Operational Security: Firewalls and IDS

Never Stand Still

Guest Lecture

Dr Nadeem Ahmed

Outline

- Firewall
  - Stateless
  - Stateful
  - Application level gateways
- IDS
  - Host Based
  - Network based
- Snort

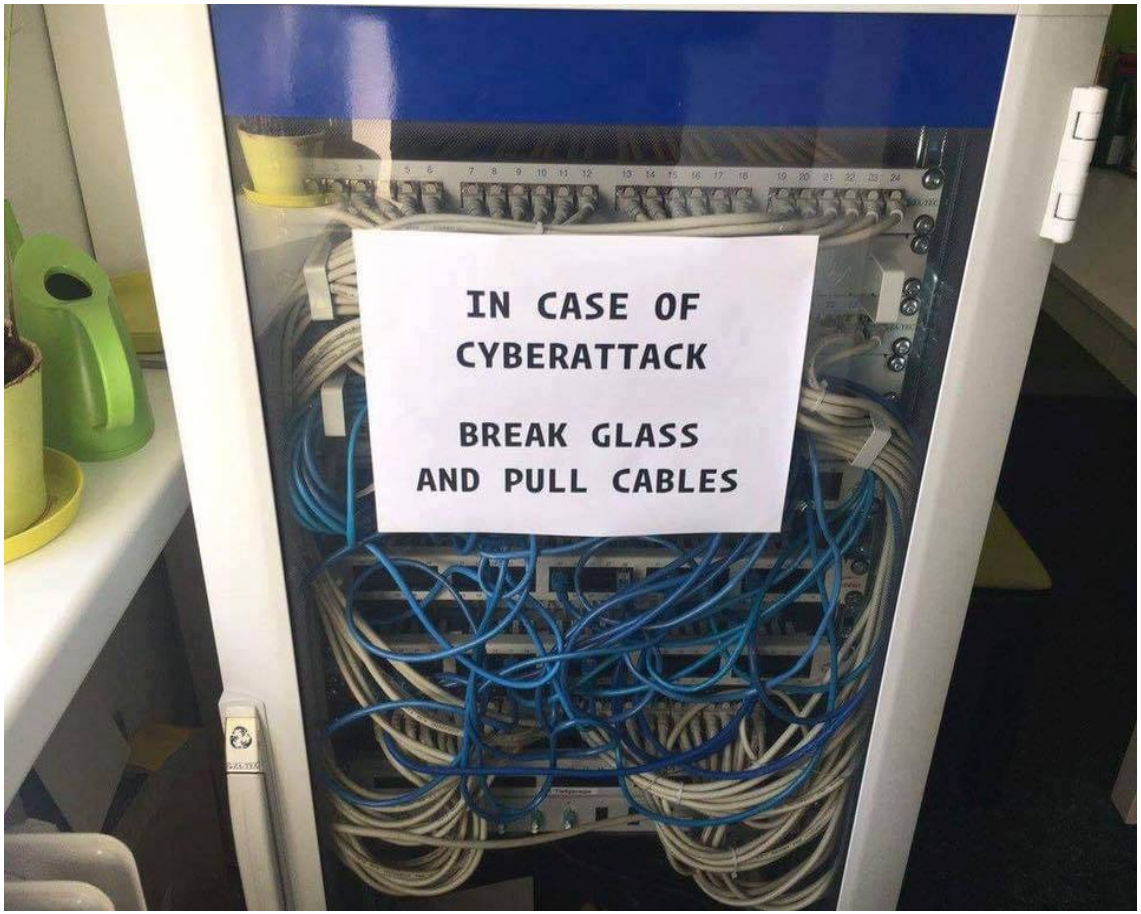
Secure System

The only system which is truly secure is the one which is switched off and unplugged, locked in a titanium lined safe, buried in a concrete bunker, surrounded by nerve gas and very highly paid armed guards

Even then I would not stake my life on it.

