UNSW AUSTRALIA

Operational Security: Firewall and IDS

Securing Wireless Networks, COMP4337/9337

Never Stand Still

Uzma Maroof

uzma.maroof@unsw.edu.au

CySPri Laboratory

http://cyspri.web.cse.unsw.edu.au/

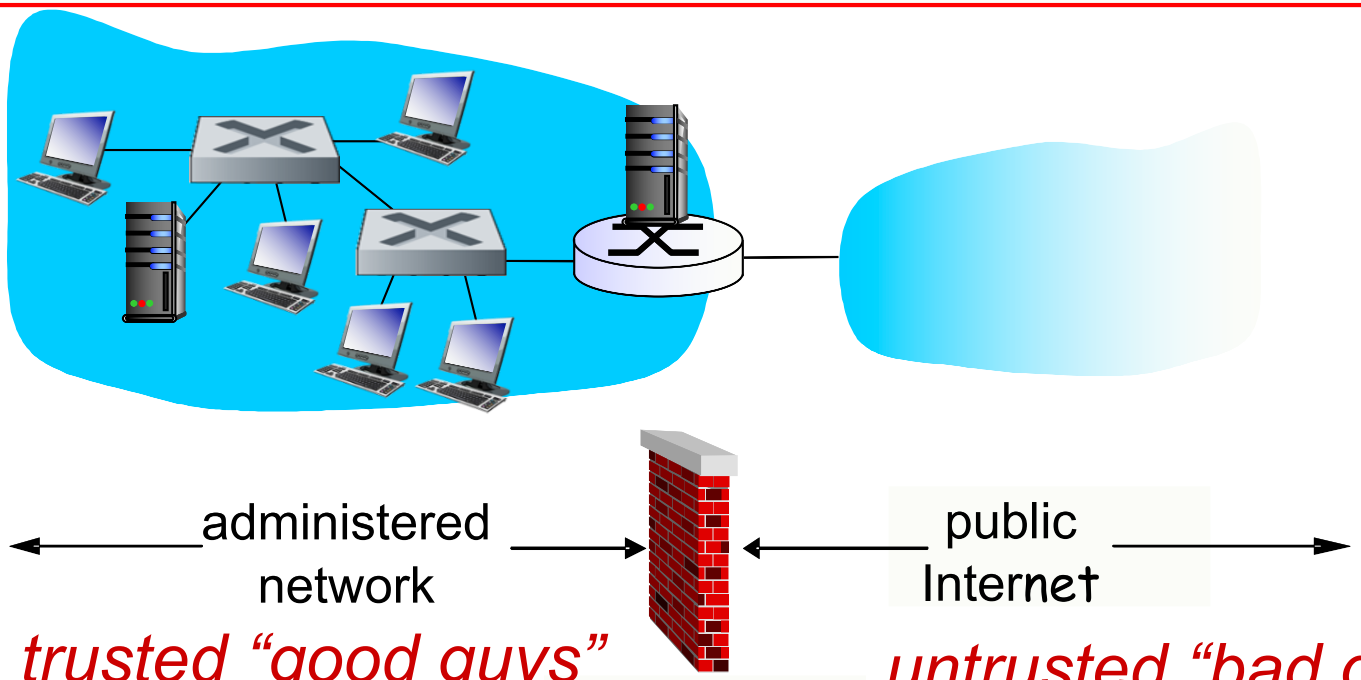
Operational Security

- World divides neatly into two camps:
- 1. Good guys?
  - Belong to the organization, should have access..
- 2. Bad guys?
  - Everyone else
  - Access must be scrutinized
- From medieval castles to modern cooperate office buildings…
  - There are always Entry/Exit points, where good and bad guys are security-checked
- How is this done in Computer Network Traffic?
- **Answer: Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS)**

Firewalls

firewall

isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others



administered network

trusted "good guys"

firewall

public Internet

untrusted "bad guys"

Firewalls: Goals

1. All traffic Outside to Inside, Inside to Outside passes through it
2. Only “authorized”??? traffic will be allowed to pass

   Defined by local security policy…
3. Firewall itself is immune to penetration

Firewalls: why

prevent denial of service attacks:

