COMP3052.SEC Computer Security

Session 06: Firewalls

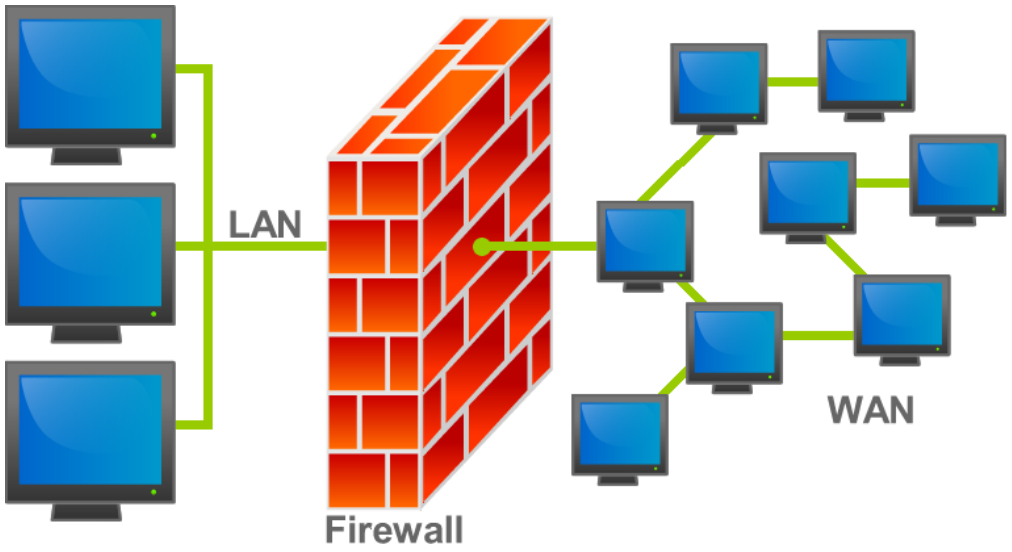
Acknowledgements

- Some of the materials we use this semester may come directly from previous teachers of this module, and other sources ...
- Thank you to (amongst others):
  - Michel Valstar, Milena Radenkovic, Mike Pound, Dave Towey, …

This Session

- Firewalls
  - Packet Filters
  - Stateful vs Stateless
- Proxies
- NAT

Firewalls



- A hardware and/or software system
- Prevents unauthorised access of packets from one network to another
- All data leaving any subnet must pass through it

Firewall Functions

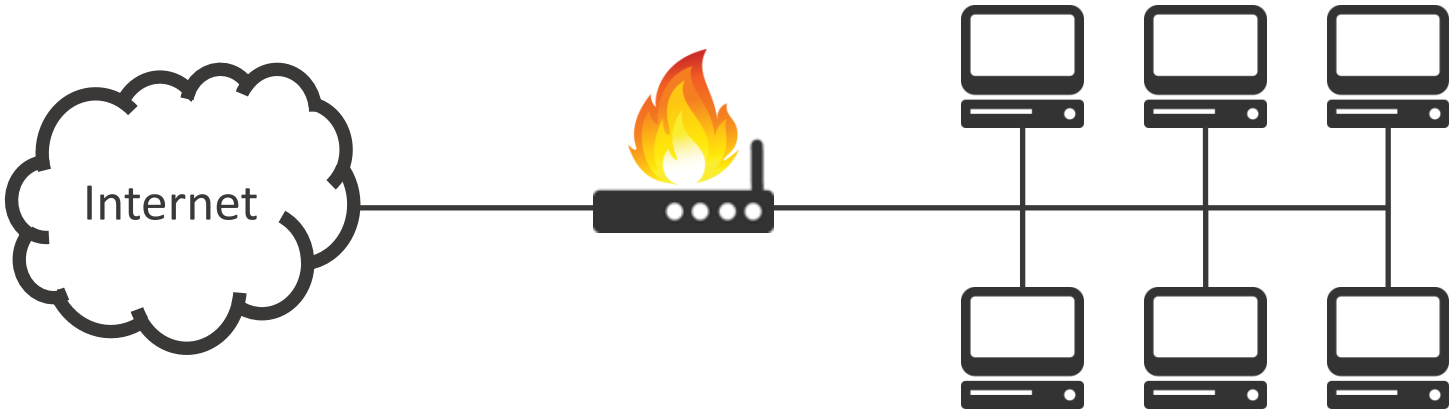
- Implements ‘single point’ security measures
- Security event monitoring through packet analysis and logging
- Network-based access control through implementation of a rule set

