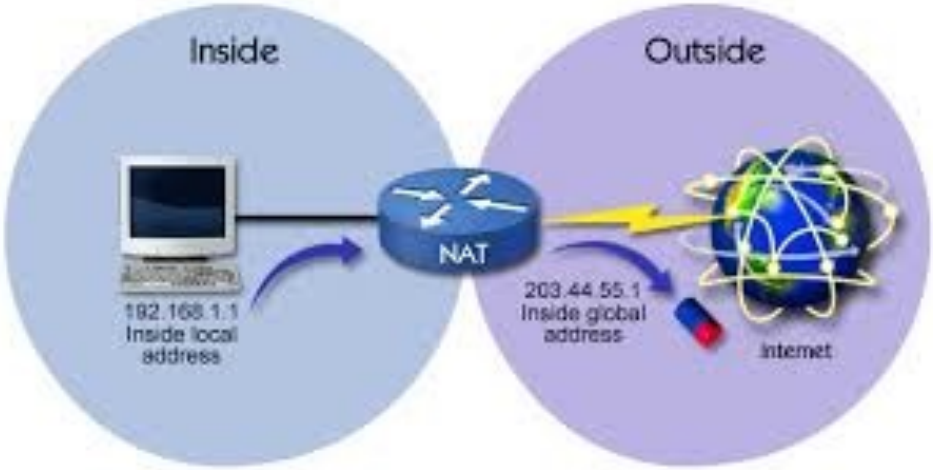
COSC 301
Network Management and Security

Lecture 22: Firewalls & NAT

Today's Focus



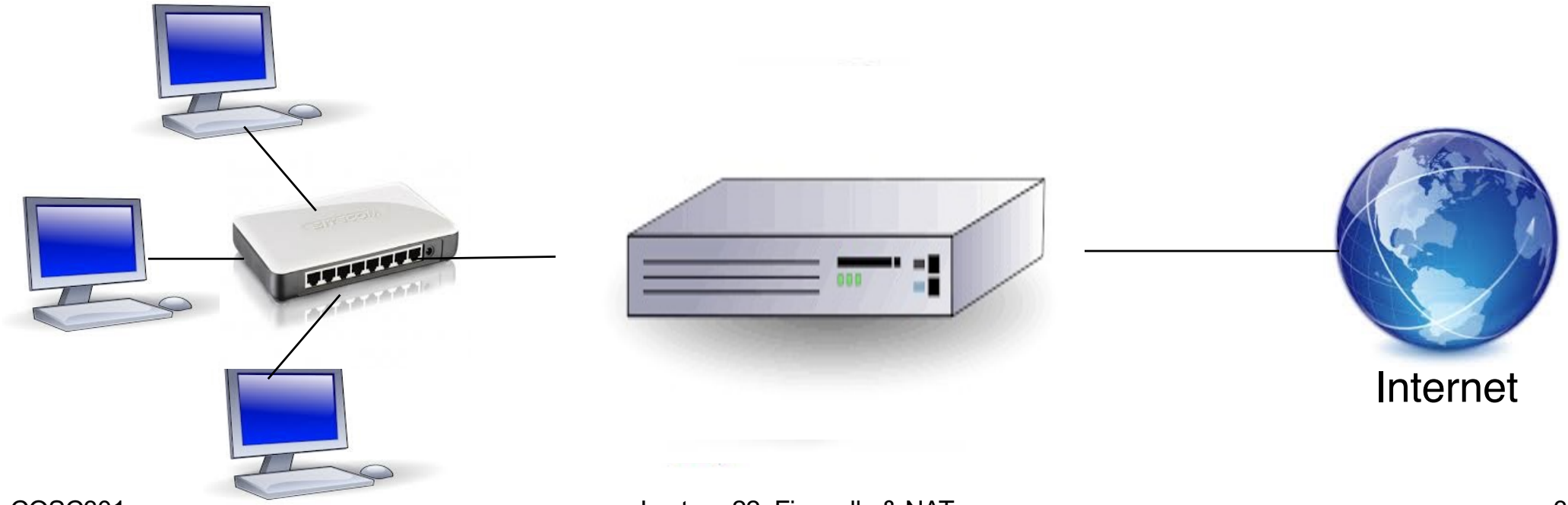
How to protect an intranet?