- SYN flooding: attacker establishes many bogus TCP connections, no resources left for “real” connections

prevent illegal modification/access of internal data

- e.g., attacker replaces CIA’s homepage with something else

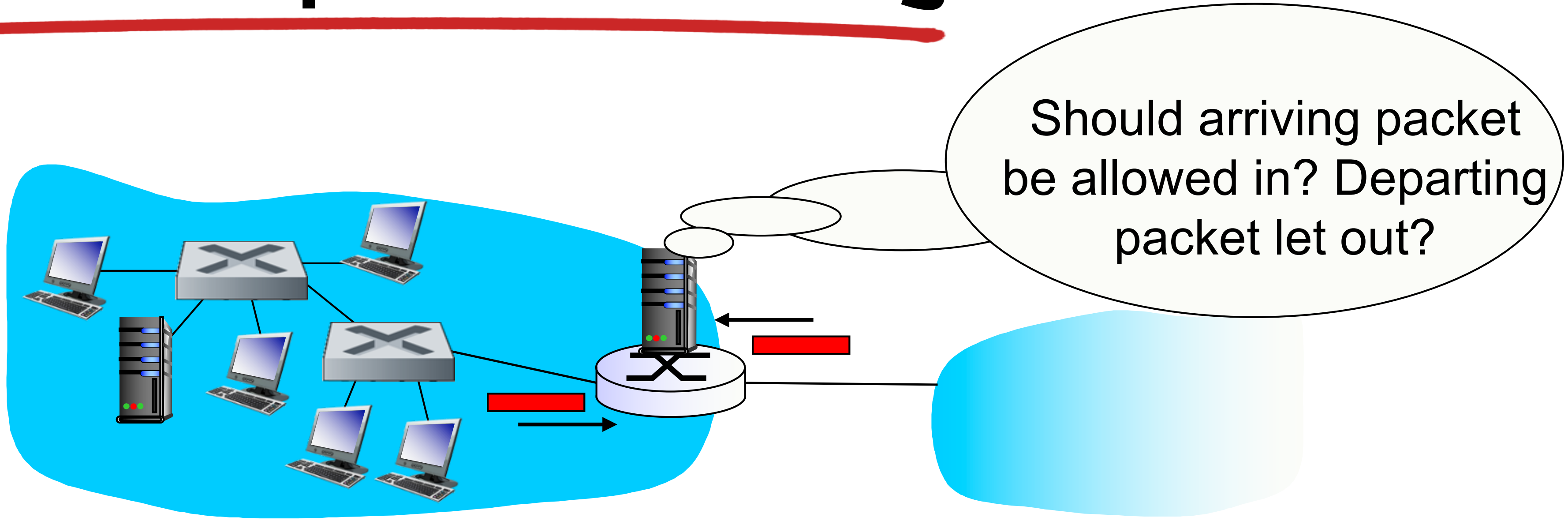
allow only authorized access to inside network

- set of authenticated users/hosts

three types of firewalls:

- stateless packet filters
- stateful packet filters
- application gateways

Stateless packet filtering



Should arriving packet be allowed in? Departing packet let out?

- Stateless??
- Makes decision on Packet-by-packet basis
- internal network connected to Internet via *router firewall*
- router *filters packet-by-packet,* decision to forward/drop packet based on???
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Stateless packet filtering: example

- *example 1:* block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23
  - *result??*
  - all incoming, outgoing UDP flows and telnet connections are blocked
- *example 2:* block inbound TCP segments with ACK=0.
  - *result??*
  - prevents external clients from making TCP connections with internal servers, but allows internal clients to connect to outside.

ACK = 0 in first segment in every TCP connection
ACK = 1 in all other segments

Stateless packet filtering: more examples

Policy	*Firewall Setting*
No outside Web access.	Drop all outgoing packets to any IP address, port 80
No incoming TCP connections, except those for institution’s public Web server only.	Drop all incoming TCP SYN packets to any IP except 130.207.244.203, port 80
Prevent Web-radios from eating up the available bandwidth.	Drop all incoming UDP packets - except DNS and router broadcasts.
Prevent your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a “broadcast” address (e.g. 130.207.255.255).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Access Control Lists

ACL for organization 222.22/16:

table of rules, applied top to bottom to incoming packets:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	[illegible]	80	any
allow	outside 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	[illegible]	[illegible]
allow	222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

Allows web surfing to internal users

Allows DNS packets to enter or leave the organization

Access Control Lists

What if a packet "arrives" with Source Port 80 and ACK = 1?

What if its sent without any prior TCP connection ?

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	[illegible]	[illegible]	ACK
allow	[illegible]	222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

SOLUTION: Block TCP ACK packets as well

But that prevents internal users from web-surfing

Stateless packet filtering

- *stateless packet filter:* heavy handed tool
  - admits packets that "make no sense," e.g., source port = 80, ACK bit set, **even though no TCP connection established:**

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

BETTER SOLUTION??
Keep Track of Connections
STATEFUL PACKET FILTERING

Stateful packet filtering

- *stateless packet filter:* heavy handed tool
  - admits packets that "make no sense," e.g., source port = 80, ACK bit set, **even though no TCP connection established:**

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- *stateful packet filter:* track status of every TCP connection
  - How does the firewall knows about a new connection setup?
    - SYN, SYNACK, ACK
  - determine whether incoming, outgoing packets "makes sense"
  - timeout inactive connections at firewall: no longer admit packets