Location

- Many different possible locations – thus many different network architectures
- Network Firewalls
  - Placed between a subnet and the internet
- Host-based Firewalls
  - Placed on individual machines
- All traffic must go through the firewall for it to function correctly

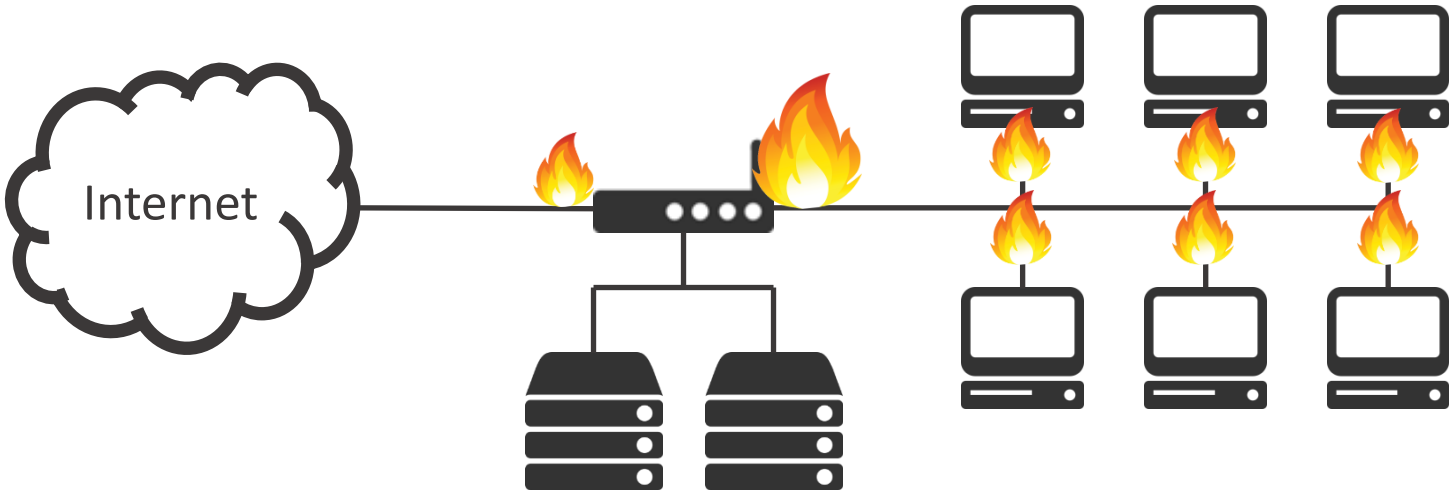
Location

- A standard home router is a good example of a network firewall



DMZ

- A demilitarized zone is a small subnet that separates externally facing services from the internal network



Firewall Basic Function

- Defends a protected network against parties accessing services that should only be available internally
- Can also restrict access from inside to outside services

Firewalls are not enough

- Cannot protect against attacks that bypass the firewall
  - E.g. Tunnelling
- Cannot protect against internal threats or insiders
  - Might help a bit by egress filtering
- Cannot protect against the transfer of virus-infected programs or files

Firewall Types

- Packet Filters
- Stateful Inspection
- Proxies
- Dynamic
- Kernel

- OSI-Based:
  - Application Layer
  - Network Layer

Packet Filters

- Specify which packets are allowed or dropped
- Rules based on:
  - Source / Destination IP
  - TCP / UDP port numbers
- Possible for both inbound and outbound traffic
- Can be implemented in a router by only examining packet headers
  - Operates on OSI layer 3 (IP) or layer 4 (TCP)

