## ****Iptables****

iptables firewall is used to manage packet filtering rules. Iptables is a rule based firewall system and it is normally pre-installed on a Unix operating system which is controlling the incoming and outgoing packets. By-default the iptables is running without any rules, we can create, add, edit rules into it.

* **Different services is used for different protocols as:**

1. iptables applies to **IPv4**.
2. ip6tables applies to **IPv6**.
3. arptables applies to **ARP**.
4. ebtables applies to **Ethernet** frames..

* **IPTables main files are:**

1. **/etc/init.d/iptables** – init script to start|stop|restart and save rulesets.
2. **/etc/sysconfig/iptables** – where Rulesets are saved.
3. **/sbin/iptables** – binary.

* **There are at present three tables.**

1. Filter
2. NAT
3. Mangle

**How to save ,start, stop and restart Iptabe Firewall.**

# service iptables save

# service iptables start

# service iptables stop

# service iptables restart

**To start IPTables on system boot, use the following command.**

#chkconfig --level 345 iptables on

### Check all IPtables Firewall Rules

# iptables -L -n –v

# service iptables status

# iptables -L

**How TO Add Port no.**

**Using Command :-**

# iptables -A INPUT -p udp -m udp --dport 106 -m state --state NEW -j ACCEPT

# iptables -A INPUT -p tcp --dport 25 -j ACCEPT

**0R**

**Directelly Add the Port in iptables file :-**

# vim /etc/sysconfig/iptables

# service iptables save

# service iptables restart

**0R**

**Using GUI :-**

Go to system -> Administrator -> Firewall -> Other Port -> Add -> click on user Defined

### Block Specific IP Address in IPtables Firewall

# iptables -A INPUT -s xxx.xxx.xxx.xxx -j DROP

### Unblock IP Address in IPtables Firewall

# iptables -D INPUT -s xxx.xxx.xxx.xxx -j DROP

### Allow Specific Network Range on Particular Port on IPtables

iptables -A OUTPUT -p tcp -d 192.168.100.0/24 --dport 22 -j ACCEPT

### Block Facebook on IPtables Firewall

# host facebook.com

facebook.com has address 66.220.156.68

# whois 66.220.156.68 | grep CIDR

CIDR: 66.220.144.0/20

### Block Specific Port on IPtables Firewall

To block outgoing connections on a specific port use:

# iptables -A OUTPUT -p tcp --dport xxx -j DROP

To allow incoming connections use:

# iptables -A INPUT -p tcp --dport xxx -j ACCEPT

### Setup Port Forwarding in IPtables

# iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 25 -j REDIRECT --to-port 2525

### Block Incoming Ping Requests on IPtables

# iptables -A INPUT -p icmp -i eth0 -j DROP

### Block Access to Specific MAC Address on IPtables

# iptables -A INPUT -m mac --mac-source 00:00:00:00:00:00 -j DROP

### Save IPtables Rules to a File

# iptables-save > ~/iptables.rules

### Restore IPtables Rules from a File

# iptables-restore < ~/iptables.rules

### Disable Outgoing Mails through IPTables

# iptables -A OUTPUT -p tcp --dports 25,465,587 -j REJECT

**command to list all rules from the Filter table of iptables?**

**Syntax:**

**iptables -t filter --list**

**or**

**iptables -t filter -L**

**Or simply;**

**iptables --list**

**or**

**iptables -L**

## ****command to list all rules from the NAT table of iptables?****

**Syntax:**

**iptables -t nat --list**

**or**

**iptables -t nat -L**

## ****command to list all rules from the Mangle table of iptables?****

**iptables -t mangle --list**

**or**

**iptables -t mangle -L**

**Flushing or deleting IPTables rules. Below command will remove all the rules from tables.**

# iptables -F