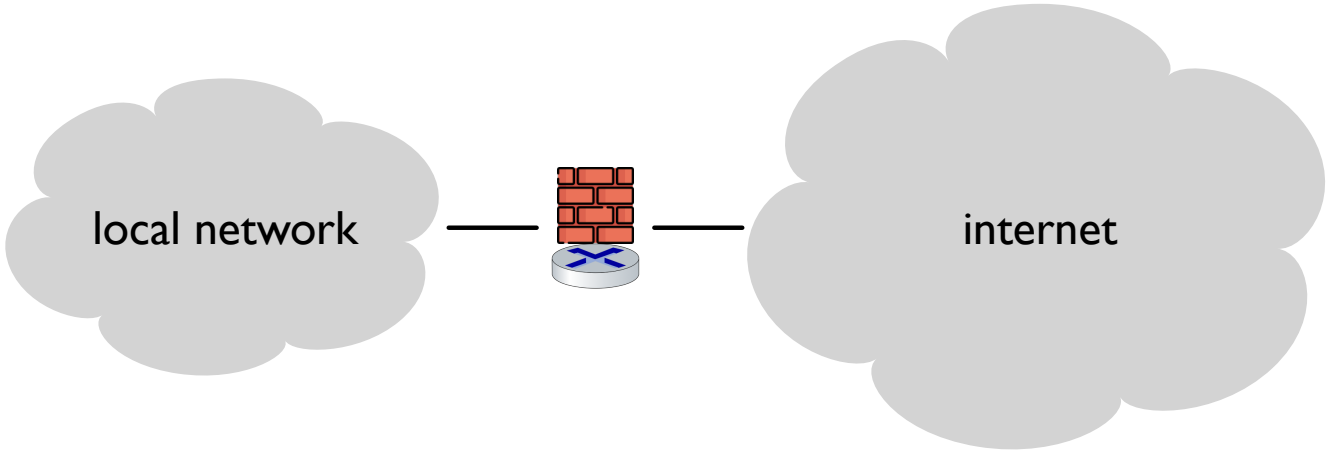
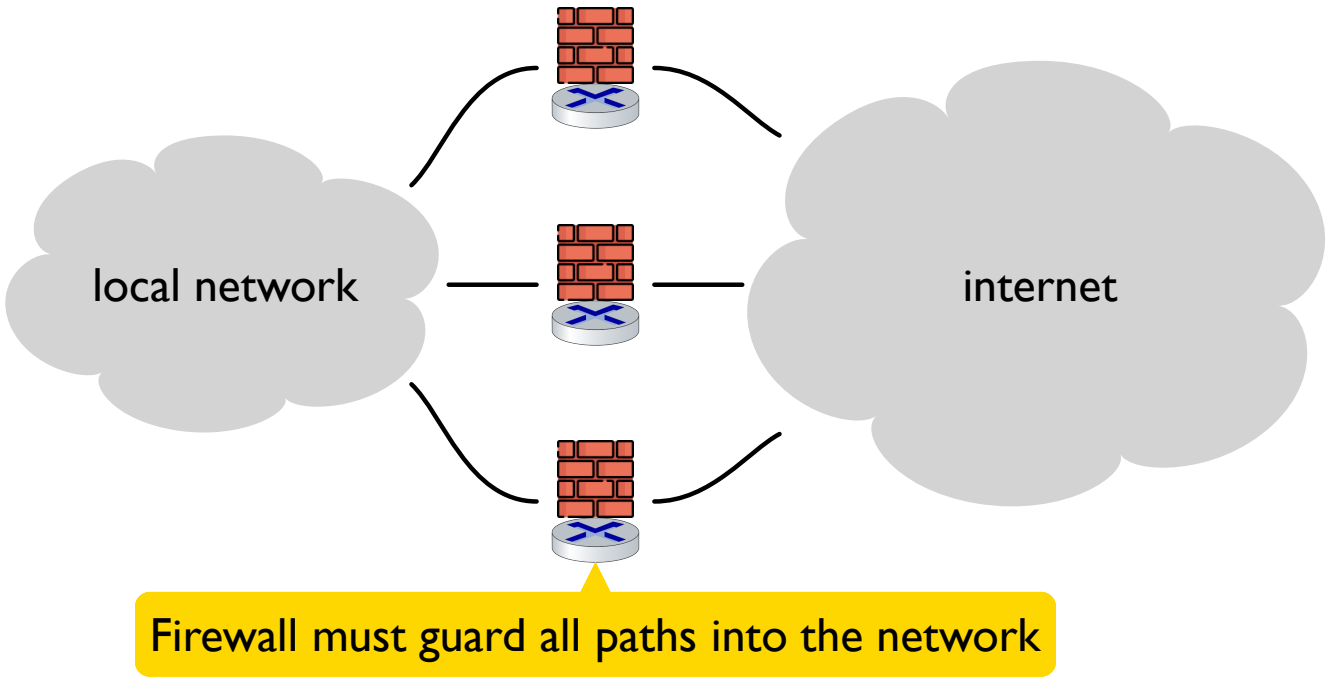
Firewalls

A **firewall** is a network link that restricts traffic in a way that is meant to improve security



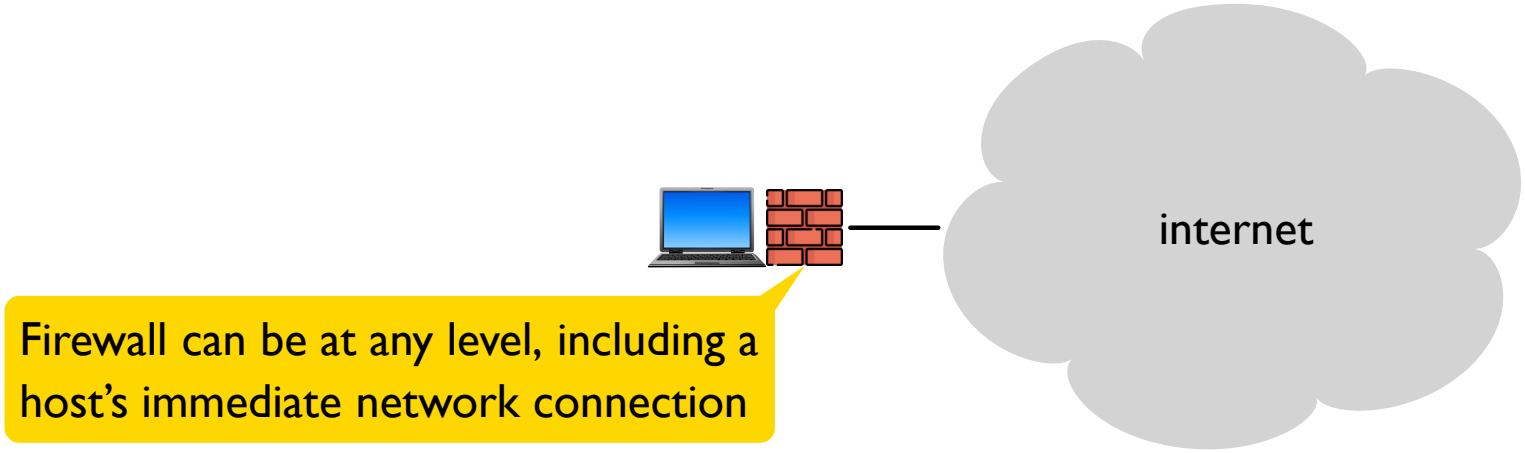
Firewalls

A **firewall** is a network link that restricts traffic in a way that is meant to improve security

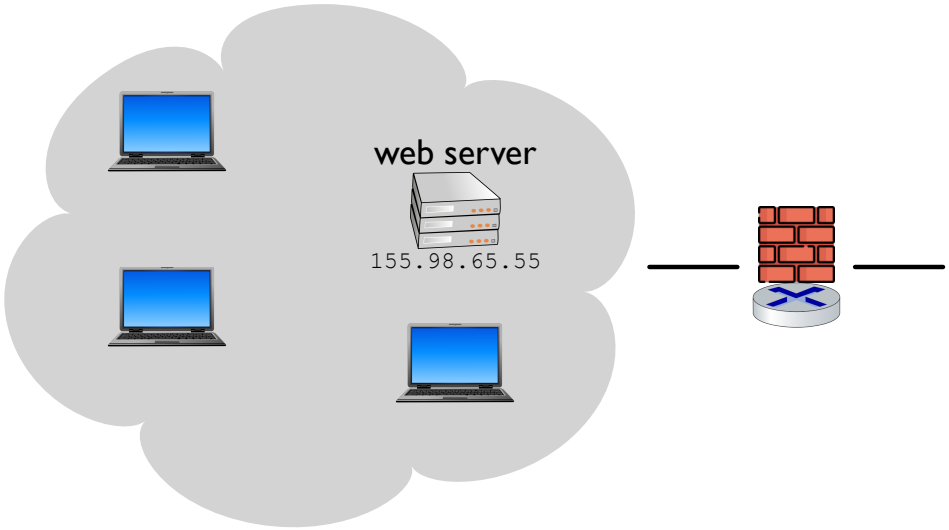


Firewalls

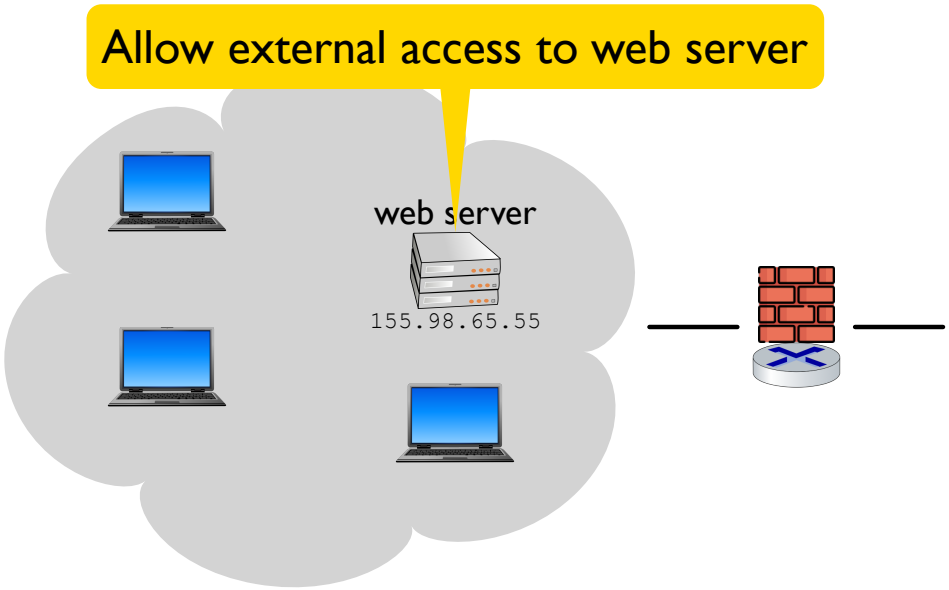
A **firewall** is a network link that restricts traffic in a way that is meant to improve security