Packet Filter Rules

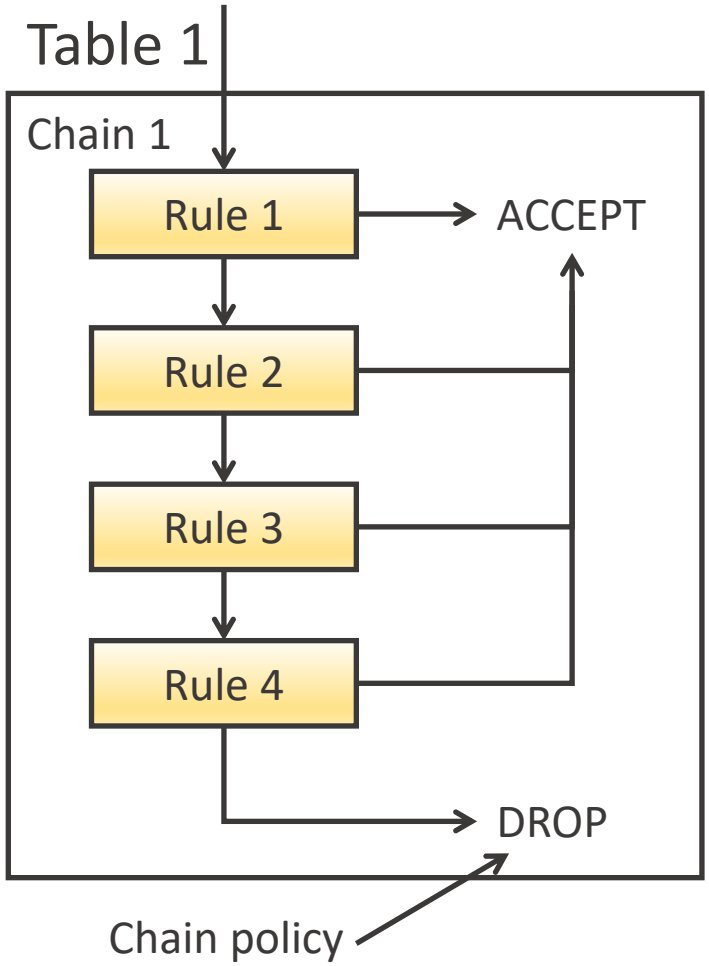
- Rule execution depends on implementation
  - IPTABLES: First rule to match is applied
  - PF: All rules are examined, the last match is applied
- Rules are organised in chains, which are logical subgroups of rules
- Depending on the packet, different chains are activated

IPTABLES

- An application that provides access to the Linux firewall rule tables
  - Not actually a firewall, but configures the firewall
  - The firewall is mostly implemented as *netfilter* modules

