5.5 FIREWALL BASING

It is common to base a firewall on a stand-alone machine running a common operating   system, such as UNIX or Linux. Firewall functionality can also be implemented as a software module in a router or LAN switch. In this section, we look some additional firewall basing considerations.

Bastion Host

A bastion host is a system identified by the firewall administrator as a critical strong point in the network's security. Typically, the bastion host serves as a platform for an   application-level or circuit-level gateway. Common characteristics of a bastion host are as follows:

 • The bastion host hardware platform executes a secure version of its operating system, making it a hardened system.

• Only the services that the network administrator considers eessential are installed on the bastion host. These could include proxy applications for DNS, FTP, HTTP, and SMTP.

• The bastion host may require additional authentication before a user is allowed access to the proxy services. In addition, each proxy service may require its own authentication before granting user access.

• Each proxy is configured to support only a subset of the standard application's command set.

• Each proxy is configured to allow access only to specific host systems. This means that the limited command/feature set may be applied only to a subset of   systems   on   the protected network.

• Each proxy maintains detailed audit information by logging all traffic, each connection, and the duration of each connection. The audit log is an essential tool for discovering and terminating intruder attacks.

• Each proxy module is a very small software package specifically designed for network security. Because of its relative simplicity, it is easier to check such modules for security flaws. For example, a typical UNIX mail application may contain over 20,000 lines of code, while a mail proxy may contain fewer than 1000.

• Each proxy is independent of other proxies on the bastion host. If there is a
problem with the operation of any proxy, or if a future vulnerability is discovered, it can be
uninstalled without affecting the operation of the other proxy applications. Also, if the user
population requires support for a new service, the network administrator can easily
install the required proxy on the bastion host.

• A proxy generally performs no disk access other than to read its initial config-
uration file. Hence, the portions of the file system containing executable code
can be made read only. This makes it difficult for an intruder to install Trojan horse sniffers or
other dangerous files on the bastion host.

• Each proxy runs as a nonprivileged user in a private and secured directory on the bastion host.

Host-Based Firewalls

A host-based firewall is a software module used to secure an individual host. Such modules are
available in many operating systems or can be provided as an add-on package. Like conventional
stand-alone firewalls, host-resident firewalls filter and restrict the flow of packets. A common
location for such firewalls is a server. There are several advantages to the use of a server-based or
workstation- based firewall:

•   Filtering rules can be tailored to the host environment. Specific corporate security
policies for servers can be implemented, with different
filters for servers used for different application.

•   Protection is provided independent of topology. Thus both internal and
external attacks must pass through the firewall.

•   Used in conjunction with stand-alone firewalls, the host-based firewall pro- vides an
additional layer of protection. A new type of server can be added to the network, with its own
firewall, without the necessity of altering the net- work firewall configuration.

Personal Firewall

A personal firewall controls the traffic between a personal computer or workstation on one side and the Internet or enterprise network on the other side. Personal fire-wall functionality can be used in the home environment and on corporate intranets. Typically, the p ersonal firewall is a software module on the personal computer. In a home environment with multiple computers connected to the Internet, firewall functionality can also be housed in a router that connects all of the home com puters to a DSL, cable modem, or other Internet interface.

Personal firewalls are typically much less complex than either server-based firewalls or stand-alone firewalls. The primary role of the personal firewall is to deny unauthorized remote access to the computer. The firewall can also monitor outgoing activity in an attempt to detect and block worms and other malware.

An example of a personal firewall is the capability built in to the Mac OS X operating system. When the user enables the personal firewall in Mac OS X, all inbound connections are denied except for those the user explicitly permits. Figure shows this simple interface.

The list of inbound services that can be selectively reenabled, with their port numbers, includes the following:

• Personal file sharing (548, 427)

• Windows sharing (139)

• Personal Web sharing (80, 427)

• Remote login - SSH (22)

• FTP access (20-21, 1024-64535 from 20-21)

• Remote Apple events (3031)

• Printer sharing (631, 515)

• IChat Rendezvous (5297, 5298)

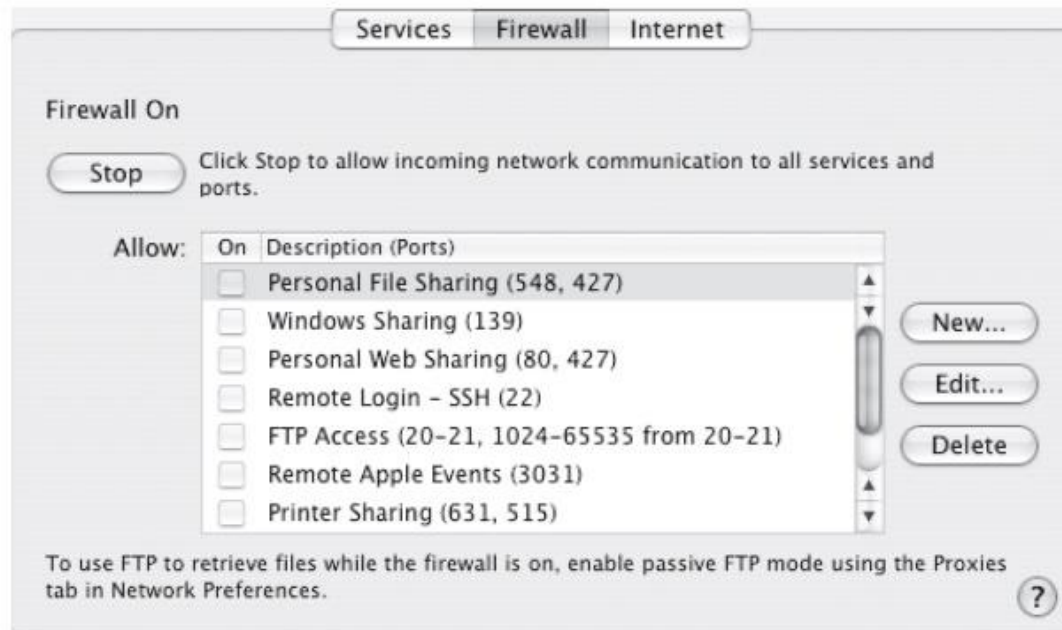• ITunes Music Sharing (3869)

• CVS (2401)

Figure 22.2   Example Personal Firewall Interface

• Gnutella/Limewire (6346)

• ICQ (4000)

• IRC (194)

• MSN Messenger (6891-6900)

• Network Time (123)

• Retrospect (497)

• SMB (without netbios-445)

• Timbuktu (407)

• VNC (5900-5902)

• WebSTAR Admin (1080, 1443)

When FTP access is enabled, ports 20 and 21 on the local machine are opened for FTP; if o thers connect to this computer from ports 20 or 21, the ports 1024 through 64535 are open.

For increased protection, advanced firewall features are available through easy-to-configure checkboxes. Stealth mode hides the Mac on the Internet by drop- ping unsolicited communication packets, making it appear as though no Mac is present. UDP packets can be blocked, restricting network traffic to TCP packets
only for open ports. The firewall also supports logging, an important tool for checking on unwanted activity.