Stateful packet filtering

- …3 ongoing connections…
- Who initiated these?
- From within the organization

source address	dest address	source port	dest port
222.22.1.7	37.96.87.123	12699	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

Stateful packet filtering

Connection should be checked for two of the rules

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

Stateful packet filtering

- *Packet Arrives:*
- *source port = 80, ACK =1*
- *dest port = 12543, Source IP = 150.23.23.155*

action	source address	dest address	protocol	source port	dest port	flag bit	check conxion
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	x

source address	dest address	source port	dest port
222.22.1.7	[illegible]	[illegible]	80
222.22.93.2	199.1.205.23	37654	80
222.22.65.143	203.77.240.43	48712	80

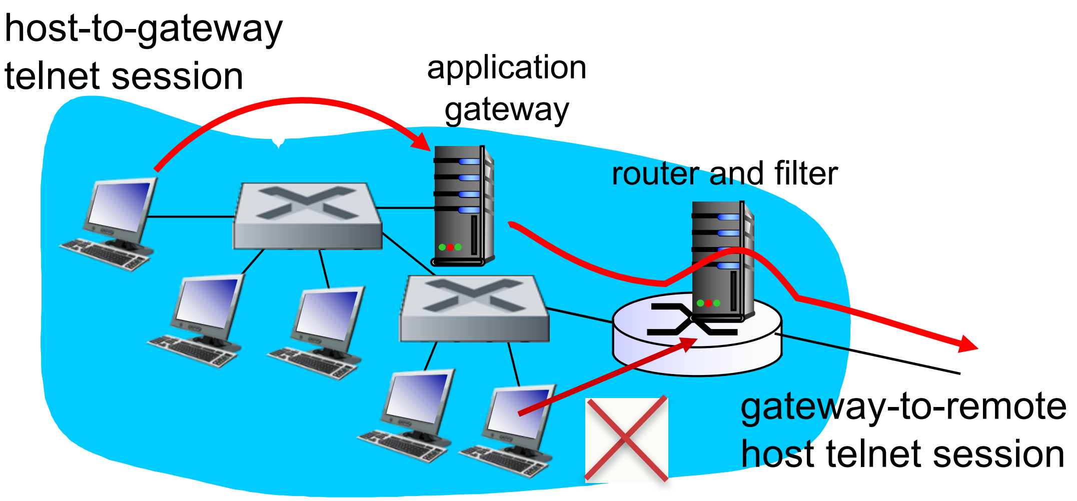
No existing connection found ==> Reject the packet

What if…

- Organization wants to provide Telnet service to a restricted set of internal users..
  - NOT some specific IP addresses..
- Also requires that users first authenticate before starting Telnet sessions..
- Beyond the capability of Stateful/Stateless filters
- User data is handled at which Layer?
- Application Layer

Application gateways

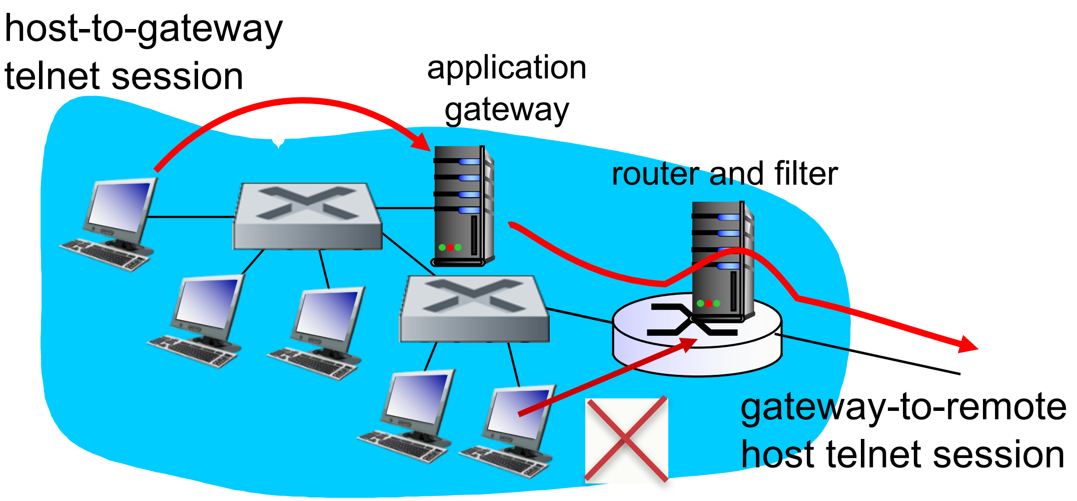
- An Application-specific server
- All application data MUST pass through it
- example: allow select internal users to telnet outside


host-to-gateway telnet session
application gateway
router and filter
gateway-to-remote host telnet session

1. require all telnet users to telnet through gateway.
2. for authorized users, gateway sets up telnet connection to dest host. Gateway relays data between 2 connections
3. router filter blocks all telnet connections not originating from gateway.

