Distributed Systems

29. Firewalls

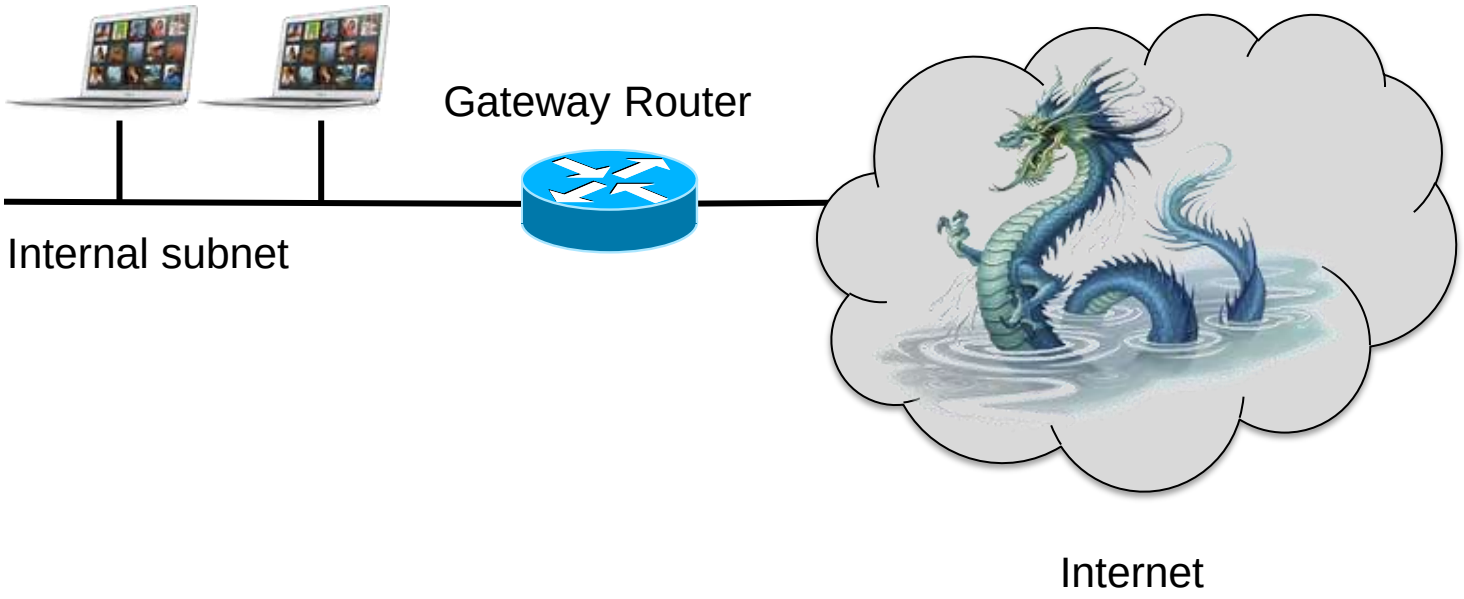
Paul Krzyzanowski

Rutgers University

Fall 2015

Network Security Goals

- Confidentiality: sensitive data & systems not accessible
- Integrity: data not modified during transmission
- Availability: systems should remain accessible



Firewall

- Separate your local network from the Internet
  - Protect the border between trusted internal networks and the untrusted Internet
- Approaches
  - Packet filters
  - Application proxies
  - Intrusion detection / intrusion protection systems

Screening router

- Border router (gateway router)
  - Router between the internal network(s) and external network(s)
  - Any traffic between internal & external networks passes through the border router

Instead of just routing the packet, decide *whether* to route it

- Screening router = Packet filter

  Allow or deny packets based on
  - Incoming interface, outgoing interface
  - Source IP address, destination IP address
  - Source TCP/UDP port, destination TCP/UDP port, ICMP command
  - Protocol (e.g., TCP, UDP, ICMP, IGMP, RSVP, etc.)