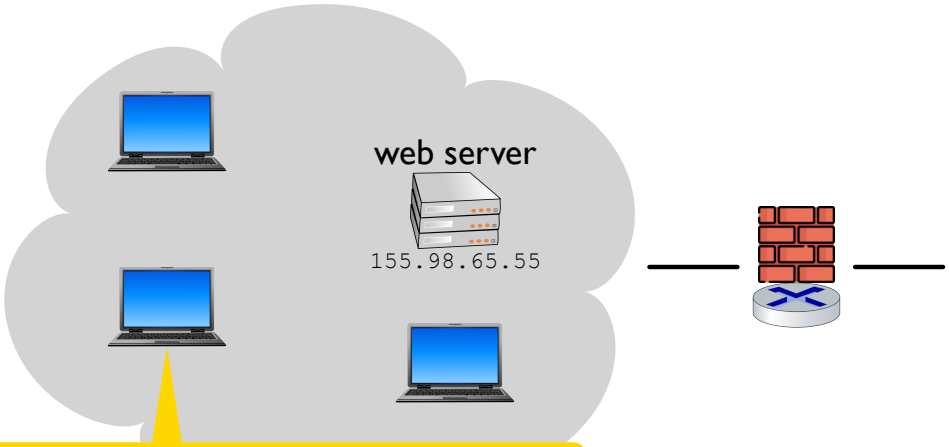
Network/Transport Layer Firewalls



Network/Transport Layer Firewalls

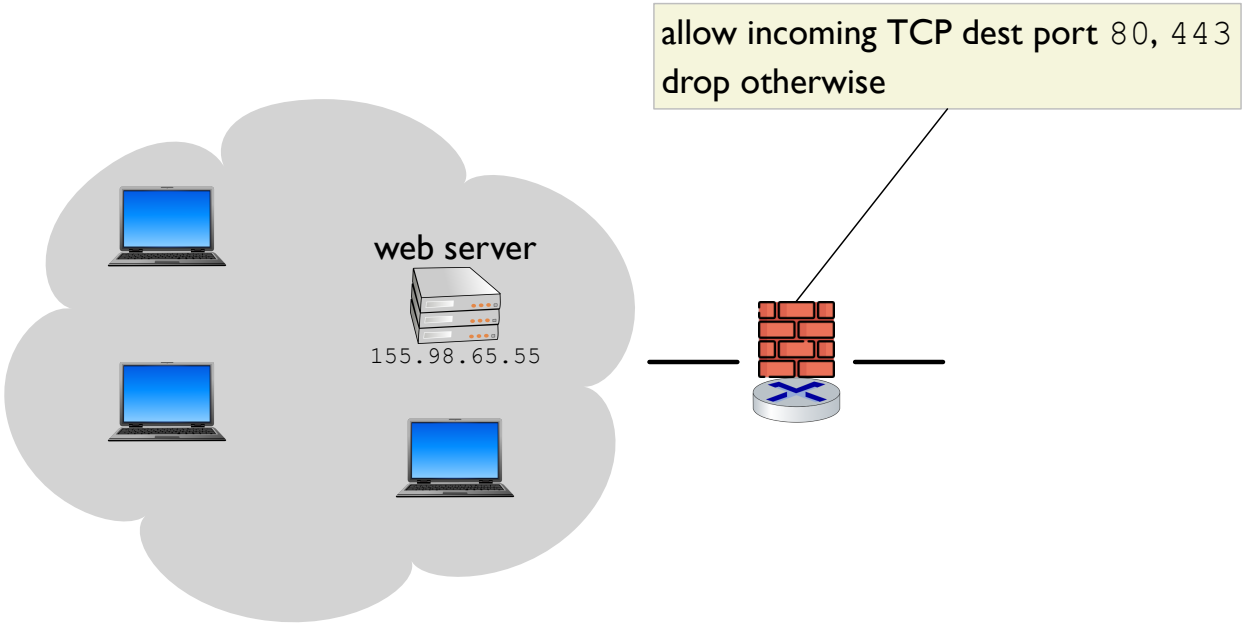


Network/Transport Layer Firewalls

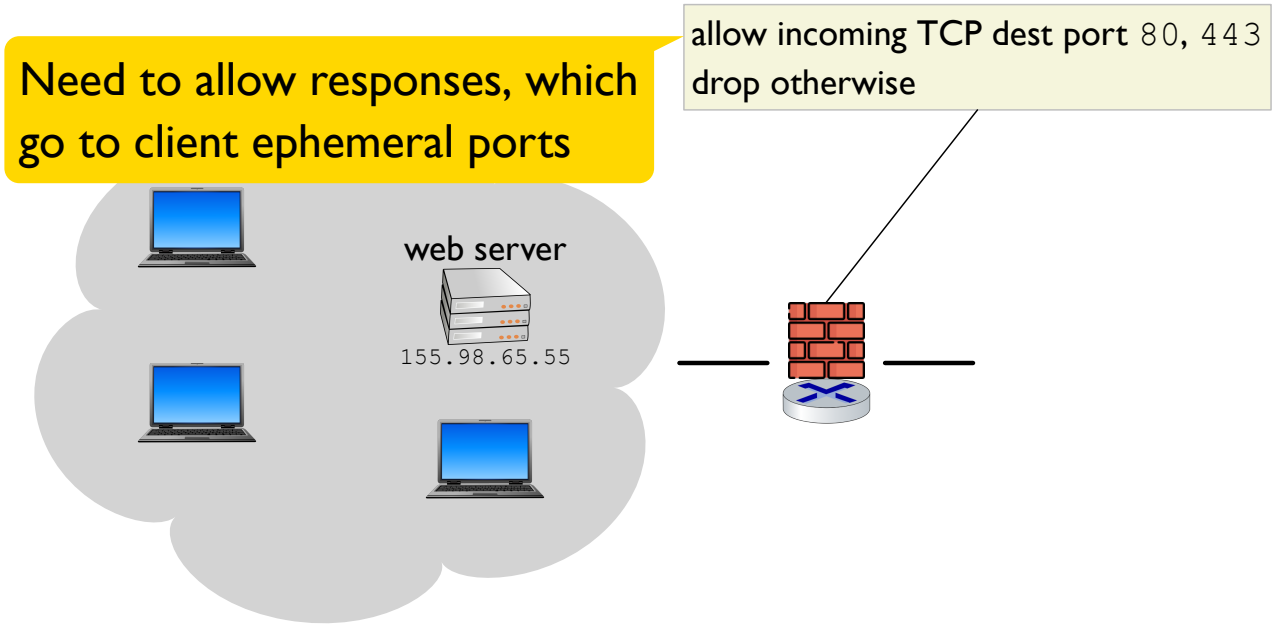


Allow internal clients to access external web servers

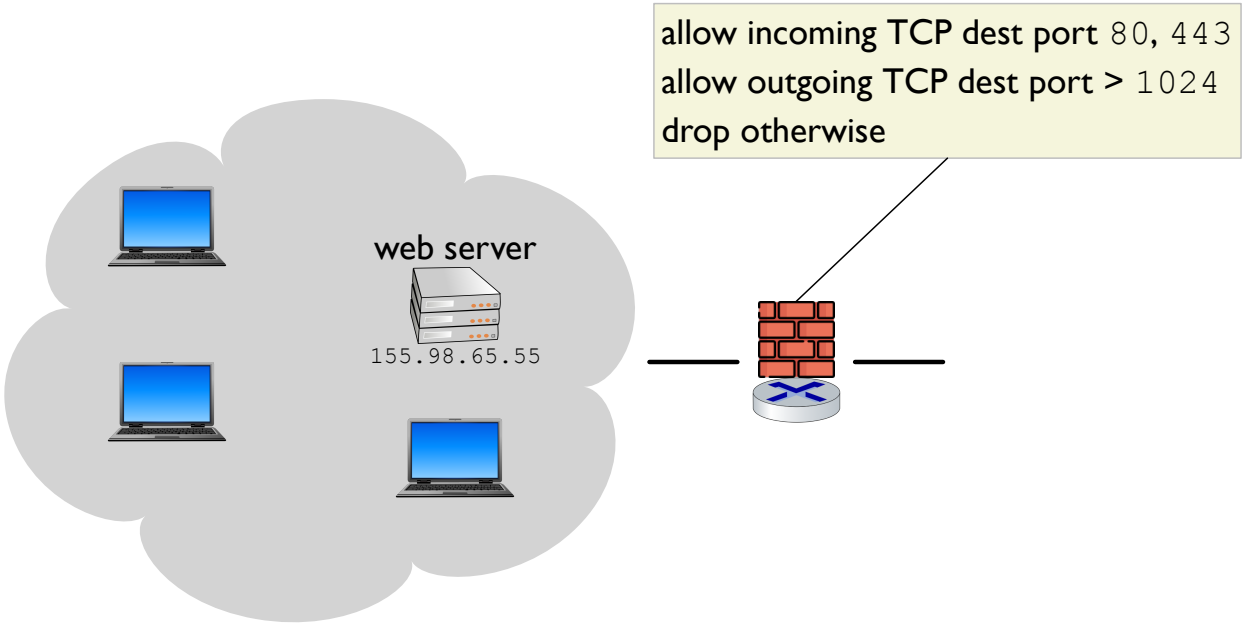
Network/Transport Layer Firewalls