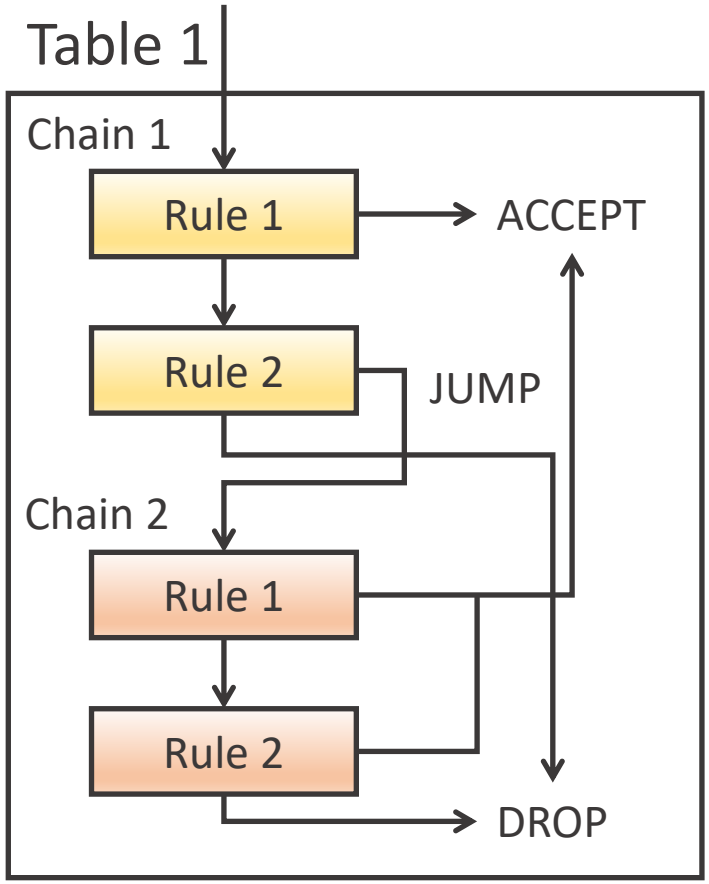
Tables and Chains

- IPTABLES uses tables to store chains
  - Default is the filtering table
- Chains are ordered lists of rules
  - Rules match, or they don't
- Matches result in a jump, else we check the next rule



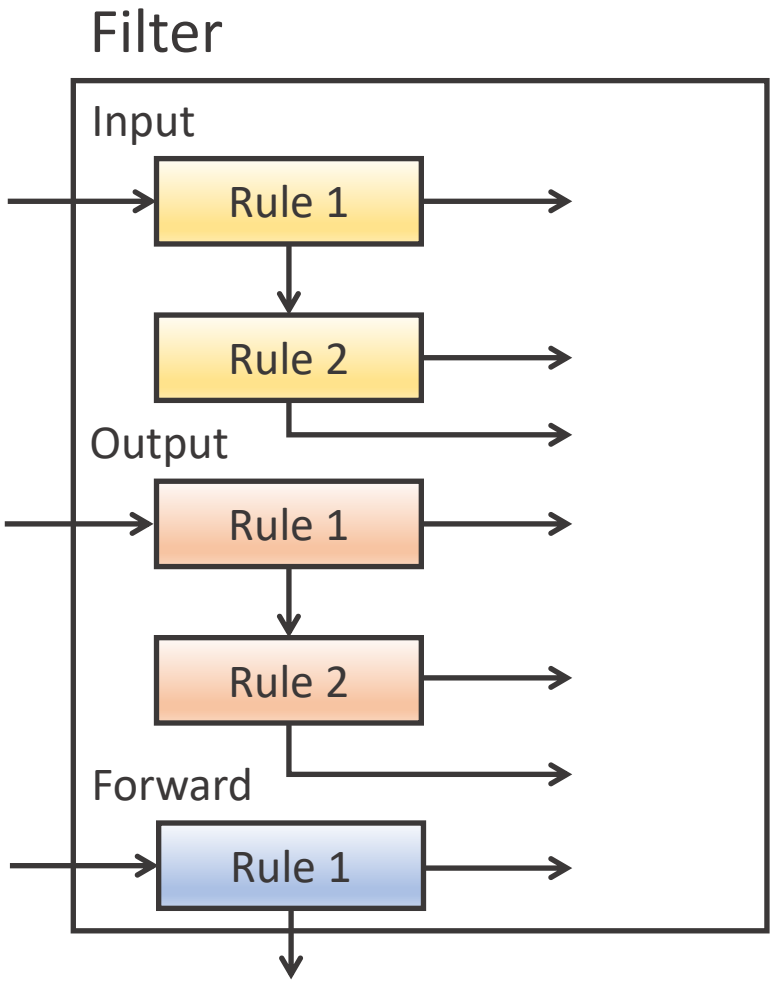
Tables and Chains

- There can be multiple chains per table
  - E.g. a TCP handling chain
- Jumps can go to ACCEPT, DROP, LOG or another chain
- Complex behaviour can be built up