-- Firewall

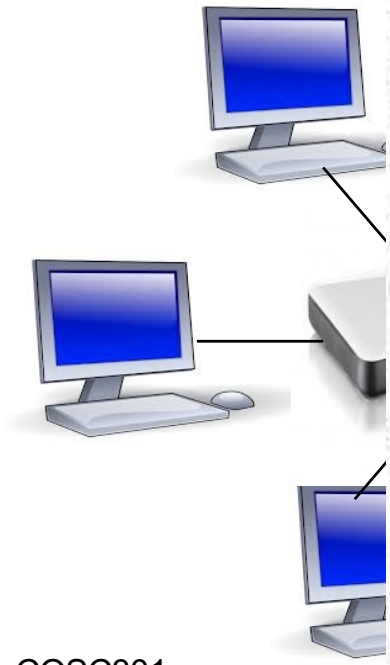
-- Network Address Translation(NAT)

What is Firewall?

- A firewall is a network security system that acts as a *check point* between an internal network and the rest of the Internet
  - All affected network traffic is routed through the firewall
  - Is configured with rules that determine which traffic to be passed and which to be blocked



- A firew…cts as a *check* …the rest of the Inte…
  - All af…e firewall
  - Is co…raffic to be pass…

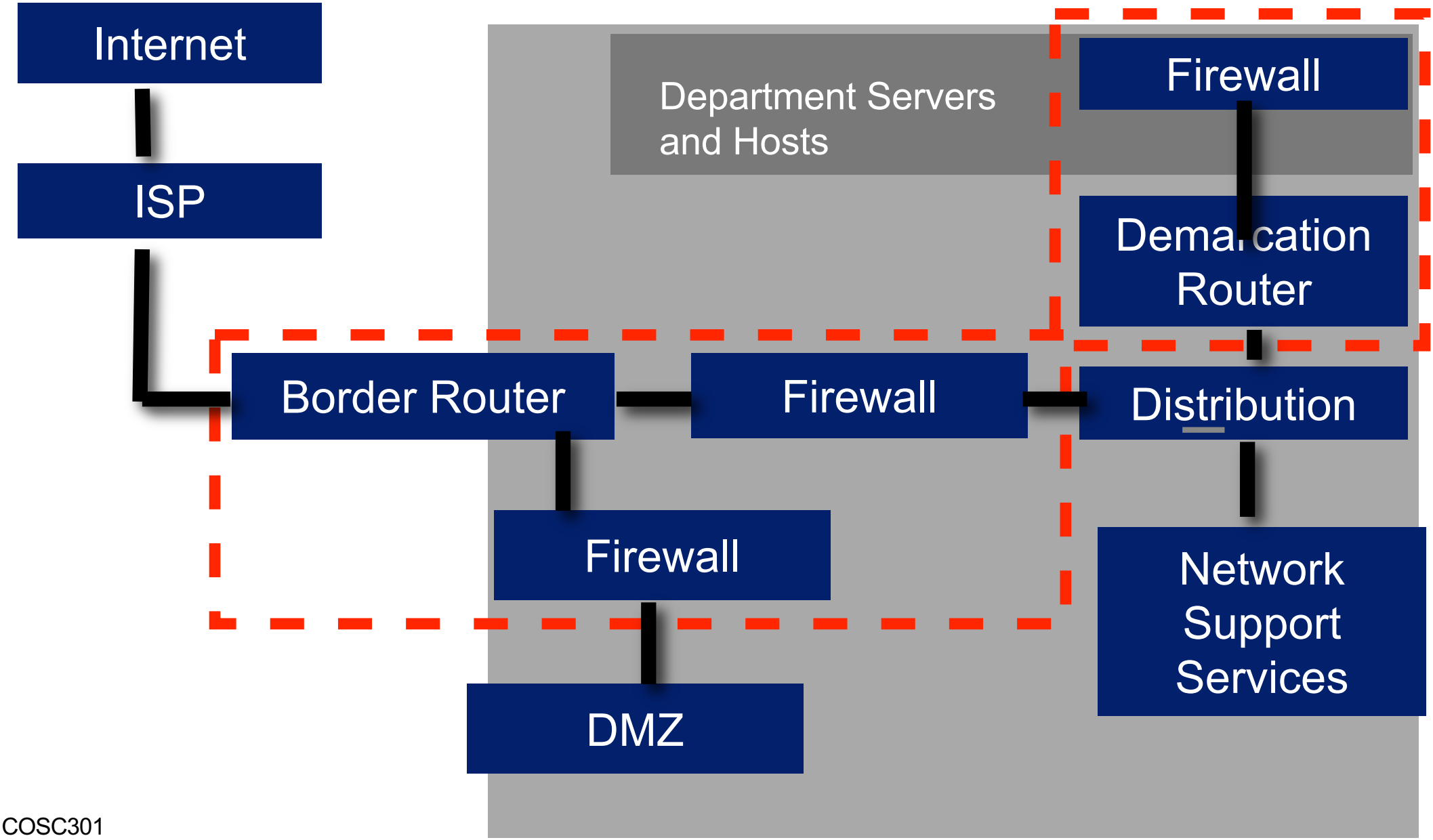


Internet

Router/Gateway

- Router
  - Primary purpose is to forward packets (Layer 3).