Application gateways

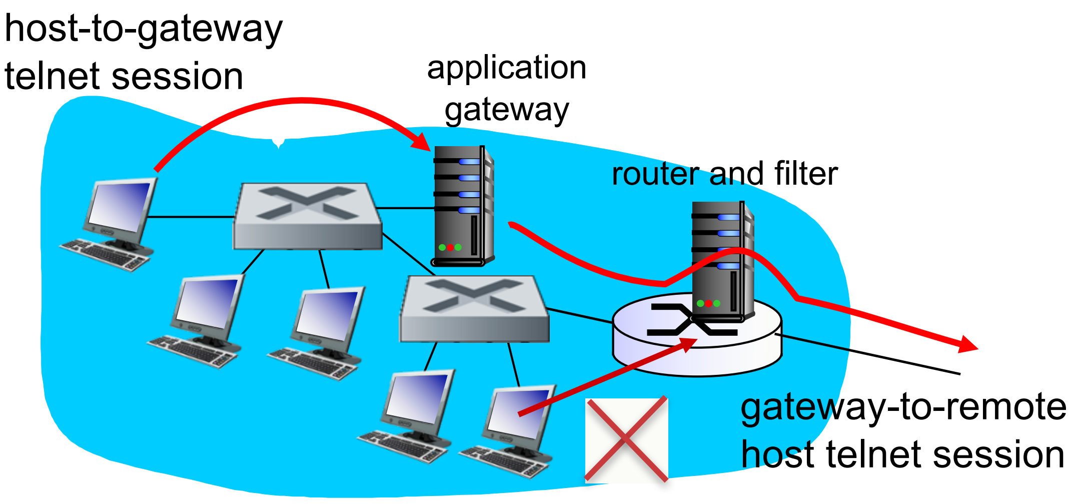
- Application running in AG, listens for incoming Telnet sessions
- Prompts users for username and passwords


host-to-gateway telnet session
application gateway
router and filter
gateway-to-remote host telnet session

- Internet networks can have multiple Application Servers
  - Telnet, HTTP, FTP, e-mail
- Organization’s email and Web-cache are Application Gateways

Application gateways

- Disadvantages?


host-to-gateway telnet session
application gateway
router and filter
gateway-to-remote host telnet session

- If multiple app's. need special treatment, each has own app. gateway
- Performance penalty
- Client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser

More Limitations of firewalls, gateways

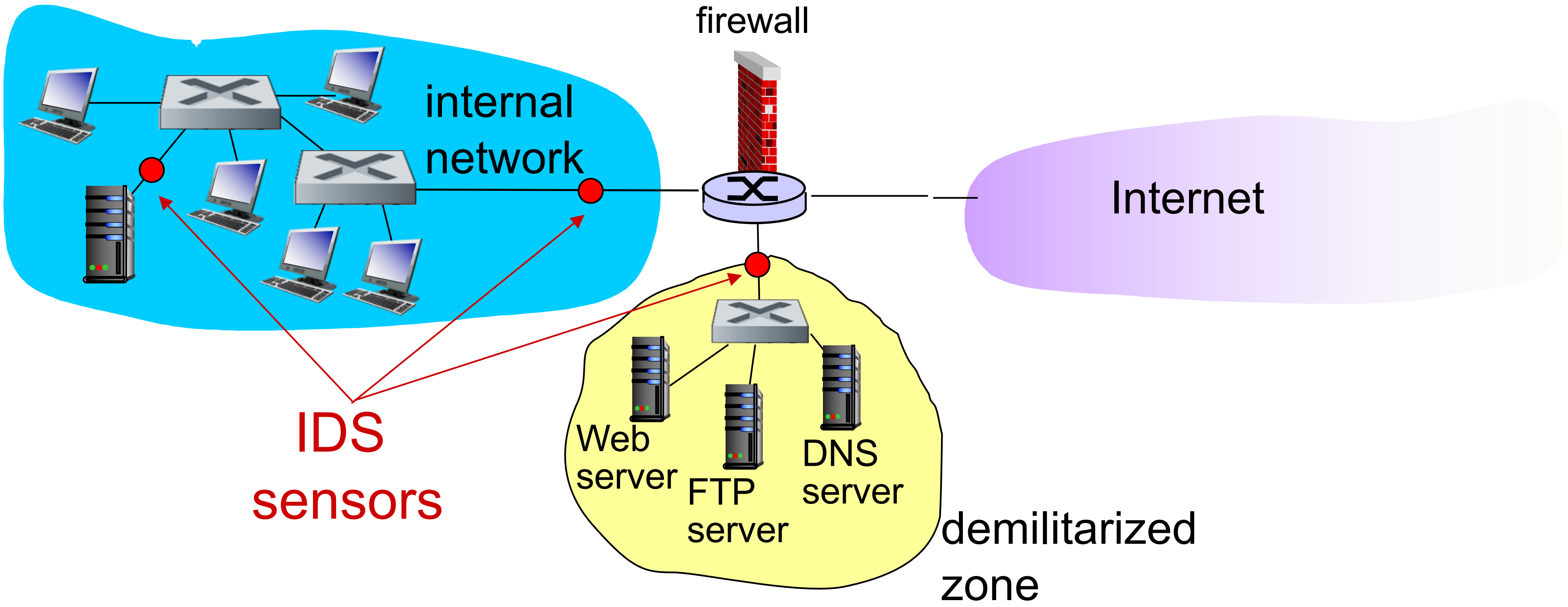
- *IP spoofing:* router can't know if data "really" comes from claimed source
- filters often use all or nothing policy for UDP
- *tradeoff:* degree of communication with outside world, level of security
- many highly protected sites still suffer from attacks