- Dr Eugene Spafford, Purdue University

Secure System



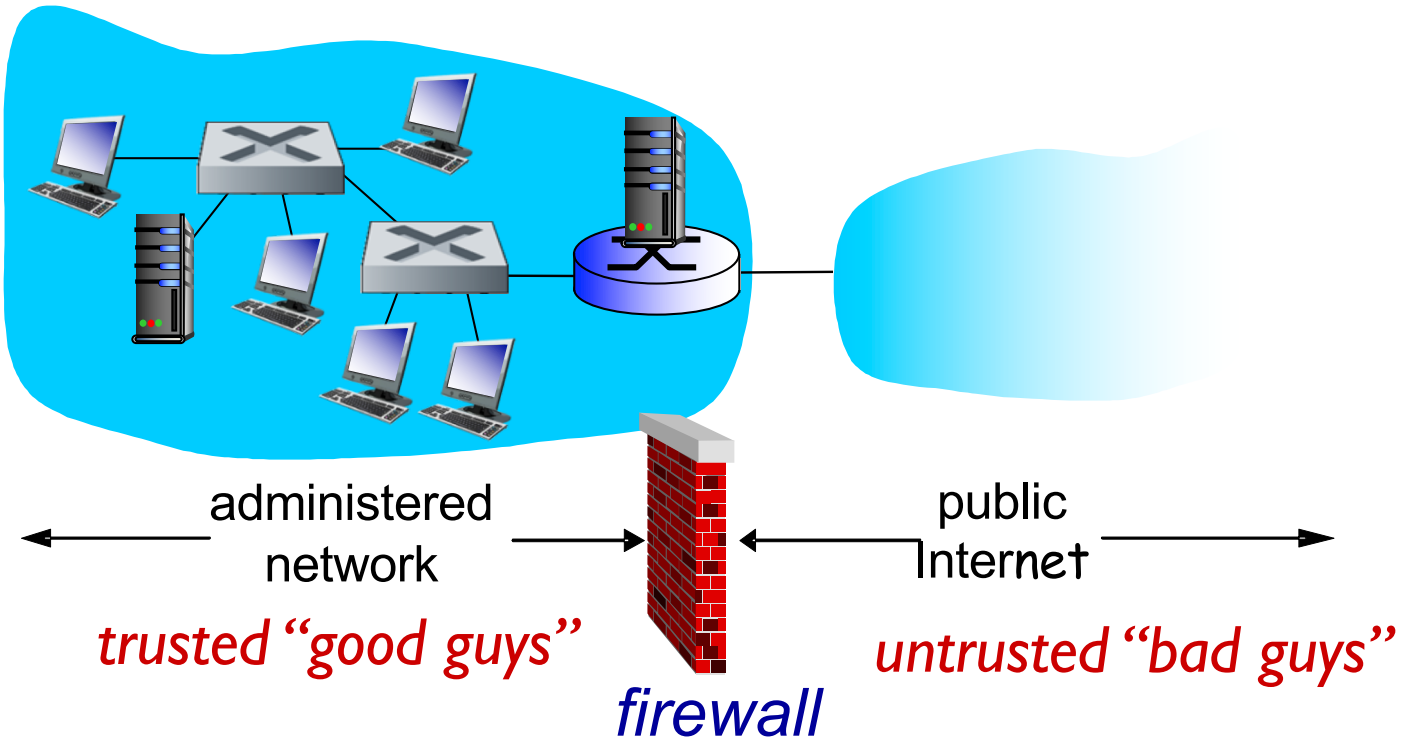
Firewalls

- Internet connectivity is essential but is vulnerable to threats
- Use firewall as a “Perimeter Defense” in part of a comprehensive security policy
- A firewall is a control point for monitoring and implementing access policies
  - Interconnects networks with different trusts

Firewalls

firewall

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



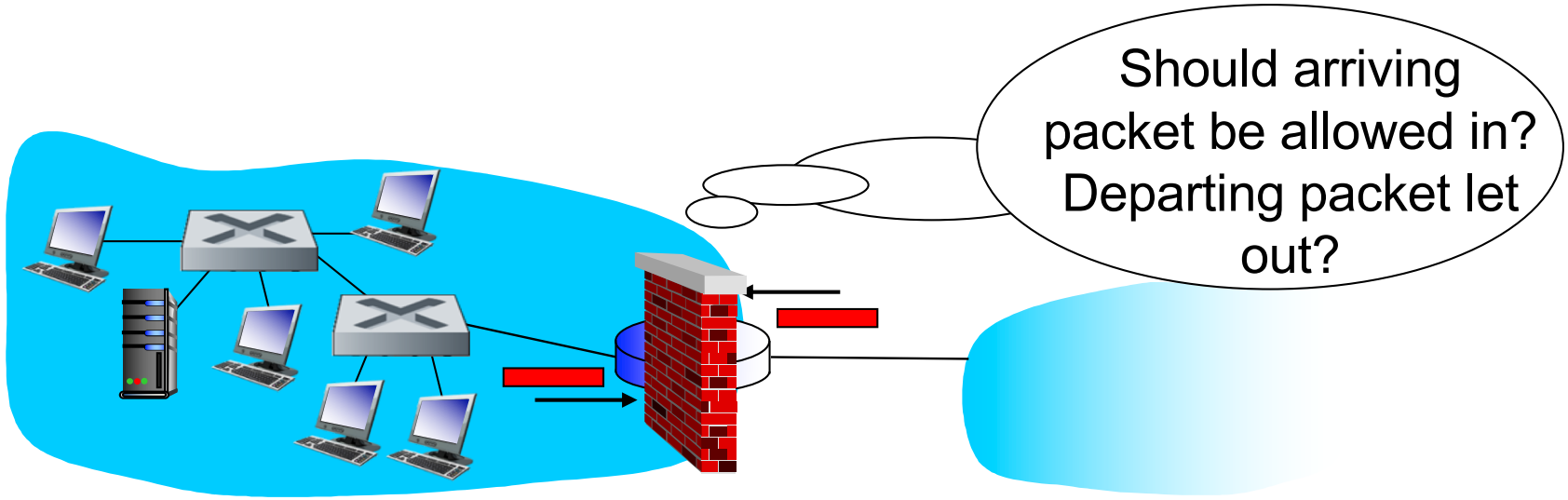
Firewalls: Why?

- 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
- Manage access for authorized users
  - which user is allowed to access what type of services outside of the intranet

Firewalls

- Three types of firewalls:
  - Stateless packet filters
  - Stateful packet filters
  - Application gateways

Stateless Packet Filters



- Internal network connected to the Internet via *router firewall*
- Firewall *filters packet-by-packet*, decision to forward/drop packet based on: 防火墙之所以防火是通过以下几点定制规则
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP flag bits (SYN, ACK, FIN)

Stateless Packet Filtering: Example

- Example 1: block incoming and outgoing datagrams with IP protocol field = 17, and with either source or dest port = 23 Protocol field = 17代表UDP 23端口代表telnet
  - result: all incoming, outgoing UDP flows and telnet connections are blocked
- Example 2: block inbound TCP segments with SYN = 1 & ACK = 0.
  - result: prevents external clients from making TCP connections with internal clients

Stateless packet filtering: more examples

Policy	*Firewall Setting*
No outside Web access.	Drop all outgoing packets to any IP address, port 80 (or HTTP ports)
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 your network from being used for a smurf DoS attack.	Drop all ICMP packets going to a "broadcast" address (e.g. 130.207.255.255/16).
Prevent your network from being tracerouted	Drop all outgoing ICMP TTL expired traffic

Access Control Lists (ACL)

ACL: table of rules, applied top to bottom to incoming packets: (action, condition) pairs [222.22/16 is the home network]

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	*
allow	outside of 222.22/16		TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.2	UDP	53	> 1023	----
deny	*	*	*	*	*	*

