iptables and ip6tables

An introduction to LINUX firewall

Imtiaz Rahman
SBAC Bank Ltd
writeimtiaz@gmail.com

AGENDA

- iptables and ip6tables
- Structure
- Policy (DROP/ACCEPT)
- Syntax
- Hands on lab

writeimtiaz@gmail.com

IPTABLES & IP6TABLES

`iptables & ip6tables` is a rule based command-line firewall utility that uses policy chains to allow or block network traffic.

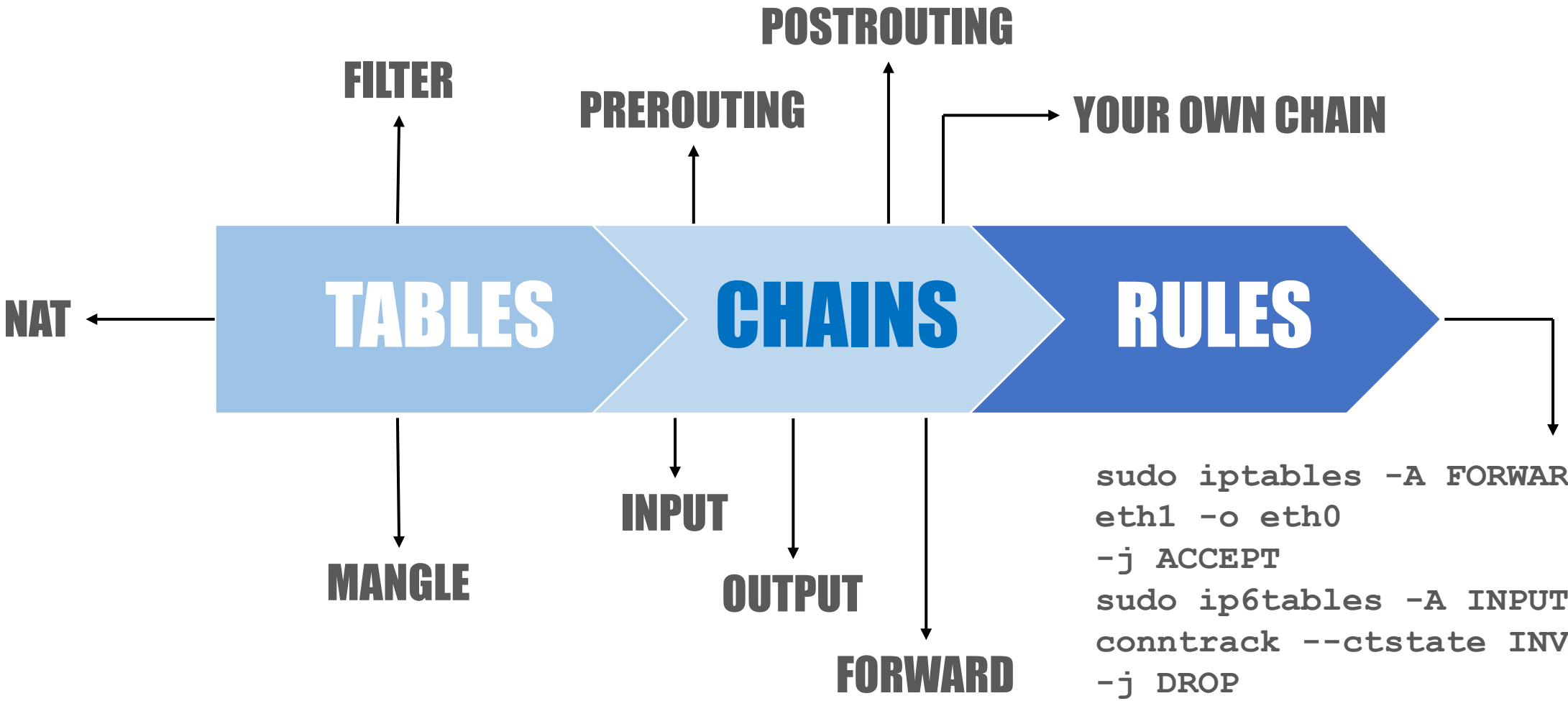
The `iptables` command is for IPv4 network traffic

The `ip6tables` command is for IPv6 network traffic

Rules should be configured separately for IPv4 and IPv6 traffic using `iptables` and `ip6tables`.

writeimtiaz@gmail.com

STRUCTURE




```
sudo iptables -A FORWARD -i
eth1 -o eth0
-j ACCEPT
sudo ip6tables -A INPUT -m
conntrack --ctstate INVALID
-j DROP
```

STRUCTURE

TABLES	CHAINS	RULES

FILTER	INPUT	FORWARD	OUTPUT		
NAT	PREROUTING	POSTROUTING	OUTPUT		
MANGLE	PREROUTING	OUTPUT	FORWARD	INPUT	POSTROUTING

```
sudo iptables -A FORWARD -i eth1 -o eth0
-j ACCEPT
sudo ip6tables -A INPUT -m conntrack
--ctstate INVALID -j DROP
```


writeimtiaz@gmail.com

STRUCTURE

FILTER

INPUT

```
sudo iptables -A INPUT -m conntrack --ctstate INVALID -j DROP
sudo ip6tables -A INPUT -m conntrack --ctstate INVALID -j DROP
```