Filter chaining

- An IP packet entering a router is matched against a set of rules (chain)

- Each rule contains criteria and an action
  - Criteria: packet screening rule
  - Actions
    - *Accept* – and stop processing additional rules
    - *Drop* – discard the packet and stop processing additional rules
    - *Reject* – and send an error to the sender (ICMP Destination Unreachable)
    - *Continue* – continue evaluating rules

Network Ingress Filtering

Basic firewalling principle

Never have a direct inbound connection from the originating host from the Internet to an internal host

- Determine which services you want to expose to the Internet
  - e.g., HTTP & HTTPS: TCP ports 80 and 443
- Create a list of services and allow only those inbound ports and protocols to the machines hosting the services.
- *Default deny model* - by default, deny all
  - Anything not specifically permitted is dropped
  - May want to log denies to identify who is attempting access

Network Ingress Filtering

- Disallow IP source address spoofing
  - Restrict forged traffic (RFC 2827)
- At the ISP
  - Filter upstream traffic - prohibit an attacker from sending traffic from forged IP addresses
  - Attacker must use a valid, reachable source address
- Disallow incoming/outgoing traffic from private, non-routable IP addresses
- Helps with DDoS attacks such as SYN flooding from lots of invalid addresses

```
access-list 199 deny ip 192.168.0.0  0.0.255.255 any  log
access-list 199 deny ip 224.0.0.0  0.0.0.255  any  log
                    ....
access-list 199 permit ip  any  any
```

Network Egress Filtering

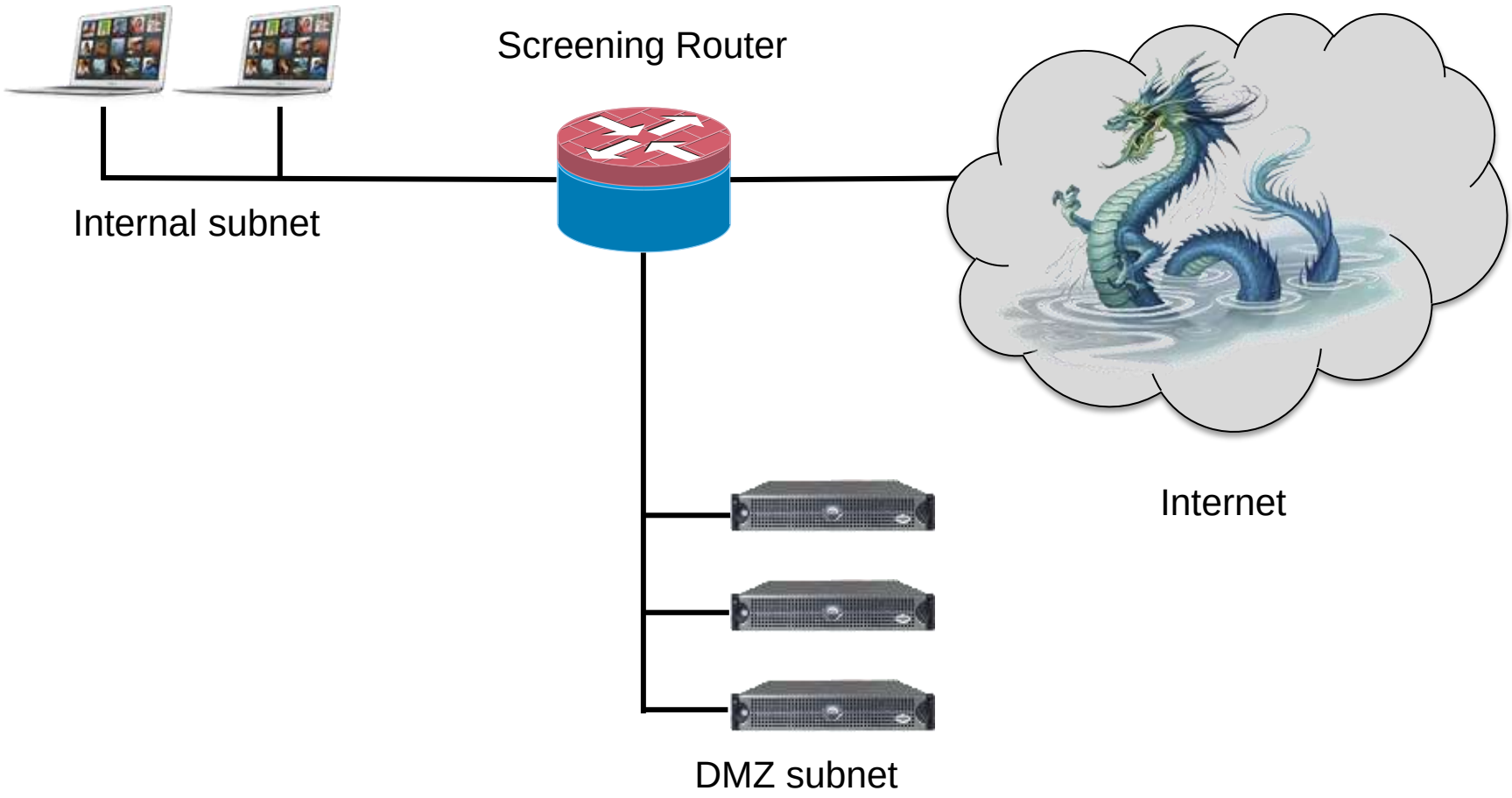
- Usually we don't worry about outbound traffic.
  - *Communication from a higher security network (internal) to a lower security network (Internet) is fine*