Network/Transport Layer Firewalls



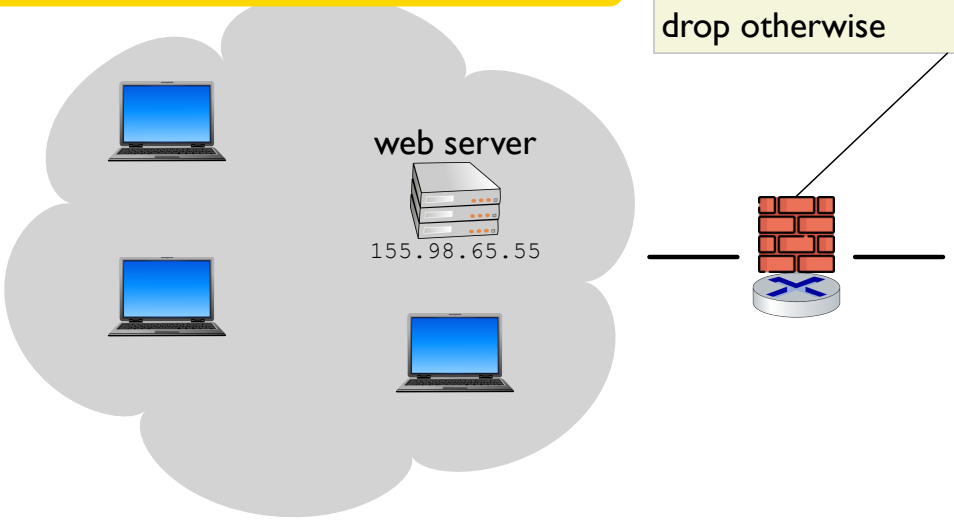
Network/Transport Layer Firewalls



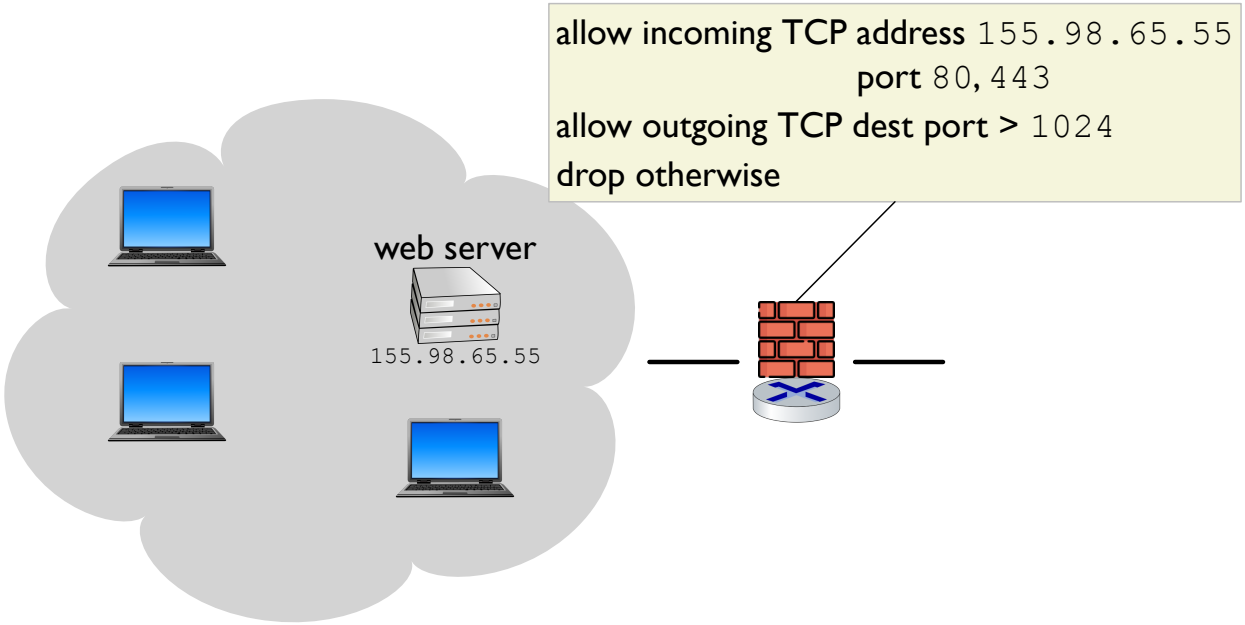
Network/Transport Layer Firewalls

Allows incoming HTTP attempts for non-servers

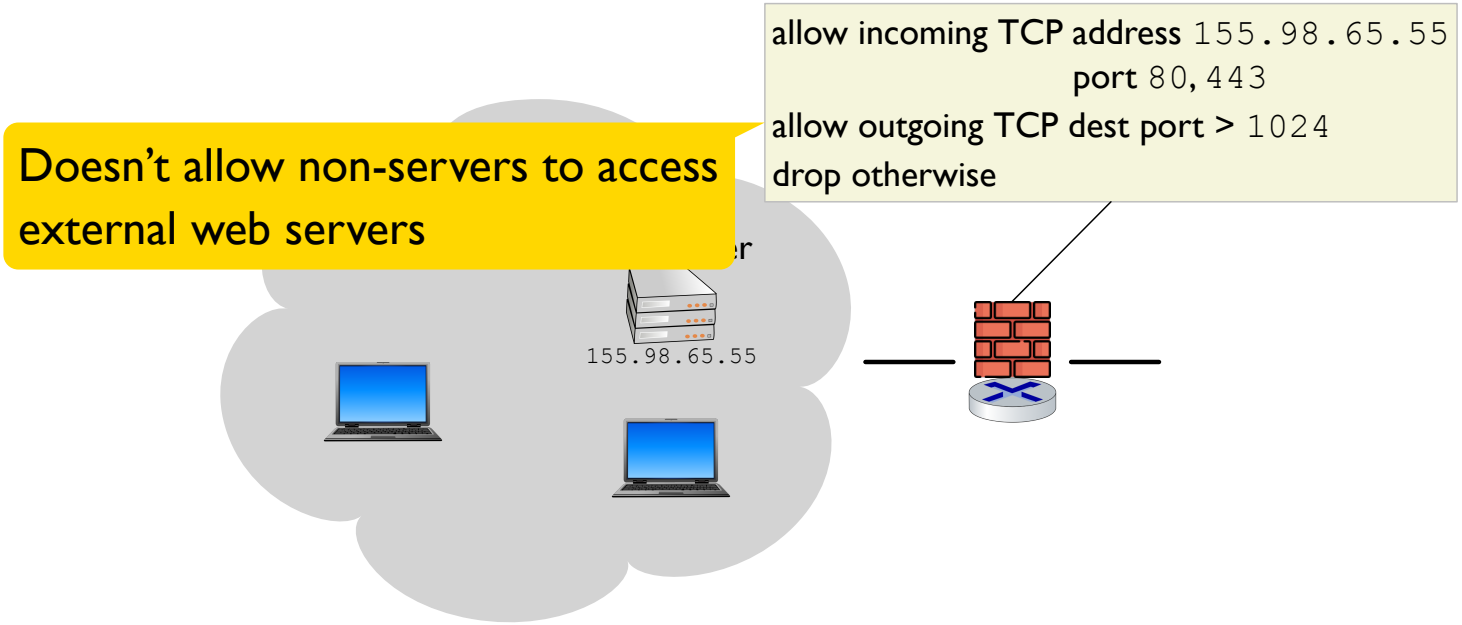
allow incoming TCP dest port `80`, `443`
allow outgoing TCP dest port > `1024`
drop otherwise