Intrusion detection systems

- Packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- *IDS: intrusion detection system*
  - *deep packet inspection:* look at packet contents
  - *examine correlation among multiple packets*

Intrusion detection systems

multiple IDSs: different types of checking at different locations



Intrusion detection systems

- Denial of Service
  - Attempts to crash a service or machine, overload network links, CPU, or fill up the disk, e.g. by sending lots of packets
- Port Scanning
  - Intruder sends packets to a list of ports trying to find open vulnerable ports. Next step could be to deliver malicious code at a vulnerable port.
- Securing Remote Shell Privileges
  - Intruder opens a shell on the victim machine, allowing arbitrary code execution.
- Network mapping
- Worms and Viruses
- OS vulnerability attacks

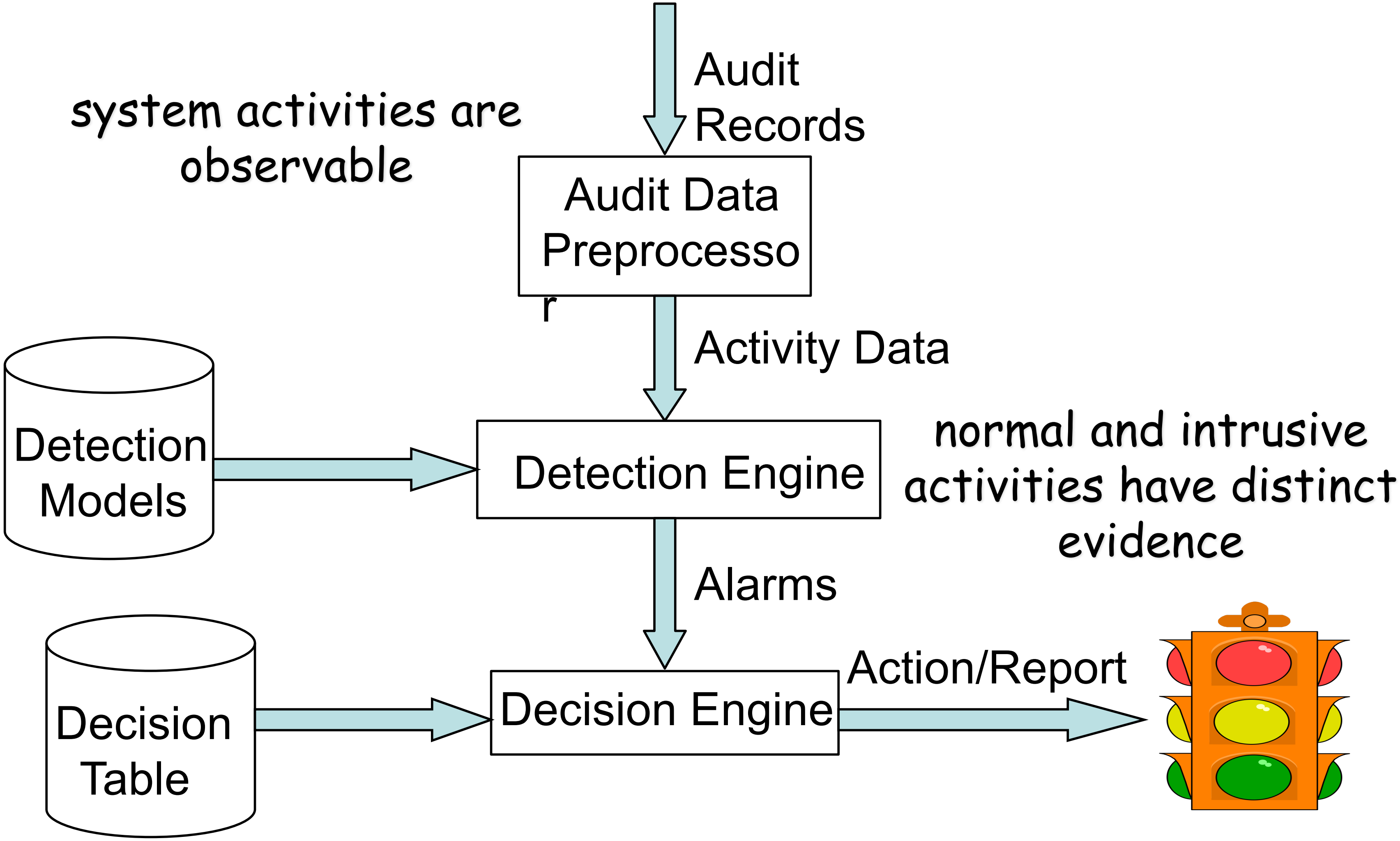
Intrusion detection systems

- Intrusion detection begins where the firewall ends.
- Preventing unauthorized entry is best, but not always possible.
