4.4.5 Configure iptables Facts

This lesson covers the following topics:

- Chains
- Actions performed
- Example iptables commands

Chains

The Linux iptables firewall utility uses *policy chains* (sets of rules) to allow or block network traffic. When a connection is initiated to your system, iptables looks for a matching rule. If it doesn't find one, it uses the default action in the tables. Be aware that iptables almost always comes pre-installed on any Linux distribution.

The filter table in iptables has three chains. The following table describes them.

Chain	Description
Input	This chain controls the behavior for incoming connections. For example, if a user attempts to ping the system, iptables attempts to match the IP address and port to a rule in the input chain.
Forward	This chain is used for packets leaving the system. These are incoming connections that aren't delivered locally. In other words, the traffic is not destined for the router; the router forwards the traffic to the destination device.
Output	This chain is used for outgoing connections. For example, if you ping testout.com, iptables checks its output chain to see what the rules are regarding ping and testout.com before allowing or denying the ping request.

Actions Performed

You can accept, drop, or reject the connections. After you define your accept rules, you should create a rule to drop all other traffic to prevent unauthorized access to the system.

Action	Result
Accept	Allows the connection.
Drop	Drops the connection. For example, an IP address in a rule with a drop action pings your system; the request is dropped. No response is sent to the user.
Reject	Rejects the connection, but will send a response back. This lets the sender know that the traffic reached a system, but was rejected.

Examples iptables Commands

The following table describes commands for iptables. Keep in mind that these are only a few examples; there are many more iptable commands.

Action	Command

List current rules	**sudo iptables -L**
Clear current rules	**sudo iptables -F**
Save iptables changes (Ubuntu)	**sudo /sbin/iptables-save** The command may be different on other Linux systems.
Drop all incoming traffic	**sudo iptables -A INPUT -j DROP**
Block connections from 192.168.0.254	**sudo iptables -A INPUT -s 192.168.0.254 -j DROP**
Block SMTP mail on port 25	**sudo iptables -A OUTPUT -p tcp --dport 25 -j REJECT**
Allow SMTP mail on port 25	**sudo iptables -A INPUT -p tcp --dport 25 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT** **sudo iptables -A OUTPUT -p tcp --sport 25 -m conntrack --ctstate ESTABLISHED -j ACCEPT**
Allow HTTP traffic on port 80	**sudo iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT** **sudo iptables -A OUTPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j ACCEPT** To allow HTTPS, you would use port 443.
Allow HTTP traffic on port Allow HTTPS traffic on port 443	**sudo iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT** **sudo iptables -A OUTPUT -p tcp -m multiport --dports 80,443 -m conntrack --ctstate ESTABLISHED -j ACCEPT**