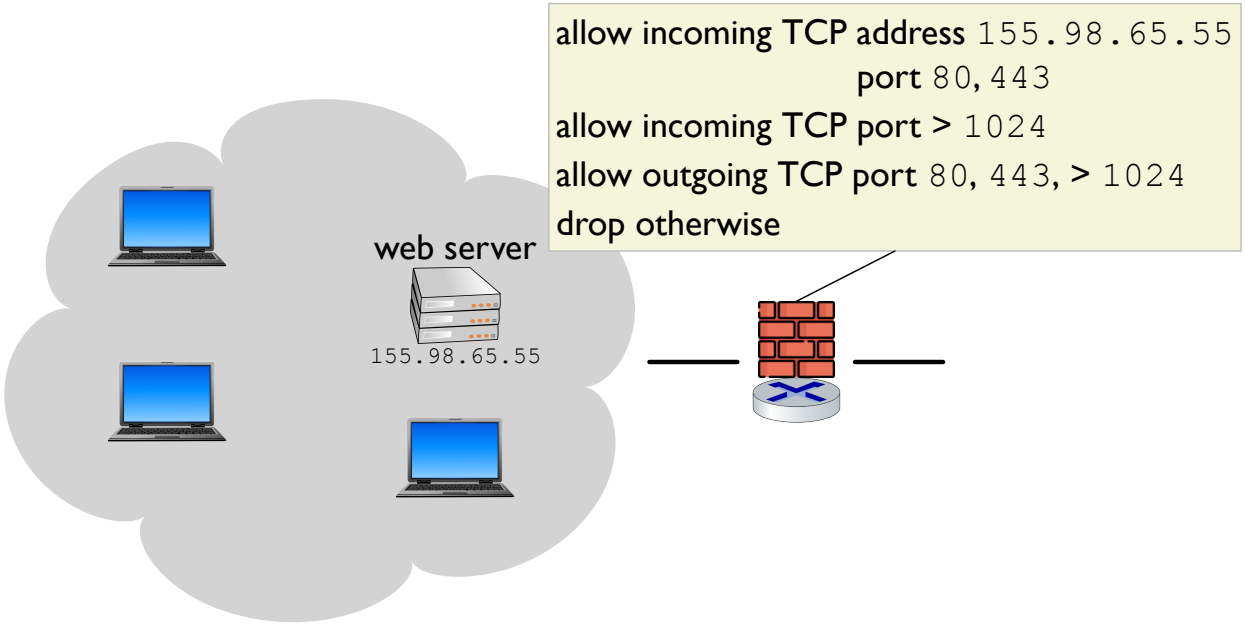
Network/Transport Layer Firewalls



Network/Transport Layer Firewalls



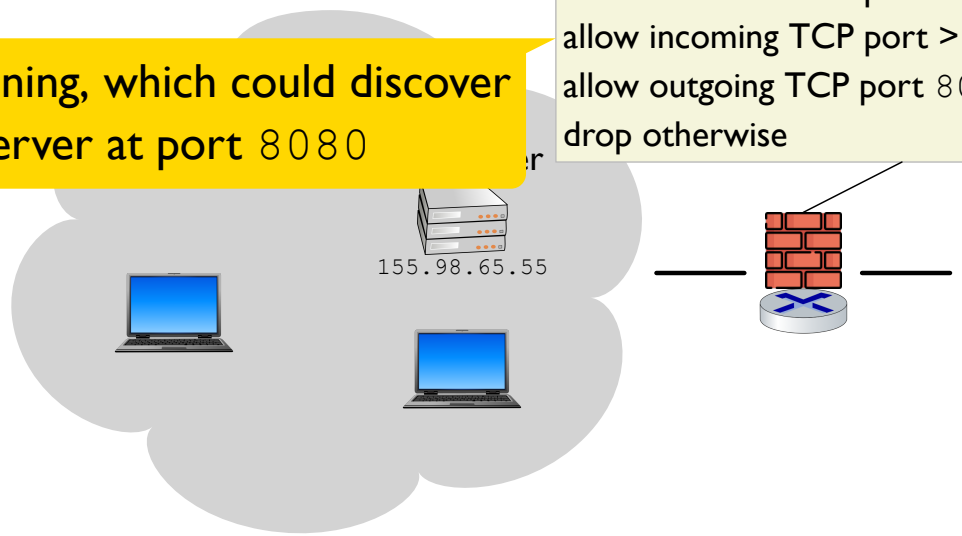
Network/Transport Layer Firewalls



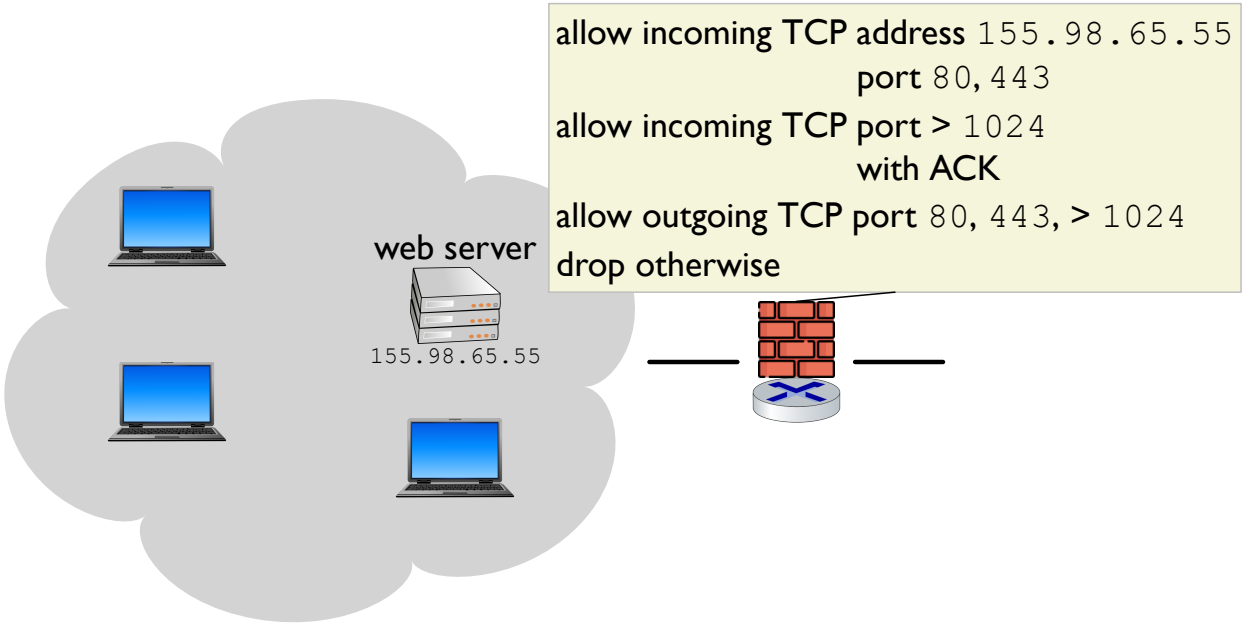
Network/Transport Layer Firewalls

allow incoming TCP address `155.98.65.55`
port `80`, `443`
allow incoming TCP port > `1024`
allow outgoing TCP port `80`, `443`, > `1024`
drop otherwise

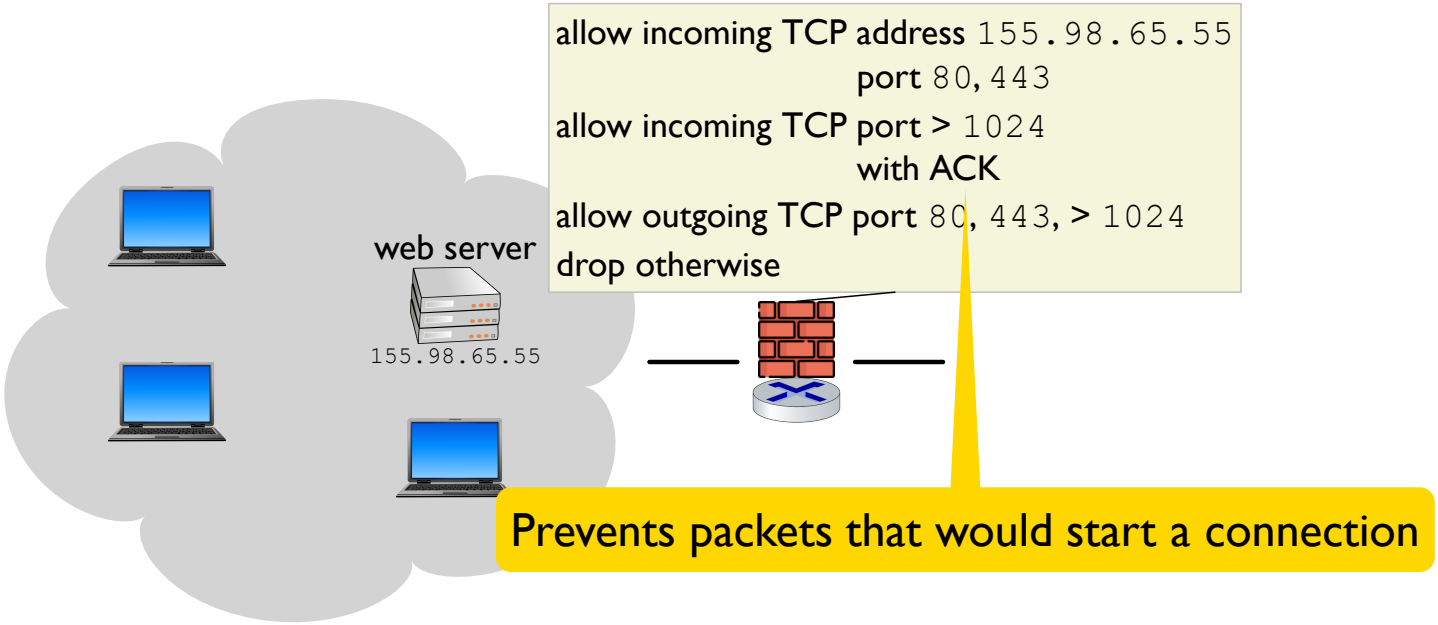
Allows port scanning, which could discover a development server at port `8080`



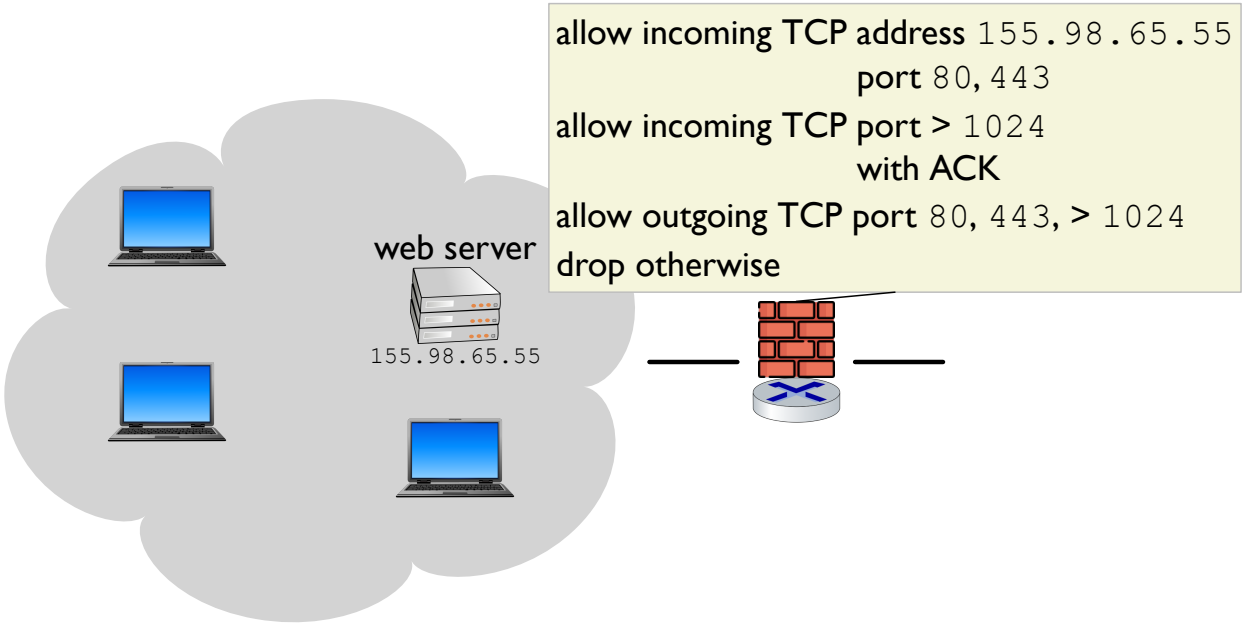
Network/Transport Layer Firewalls



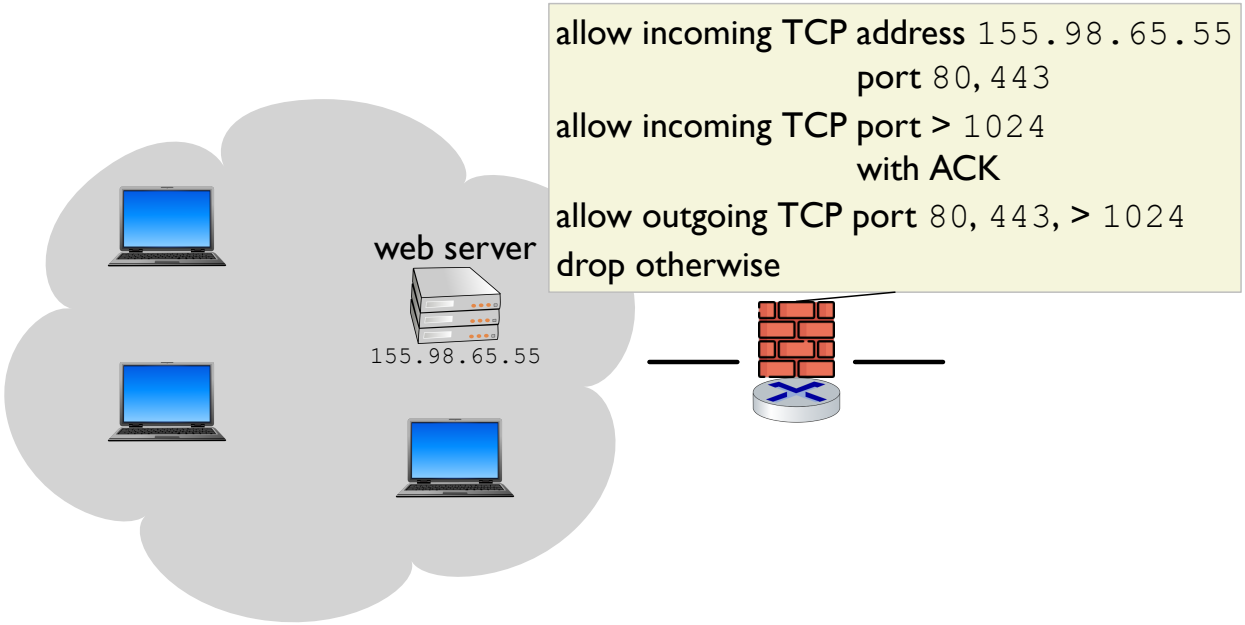
Network/Transport Layer Firewalls



Network/Transport Layer Firewalls



Network/Transport Layer Firewalls

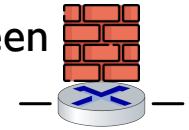


Options for DNS:

- Allow UDP port `53` and > `1024`
- Make internal hosts use an internal DNS server, and allow UDP only for that server

Example Firewall

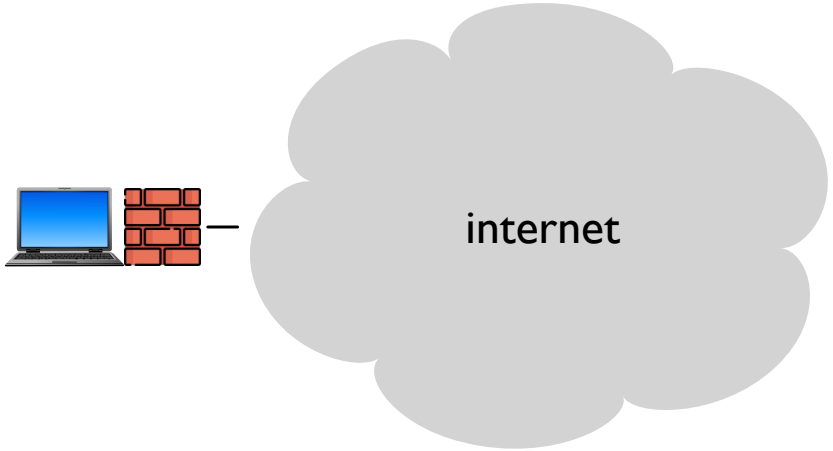
On Linux, `iptables` implements a NAT-capable firewall

- Can work as a host-specific firewall on user machine 
- Can work as a firewall router when forwarding packets between interfaces 

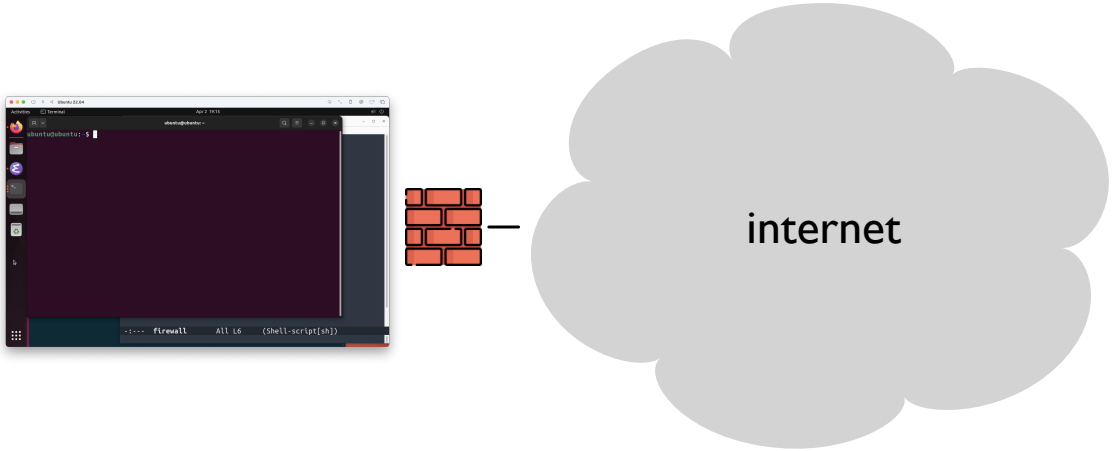
```
$ iptables -A INPUT -p tcp --dport 80 -j DROP

$ iptables -A OUTPUT -d 75.126.153.206 -j DROP

$ iptables -A INPUT -i eth1 -s 10.0.0.0/8 -j DROP
```

Windows and macOS have firewall options in their system-settings dialogs

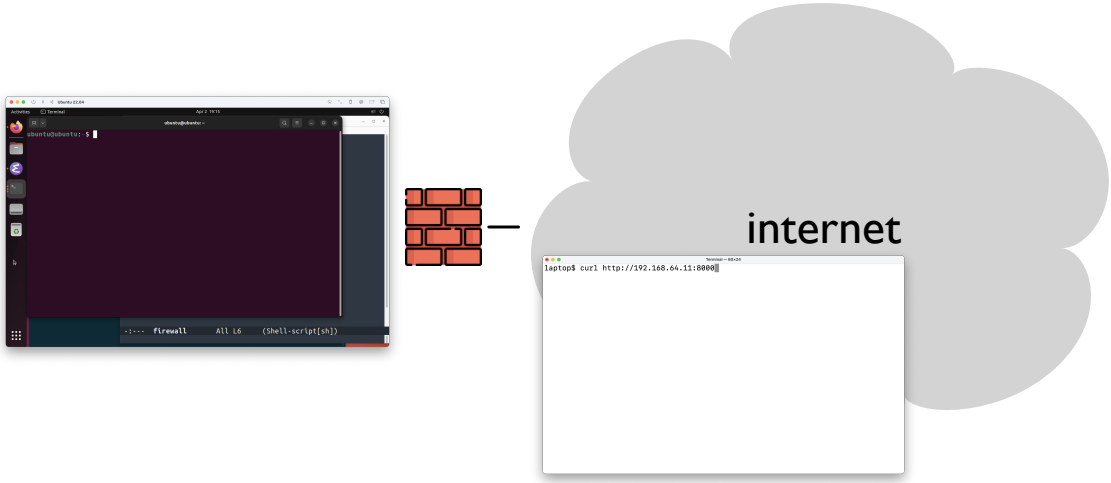
Demo



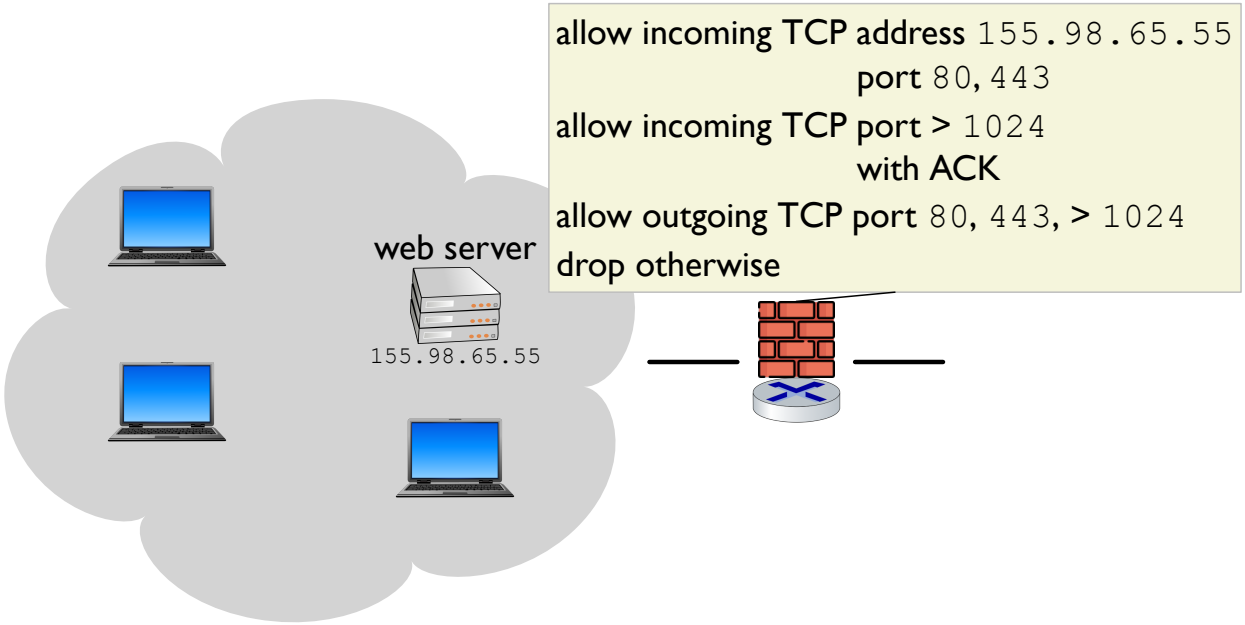
Demo



Demo

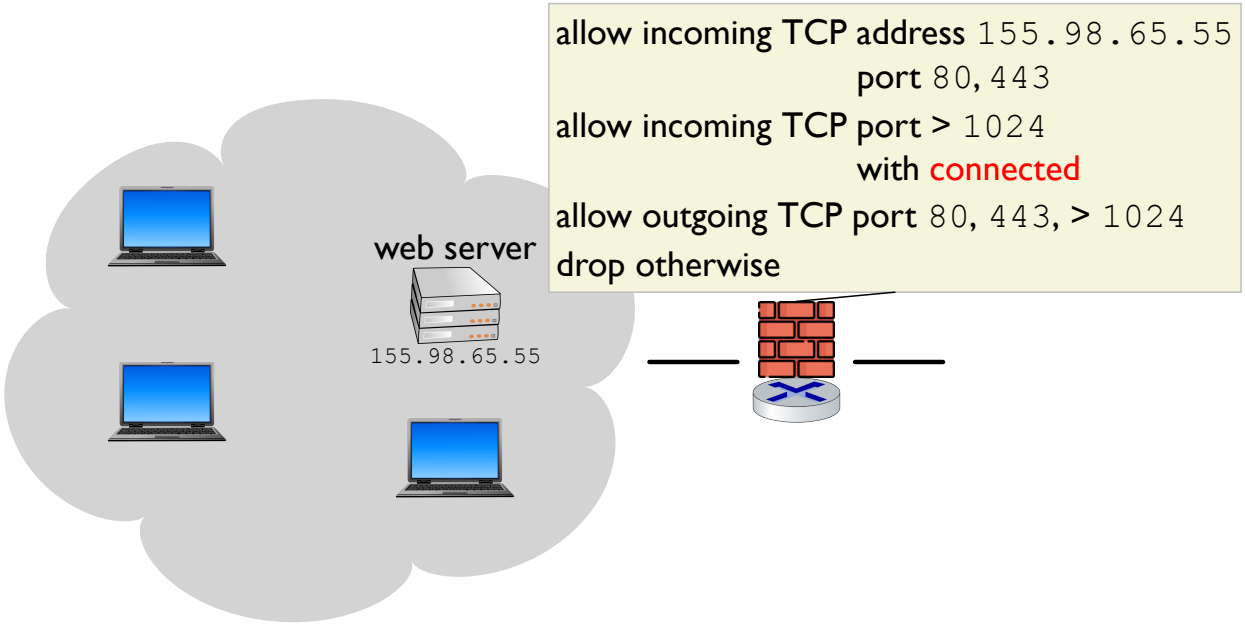

ubuntu@ubuntu: $
-:--- firewall All L6 (Shell-script[sh])
internet
laptop$ curl http://192.168.64.11:8000