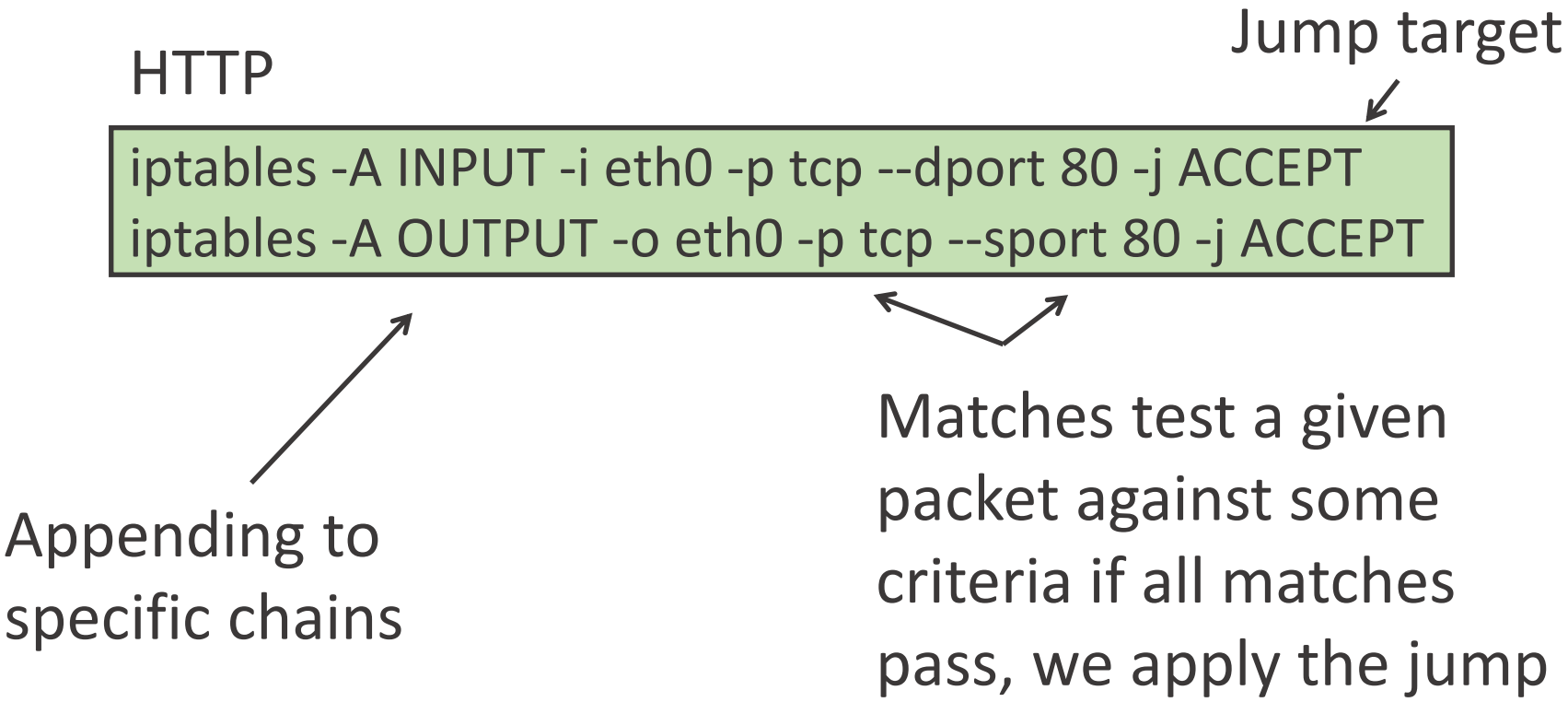
Defaults

- There are built-in tables in IPTABLES:
  - Filter (default)
  - NAT
  - Mangle – Packet alteration
  - Raw – Skips connection tracking
  - Security – mandatory access control
- The default table is the filtering table, including Input, Output and Forward chains



Rules Examples

- Using the command line, we add rules onto the end of chains



Policies

- Permissive (Black listing) – allow everything except dangerous services
  - Easy to make a mistake or forget something
- Restrictive (White listing) – block everything except designated useful services
  - More secure by default
  - Fairly easy to DoS yourself!

