Welcome Cyber#1

Reader:	reader.codaisseur.com
Slack:	codaisseur-school.slack.com
Discord:	https://discord.gg/qyehPh

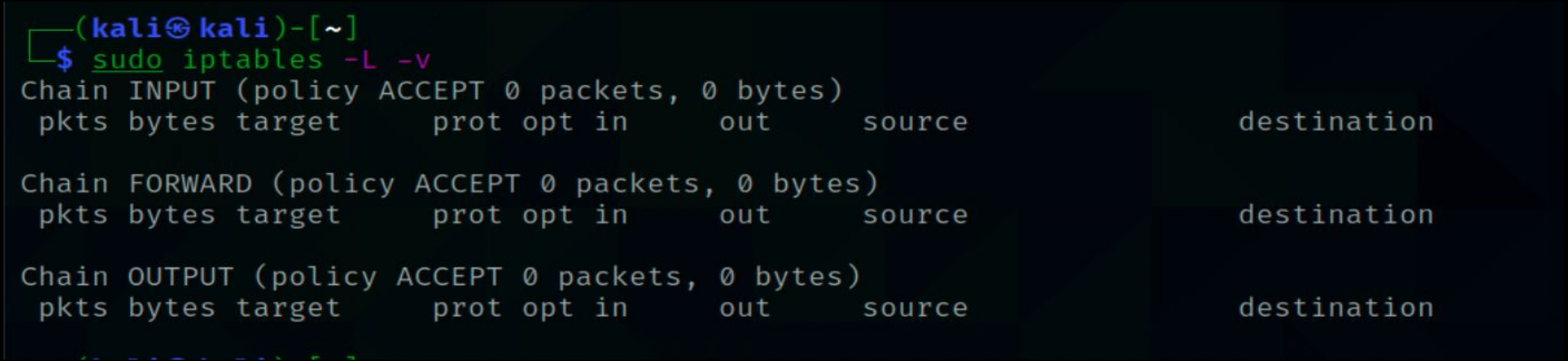
Linux firewall

IPtables

Main entrance
10.110.0.9

Exit -> internet
(10.110.0.9)

Main entrance
10.110.0.9



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Chains...

- Input
- Forward
- Output

Input...

Incoming connections

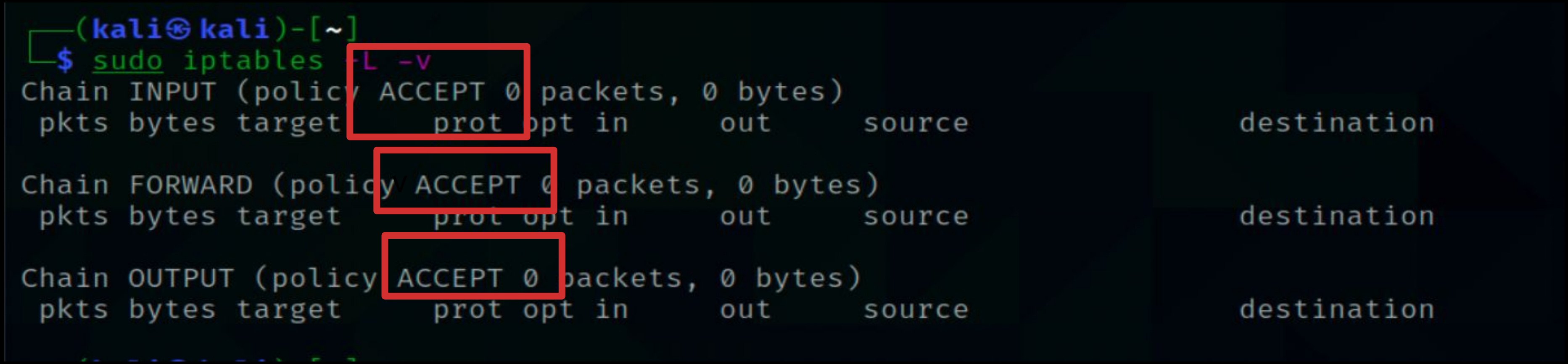
Forward...

