Networks and Firewalls

Lecture 14 - ECS198F SQ26

TCP/IP Model

HTTPS, SSH, VoIP, ...

TCP, UDP

Routers

Laptops, servers, switches

iptables flags

-A [INPUT/OUTPUT]	does this rule apply to incoming or outgoing traffic?
-p [tcp/udp]	does this rule apply to TCP or UDP?
--sport {#}	which source port are we filtering (if any?)
--dport {#}	which destination port are we filtering (if any?)
-j [ACCEPT/DROP]	are we accepting or dropping the matched traffic?

E.g. `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`

More iptables flags

-P [ACCEPT/DROP] set default policy

E.g. `iptables -P INPUT DROP`

Together

What do these two rules do in conjunction?

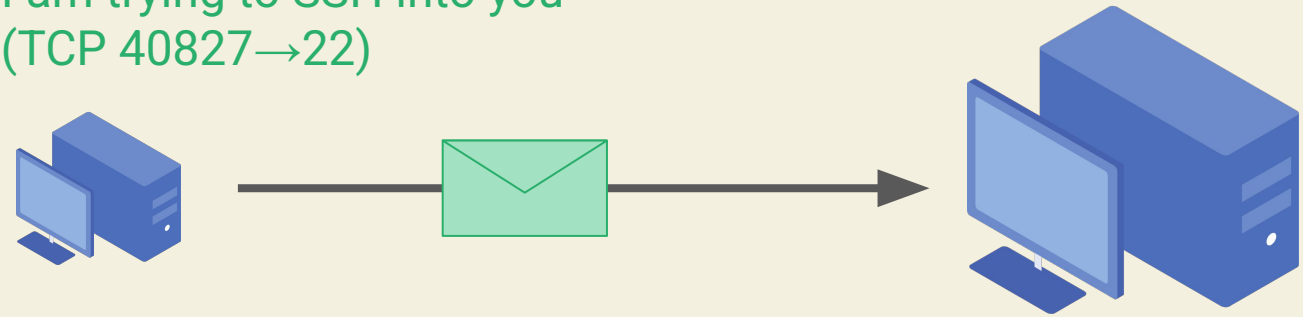
```
iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -P INPUT DROP
```

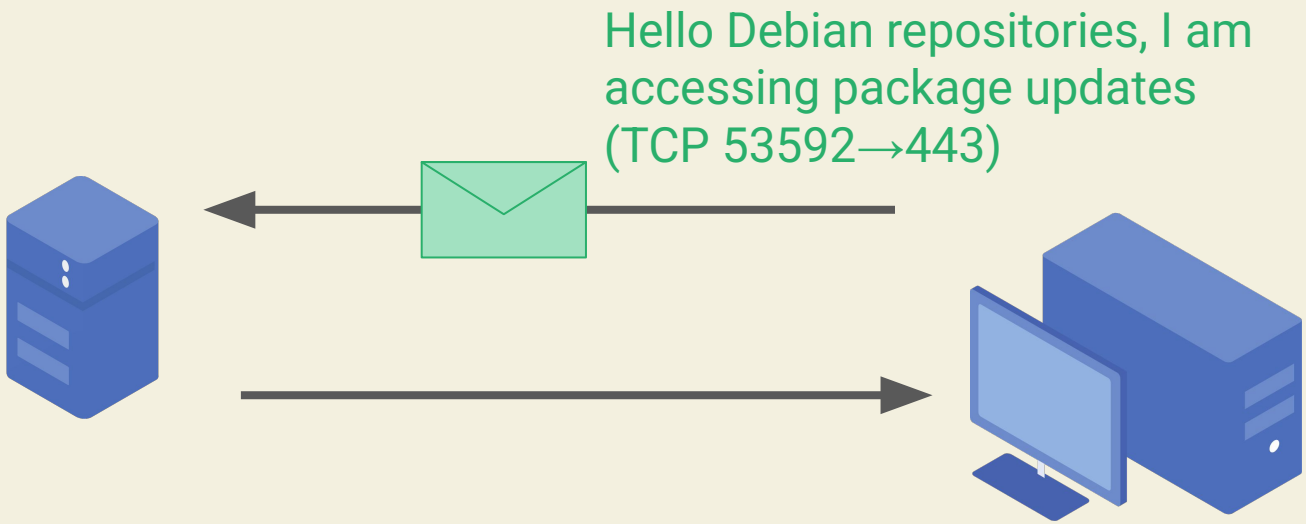
Diagram

If you are accessing my TCP port 22, ACCEPT!
Otherwise, DROP!