- Why might we want to restrict it?
  - Consider: if a web server is compromised & all outbound traffic is allowed, it can connect to an external server and download more malicious code
    ... or launch a DoS attack on the internal network
  - Also, log which servers are trying to access external addresses

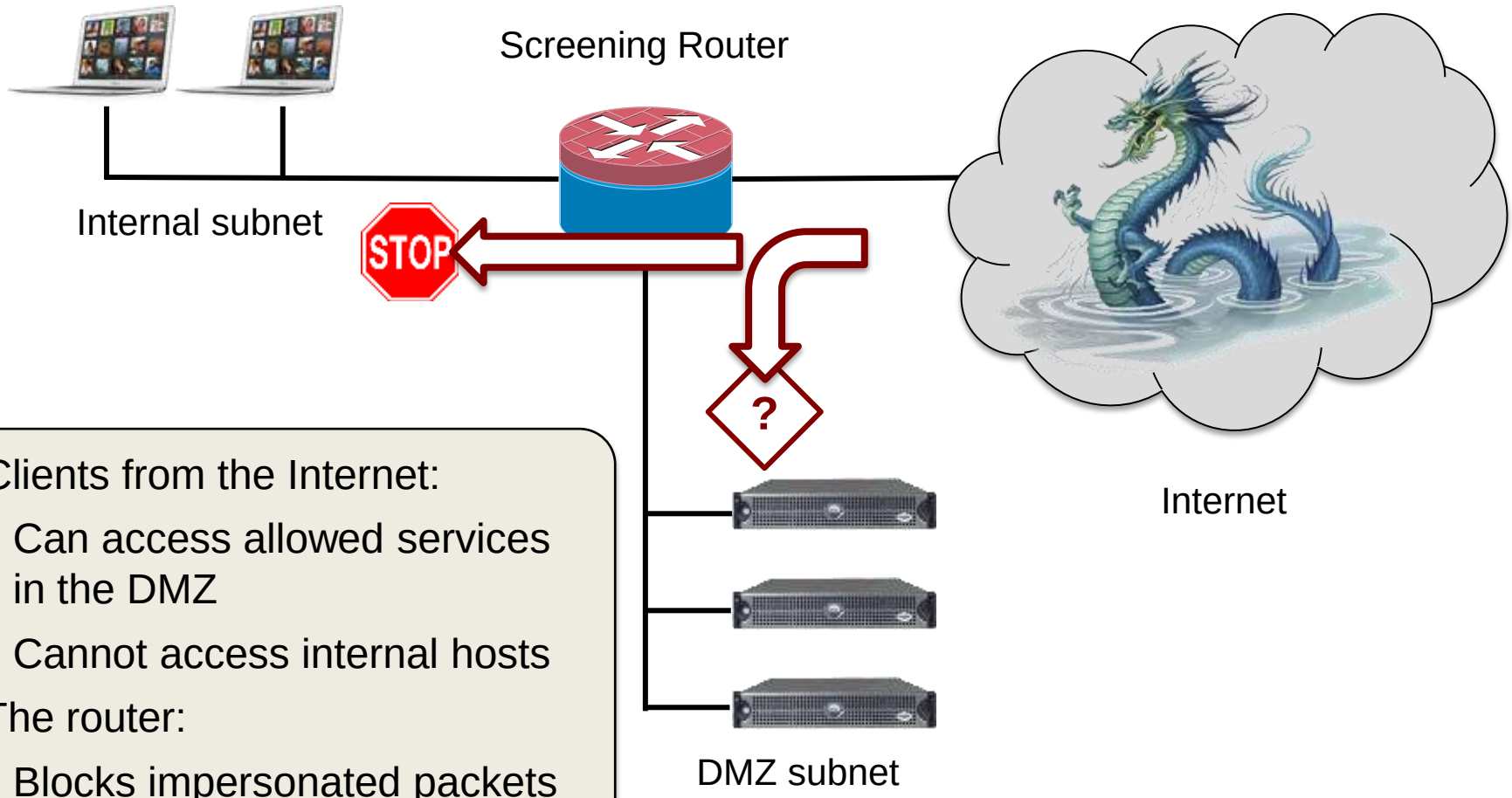
Stateful Inspection

- Retain state information about a stream of related packets
- Examples
  - TCP connection tracking
    - Disallow TCP data packets unless a connection is set up
  - ICMP echo-reply
    - Allow ICMP echo-reply only if a corresponding echo request was sent.
  - Related traffic
    - Identify & allow traffic that is related to a connection
    - Example: related ports in FTP

