**LAB Manual v1.0**

**To install iptables on centos**

**🡺Install iptables**

1. # Yum install iptables-services

**Listing Rules as Tables**

**🡺To view default policy for all chains in filter table**

1. #iptables -L | grep policy

🡺**To list rules**

1. #sudo iptables -L
2. #sudo iptables -L INPUT

**🡺TO view actual rules commands in each chain**

1. #sudo iptables -S

🡺**To view specific chain rules**

1. #iptables -S INPUT

🡺**Listing rules by number for all chain**

1. #iptables -L --line-number
2. #iptables -L INPUT --line-numbers

**Showing Packet Counts and Aggregate Size**

* **For all chain**

1. #iptables -L -v

* **For specific chain**

1. #iptables -L INPUT -V

**Resetting Packet Counts and Aggregate Size**

**🡺To clear the counters for all chains and rules, use the -Z option by itself:**

1. #sudo iptables -Z

**🡺To clear the counters for all rules in a specific chain, use the -Z option and specify the chain.**

1. #sudo iptables -Z INPUT

**🡺To clear the counters for a specific rule, specify the chain name and the rule number**.

1. #sudo iptables -Z INPUT 1

**Deleting Rules by Chain and Number**

🡺**To delete iptables rules by chain and line number. First find the rule number as**

1. #sudo iptables -L INUPT --line-numbers
2. and then use
3. #sudo iptables -D INPUT 3

**Deleting Rules by Specification**

🡺**To delete iptables rules is by rule specification**.

1. #iptables -S to view which rule to delete
2. #sudo iptables -D INPUT -m conntrack --ctstate INVALID -j DROP

🡺**Saving iptables rules**

1. #service iptables save
2. #service iptable restart

🡺**Backup/Restore of Rules**

* **To Backup Rules**

1. #iptables-save > /etc/sysconfig/iptables\_rules

**🡺To Restor Rules**

1. #iptables-restore < /etc/sysconfig/iptables\_rules

**🡺Flushing a Single Chain**

**(We can delete/flush all chains or a specific one)**

* **To flush a specific chain.**

1. #sudo iptables -F INPUT

**🡺To flush all chains becare full**

1. #sudo iptables -F

**(Flushing All Rules, Deleting All Chains, and Accepting All)Defaul state of firewall)**

1. #sudo iptables -t nat -F ,flush nat table
2. #sudo iptables -t mangle -F ,flush mangle table
3. #sudo iptables -F ,flush filter table
4. #sudo iptables -X ,delete all non default chains

**🡺To change a default policy TO DROP/ACCEPT**

1. #iptables -P INPUT DROP OR ACCEPT
2. #iptables -L | grep policy

NOTE: Recommended is that you should l have default policy of accept and

then explicitly drop connection on each chain That way, if there are any problems and the rules are

flushed, you will still be able to access the machine over the network

1. #iptables -A INPUT -j DROP

**🡺To delete all rules from all chains**

#iptables -F and save/restart

**Examples**

**Allowing Loopback Connections**

**To accept all traffic on your loopback interface, run these commands:**

1. #sudo iptables -A INPUT -i lo -j ACCEPT
2. #sudo iptables -A OUTPUT -o lo -j ACCEPT

🡺**Allowing Established and Related Incoming Connections from any interface**

1. #sudo iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

**Allowing Established Outgoing Connections**

**🡺Allow outgoing traffic of all established connections, which are typically the response to legitimate incoming connections. This command will allow that:**

1. #sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT

🡺 **Allowing Internal Network to access External(eth1=lan and eth0=wan)**

For this to work you must have ipforwarding enabled on your system

1. #sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT

**🡺 Blocking an IP Address**

1. #sudo iptables -A INPUT -s 192.168.1.9 -j DROP (all traffic will be blocked on all interfaces)

