Implementation of Personal Firewalls for Handheld Devices

Nwe Wady, Khaing Khaing Wai
Computer University, Maubin
zonun.wady@gmail.com, khaingkhaing.73@gmail.com

Abstract

The Internet has made large amounts of information available to the average computer user at home, in business and in education. For many people, having access to this information is no longer just an advantage, it is essential. Yet connecting a private network to the Internet can expose critical or confidential data to malicious attack from anywhere in the world. Firewalls can protect both individual computers and corporate networks from hostile intrusion from the Internet, but must be understood to be used correctly. A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. Personal firewalls are typically designed for end-users. Personal Firewall is able to control network traffic by prompting the user. Personal firewalls may also provide some levels of intrusion detection, allow the software to terminate or block connectivity where it suspects an intrusion is being attempted. This paper is proposed to implement personal firewall used in laptops, personal computers and Personal Digital Assistants (PDA) for personal use.

1. Introduction

Computer networks are generally designed to do one thing above all others: allow any computer connected to the network to freely exchange information with any other computer also connected to the same network. In an ideal world, this is a perfect way for a network to operate facilitating universal communications between connected systems. Individual computers are then free to decide who they want to communicate with, what information they want to allow access to and which services they will make available. This way of operating is called “host based security”, because individual computers or hosts implement security mechanisms.

A firewall inspects network traffic passing through it, and denies or permits passage based on a set of rules. A firewall is a dedicated appliance, or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules. A firewall's basic task is to regulate some of the flow of traffic between computer networks of different trust levels. A firewall regulates some of the flow of traffic between computer networks of different trust levels. A firewall prevents network intrusion to the private network.

Personal firewalls are network devices which enforce an organization's security policy. Since their development, various methods have been used to implement personal firewalls. These methods filter network traffic at one or more of the seven layers of the network model, most commonly at the application, transport, and network, and data-link levels. In addition, researchers have developed some newer methods, such as protocol normalization and distributed personal firewalls, which have not yet been widely adopted.

This system is designed to use personal firewall application in personal computers, laptops, notebooks, personal digital assistants and other types of computer for personal use only.

2. Theoretical background

In this section, we introduce the background theories used to implement the Firewalls.

2.1 Firewall architecture

In order to keep a corporate network secure, companies protect and isolate their internal systems from the Internet with a network firewall. Simply put, a firewall prevents certain outside connections from entering your network. A firewall will trap inbound or outbound packets, analyze them, and then either permit access or discard them. The firewall (sometimes referred to as a bastion host) is a subsystem of computer software and hardware that intercepts data packets before allowing them into or out of a Local Area Network (LAN) or internet. A

firewall makes decisions on whether or not data is allowed to pass based upon a security policy. For each packet of data, the firewall compares known components of the packet to a security rule set and decides if the packet should be allowed to pass. In addition, a firewall may have security rules that involve altering the packet in some basic ways before passing the data. With a sensible security policy and a security rule set designed to implement that policy, a firewall can protect a LAN or internet from attacks [2].

2.2 Firewall types

There are a number of different kinds of technique which may be employed by a Firewall in order to correctly identify a conversation and act on it. The techniques used by a particular Firewall have an impact on the accuracy with which it can identify traffic, the level of sophistication of the checks it can implement, but also it's complexity and therefore cost and likelihood that it incorporates bugs. The main function of a firewall is to centralize access control. A firewall serves as the gatekeeper between the untrusted Internet and the more trusted internal networks. If outsiders or remote users can access the internal networks without going through the firewall, its effectiveness is diluted [5].

A true firewall is the hardware and software that intercepts the data between the Internet and your computer. All data traffic must pass through it, and the firewall allows only authorized data to pass into the corporate network [2]. Firewalls are typically implemented using one of four primary architectures:

- Packet Filters
- Circuit-level Gateways
- Application Proxies
- Network Address Translation

2.2.1 Application proxies

An application-level firewall is a proxy server that understands the particular application it is providing proxy services for, and it intercepts network traffic for a specific kind of application . Application-level firewalls are generally implemented to work at application level. The main difference between the packet-filtering firewall and the application-level firewall is that the application-level firewall must understand the application. Application-level firewalls are more secure than packet-filtering firewalls as they can be programmed to allow or deny network traffic based on information contained in the payload session of the packet, not just the header information. Moreover, the application-level firewall does not allow direct connections between an internal host of the protected network and an external host on the outside network. All communications between an internal host and an external host are handled by the proxy. Thus, the application-level firewall hides the network information of the internal network and reduces potential threats to the internal network. The disadvantage of application-level firewalls is each proxy service requires its own proxy. For example, FTP, HTTP and TELNET require their own proxies, namely FTP proxy, HTTP proxy and TELNET proxy. As a result, the application-level firewall must understand each proxy service it provides. The TIS (Trusted Information Systems) Firewall Toolkit (FWTK) is an instance of the application-level firewall. FWTK includes a number of proxy servers of different types such as FTP, Telnet, Rlogin, HTTP, Gopher, SMTP and NNTP [1].