  - Demarcates a broadcast zone (e.g. Ethernet).
  - May demarcate management borders.
  - Used to shield the border of networks.
  - Often some firewall capabilities. (Layer 4)
- Gateway
  - A very broad term.
  - Application Layer Gateway: Email, Web
  - A gateway can convert between two different types of network, e.g. VoIP / PSTN

Sample Large Networks



Border Router

- Coarse-grained inspection.
- Block offensive networks from getting inside your network.
  - Route to null(0) or drop at firewall.
- Hide parts of interior network from outside.
- Stop interior hosts from accessing internet directly.
  - Force use of web proxy or e-mail gateway.


NORTH
KOREA
Military
Demarcation
Line
Demilitarized Zone (DMZ)
2nd Tunnel
4th Tunnel
38th Parallel
1st Tunnel
3rd Tunnel
SOUTH
KOREA

Firewall

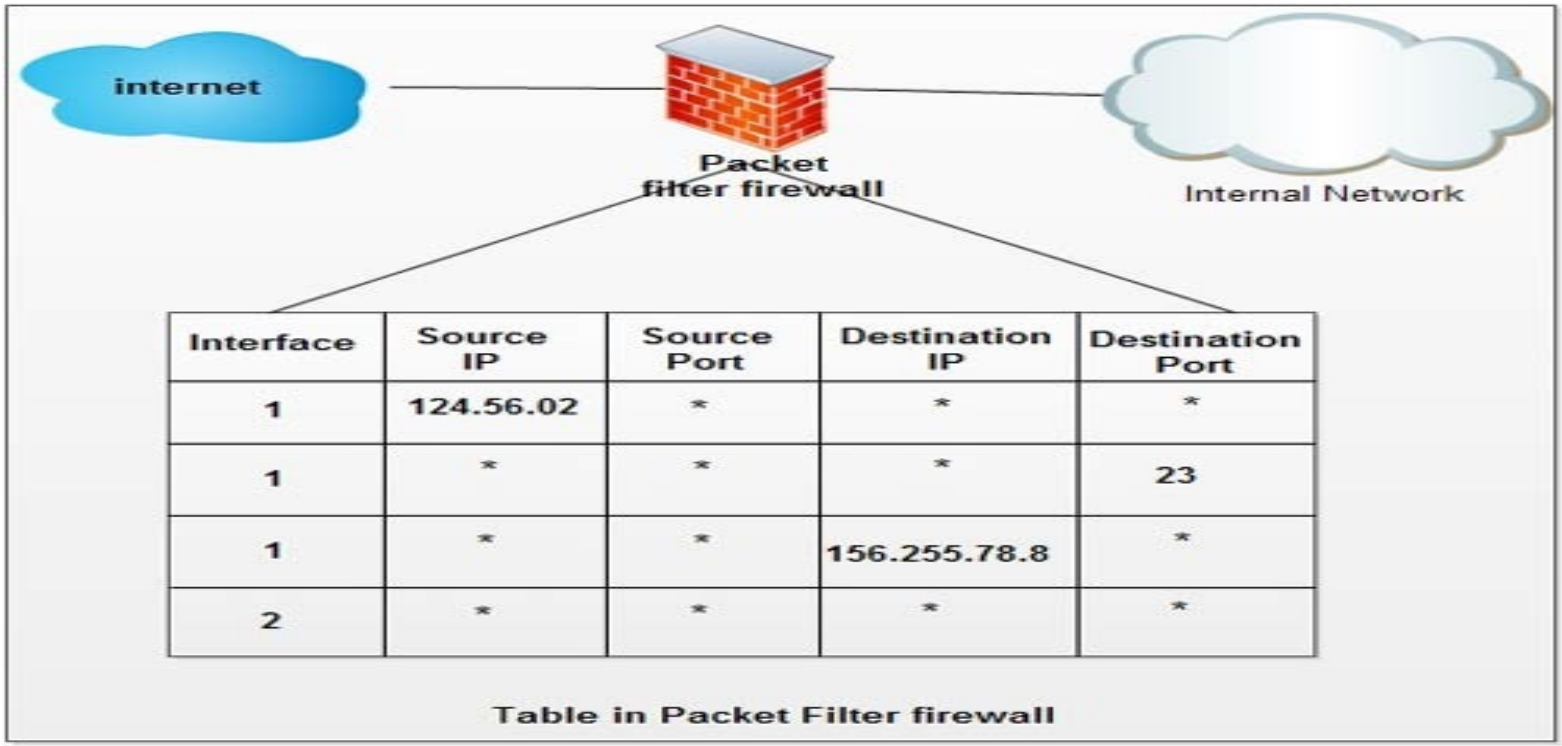
- Commonly done on the router.
- Used to implement a finer-grained access policy.
- Protects against illegitimate packets.
- Position
  - **Inside of router**: Routers are faster, better equipped for simple dropping
  - **In front of infrastructure:** Firewalls incur some delay, but it is usually negligible when compared with the Internet.
- Individual hosts commonly have firewalls.
  - Fast becoming the out-of-box configuration.