Allows Web Surfing to internal users

Allows DNS to operate

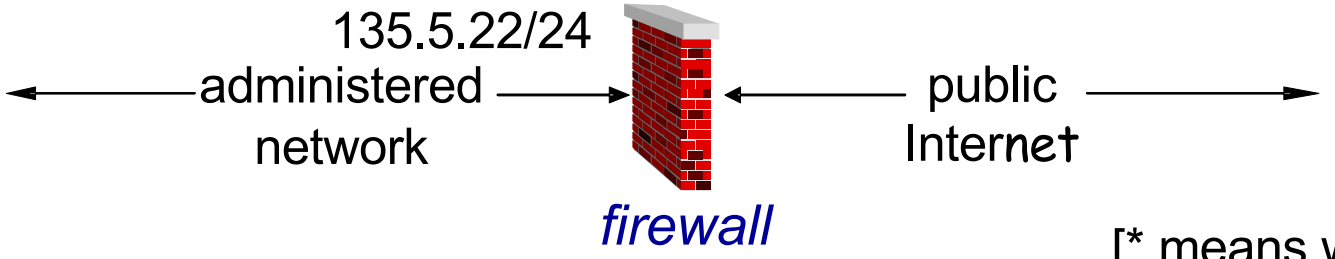
Access Control Lists

Two default policies:

- Discard/Deny – prohibit unless explicitly permitted
  - more conservative, controlled, services only added on case to case basis
- Forward/Allow – permit unless explicitly prohibited
  - Easier to manage but less secure

具体情況

Quiz on Stateless Packet Filter



[* means wild card/any]

action	source address	dest address	protocol	source port	dest port	flag bit
deny	222.22/16	*	*	*	*	*
allow	135.5.22.11/24	*	TCP	*	80	*
deny	135.5.22/24	*	TCP	*	80	*
allow	*	*	*	*	*	*

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 has been initiated

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 connection
  - track TCP connection setup (SYN), teardown (FIN): determine whether incoming, outgoing packets "makes sense"
  - timeout inactive connections at firewall: no longer admit packets

Stateful Packet Filtering

- ACL augmented to check connection state table before admitting packet for the rule

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	*	
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	*	*	*	*	*	*	

Stateful Packet Filtering

- ACL rule

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

- Connection table

source address	dest address	protocol	source port	dest port	Timer
222.22.2.2	199.1.205.1	TCP	12559	80	Valid
222.22.22.77	203.77.5.55	TCP	47855	80	Valid

Packet arrives: Source IP 199.5.5.20, Source port 80, ACK = 1,
Destination IP=222.22.2.2, Destination port = 36500

No existing connection found in Connection table: Reject the packet

Application Gateways

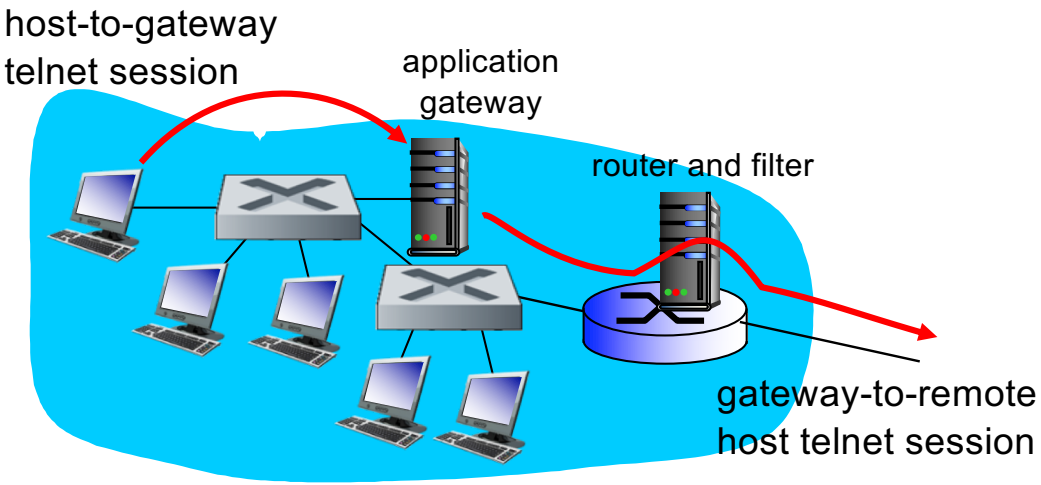
基于用户的访问而不是基于ip的访问

- Firewalls only read packet headers
- What if you want to allow user based access instead of host based (using IP addresses)?
  - Requires user authentication
  - This is beyond the capability of stateless/stateful filters

- Application layer is involved
  - overhead more than inspecting packets at the network and transport layers

Application Gateways

- An application specific filter
  - Example: allow select internal users to telnet outside
- AG prompts for username/passwords



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.