3. Proposed system

This system is aimed to propose the firewall as personal use.

3.1 Firewall capabilities

A firewall defines a single choke point that keeps unauthorized users out the protected network. A firewall provides a location for monitoring security-related events. Audits and alarms can be implemented on the firewall system. A firewall is a convenient platform for several Internet functions that are not security related. A firewall can serve as the platform for IPSec. Using the tunnel mode capability, the firewall can be used to implement virtual private network [4].

In many situations it is necessary for the firewall to allow incoming traffic on ports and protocols that normally are not open. For example, incoming UDP traffic may not be allowed to enter through the firewall unless there is pending request waiting for a response [3].

3.2 Main function of personal firewall

The main functions of personal firewall would be:

- Offer clearly explained configuration options
- Filtering of outgoing/incoming traffic
- Hide all ports to make system invisible to scan
- Protect the system from attacks
- Track potential and actual threats

- Immediately alert user to serious attacks

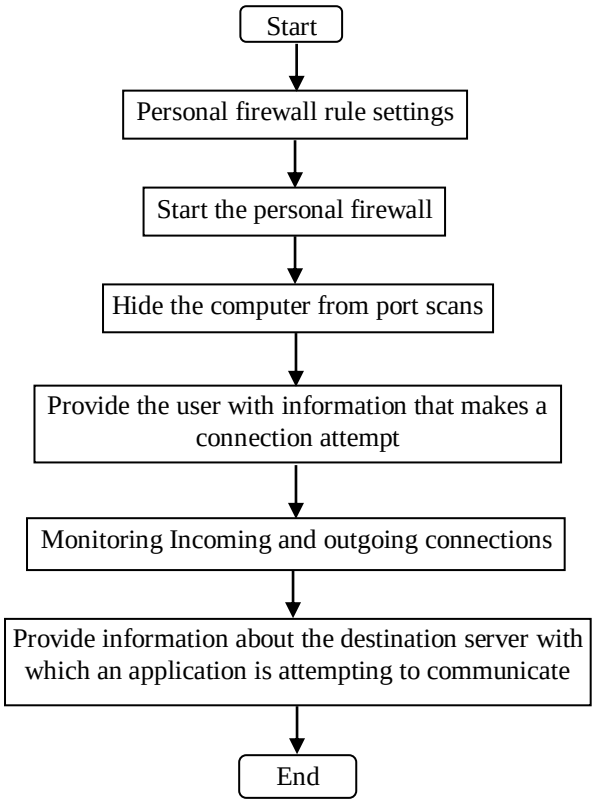

Figure 3.1 System flow diagram

In this system, rule settings of firewall are setting up and start the firewall. Computer can be hiding from the ping by using block ping. Opening or closing ports are scanned by using port scanner. User can allow or deny port by using this system.

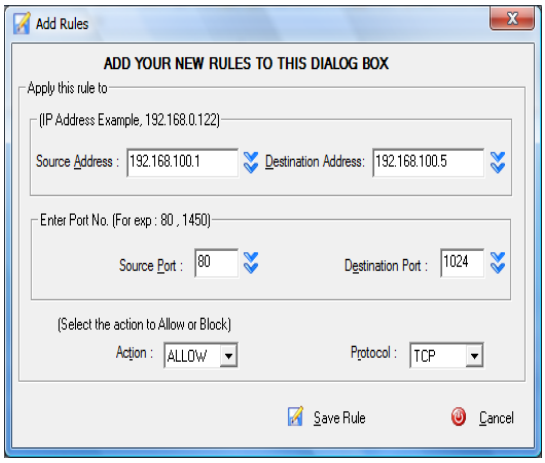

Figure 3.2 Adding rule setting

In figure 4.2, user can add rules for this personal firewall. User types source address, destination address, source port, destination port, choose allow or denied and choose the protocol. This system automatically adds this rule.

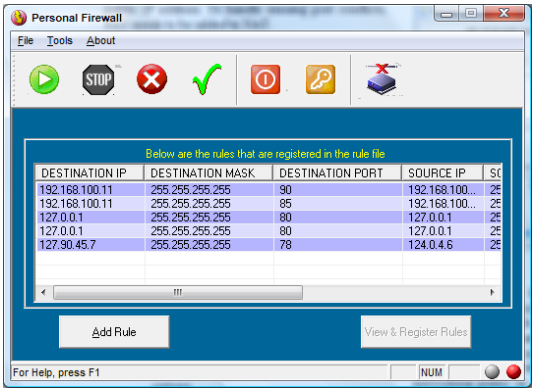

Figure 3.3 View registering rule

All registering rules are shown in this figure. This has destination IP, destination mask, destination port, source IP, source mask, source port, protocol and action.