Gateway

- Can be used to implement a Web Proxy.
  - Use can be enforced by router / firewall.
- Can be used as e-mail filtering solution.
  - e.g. all outgoing and incoming mail must go through a mailhub—only authorised hosts can be e-mail servers.
  - All e-mail is scanned for viruses and SPAM.

1st : Packet-Filter Firewall

- Forward or block packets based on the information in network-layer and transport-layer headers
  - Source and destination addresses
  - Source and destination port addresses
  - Type of protocol (TCP or UDP)



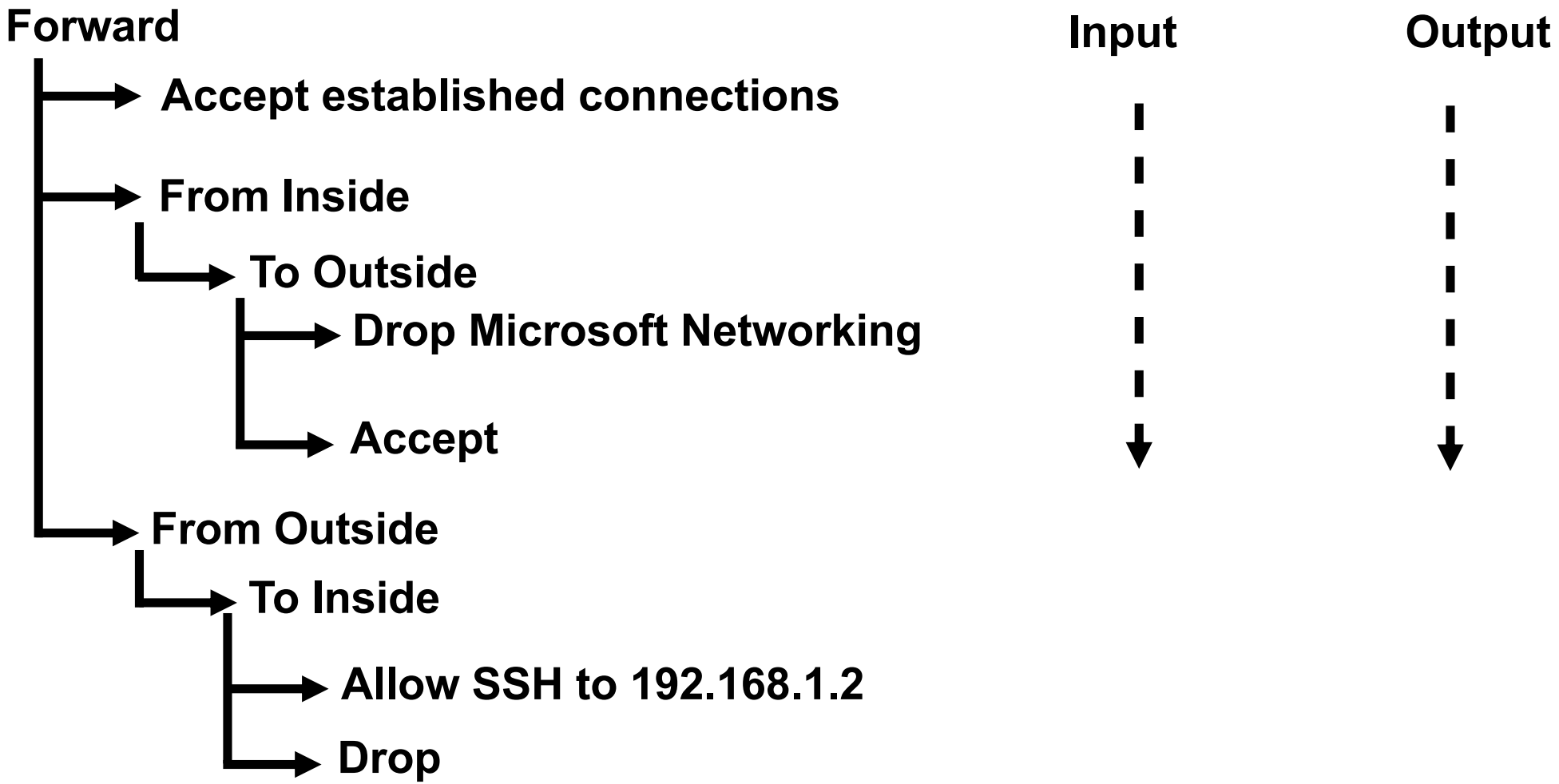
Interface	Source IP	Source Port	Destination IP	Destination Port
1	124.56.02	*	*	*
1	*	*	*	23
1	*	*	156.255.78.8	*
2	*	*	*	*

Table in Packet Filter firewall

Packet Filter Process

- Think of a firewall as a set of inverted trees.
  - Input, Output and Forward
  - Create a chain for each combination of {in,out}
  - Each packet starts at the top of its respective tree.
- Packet is inspected one test at a time
  - Accept or drop (processing stops)
  - Jump into another rule-set (continue processing)
  - Return from a rule-set (or fall-off a rule-set)
  - Falling off the tree's rule-set invokes the default policy for that tree.

Tree of Chains



If a rule in the firewall exists to block telnet access, it will block the TCP protocol for port number 23