- Threats can come from both outside and inside the network.

Elements of Intrusion Detection

- Primary assumptions:
  - System activities are observable
  - Normal and intrusive activities have distinct evidence
- Components of intrusion detection systems:
  - From an algorithmic perspective:
    - Features - capture intrusion evidences
    - Models - piece evidences together
  - From a system architecture perspective:
    - Various components: audit data processor, knowledge base, decision engine, alarm generation and responses

Components of Intrusion Detection System



system activities are observable

normal and intrusive activities have distinct evidence

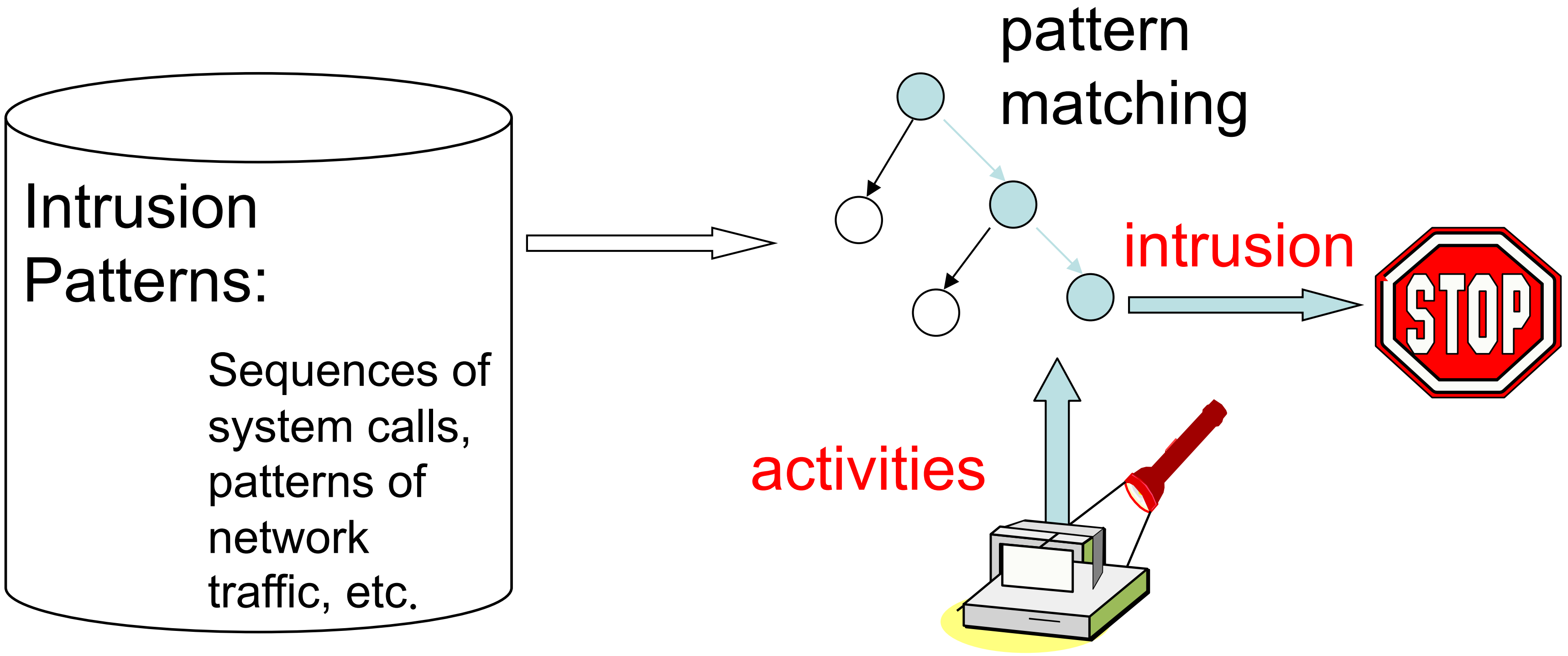
Intrusion Detection Approaches

- Modeling
  - Features: evidences extracted from audit data
  - Analysis approach: piecing the evidences together
    - Misuse detection (a.k.a. signature-based)
    - Anomaly detection (a.k.a. statistical-based)
- Deployment: Network-based or Host-based
  - Network based: monitor network traffic
  - Host based: monitor computer processes