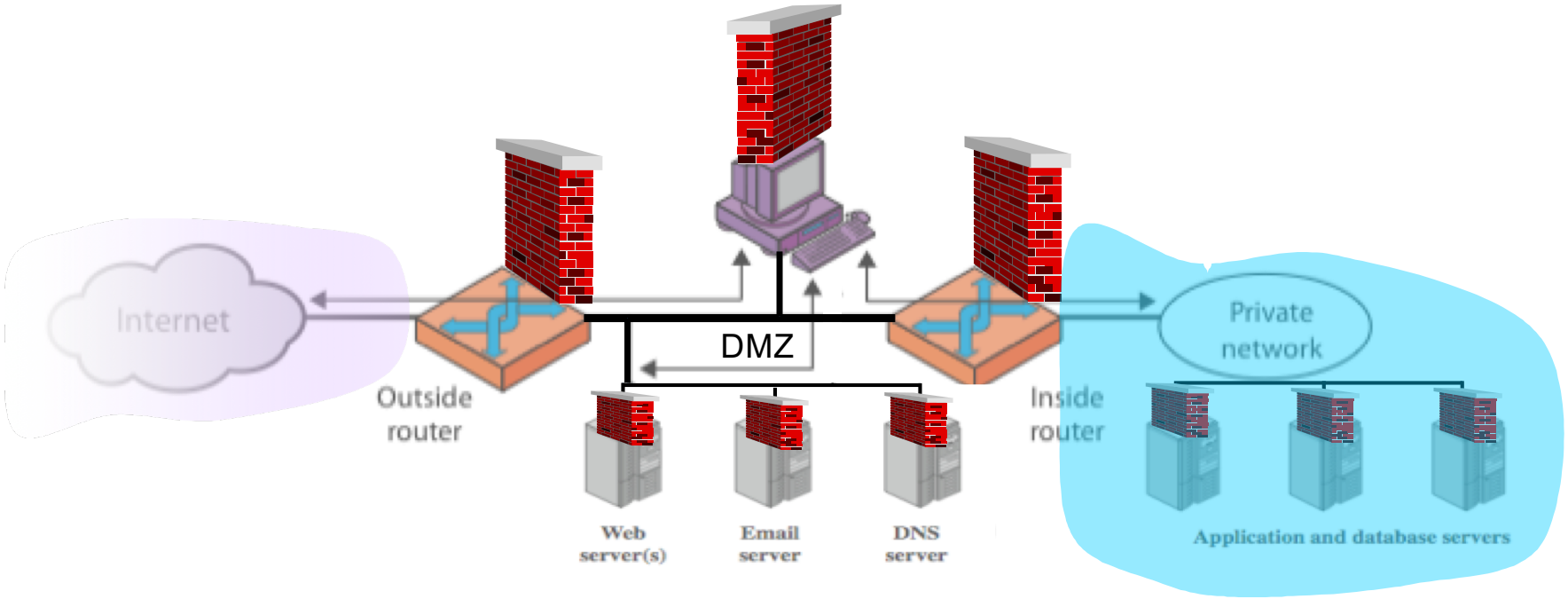
Host based Firewalls

- A software module to secure an individual host
- Available in many OS and often used in servers

- Can tailor filtering rules to match the host environment
- Independent of the network topology
- Provides additional layer of protection

就是在两个防火墙之间在设立一个非军事
隔离区,用来与外网交互,二其与内网以一种安全的方式交互

Firewall Configurations



- DMZ: De Militarized Zone that hosts organisation's external facing services
- Outside router only advertises servers in the DMZ

Limitations of firewalls/gateways

Text

- IP spoofing: router can't know if data "really" comes from claimed source
- if multiple app's. need special treatment, each has own app. gateway
- client software must know how to contact gateway.
  - e.g., must set IP address of proxy in Web browser
- 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

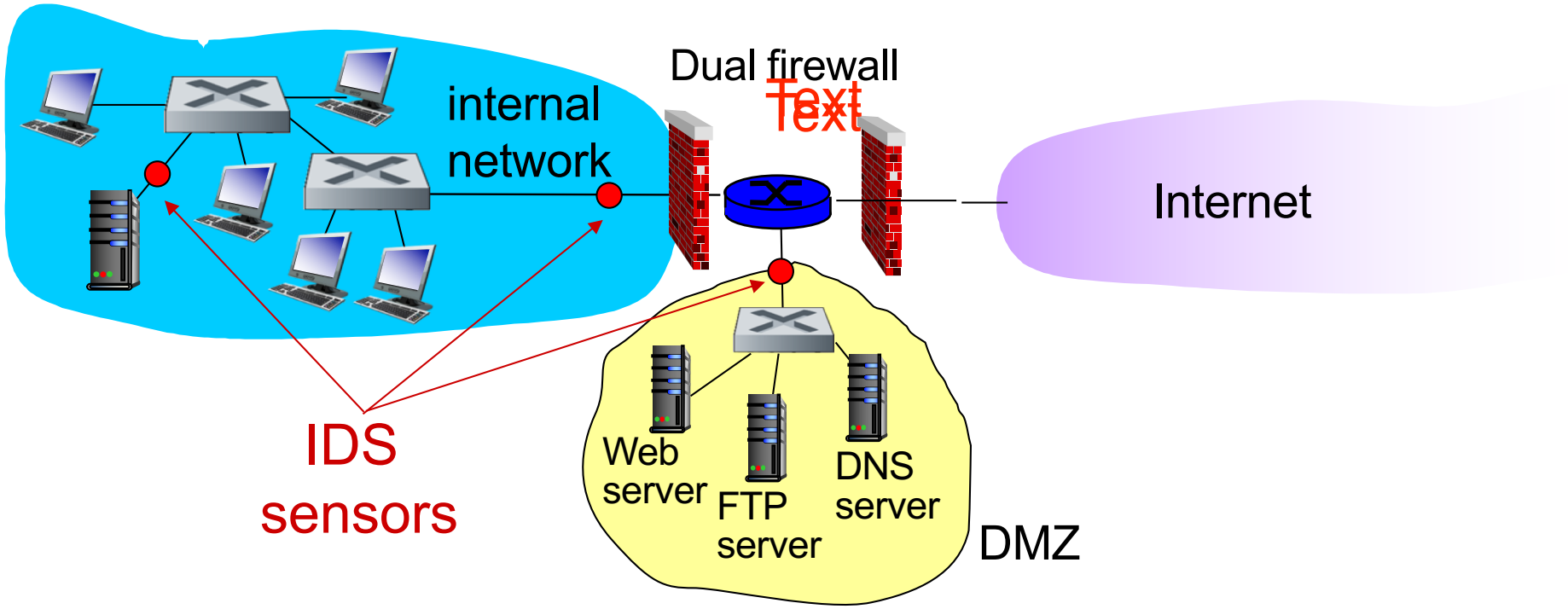
- Packet filtering:
  - operates on TCP/IP headers only
  - no correlation check among sessions
- IDS: intrusion detection system
  - deep packet inspection: look at packet contents (e.g., check character strings in packet against database of known virus, attack strings)
  - examine correlation among multiple packets
    - port scanning
    - network mapping
    - DoS attack

