A firewall is a software system based on a set of rules for filtering network traffic. Its function is to

protect a computer in a local area network from unauthorized access. The first generation of firewalls,

deployed in the late 1980s, carried out packet filtering; they discarded individual packets that did not

match a set of acceptance rules. Such firewalls operated below the transport layer and discarded packets

based on the information in the headers of physical, data link, and transport layer protocols.

The second generation of firewalls operate at the transport layer and maintain the state of all connections

passing through them. Unfortunately, this traffic-filtering solution opened the possibility of

denial-of-service (DoS) attacks. A DoS attack targets a widely used network service and forces the

operating system of the host to fill the connection tables with illegitimate entries. DoS attacks prevent

legitimate access to the service.

The third generation of firewalls “understand” widely used application layer protocols such as FTP,

HTTP, TELNET, SSH, and DNS. These firewalls examine the header of application layer protocols and

support intrusion detection systems (IDSs).

Firewalls screen incoming traffic and sometimes filter outgoing traffic as well. A first filter encountered

by the incoming traffic in a typical network is a firewall provided by the operating system of the

router; the second filter is a firewall provided by the operating system running on the local computer

(see Figure 11.5).

Typically, the local area network (LAN) of an organization is connected to the Internet via a router.

A router firewall often hides the true address of hosts in the local network using the Network Address

Translation (NAT) mechanism. The hosts behind a firewall are assigned addresses in a “private address

range,” and the router uses theNAT tables to filter the incoming traffic and translate external IP addresses

to private ones.2

not cross a router. Once a client from a different LAN attempts to use the service, the packets may

be discarded by the router’s firewall. The application may no longer work if the router is not properly

configured.

Now let’s examine the firewall support in several operating systems. Table 11.1 summarizes the

options supported by various operating systems running on a host or on a router.

A rule specifies a filtering option at (i) the network layer, when filtering is based on the destination/

source IP address; (ii) the transport layer, when filtering is based on destination/source port

number; or (iii) the MAC layer, when filtering is based on the destination/source MAC address.

In Linux or Unix systems the firewall can be configured only as a root using the sudo command. The

firewall is controlled by a kernel data structure, the iptables. The iptables command is used to set up, maintain, and inspect the tables of the IPv4 packet filter rules in the Linux kernel. Several tables may

be defined; each table contains a number of built-in chains and may also contain user-defined chains. A

chain is a list of rules that can match a set of packets: The INPUT rule controls all incoming connections;

the FORWARD rule controls all packets passing through this host; and the OUTPUT rule controls all outgoing connections from the host. A rule specifies what to do with a packet that matches: Accept, let

the packet pass; Drop, discharge the packet; Queue, pass the packet to the user space; or Return, stop

traversing this chain and resume processing at the head of the next chain. For complete information on

the iptables, see http://linux.die.net/man/8/iptables.

To get the status of the firewall, specify the L (List) action of the iptables command:

sudo iptables -L

As a result of this command the status of the INPUT, FORWARD, and OUTPUT chains will be displayed.

To change the default behavior for the entire chain, specify the action P (Policy), the chain name,

and the target name; e.g., to allow all outgoing traffic to pass unfiltered, use

sudo iptables -P OUTPUT ACCEPT s

To add a new security rule, specify: the action, A (add), the chain, the transport protocol, TCP or UDP,

and the target ports, as in:

sudo iptables -A INPUT -p -tcp -dport ssh -j ACCEPT

sudo iptables -A OUTPUT -p -udp -dport 4321 -j ACCEPT

sudo iptables -A FORWARD -p -tcp -dport 80 -j DROP

To delete a specific security rule from a chain, set the action D (Delete) and specify the chain name

and the rule number for that chain. The top rule in a chain has number 1:

sudo iptables -D INPUT 1

sudo iptables -D OUTPUT 1

sudo iptables -D FORWARD 1

By default, the Linux virtual machines on Amazon’s EC2 accept all incoming connections.

The ability to access that virtual machine will be permanently lost when a user accesses an EC2

virtual machine using ssh and then issues the following command:

sudo iptables -P INPUT DROP.

The access to the Windows 7 firewall is provided by a GUI accessed as follows:

Control Panel -> System & Security -> Windows Firewall -> Advanced

Settings

The default behavior for incoming and/or outgoing connections can be displayed and changed from

the window Windows Firewall with Advanced Security on Local Computer.

Access to the Windows XP firewall is provided by a graphical user interface (GUI) accessed by

selecting Windows Firewall in the Control Panel. If the status is ON, incoming traffic is blocked by

default and a list of Exceptions (as noted on the Exceptions tab) defines the connections allowed. The

user can only define exceptions for TCP on a given port, UDP on a given port, and a specific program.

Windows XP does not provide any control over outgoing connections.

Antivirus software running on a local host may provide an additional line of defense. For example,

the Avast antivirus software (see www.avast.com) supports several real-time shields. The Avast network shield monitors all incoming traffic; it also blocks access to known malicious Web sites. The

Avast Web shield scans the HTTP traffic and monitors all Web browsing activities. The antivirus also

provides statistics related to its monitoring activities.