Like a router

Output...

ntp
Icmp,
http,
updates?

Chain end...

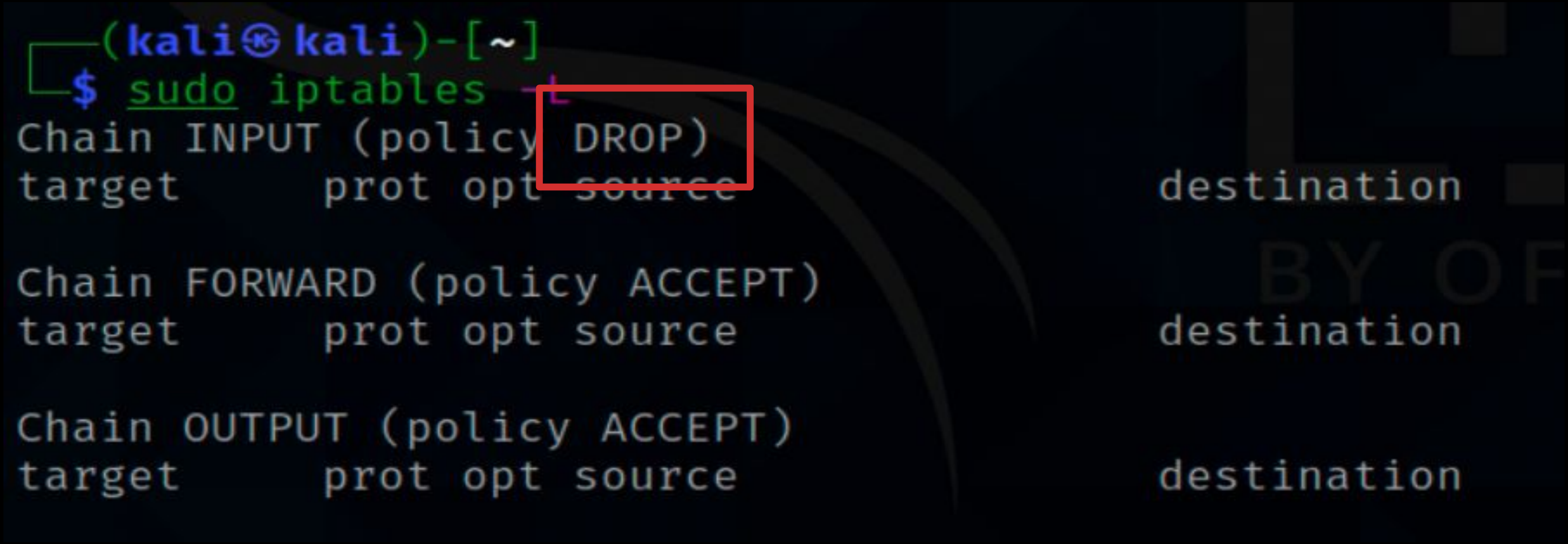


```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
```