包过滤只是
操作在tcp/ip的header上
没有相关检查在sessions期间

ids
还要检查包里的内容
还要相关性检查
端口扫描
网络映射检查
拒绝服务检查

Intrusion detection systems

multiple IDSs: different types of checking at different locations



Intrusion detection systems

- Intrusion [RFC 2828 Internet Security Glossary]
  - A security event or a combination of security events in which an intruder gains or attempts to gain, access to a system (or system resources) without having authorization to do so
  - Intruder may be from outside the network or a legitimate user of the network
  - Intruder attacks range from gentle (just looking around) to the serious (reading privileged data, perform un-authorized modifications, disrupt services etc.)
- Intrusion detection
  - A security service that monitors and analyzes system events for the purpose of finding, and providing real-time or near real-time warning of attempts to access system resources in an un-authorized manner

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, viruses, trojans
- OS vulnerabilities attacks

Text

Intrusion Techniques

- Target identification and information gathering
  - OSINT (Open Source Intelligence)
  - Nmap
- Gaining Access
  - Vulnerability identification
  - Acquire passwords (guess or brute force)
  - Install reverse shell
- Privilege Escalation
  - Exercise access rights of owner

Intrusion Techniques

- Motivated by thrill of access and status
  - hacking community a strong meritocracy
  - status is determined by level of competence

- Benign intruders might be tolerable
  - do consume resources and may slow performance
  - can't know in advance whether benign or malign

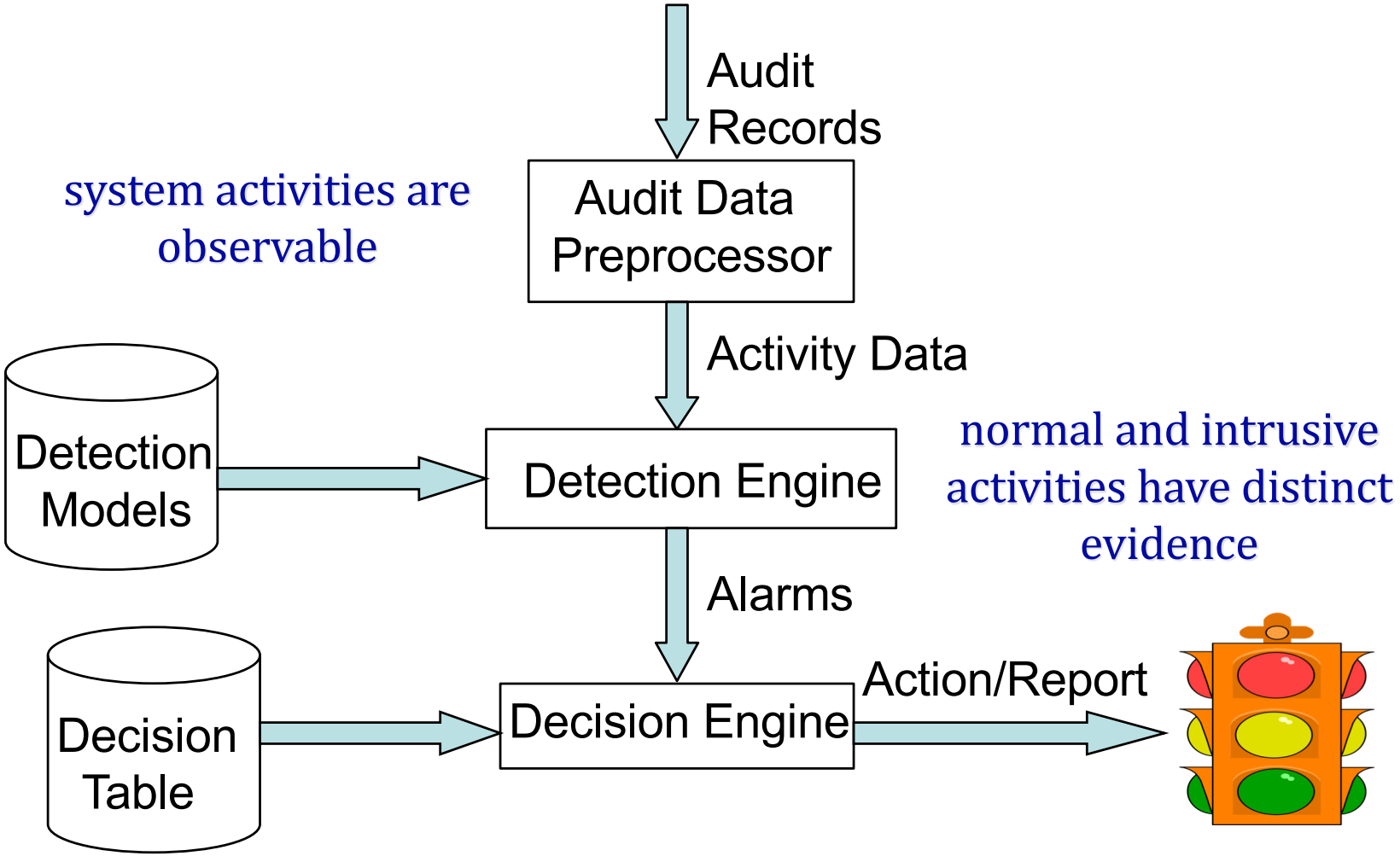
- Awareness led to establishment of Computer Emergency Response Teams (CERTs)
  - collect / disseminate vulnerability info / responses
  - hackers also have access to CERT reports

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



Elements of Intrusion Detection

- Audit
  - Recording of all security relevant events of a supervised system
  - Collects the input for intrusion detection module

- Audit data delivers information on:
  - Who accessed?
  - When, where and how?
  - Who's and which resource?