IP rules

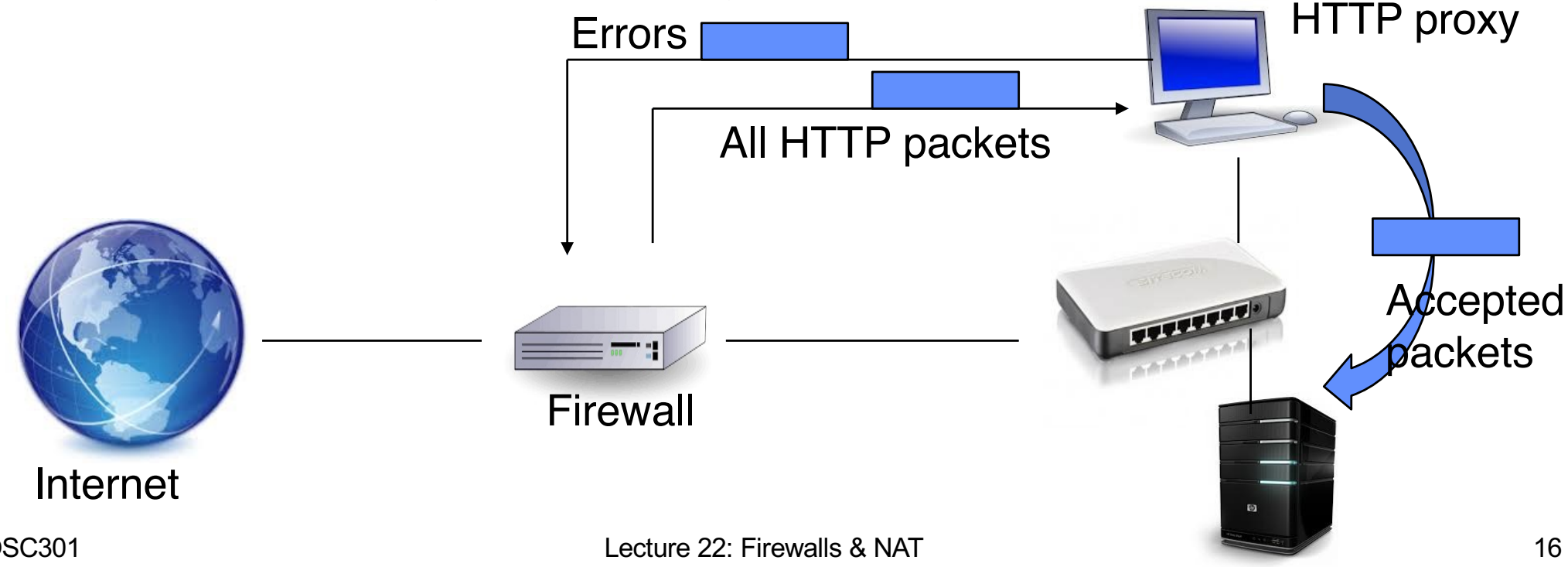
- To allow all incoming SSH
  - iptables –A INPUT –p tcp –dport 22 –m conntrack –ctstate NEW,ESTABLISHED –j ACCEPT
  - iptables –A OUTPUT –p tcp –sport 22 –m conntrack –ctstate ESTABLISHED –j ACCEPT
- To allow all outgoing SSH
  - iptables –A OUTPUT –p tcp –dport 22 –m conntrack –ctstate NEW,ESTABLISHED –j ACCEPT
  - iptables –A INPUT –p tcp –sport 22 –m conntrack –ctstate ESTABLISHED –j ACCEPT

2nd: Stateful Firewall

- Performs the work of the packet-filter firewall but operates up to layer 4 (transport layer)
- Stateful packet inspection
  - Keep track of the state of network connections
    - SYN, SYN-ACK, ACK, ESTABLISHED, sequence number, port, IP, …
  - Determines whether a packet is the start of a new connection, a part of an existing connection, or not part of any connection using the maintained states.
  - UDP is connectionless, so tracking is a little less precise, but still good enough, so long as the source port is random.
  - CPU intensive checking is performed at the time of setup of the connection. They may not be suitable for border routers on larger networks

3rd: Proxy Firewall

- Filter message based on the information available in the message itself (application layer)
  - Sometimes called application gateway
  - To detect if an unwanted protocol is attempting to bypass the firewall on an allowed port, or detect if a protocol is being abused in any harmful way



Firewall can Guard Against

- Near-local spoofing
  - where packets come in on the wrong interface.
- Ping-floods against internal hosts
  - though the firewall still gets flooded.
- Syn-Ack attacks
  - Limit TCP half-open connections to say 20/min.
- Fragment attacks
  - stateful firewalls.

Firewall isn't a Panacea

- Spoofing internet hosts
  - solved using tools such as SSL
- Flooding your internet connection
  - requires upstream co-operation. No protocol support for this, e.g. DoS and DDoS
- Detecting network anomalies
  - requires checking of logs, Intrusion Detection Systems
- Poor policy will quickly degrade security.