**🡺Blocking Connections to a Network Interface**

1. #sudo iptable -A IPUT -s 192.168.1.9 -i eth0 -j DROP

**🡺To notify the user about connection drops**

1. #sudo iptables -A INPUT -s 203.0.113.51 -j REJECT

🡺**Blocking connection from a specific network**

1. #sudo iptables -A INPUT -p tcp -s 192.168.1.0/24 -j DROP

**🡺Blocing connection from a specific network to a specific network**

1. #sudo iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.2.0/24 -j DROP

**🡺Blocking connection from a specific sip/network to a specific dip and port**

1. #sudo iptables -A FORWARD -s 192.168.1.0/24 -d 192.168.2.2 -p tcp --dport 80 -j DROP

**Allowing Outgoing SSH**

**🡺To allow ssh/web access to system FROM ANY ONE ON ANY INTERFCE**

1. #iptables -A INPUT -p tcp --dport 80 -j ACCEPT
2. #iptables -A INPUT -p tcp --dport 22 -j ACCEPT

**🡺Allowing New and establish connection from local server to remote server**

1. sudo iptables -A OUTPUT -p tcp --dport 22 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
2. sudo iptables -A INPUT -p tcp --sport 22 -m conntrack --ctstate ESTABLISHED -j ACCEPT

🡺To allow communication from any source to specific destination ip and port on specfic

interface with source port range

1. #iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p tcp --sport 1024:65535 --dport 80 -j ACCEPT

🡺**To allow communication from any source to specific destination ip and multiple port on**

**specfic interface with source port range.**

1. #iptables -A FORWARD -s 0/0 -i eth0 -d 192.168.1.58 -o eth1 -p tcp --sport 1024:65535 -m multiport --dports 80,443 -j ACCEPT
2. #iptables -A FORWARD -d 0/0 -o eth0 -s 192.168.1.58 -i eth1 -p tcp -m state --state ESTABLISHED -j ACCEPT

**Allowing MySQL to Specific Network Interface(MySql)**

**🡺To allow incoming MySQL connections from a specific IP address or subnet, specify the source.**

1. #sudo iptables -A INPUT -p tcp -s 192.168.1.0/24 --dport 3306 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
2. #sudo iptables -A OUTPUT -p tcp --sport 3306 -m conntrack --ctstate ESTABLISHED -j ACCEPT

**🡺Allowing MySQL to Specific Network Interface**

1. #sudo iptables -A INPUT -i eth1 -p tcp --dport 3306 -m conntrack --ctstate NEW,ESTABLISHED -j ACCEPT
2. #sudo iptables -A OUTPUT -o eth1 -p tcp --sport 3306 -m conntrack --ctstate ESTABLISHED -j ACCEPT

**🡺Dropping all other connection**

1. #iptables -A INPUT -j DROP

**🡺Inserting a rules at specific location in a chain**

1. #iptables -I INPUT 2 -p tcp --dport 23 -j ACCEPT

**PORT ADDRESS TRANSLATION**

**🡺Many to one port address translation**

1. #iptables -A POSTROUTING -t nat -o eth0 -s 192.168.1.0/24 -d 0/0 -j MASQUERADE (eth0 is outgoing interface
2. #iptables -A FORWARD -t filter -o eth0 -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
3. #iptables -A FORWARD -t filter -i eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

**🡺Directory editing iptables files to enter rules**

**By creating or editing your /etc/sysconfig/iptables file to look similar to the following basic example, which leaves ports 22 and 80 open:**

1. $ cat /etc/sysconfig/iptables
2. \*filter
3. :INPUT ACCEPT [0:0]
4. :FORWARD ACCEPT [0:0]
5. :OUTPUT ACCEPT [214:43782]
6. -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
7. -A INPUT -p tcp -m tcp --dport 80 -j ACCEPT
8. -A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
9. -A INPUT -i lo -j ACCEPT
10. -A INPUT -j REJECT --reject-with icmp-port-unreachable
11. COMMIT

Save and exit and restart

1. #systemctl restart iptables