Network Design: DMZ



Network Design: DMZ



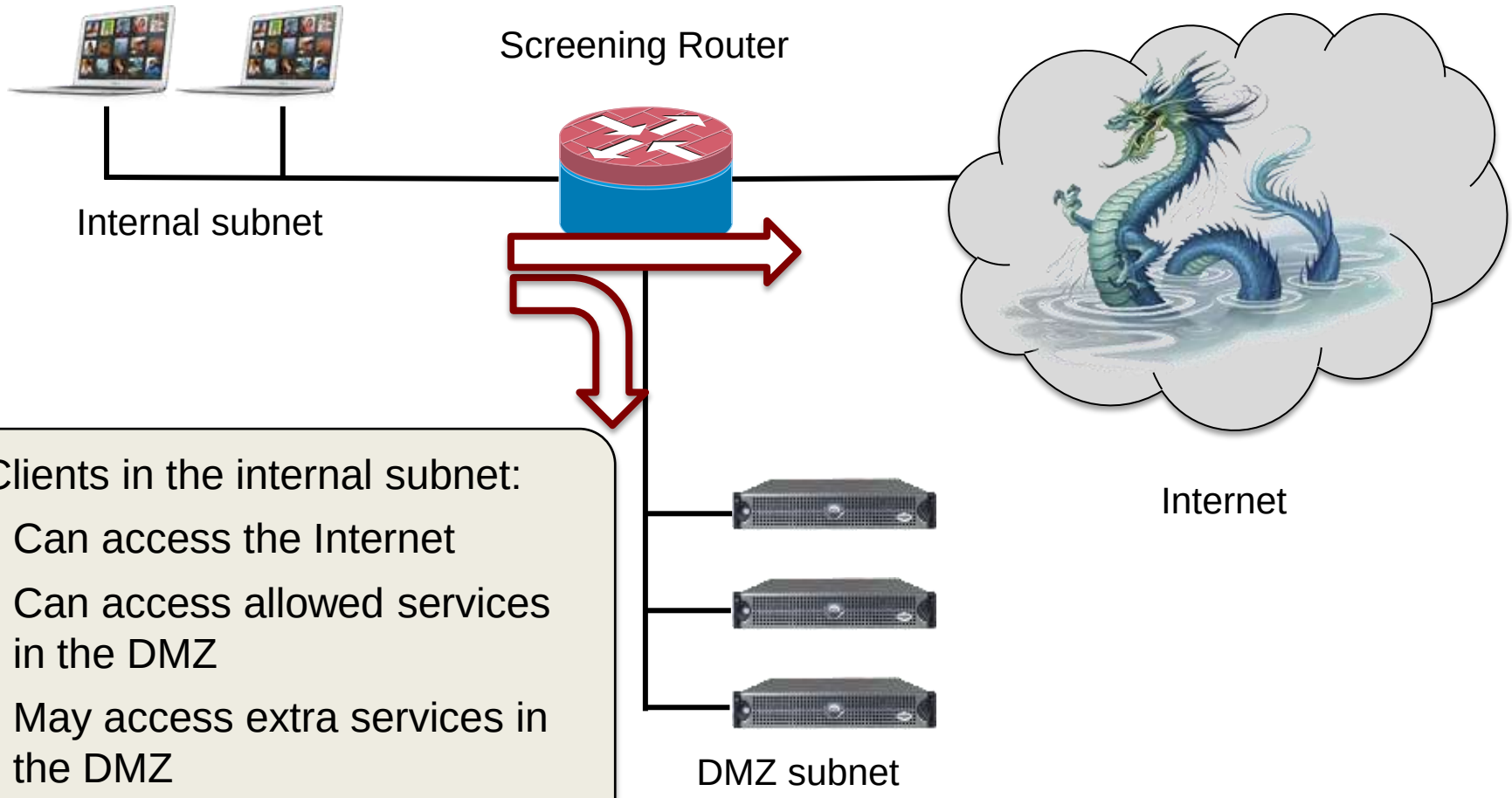
Clients from the Internet:

- Can access allowed services in the DMZ
- Cannot access internal hosts

The router:

- Blocks impersonated packets

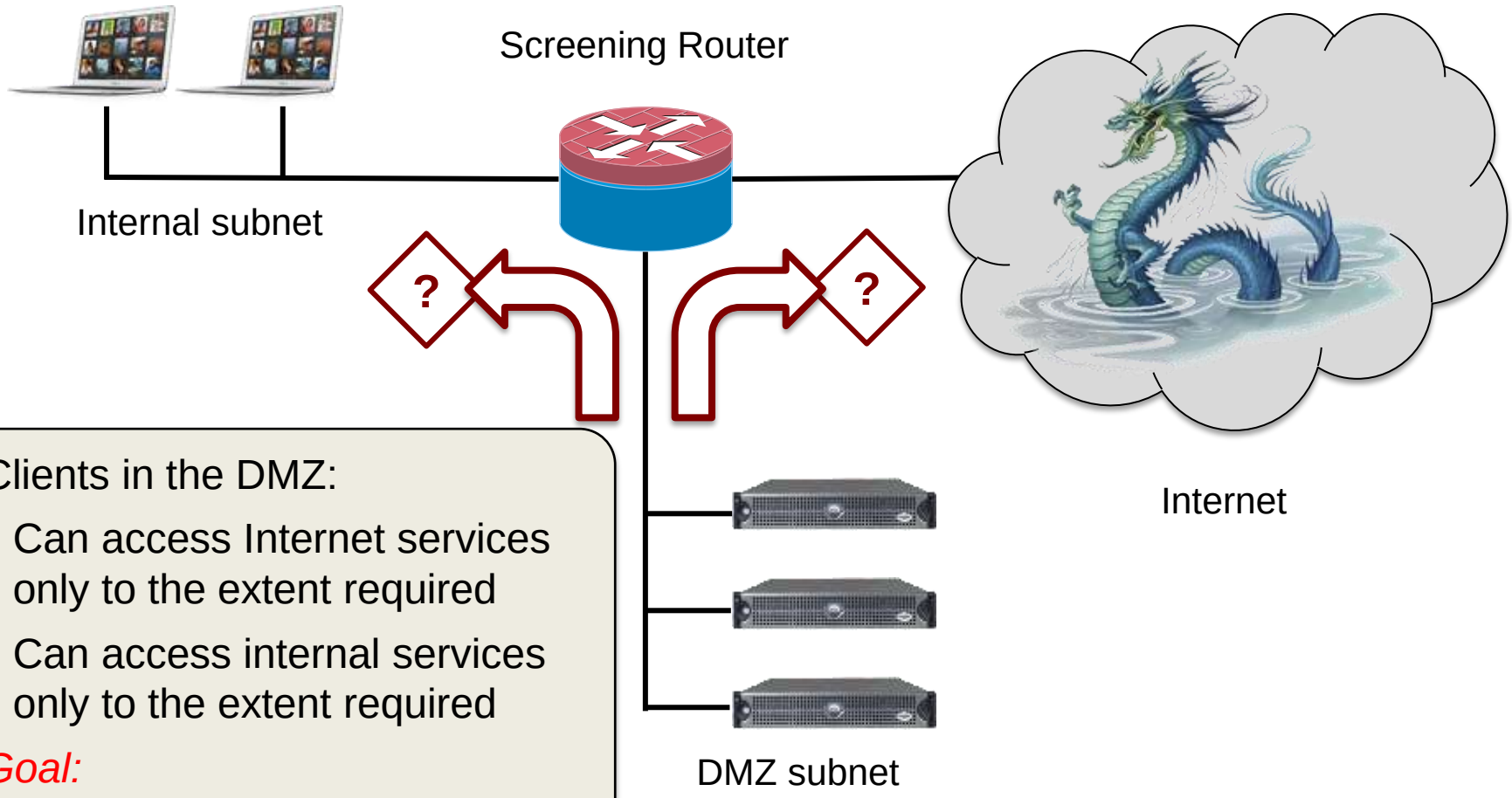
Network Design: DMZ



Clients in the internal subnet:

- Can access the Internet
- Can access allowed services in the DMZ
- May access extra services in the DMZ

Network Design: DMZ



Clients in the DMZ:

- Can access Internet services only to the extent required
- Can access internal services only to the extent required

Goal:
Limit possible damage if DMZ machines are compromised

Application-Layer Filtering

- Deep packet inspection
  - Look beyond layer 3 & 4 headers
  - Need to know something about application protocols & formats to do this
- Example
  - URL filtering
    - Normal source/destination host/port filtering +
      URL pattern/keywords, rewrite/truncate rules, protocol content filters
    - Detect ActiveX and Java applets; configure specific applets as trusted
    - Filter others from the HTML code

IDS/IPS

- Intrusion Detection/Prevention Systems
  - Identify threats and attacks

- Types of IDS
  - Protocol-based
  - Signature-based
  - Anomaly-based

Protocol-Based IDS

- Reject packets that do not follow a prescribed protocol
- Permit return traffic as a function of incoming traffic
- Define traffic of interest (filter), filter on traffic-specific protocol/patterns
- Examples
  - DNS inspection: prevent spoofing DNS replies: make sure they match IDs of DNS requests
  - SMTP inspection: restrict SMTP command set (and command count, arguments, addresses)
  - FTP inspection: restrict FTP command set (and file sizes and file names)

Signature-based IDS

- Don't search for protocol violations but for exploits in programming
- Match patterns of known “bad” behavior
  - Viruses
  - Malformed URLs
  - Buffer overflow code

Anomaly-based IDS

- Search for statistical deviations from normal behavior
  - Measure baseline behavior first

- Examples:
  - Port scanning
  - Imbalance in protocol distribution
  - Imbalance in service access

Application proxies

- Proxy servers
  - Intermediaries between clients and servers
  - Stateful inspection and protocol validation

External client Proxy server Real server

- Dual-homed host
- Bastion host

The End