Private Network

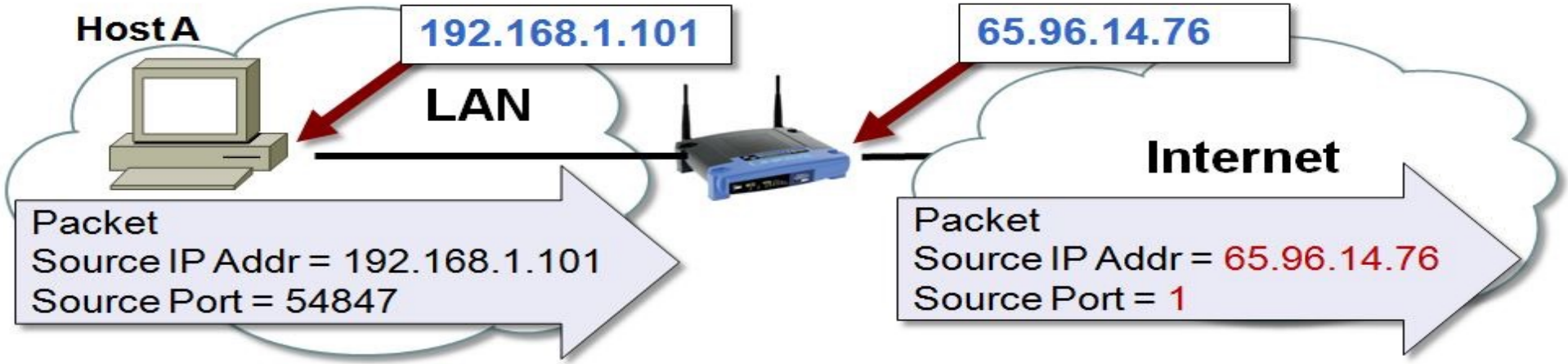
- *Private IP* network is an IP network that is not directly connected to the Internet
- IP addresses in a private network can be assigned arbitrarily.
  - Not registered and not guaranteed to be globally unique
- NAT is a way to conserve IP addresses
  - hide a number of hosts behind a single IP address - A short term solution to IP address depletion
  - Uses private addresses:
    - 10.0.0.0-10.255.255.255,
    - 172.16.0.0-172.32.255.255 or
    - 192.168.0.0-192.168.255.255

SNAT and DNAT

- Source NAT (SNAT)
  - the destination IP address is maintained and the source IP address is changed.
  - allows a host on the “inside” of the NAT to initiate a connection to a host on the “outside” of the NAT.
- Destination NAT (DNAT)
  - the destination address is changed and the source IP address is maintained.
  - allows a host on the “outside” to connect to a host on the “inside”.
- Port Address Translation (PAT)
  - NAT overloading
  - uses one IP address for all clients to multiple ports

NAT Table

- The NAT table is the heart of the whole NAT operation, which takes place within the router (or any NAT-enabled device) as packets arrive and leave its interfaces.



NAT Translation Table

	Local IP Address	Source Port #		Internet IP Address	Source Port #
process X, Host A →	192.168.1.101	54,847	=	65.96.14.76	1
Host B →	192.168.1.103	24,123	=	65.96.14.76	2
process Y, Host A →	192.168.1.101	42,156	=	65.96.14.76	3
Host C →	192.168.1.102	33,543	=	65.96.14.76	4

NAT Concerns

- Performance
  - Modifying the IP header by changing the IP address requires that NAT boxes recalculate the IP header checksum
  - Modifying port number requires that NAT boxes recalculate TCP checksum
- End-to-end connectivity
  - NAT destroys universal end-to-end reachability of hosts on the Internet.
  - A host in the public Internet often cannot initiate communication to a host in a private network.
  - The problem is worse, when two hosts that are in a private network need to communicate with each other.
    - Port forwarding
    - TCP hole punching

Summary

- Firewall
  - What is a firewall?
  - How does it work?
  - Where to deploy firewalls?
  - Types of firewall
  - Security issues
- NAT
  - What is NAT and how does it work?
  - Source NAT
  - Destination NAT

References

- https://www.howtogeek.com/177621/the- beginners-guide-to-iptables-the-linux-firewall/
- RFC 2647
  Benchmarking Terminology for Firewall Performance
- http://www.netfilter.org/ (iptables)
- http://www.freebsd.org/doc/en/books/handbook/firewalls-ipfw.html