- Audit data requires integrity protection
  - Attacker can wipe out traces of malicious behavior

Intrusion Detection Approaches

- 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)

Signature based IDS

- Uses predefined proper (or bad) set of rules and patterns
  - Event audit analysis reveals signatures for known past attacks

- ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets as an attack

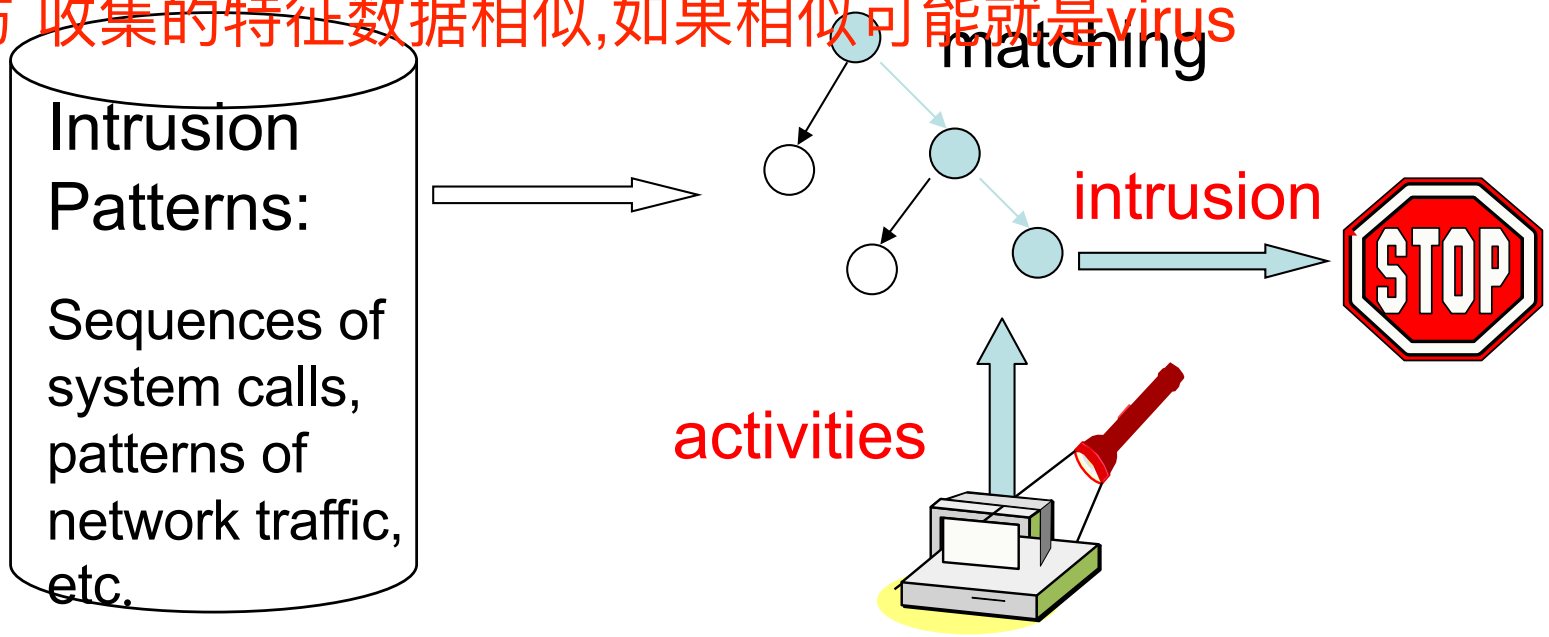
- Mostly based on Pattern Matching systems
  - An IDS that watches web servers might be programmed to look for the string “phf” as an indicator of a CGI program attack (for example, the ``phf'' in ``GET /cgi-bin/phf?'')

Signature based IDS

这种是基于标志的入侵检测

,就是查看网络数据包是否含有某些头信

测特征是否与 收集的特征数据相似,如果相似可能就是virus



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

"attack detected" 就是用grep来找到标志位

Problems?

Can't detect new attacks

Signature based IDS

Drawbacks:

- Requires prior knowledge of potential attacks and only work if the attack signature is in the database
- Signature database requires continuous updating
- Higher rate of “false negative” with outdated database

Anomaly based IDS

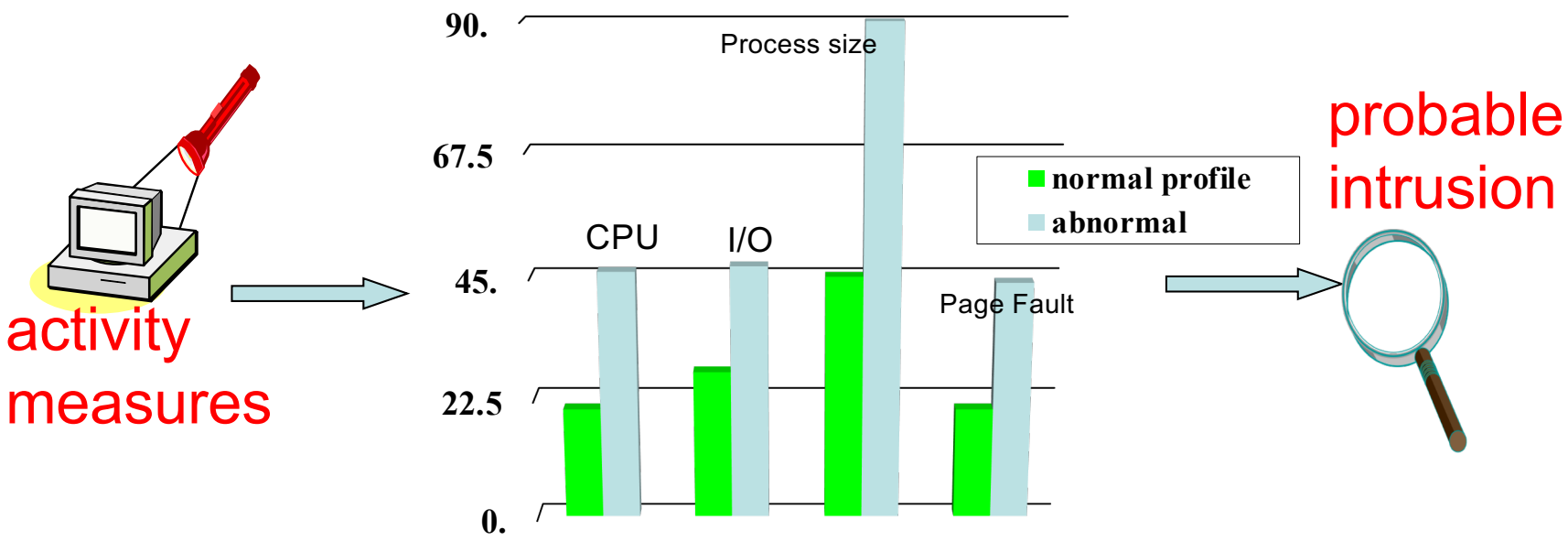
- Consider normal/expected behavior of legitimate users over a period of time; apply statistical tests to detect intruder