IPTABLES Policies

- To use a blacklisting policy, we want to accept by default, then have rules that drop:

```
iptables -P INPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -P OUTPUT ACCEPT
```

```
iptables -A INPUT -s X.X.X.X -j DROP
iptables -A OUTPUT -p tcp --dport ssh -j DROP
```

- For a whitelisting policy, we want to drop by default, then let certain packets through:

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP
```

```
iptables -A INPUT -p tcp --dport ssh -j ACCEPT
iptables -A OUTPUT -s 192.168.0.2 -j ACCEPT
```

Packet Filter Issues

- Packet filters are simple, low level and have high assurance
- But, they cannot:
  - Prevent attacks that exploit application-specific vulnerabilities
  - Do not support higher-level authentication schemes

Stateful Packet Filters

- A stateful firewall always keeps track of the state of network connections.
- Once a particular kind of traffic has been approved by a stateful firewall, it is added to a state table/connection table.
- Understand requests and replies
  E.g. 3-way Handshake: SYN, SYN/ACK, ACK

Connection Table Example

Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.0.2	1030	210.9.88.29	80	established
192.168.0.4	22	216.32.42.123	22	established

- ACK packets are used to keep track of the session – the connection is ongoing
- Packets without the ACK are the connection establishment messages

IPTABLES Rules

- IPTABLES has modules for stateful packet filtering
- Allow incoming / outgoing SSH connections

```
iptables -A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED –j ACCEPT
```

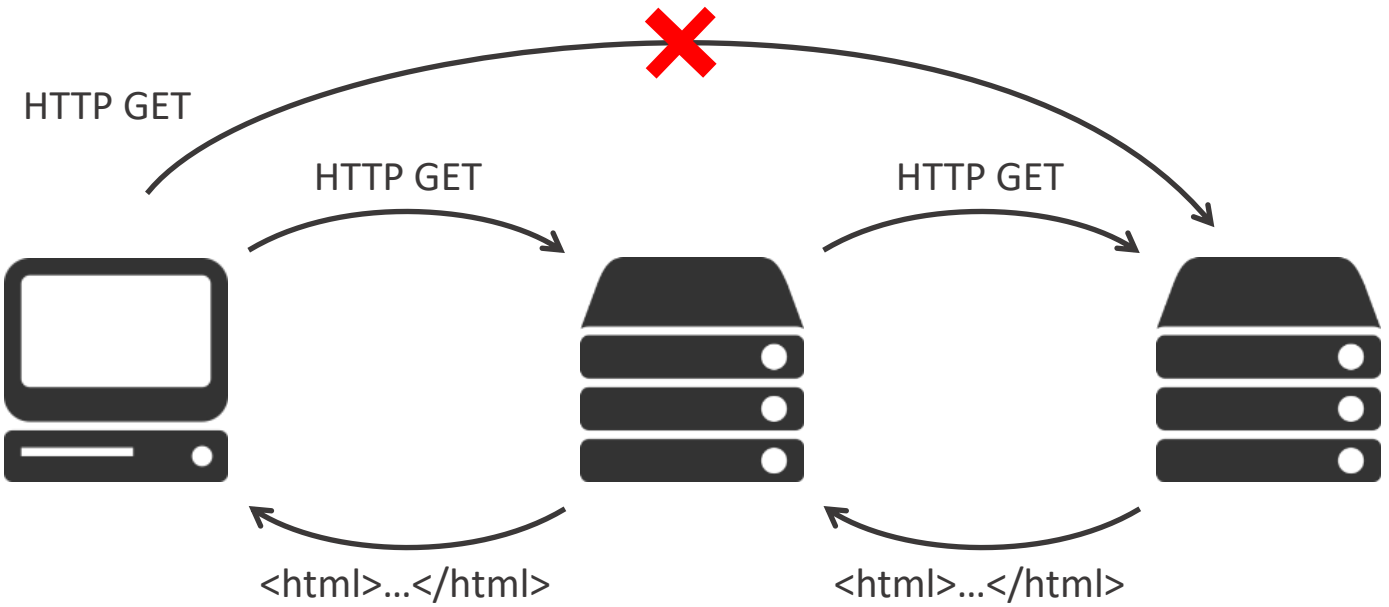
- Allow HTTP(S):

```
iptables -A INPUT -i eth0 -p tcp --dport 80 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
```