Signature based IDS

- ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets, as an attack.
- Mostly based on Pattern Matching systems
- For example, an IDS that watches web servers might be programmed to look for the string “phf” as an indicator of a CGI program attack.
- The IDS might simply looks for a sub string within a stream of data carried by network packets.
- When it finds this sub string (for example, the ``phf'' in ``GET /cgi-bin/phf?''), it identifies those network packets as vehicles of an attack.

Signature based IDS



Intrusion Patterns:

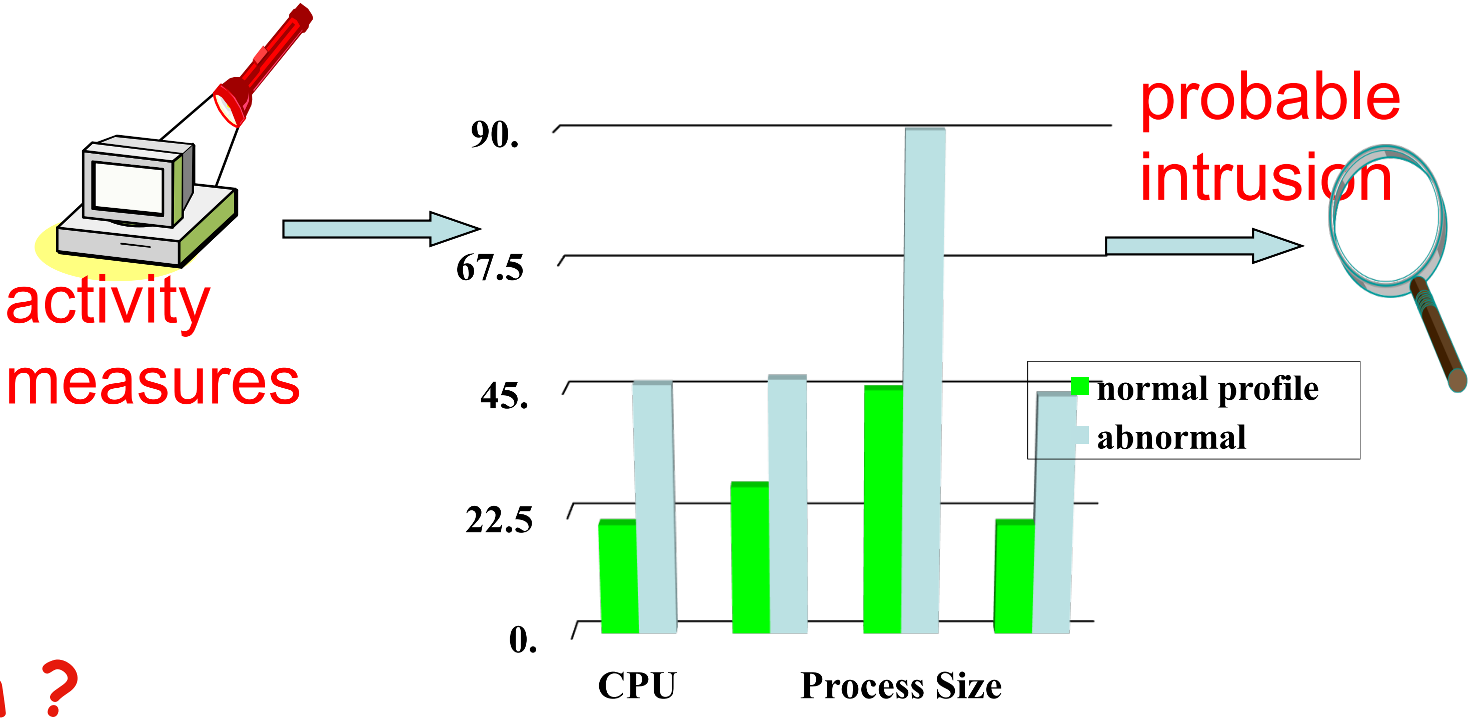
Sequences of system calls, patterns of network traffic, etc.

Example: ***if*** (traffic contains "x90+de[^\r\n]{30}")
then "attack detected"
Problems?

Can't detect new attacks

Anomaly Detection

Define a profile describing "normal" behavior, then detects deviations.


activity measures

probable intrusion

Any problem ?