- Intruder unlikely to mimic the behavior pattern of the legitimate user
  - Profile based (time/duration/IP for login)
  - Threshold based (various events such as %age of ICMP traffic)

- An attack scenario needs not to be defined a priori

异常检测是更具是先定义一组系统“正常”情况的数值，如CPU利用率、内存利用率、文件校验和等（这类数据可以人为定义，也可以通过观察系统、并用统计的办法得出），然后将系统运行时的数值与所定义的“正常”情况比较，得出是否有被攻击的迹象。这种检测方式的核心在于如何精确定义所谓的“正常”情况。

Anomaly Detection



- Define a profile describing normal behavior, then detect deviations

Anomaly Detection

- Relatively high “false positive” rates
  - Anomalies could be just new normal activities
  - Anomalies caused by other elements faults e.g., router misconfigurations

- Privacy of users
  - Collecting specific user patterns
  - Work related and personal habits

- ”false negative”, if a normal behavior pattern matches an attack pattern

IDS Deployment

- Network based
  - Monitor network traffic
- Host based
  - Monitor single host activity and computer processes
- Hybrid
  - Permits combined analysis of system events and network traffic

Host based IDS

- Specialized software to monitor system activity for detecting suspicious behavior
  - 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

Network IDS

- NIDS monitors traffic at selected points on a network
  - In near real-time to detect intrusion patterns
- Deploying sensors at strategic locations
  - 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
  - Easily defeated by encryption

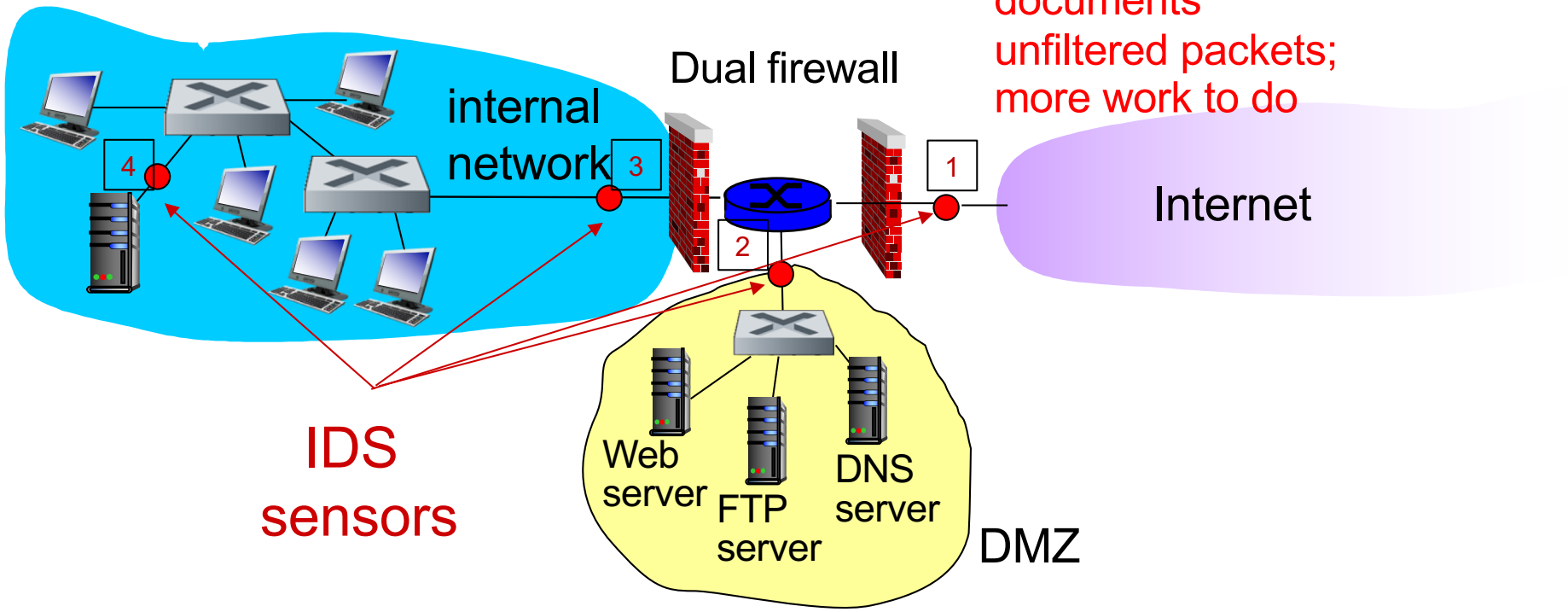
NIDS Deployment

4. Special IDS to provide additional protection for critical systems

3. protect major backbones; monitor internal/external attacks

2. monitor filtered packets

1. monitor and documents unfiltered packets; more work to do



Wireless IDS

- Wireless inherent characteristics provide the relative ease of accessing (and injecting) network communications
  - Each frame is broadcasted
- On the other hand, there are complexities involved in monitoring wireless communications
  - 2 common frequency bands (5GHz and 2.4GHz)
  - Several channels within each band
- A wireless sensor can monitor a single channel at a time
  - A sensor will miss malicious activity occurring on other channels when it is monitoring one particular channel
  - Attacker can launch attack simultaneously on two different channels

