8.1.7 Linux iptable Facts

iptables is a command line firewall utility for Linux operation systems that uses three different policy chains to allow or block network traffic. When a connection is initiated to your system, iptables looks for a rule in its list to match it to. If it doesn't find one, it resorts to the default action in the tables.

iptables almost always comes pre-installed on any Linux distribution. To update or install iptables, just retrieve the iptables package by entering the following command:

Chains

iptables uses three chains: input, forward, and output.

Chain	Description
Input	This chain controls the behavior for incoming connections. For example, if a user attempts to ping your system, iptables attempts to match the IP address and port to a rule in the input chain.
Forward	This chain is used for incoming connections that aren't delivered locally. For example, if iptables are being used on a router, the traffic is not destined for the router, but the router will forward the traffic to the destination device.
Output	This chain is used for outgoing connections. For example, if you try to 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 need to decide what action you want the rules to perform. 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, if someone pings your system, the request is dropped, and no response is sent to the user.
Reject	Does not allow the connection, but will send a response back. This lets the sender know that he reached a system, but was rejected.

Examples

These are some examples of the uses and commands for iptables. Keep in mind that these are a only few examples, are there are many more.

Action	Result
sudo iptables -L	Lists all the current rules.
sudo iptables -F	Clears all the current rules.
sudo /sbin/iptables-save	Saves changes to the iptables on Ubuntu systems. The command may differ on other Linux systems.
sudo iptables -A INPUT -j DROP	Drops all incoming traffic.
sudo iptables -A INPUT -s 192.168.0.254 -j DROP	Blocks all connections associate with the IP address of 192.168.0.254.
sudo iptables -A OUTPUT -p tcp --dport 25 -j REJECT	Blocks 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	Allows SMTP mail on port 25.
sudo iptables -A INPUT -p tcp --dport 80 -m conntrack --ctstate	Allows HTTP traffic on port 80 on a web server. To allow

NEW,ESTABLISHED -j ACCEPT sudo iptables -A OUTPUT -p tcp --sport 80 -m conntrack --ctstate ESTABLISHED -j ACCEPT	HTTPS, you would use 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	Allows both HTTP and HTTPS on ports 80 and 443 on a web server.