DROP/ACCEPT

FORWARD

```
sudo iptables -A FORWARD -i eth1 -o eth0 -j ACCEPT
sudo ip6tables -A FORWARD -i eth1 -o eth0 -j ACCEPT
```

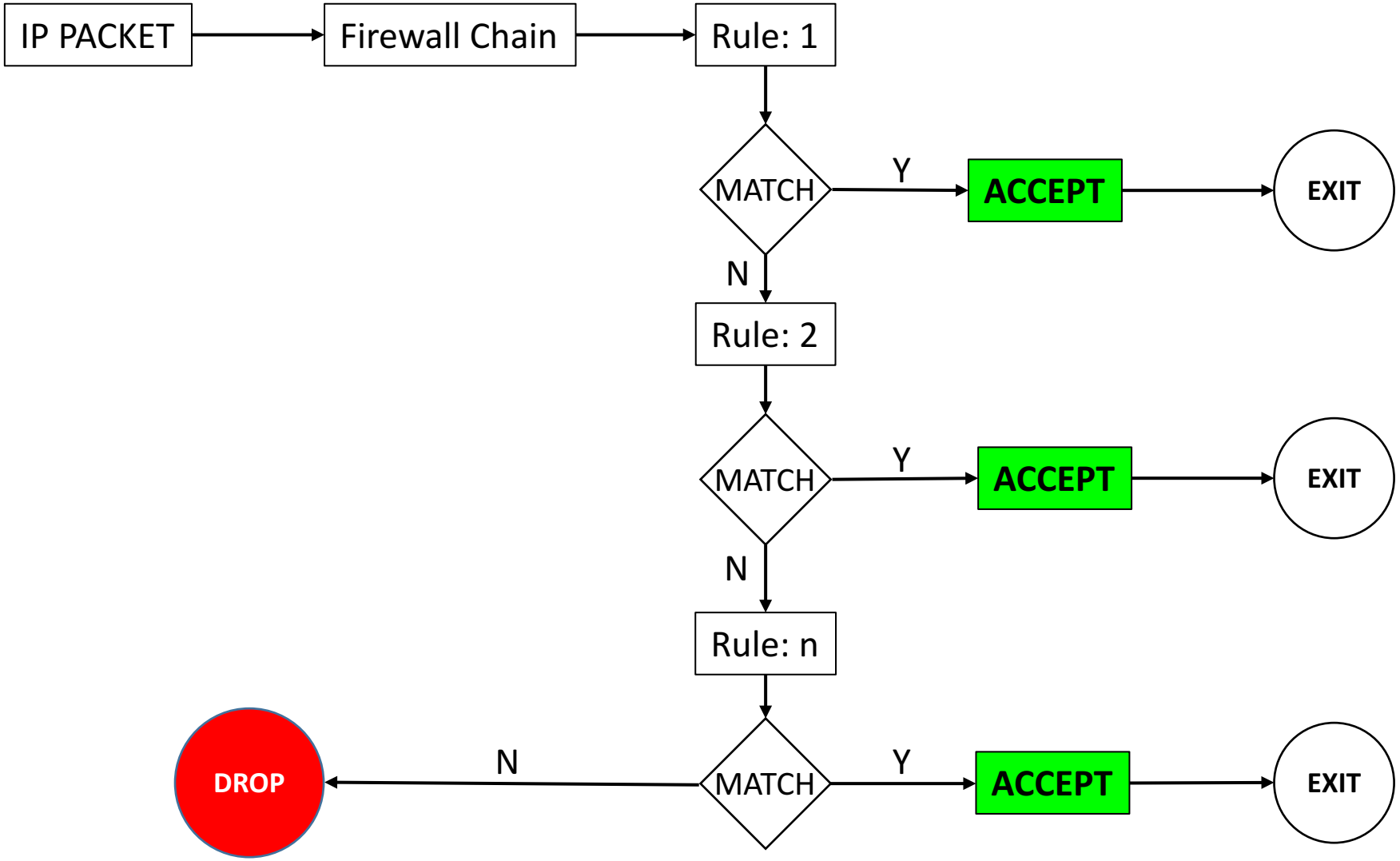
DROP/ACCEPT

OUTPUT

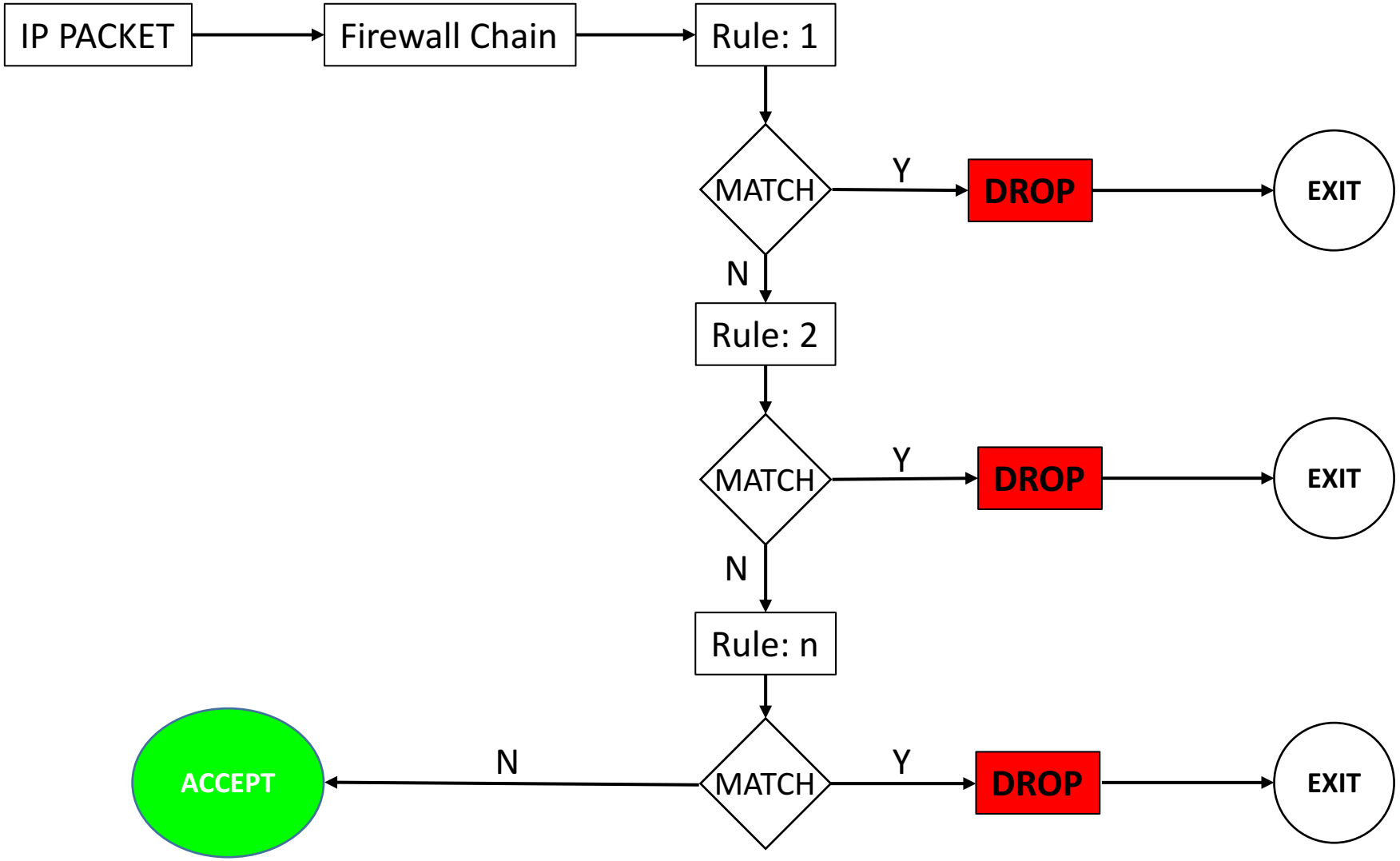
```
sudo iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
sudo ip6tables -A OUTPUT -m conntrack --ctstate ESTABLISHED -j ACCEPT
```

DROP/ACCEPT

POLICY DROP


IP PACKET
Firewall Chain
Rule: 1
MATCH
Y
ACCEPT
EXIT
N
Rule: 2
MATCH
Y
ACCEPT
EXIT
N
Rule: n
DROP
N
MATCH
Y
ACCEPT
EXIT

POLICY ACCEPT



SYNTAX

iptables

```
sudo iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -P INPUT DROP
sudo iptables -D INPUT -p tcp --dport 21 -j ACCEPT
sudo iptables -I INPUT 2 -p tcp --dport 21 -j ACCEPT
```

ip6tables

```
sudo ip6tables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
sudo ip6tables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo ip6tables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo ip6tables -P INPUT DROP
sudo ip6tables -D INPUT -p tcp --dport 21 -j ACCEPT
sudo ip6tables -I INPUT 2 -p tcp --dport 21 -j ACCEPT
```

SYNTAX

```
sudo ip6tables -t FILTER -A INPUT -p tcp --dport ssh -s 2001:db8:1001::1 -j ACCEPT
```

table chain match target

writeimtiaz@gmail.com

SYNTAX (for the LAB)

```
-A - Append rule to a rule chain.
-L - List the current filter rules.
-p - The connection protocol used.
-j - Jump to the specified target. (ACCEPT, REJECT, DROP, LOG)
--log-prefix - When logging, put this text before the log message.
--log-level - Log using the specified syslog level.
-I - Inserts a rule.
-v - Display more information in the output.
-P Policy
-D Delete rule from a rule chain
-R Replace rule
--line-numbers Output with line number
```


writeimtiaz@gmail.com

Hands on LAB