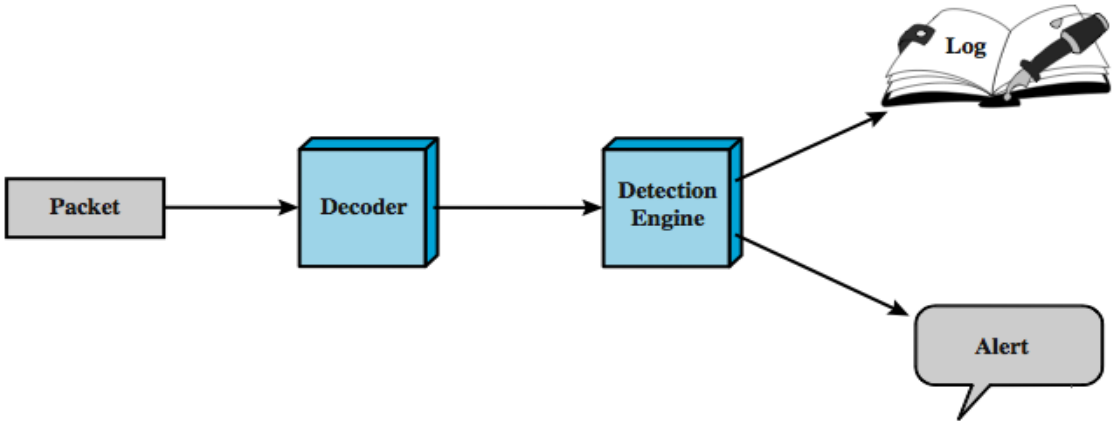
Wireless IDS

- Wireless sensors normally perform channel scanning
  - They can monitor each channel a few times per second
    - Attacker can attack in short bursts on un-scanned channels
  - Each sensor sees only a fraction of the activity on each channel
    - Forensics data is incomplete
- Wireless IDS can use specialized hardware with multiple radios and antennas
- The actual range of the wireless sensor depends on the surrounding facilities, location of people within the facility and other changing characteristics

Snort IDS

- An open source light weight IDS
  - Real time packet capture and rules analysis
  - Can work in inline or passive modes

- Components:
  - Decoder
  - Detector
  - Logger
  - Alerter



SNORT Rules

- use a simple, flexible rule definition language
- each rule consists of a fixed header and zero or more options

  action protocol SIP Sport <dir> DIP Dport [options]

Action	Description
alert	Generate an alert using the selected alert method, and then log the packet.
log	Log the packet.
pass	Ignore the packet.
drop	Drop the packet and log.
reject	Drop the packet, log it, and then send a TCP reset if the protocol is TCP or an ICMP port unreachable message if the protocol is UDP.
sdrop	Silently drop the packet but do not log.

  - Last three actions only in inline mode
  - Protocols supported : TCP, UDP, IP & ICMP
  - Direction -> & < >

SNORT Rule Options (subset)

meta-data
msg Defines the message to be sent when a packet generates an event. **reference** Defines a link to an external attack identification system, which provides additional information. **classtype** Indicates what type of attack the packet attempted. **sid** Signature ID for the rule
payload
content Enables Snort to perform a case-sensitive search for specific content (text and/or binary) in the packet payload. **depth** Specifies how far into a packet Snort should search for the specified pattern. Depth modifies the previous content keyword in the rule. **offset** Specifies where to start searching for a pattern within a packet. Offset modifies the previous content keyword in the rule. **nocase** Ignore case. Nocase modifies the previous content keyword in the rule.
non-payload
ttl Check the IP time-to-live value. This option was intended for use in the detection of traceroute attempts. **id** Check the IP ID field for a specific value. Some tools (exploits, scanners and other odd programs) set this field specifically for various purposes, for example, the value 31337 is very popular with some hackers. **dsize** Test the packet payload size. This may be used to check for abnormally sized packets. In many cases, it is useful for detecting buffer overflows. **flags** Test the TCP flags for specified settings. **seq** Look for a specific TCP header sequence number.
post-detection
logto Log packets matching the rule to the specified filename. **session** Extract user data from TCP Sessions. There are many cases where seeing what users are typing in telnet, rlogin, ftp, or even web sessions is very useful.

SNORT Rules

log udp any any -> 192.168.1.0/24 1:1024

Log UDP traffic with any source IP any source port and destination is any IP within 192.168.1.0/24 and destination port any port less than and equal to 1024

alert tcp any any -> any any (flags: SF; msg: "Possible SYN FIN scan";)

Alert if both SYN and FIN flags set at the same time

alert tcp any any -> any any (msg:"Possible exploit"; content:"|90|"; offset:40; depth:75; dsize: >6000;)

Alert for NOP instructions between bytes 40 and 75 of the data portion of a packet and payload size is > 6000 bytes.

Reading list

Kurose Ross, Computer Networking: A Top-Down Approach, Chapter 8

CyBoK Network Security Knowledge Area

https://www.cybok.org/media/downloads/Network_Security_KA_-_Issue_1.0_January_2019.pdf

Firewall Best Practices

https://www.net.in.tum.de/fileadmin/TUM/NET/NET-2016-09-1/NET-2016-09-1_01.pdf

NIST Guide to Intrusion Detection and Prevention Systems

https://csrc.nist.gov/publications/detail/sp/800-94/final

Snort Manual

http://manual-snort-org.s3-website-us-east-1.amazonaws.com