Network/Transport Layer Firewalls

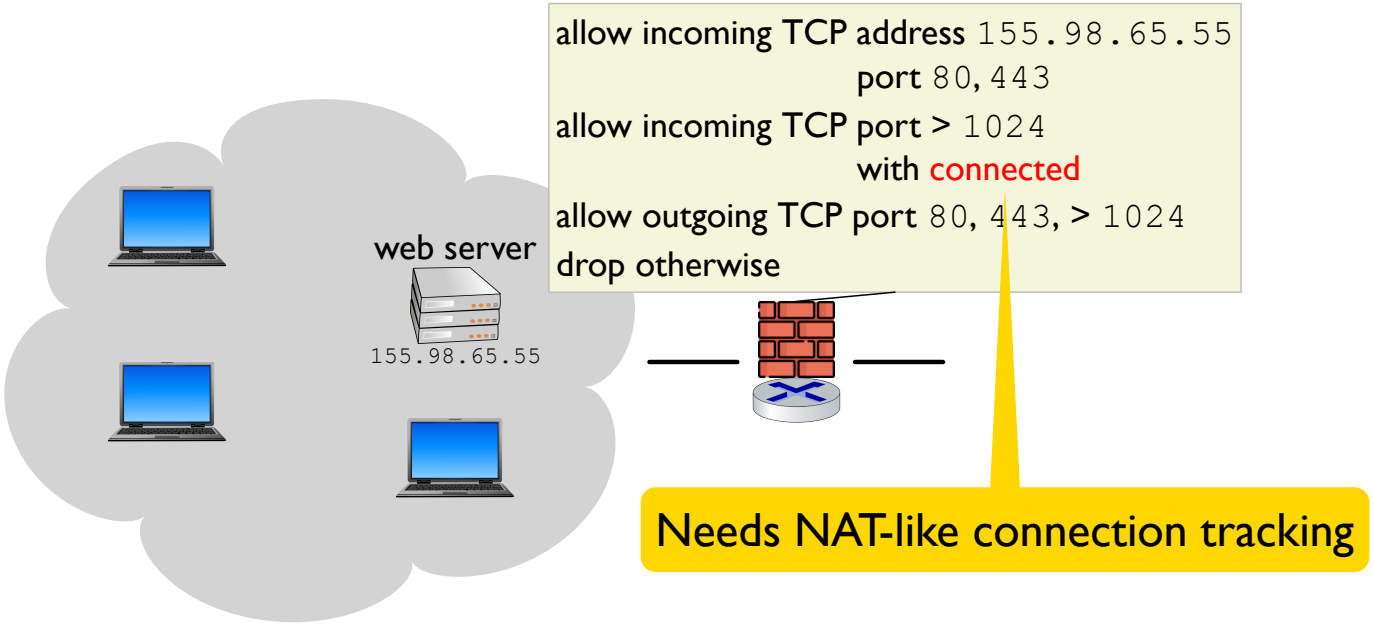


Stateless firewalls like this are **packet filter firewalls**

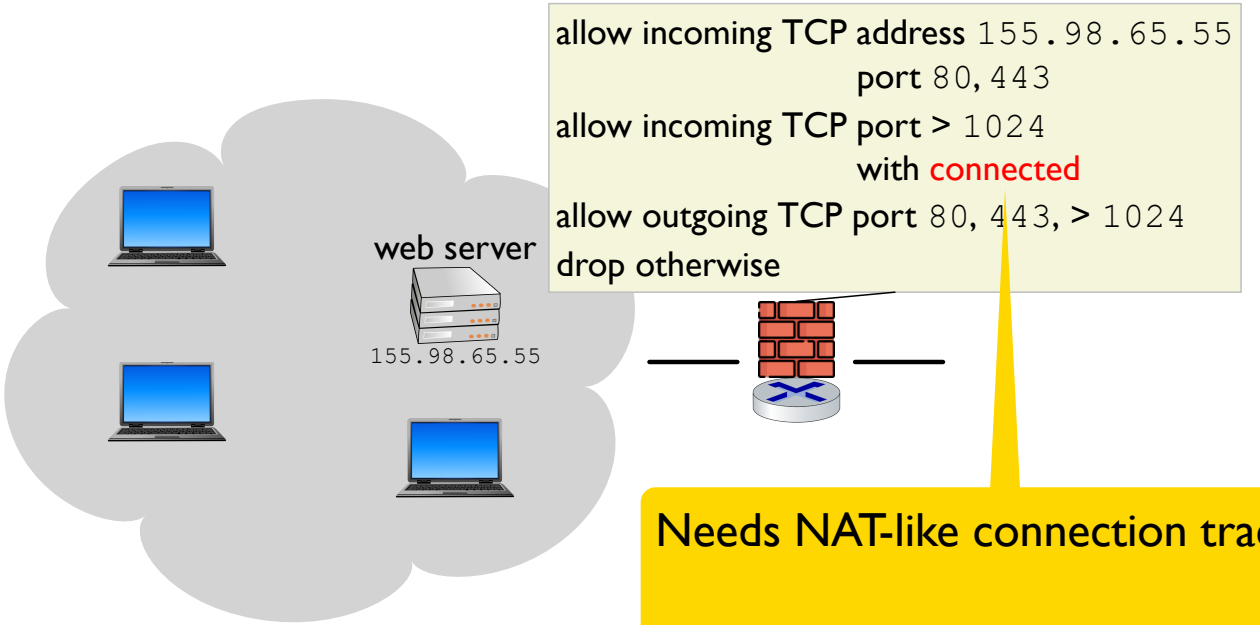
Network/Transport Layer Firewalls



Network/Transport Layer Firewalls



Network/Transport Layer Firewalls



allow incoming TCP address `155.98.65.55`
port `80, 443`
allow incoming TCP port > `1024`
with connected
allow outgoing TCP port `80, 443, > 1024`
drop otherwise

Needs NAT-like connection tracking

Firewall and NAT functionality
are often bundled together

More Filters

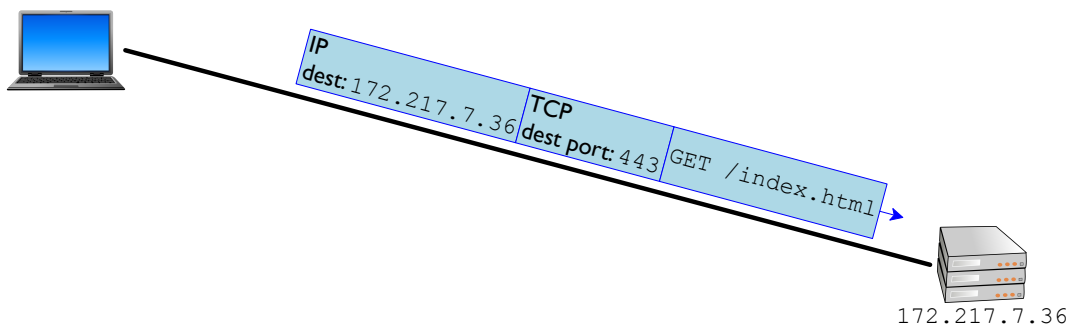
Instead of looking only at headers at the network/transport layer, a firewall could inspect packet payloads, and maybe keep even more state about inferred connections

This idea is sometimes called **deep packet inspection**

Less common now than in the early 2000s, because payloads are now more often encrypted

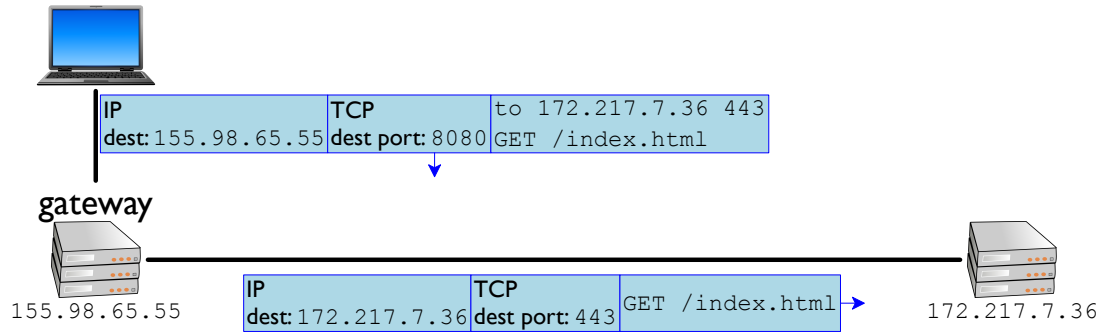
Application Gateways

Unlike filtering at the network/transport layer, an **application gateway** requires the cooperation of applications



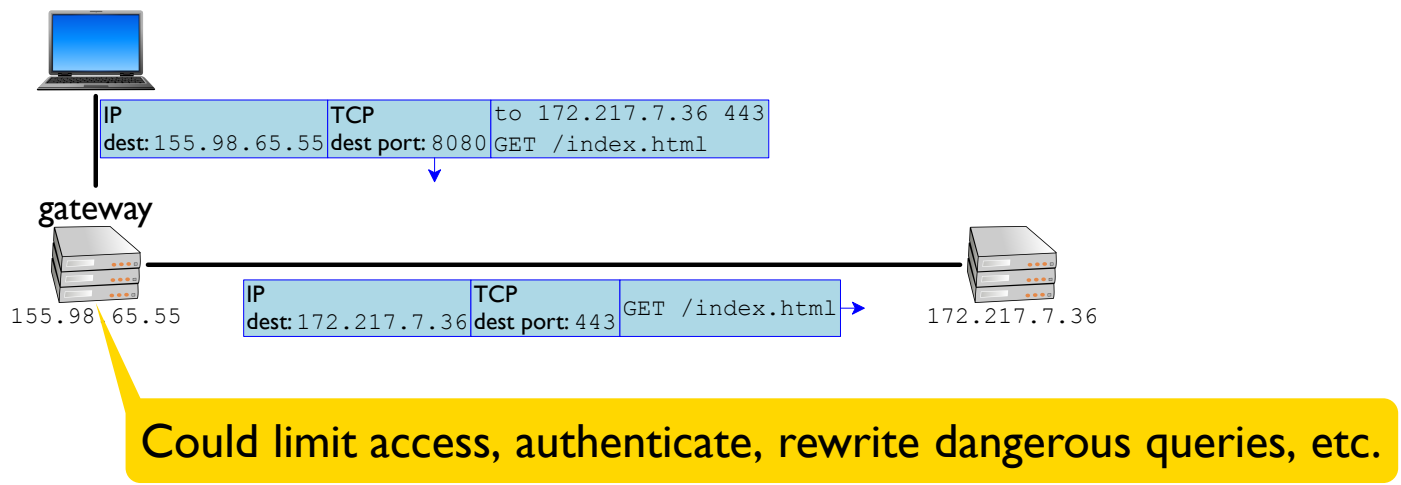
Application Gateways

Unlike filtering at the network/transport layer, an **application gateway** requires the cooperation of applications