Chains end...

```
iptables --policy INPUT DROP
```

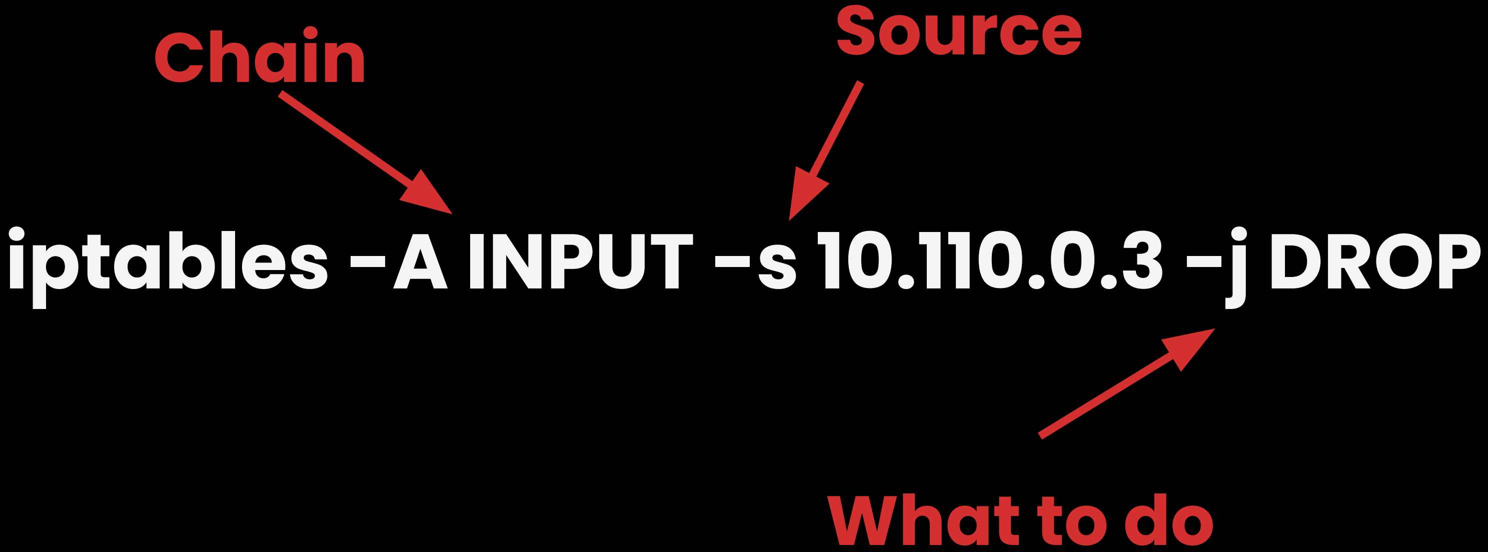
Chains end...



```
┌──(kali㉿kali)-[~]
└─$ sudo iptables -L
Chain INPUT (policy DROP)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

What? Rules?

Rules...



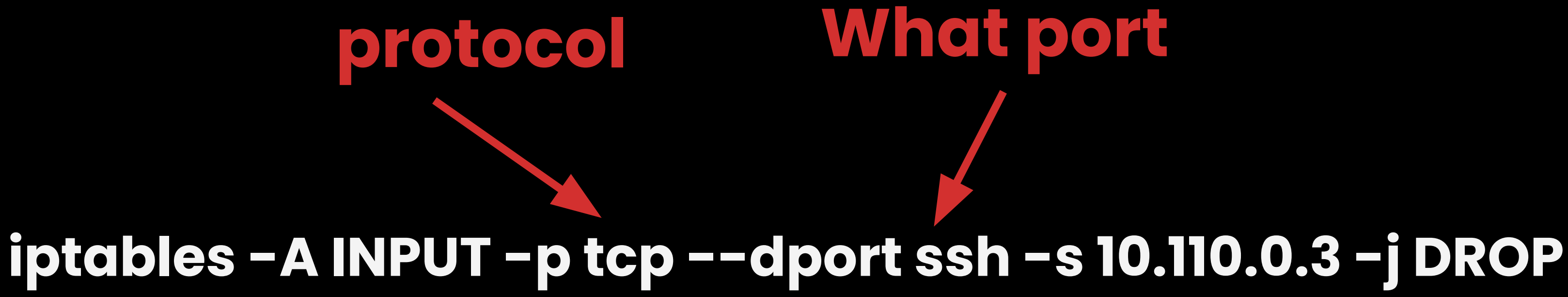
Chain

Source