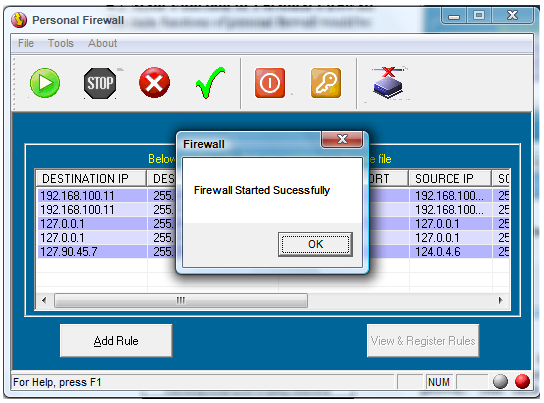

Figure 3.4 Starting firewall

Personal firewall is started from this figure. User clicks Firewall Start button. The system starts the firewall and user can use personal firewall facilities.

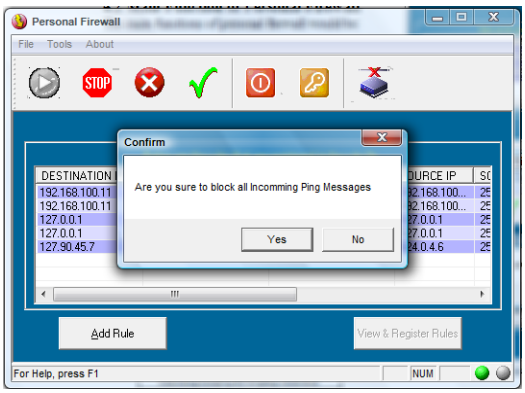

Figure 3.5 Blocking all incoming ping message

User can block incoming ping from this figure. User clicks block ping button. This system blocks all incoming message from the network.

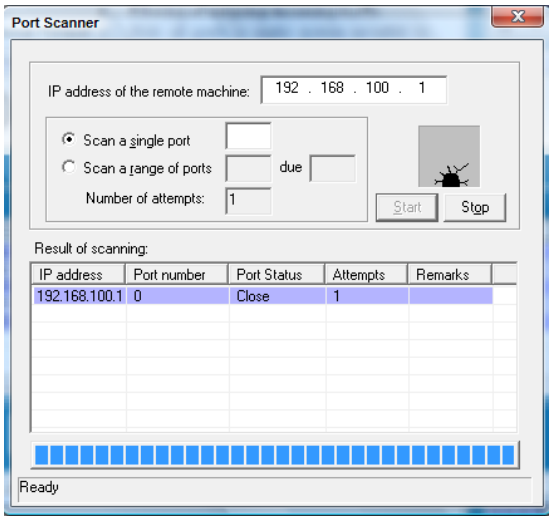

Figure 3.6 Port scanner

User can search opening or closing port from this figure. User types IP address and choose single port scan or a range of port. Then choose number of attempt and clicks start. This system automatically searches the port scanning and displays scanning port status on the result of scanning table.

This system can be used in handled devices like laptops, personal computer and personal digital assistants to avoid attacking from network or internet.

4. Conclusion

A typical home network configuration shares home PCs and printers behind a residential gateway, with each PC protected by antivirus software. The residential gateway is a router with a NAT firewall (such as current broadband cable/DSL routers equipped with multiple 10/100 Ethernet networking ports) or a PC configured for NAT or ICS. In the latter case, the PC must be equipped with robust personal firewall software to protect itself and all PCs on the home network. If these residential gateway options are not possible, each PC connected to the Internet must be protected by personal firewall software. Good security is multilayered, and includes ISP security measures to detect and block attacks. Within the home or home network, implementing ICS or NAT on the home network gateway device hides the IP addresses of networked PCs. The addition of firewall software on the gateway device or on each networked PC provides another layer of protection, as does regularly monitoring the logs generated by the firewall software. For further protection, users can enable password protection on each networked PC. Finally, the ultimate protection is to power off networked PCs that are not in use for extended periods of time.

Handheld computers are important computing tools due to their size and light weight. However, handheld devices also become attackers' targets as they become more popular. The system reviewed some security threats to handheld computers and proposed several possible solutions. The system highlighted the difficulty of building a personal firewall in PC operating system.

Personal firewall can be installed in personal computers, laptops, notebooks and personal digital assistants. A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. Provide information about the destination server which an application is attempting to communicate. Prevent unwanted network traffic from locally installed applications. By using this system, user can successfully access network security.

References

[1] “Design and Implementation of Personal Firewalls for Handheld Devices” Jianyong Huang, Willy Susilo and Jennifer Seberry Centre for Computer Security Research School of Information Technology and Computer Science University of Wollongong, Wollongong, NSW 2522, Australia.

[2] “Firewall Architecture” Understanding the purpose of a firewall when connecting to ADSL network services. *A Nextep Broadband White Paper June 2001*

[3] “Firewalls: how secure are they?” Australian PC USER, pages 52{56, September 2002.

[4] “Trusted Information Systems (TIS) Firewall Toolkit (FWTK)”. http://www.fwtk.org.

[5] William R. Cheswick, Steven M. Bellovin, and Aviel D. Rubin. Firewalls and Internet Security: Repelling the Wily Hacker. AddisonWesley Professional, second edition, 2003.