screen**. If you select **To screen**, the log information will appear in the Firewall Filter application screen and the log data will also be saved in the log file. Double-clicking on the Firewall Filter icon will display the log data.

Icons

These options define where the Firewall Filter icon will appear when the program is active. If you select **Always on top**, then the program icon will appear whenever Personal Firewall is active. This is in addition to the Firewall Filter application icon that appears in the Windows program group.

If you select **Hide**, then the icon will still appear in the Windows program group. In this case, you can still open the Personal Firewall window by double-clicking on the icon in the Personal Firewall group.

Log Directory

The log directory is the directory that Personal Firewall uses for log files. The default directory is the same directory that contains the program files.

Modifying Configuration in FW Filter

You can modify the configuration for the currently running version of Personal Firewall using the System menu in the FW Filter application. The options in this menu are the same as the ones in the Configuration application, but any modifications are for the currently running program, and will be lost if you restart Personal Firewall or Windows.

5 LOG VIEWER

The log viewer is used to display the information from the log file. This section describes the log viewer operations.

To open the log viewer, double-click on the icon.

If there is no current log, then an Open Log File screen appears. You can copy, delete or rename a file using the command buttons in this screen. To open a log file from this screen, highlight the file name and press **OK**.

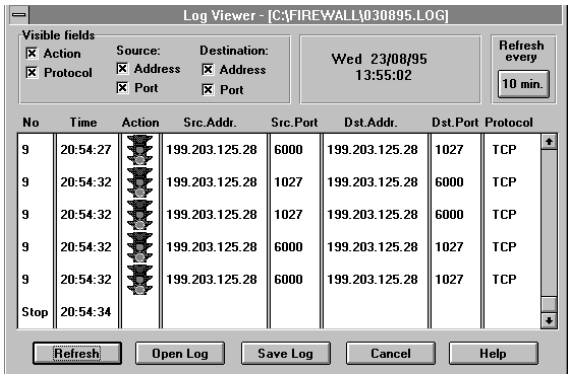
If there is a current log, the Log Viewer appears automatically.

Log File Names

Personal Firewall automatically assigns log file names according to dates, in the format <*ddmmyy*>.*log*. For example, *250895.log* corresponds to August 25, 1995. The current day's log entries are stored in a file called *today.log*. At the end of each day, *today.log* is renamed with the current date.

To view a log file, highlight a log file name

Select a log file and press **OK**. The Log Viewer appears.



Display Fields

The **Visible fields** options at the top of the screen determine which log file information is displayed.

Select or turn of any field as desired. Since this is a view screen, these options have no affect on the actual log file data.

Log Date and Time

The **Date** area at the top of the screen shows the current date and time, if this is the current log, or the date of the displayed log.

Log Display Refresh

The information displayed in this screen can be refreshed only if it is the current log. The **Refresh interval** button at the top of the screen is used to define how often the log screen is repainted with updated information (refreshed). To automatically refresh the screen, press the **Refresh** button at the bottom of the screen.

Log File Operations

1. To open a new log file, press **Open Log**.

2. To save the currently displayed log file, press **Save Log**. This is useful, for instance when you want to save only part of the current day's log in a separate file.

Using the Firewall Filter

If your program is configured to send the log to the screen as well as to a file, you can view the current log by double-clicking on the FW Filter application icon. This log display contains the full log messages.

GLOSSARY

Firewall
A collection of components placed between two networks in order to prevent unwanted penetration of them.

Gateway
A piece of hardware placed between networks in order to expand their scope.

IP Address
Internet Protocol Address. A standard address used when transferring files between computers to identify the source and destination computers. Each host on the Internet can be identified using this 32-bit address.

Protocol
Standard data formats or file transfer rules which are understood by many different types of hardware and software components.

TCP
A protocol used for network file transfers.

TCP/IP
The data transfer protocol used on the Internet, that defines how the data should be packaged and how the source and destination should be identified.

UDP

A protocol used for network file transfers.