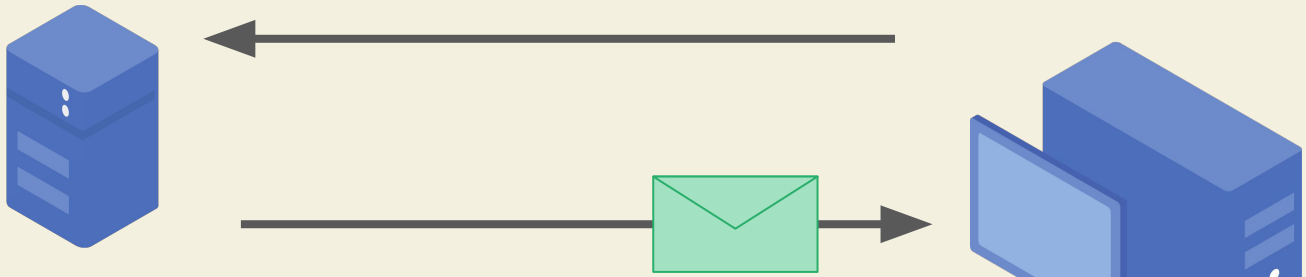
I am trying to SSH into you (TCP 40827→22)



Diagram

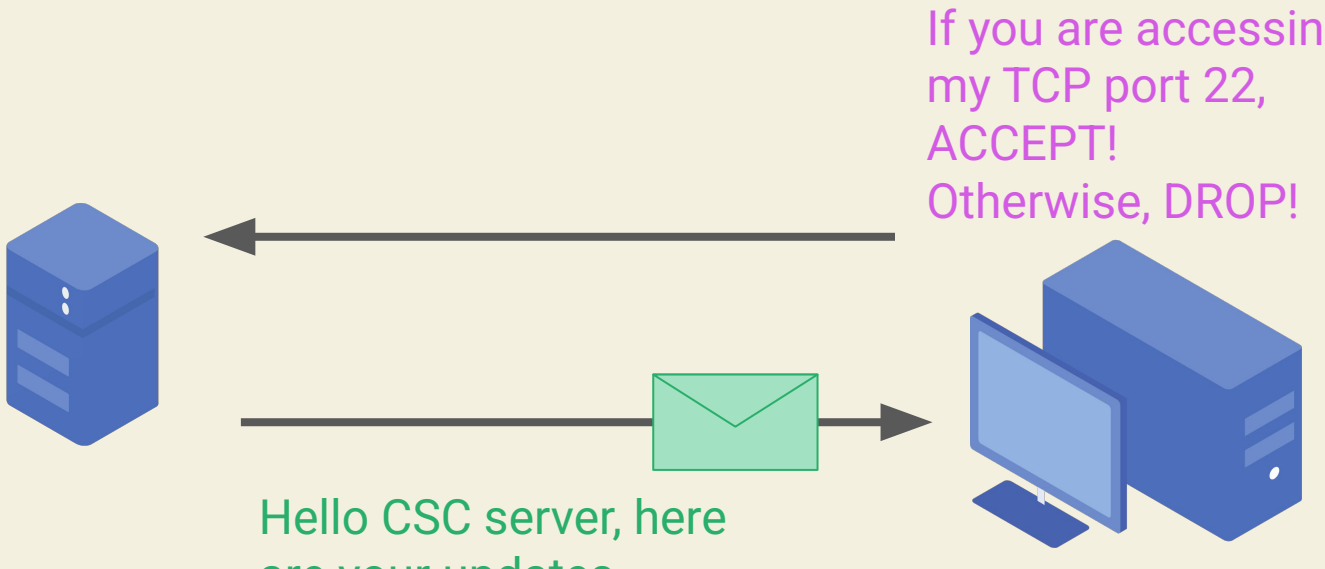

Hello Debian repositories, I am accessing package updates (TCP 53592→443)

Diagram

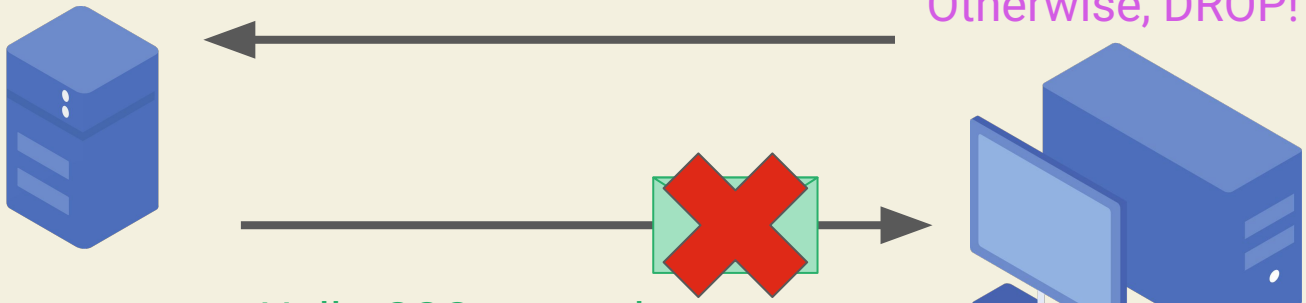


Hello CSC server, here are your updates (TCP 443→53592)

Diagram


If you are accessing my TCP port 22, ACCEPT! Otherwise, DROP!
Hello CSC server, here are your updates (TCP 443→53592)

Diagram



If you are accessing my TCP port 80, ACCEPT! Otherwise, DROP!

Hello CSC server, here are your updates (TCP 443→**53592**)

Stateful Firewall

If our computer sends outgoing communications, we should accept the responses dynamically

“Keeping track of state”

```
iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
```

Firewall: Words of Caution

Firewalls filter all traffic. You can accidentally lock yourself out (~permanently)

Make sure that you always permit SSH (or have some other way of getting back in)

Don’t sacrifice availability!