```
iptables -A INPUT -s 10.110.0.3 -j DROP
```

What to do

Rules...



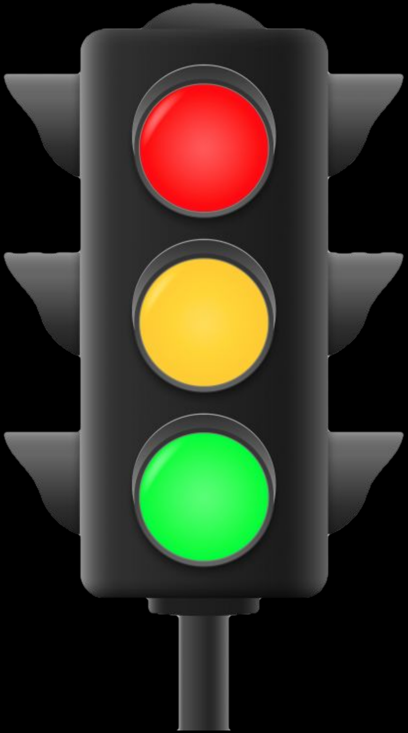
protocol

What port

```
iptables -A INPUT -p tcp --dport ssh -s 10.110.0.3 -j DROP
```

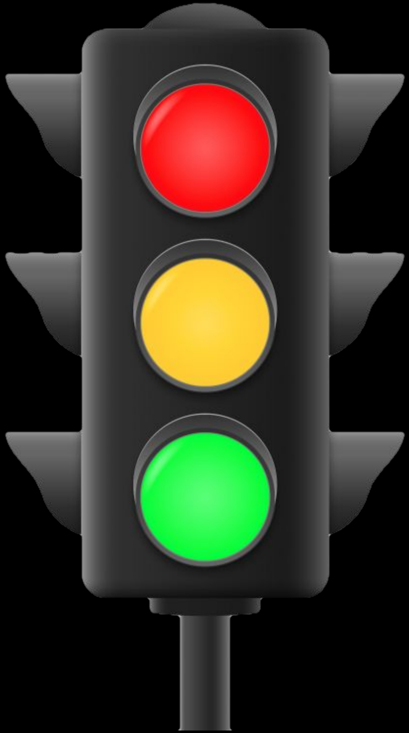
Careful...

SSH?



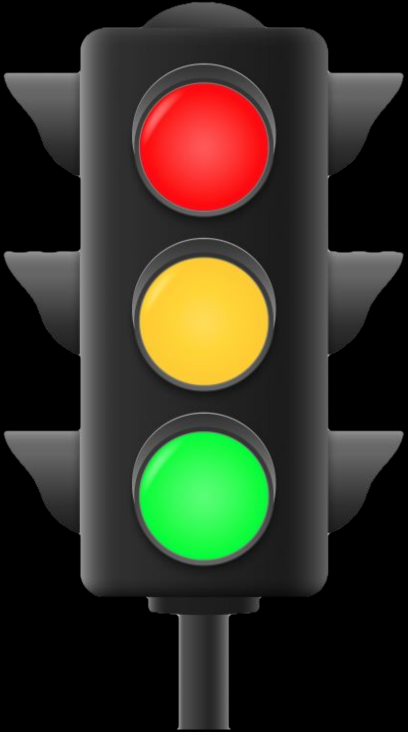
Careful...

2-way traffic!



Careful...

SSH?



Set to default

= 10 mins

BREAK

Saving...

```
sudo sh -c "iptables-save >
/etc/iptables.rules"
```

Saving...

```
sudo sh -c "iptables-apply <
/etc/iptables.rules"
```

Saving...