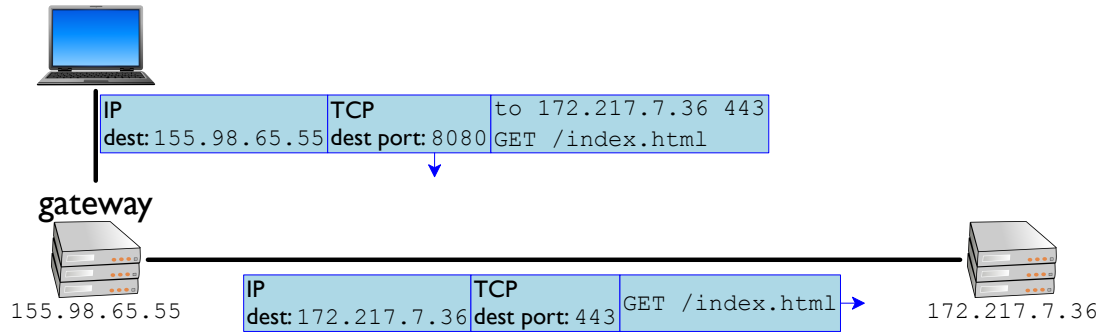
Application Gateways

Unlike filtering at the network/transport layer, an **application gateway** requires the cooperation of applications



Application Gateways

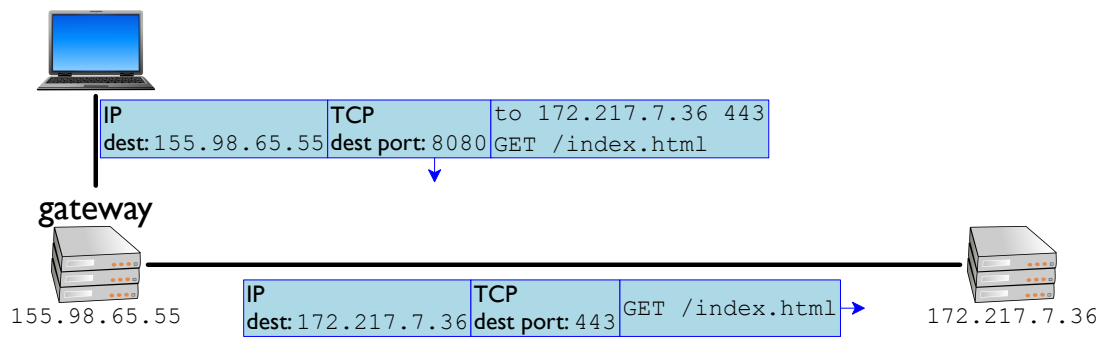
Unlike filtering at the network/transport layer, an **application gateway** requires the cooperation of applications



Most applications that use HTTP honor the `HTTP_PROXY` environment variable

Application Gateways

Unlike filtering at the network/transport layer, an **application gateway** requires the cooperation of applications

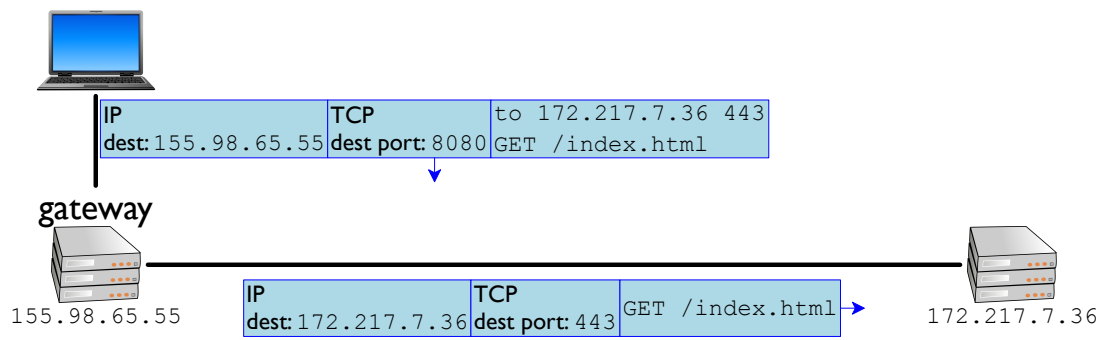


Most applications that use HTTP honor the `HTTP_PROXY` environment variable

Proxy-request protocols include HTTP and SOCKS5

Application Gateways

Unlike filtering at the network/transport layer, an **application gateway** requires the cooperation of applications

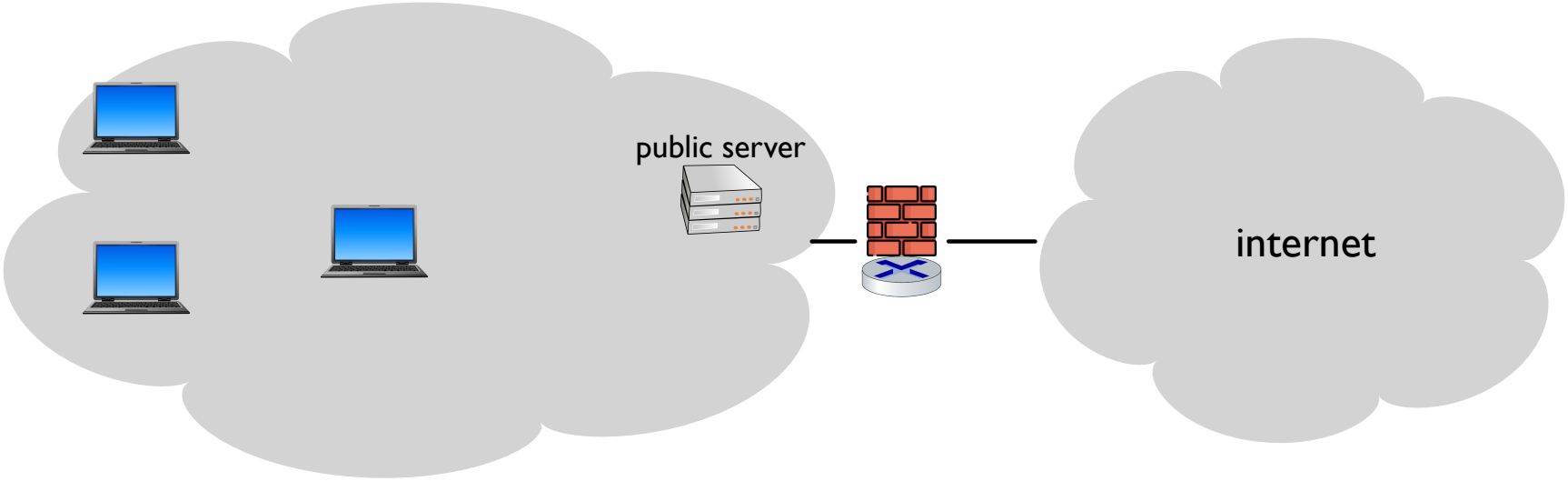


Most applications that use HTTP honor the `HTTP_PROXY` environment variable

These kinds of proxies tend to be slow and inconvenient

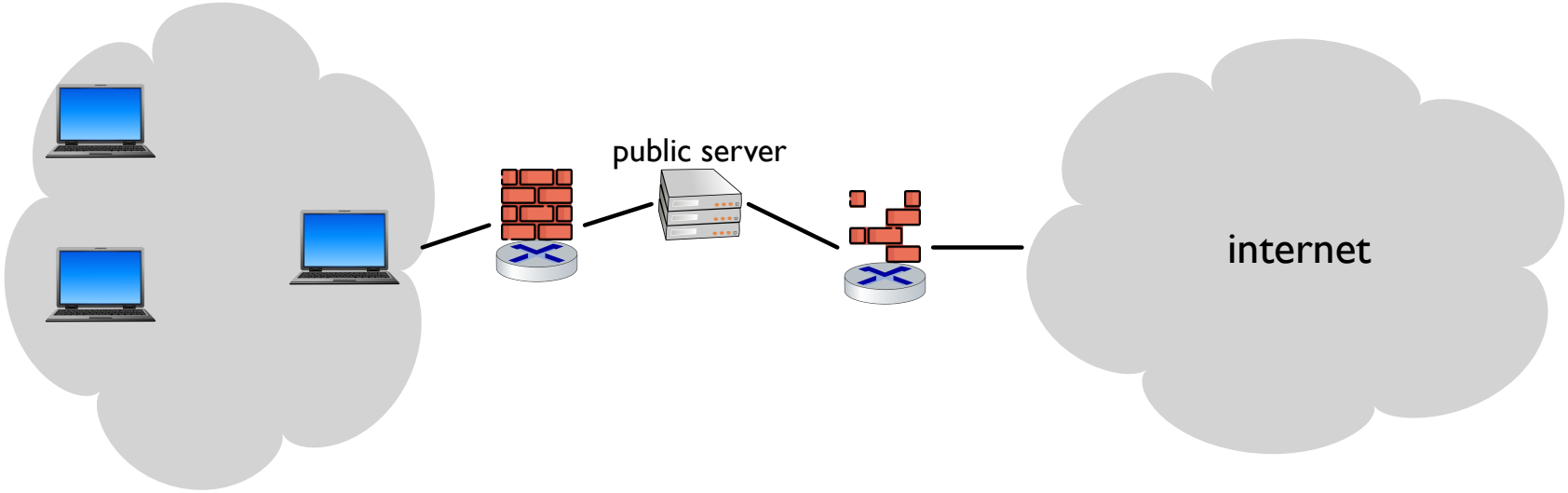
DMZ

Organizing some servers into a **demilitarized zone (DMZ)** is one common way to manage access