```
iptables -A INPUT -i eth0 -p tcp --dport 443 -m state --state NEW,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -o eth0 -p tcp --sport 443 -m state --state ESTABLISHED -j ACCEPT
```

Proxy Servers

- Proxy servers initiate a connection on our behalf
- They can block certain access, and scan for malicious files or web pages

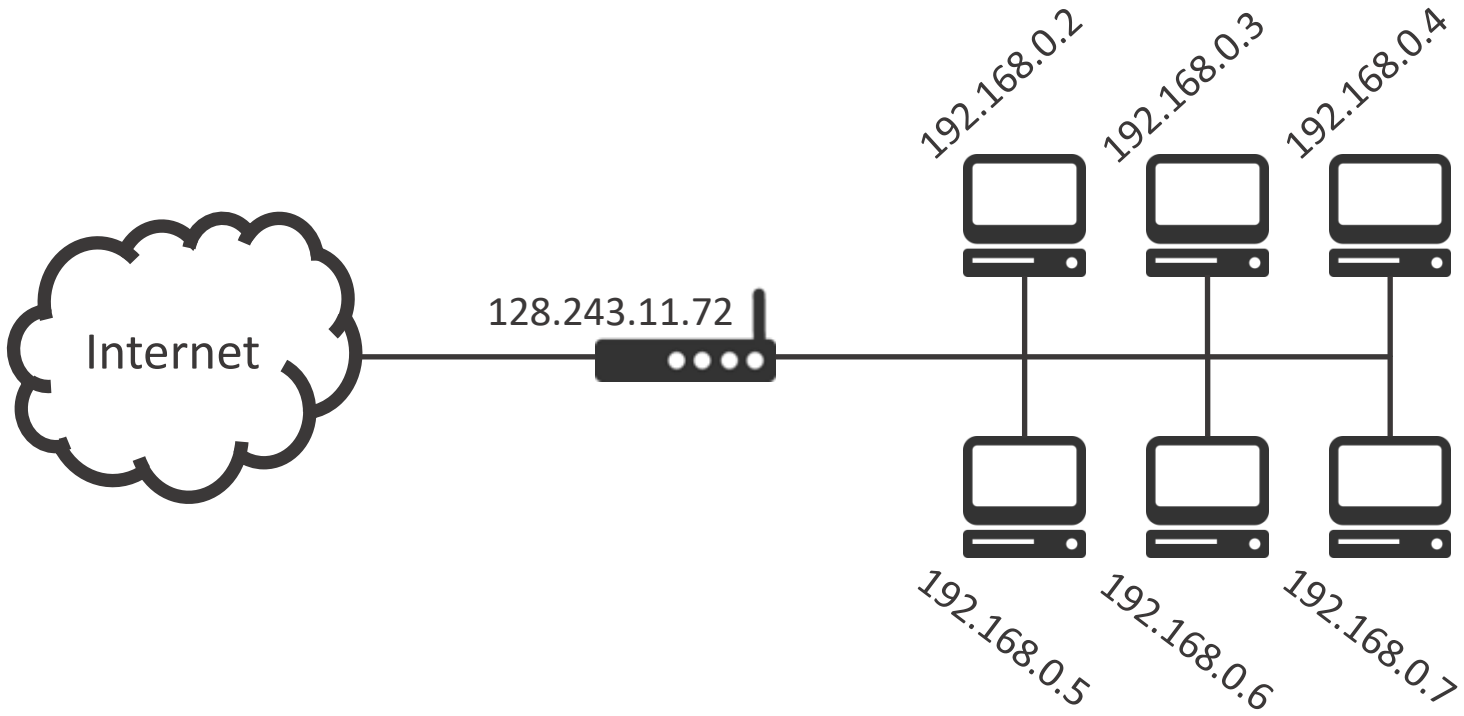


Proxy Servers

- Issues
  - Large overhead per connection
  - More expensive than packet filtering
  - Configuration is complex
  - A separate server is required for each service

Network Address Translation (NAT)

- The shortage of IP addresses mean that most routers now perform NAT automatically



Network Address Translation

- The implicit advantage in NAT is that your machine is almost totally hidden from the internet
- Only established connections are forwarded to your internal machine
  - Or, specific port forwarding rules

Summary

- Firewalls
  - Packet Filters
  - Stateful vs Stateless
- Proxies
- NAT