```
sudo sh -c "iptables-restore < /etc/iptables.rules"
```

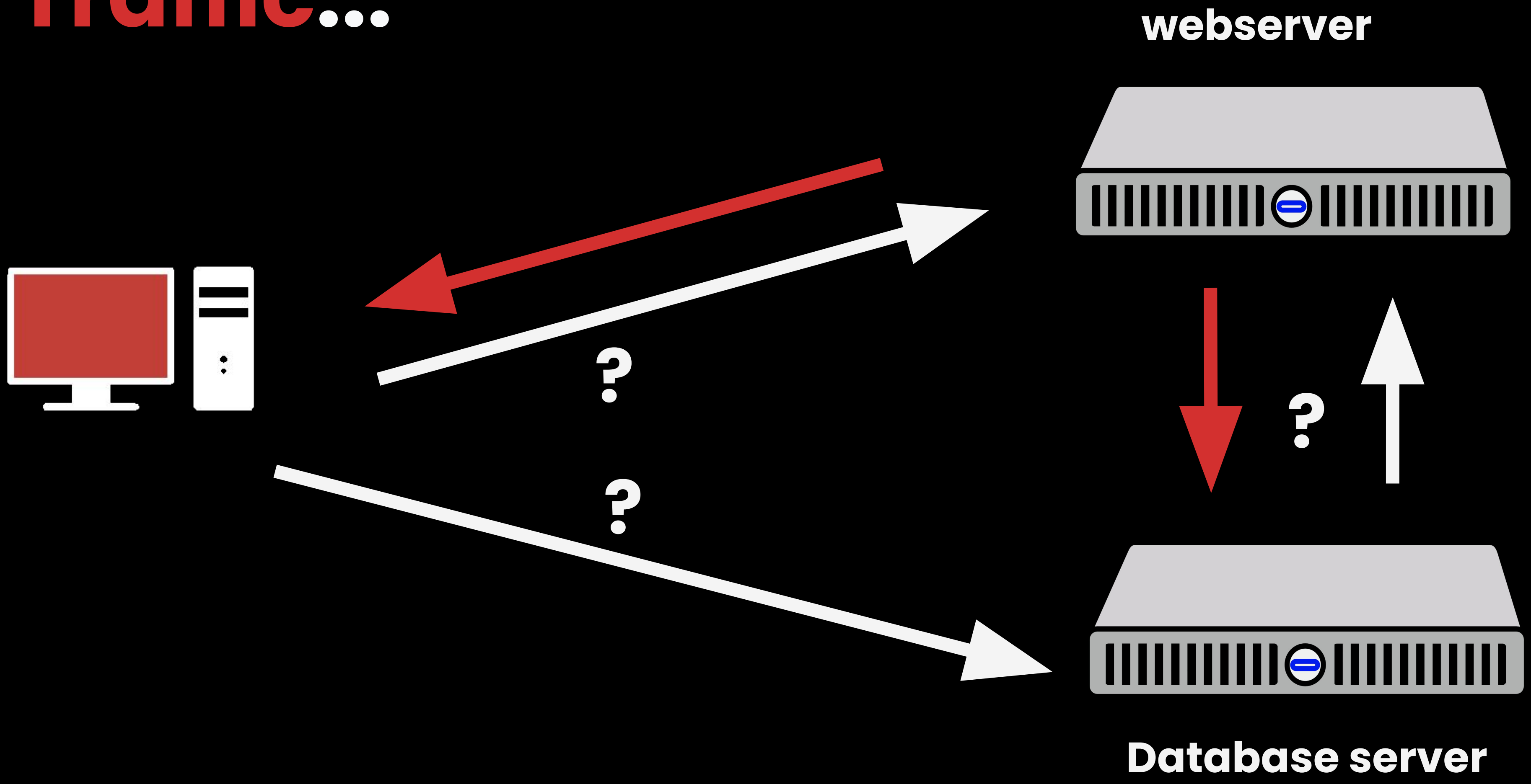
help...

https://help.ubuntu.com/community/IptablesHowTo

FUN!

2 servers...

Traffic...



Steps...

Phase 1: Planning
Phase 2: Execute
Phase 3: Test

Steps...

Phase 1: Planning -> What traffic?

Phase 2: Execute -> Implement!

-> SSH?

Phase 3: Test -> Test-tEst-tesT

Teams...

Pepijn, Yann, Willemijn
Shangram, Raj, Camilia

Yvonne, Prawesh, Ximena,
Tjitze, Bozana, Filipe

boxes...

alpha-web.codaisseur.academy
alpha-db.codaisseur.academy

beta-web.codaisseur.academy
beta-db.codaisseur.academy