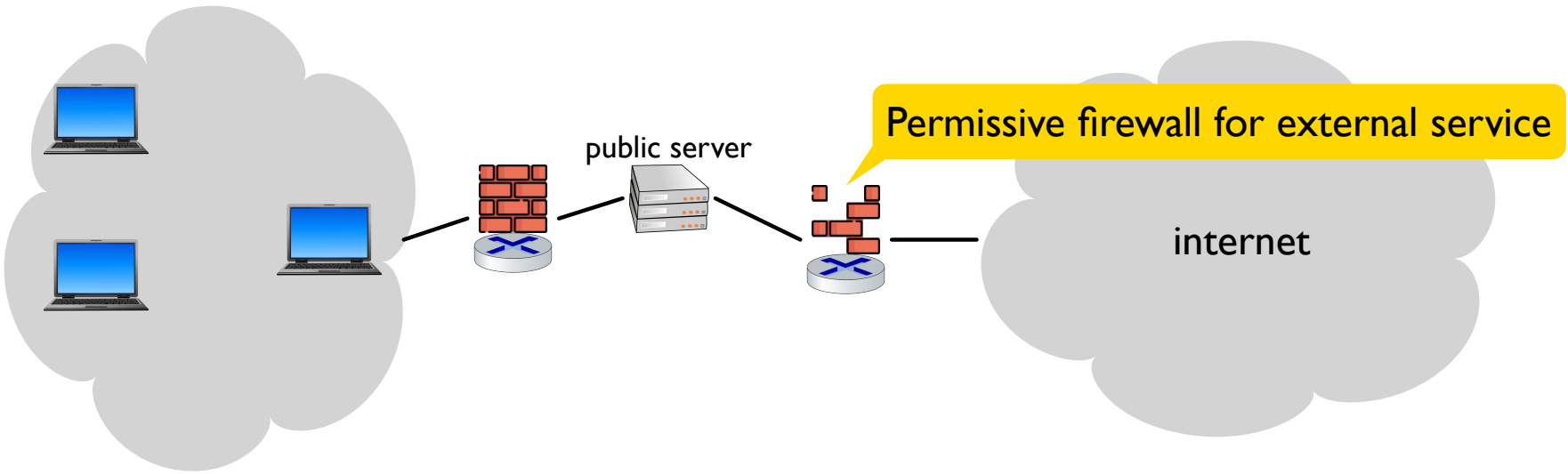
DMZ

Organizing some servers into a **demilitarized zone (DMZ)** is one common way to manage access



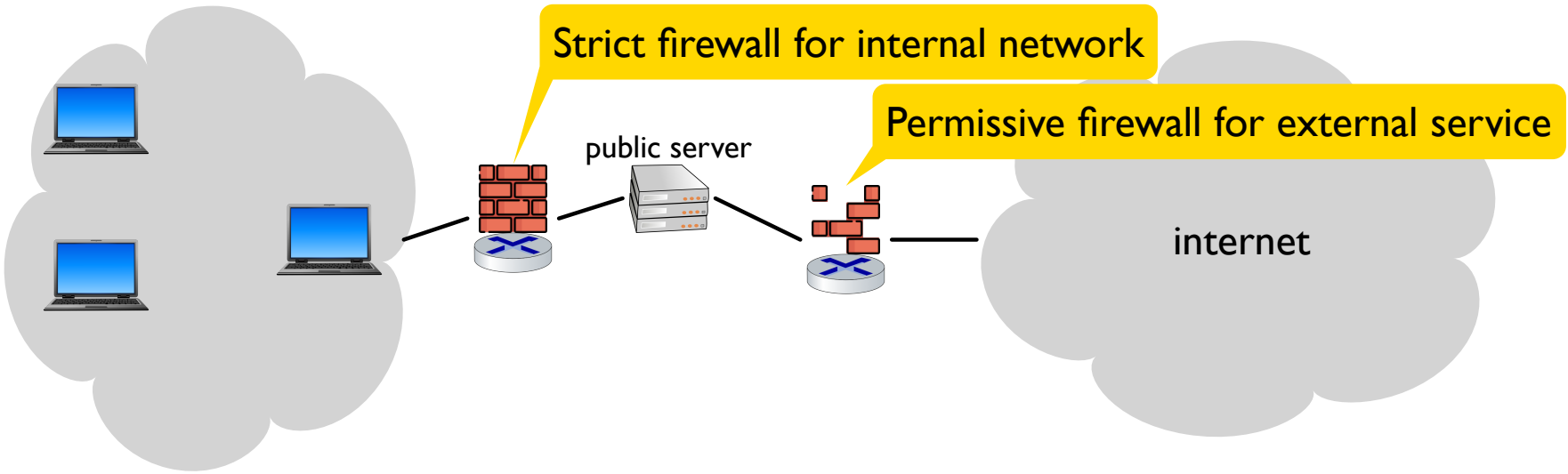
DMZ

Organizing some servers into a **demilitarized zone (DMZ)** is one common way to manage access



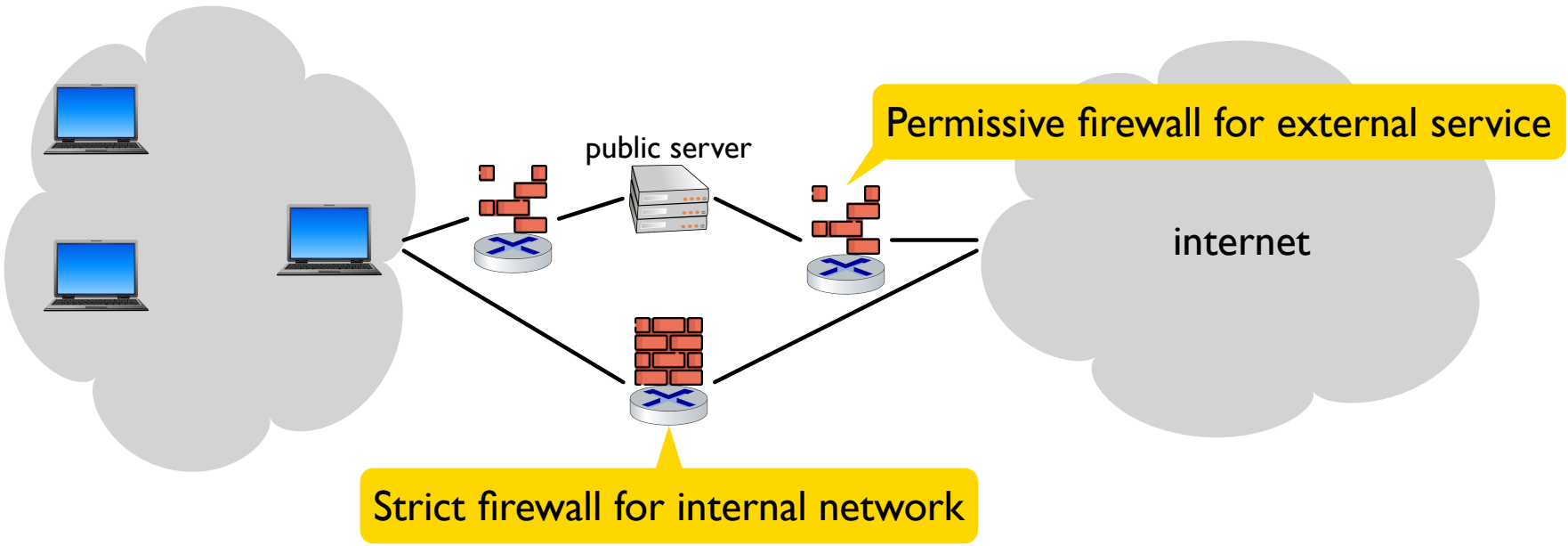
DMZ

Organizing some servers into a **demilitarized zone (DMZ)** is one common way to manage access



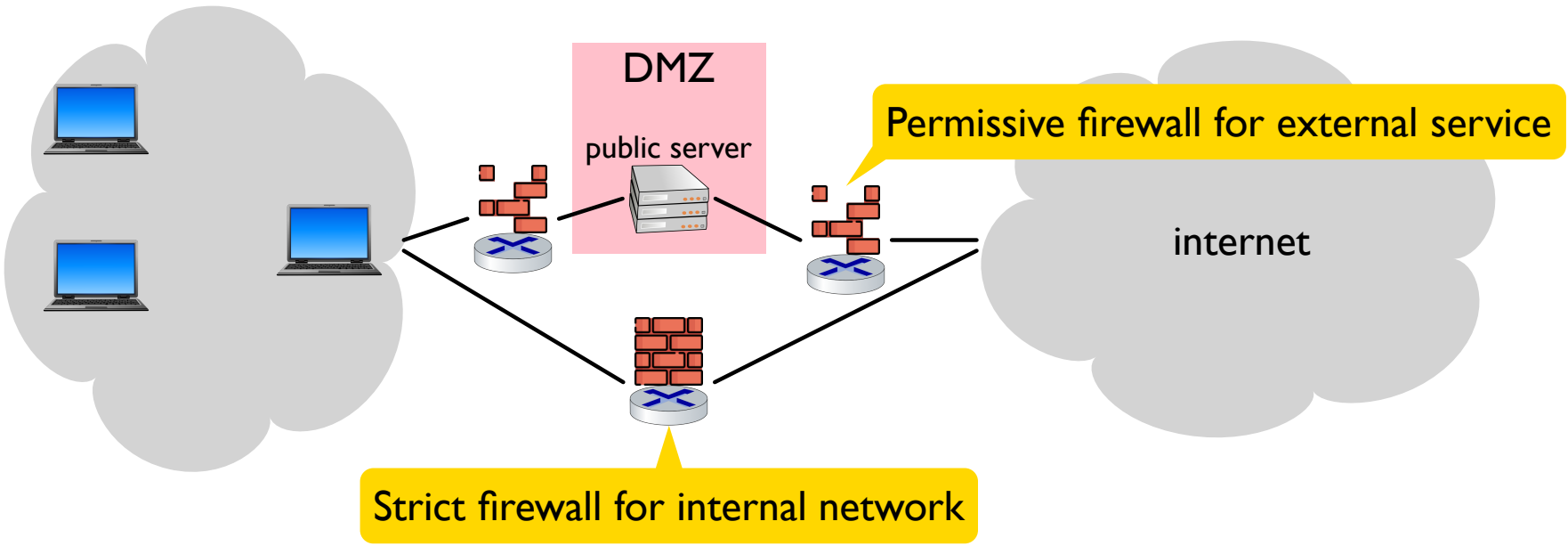
DMZ

Organizing some servers into a **demilitarized zone (DMZ)** is one common way to manage access



DMZ

Organizing some servers into a **demilitarized zone (DMZ)** is one common way to manage access



Summary

A **firewall** is part of a security-in-depth architecture that prevents security breaches through message filtering, especially at the packet level

Firewall configuration relies on many networking concepts across several layers