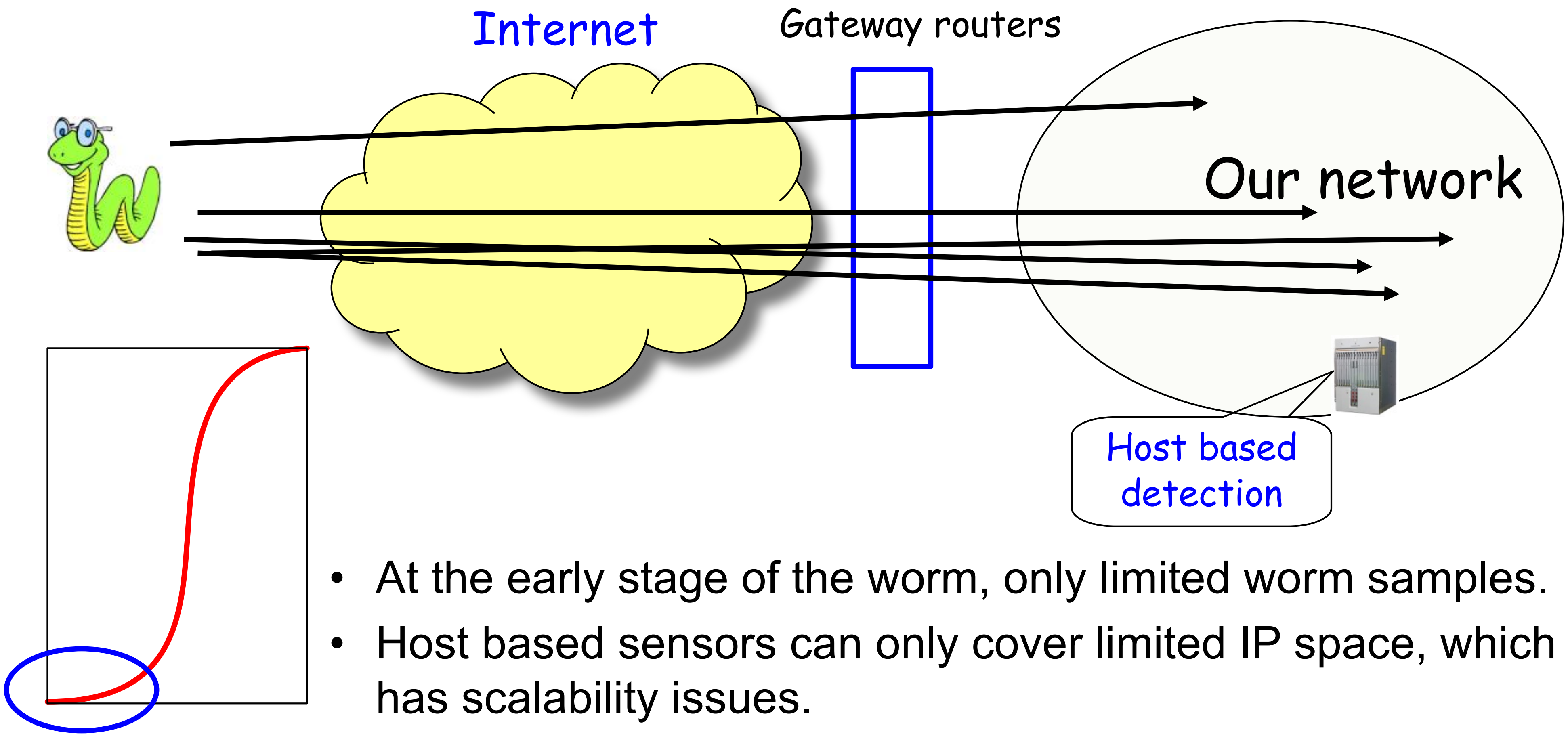
- Relatively high false positive rates
- Anomalies can just be new normal activities.
- Anomalies caused by other element faults
  - E.g., router failure or misconfiguration, P2P misconfig
- Which method will detect DDoS SYN flooding ?

Host-Based IDSs

- Use OS auditing and monitoring mechanisms to find applications taken over by attacker
    - Log all relevant system events (e.g., file/device accesses
    - Monitor shell commands and system calls executed by user applications and system programs
    - Pay a price in performance if every system call is filtered
- Problems:
    - User dependent: install/update IDS on all user machines!
    - If attacker takes over machine, can tamper with IDS binaries and modify audit logs
    - Only local view of the attack

symantec. McAfee Proven Security

Network Based IDSs



- At the early stage of the worm, only limited worm samples.
- Host based sensors can only cover limited IP space, which has scalability issues.
- Thus they might not be able to detect the worm in its early stage.

Network IDSs

- Deploying sensors at strategic locations
  - For example, Packet sniffing via tcpdump at routers
- Inspecting network traffic
  - Watch for violations of protocols and unusual connection patterns
  - Look into the packet payload for malicious code
- Limitations
  - Cannot execute the payload or do any code analysis !
  - Record and process huge amount of traffic
  - May be easily defeated by encryption