# Firewalls

Tips 1:

A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet (the local network to which you are connected) must pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Tips 2:

Several types of firewalls exist:

- **Packet filtering:** The system examines each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
- **Circuit-level gateway implementation:** This process applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- **Acting as a proxy server:** A proxy server is a type of gateway that hides the true network address of the computer(s) connecting through it. A proxy server connects to the internet, makes the requests for pages, connections to servers, etc., and receives the data on behalf of the computer(s) behind it. The firewall capabilities lie in the fact that a proxy can be configured to allow only certain types of traffic to pass (for example, HTTP files, or web pages). A proxy server has the potential drawback of slowing network performance, since it has to actively analyze and manipulate traffic passing through it.
- **Web application firewall:** A web application firewall is a hardware appliance, server plug-in, or some other software filter that applies a set of rules to a HTTP conversation. Such rules are generally customized to the application so that many attacks can be identified and blocked.

Tips 3:

In practice, many firewalls use two or more of these techniques in concert.

In Windows and macOS, firewalls are built into the operating system.

Third-party firewall packages also exist, such as Zone Alarm, Norton Personal Firewall, Tiny, Black Ice Protection, and McAfee Personal Firewall. Many of these offer free versions or trials of their commercial versions.

In addition, many home and small office broadband routers have rudimentary firewall capabilities built in. These tend to be simply port/protocol filters, although models with much finer control are available.

Tips 4:

Important TermsIn the previous section, you were introduced to the term filtering point. Types of rules, referred to as a table, can be placed on a filtering point. A filtering point can have one or more sets of rules because iptables performs multiple functions: either filter (block or allow) the data, perform a NAT operation on the packet, or mangle the packet. The combination of the filtering point plus the table (filter, nat, or mangle) are combined into a single set of rules called a chain.Consider a chain to be a set of rules that determines what actions to take on a specific packet. For example, a rule on the "filter INPUT" chain could block an incoming packet based on the source IP address. Another rule could be used to allow packets destined for a specific network port.The order of the rules is also important. Once a matching rule is found, an action (called a target) takes place and additional rules are ignored (with one exception, as noted next). Here are the different types of targets:

- ACCEPT: Allow the packet to continue to the next step (filtering point, routing decision, and so on).
- DROP: Do not allow the packet to continue to the next step; just discard it.
- REJECT: Do not allow the packet to continue to the next step but send a response message to the origin of the packet informing it of the rejection. This is different than DROP because with DROP the origin of the packet is never informed of what happens with the packet.
- LOG: Create a log entry. Note that a target of ACCEPT, DROP, or REJECT results in no further rules being evaluated, but LOG will result in creating the log entry and then continuing to evaluate additional rules. So, you can create a rule to log a connection attempt and then DROP or REJECT the attempt with another rule.

Each chain also has a default chain policy. If you have not edited a chain, this should be set to ACCEPT. This means that if a packet does not match any DROP or REJECT rules in the chain, the default policy of ACCEPT will allow it to continue to the next step.On systems where security is paramount, you might want to change this default rule to DROP. This means that the only packets that are allowed to move to the next step in the process are those that match an ACCEPT rule in the chain.All of these terms (filtering point, table, chain, rule, and default chain policy) will become clearer as examples are provided during

this chapter. So, if some of these terms are a bit fuzzy now, they should make more sense as you explore using the iptables command to implement firewall rules.

Each chain also has a default chain policy. If you have not edited a chain, this should be set to ACCEPT. This means that if a packet does not match any DROP or REJECT rules in the chain, the default policy of ACCEPT will allow it to continue to the next step.On systems where security is paramount, you might want to change this default rule to DROP. This means that the only packets that are allowed to move to the next step in the process are those that match an ACCEPT rule in the chain.All of these terms (filtering point, table, chain, rule, and default chain policy) will become clearer as examples are provided during this chapter. So, if some of these terms are a bit fuzzy now, they should make more sense as you explore using the iptables command to implement firewall rules.