الجامعة الافتراضية السورية

أمن الشبكات
Network and Infrastructure Security

د. محمد العصورة

Dr. Mohammed Assora

دكتوراه في امن شبكات الحواسب

PhD. In Computer Network Security

Objectives of Lecture

- Examine some types of network security technologies
- Understand how these security technologies work,
- Understand what type of threats can be stopped by each type
- Understand the limitation (what they cannot do) of each type

Contents

1. Firewalls

- What is a Firewall?
- What types of Firewall are there?
- What use are Firewall?
- How are Firewalls configured?
- What problems do Firewalls introduce?
- What do not Firewalls do?
- How do you get round Firewalls
- Firewalls in context

What is a Firewall?

- A Firewall is a network security device designed to restrict access to resources (information or services) according to security policy.

- Firewall is not a magic solution to network security problems, nor are they a complete solution for remote attacks or authorised access to data

What is a Firewall?

- A firewall is a network security device
- It serves to connect two parts of a network to control the traffic (data) which is allowed to flow between them.
- Often installed between an entire organisation's network and the Internet
- Can also protect smaller departments

Where does a Firewall go?

- A Firewall must be the single path of communication between protected and unprotected networks
- A firewall can only filter traffic which passes through it
- If traffic can get to a network by other means, the Firewall cannot block it

What different types of Firewall are there?

There are four basic types:

1. Packet filter
2. Circuit-level proxy
3. Stateful packet filter
4. Application-level proxy

Packet filter

TCP/IP packet filtering router

A router which can throw packets away

Examines TCP/IP headers for every packet going through the Firewall, in either direction

Choice of whether to allow or block packet based on:

1. IP source and destination address
2. TCP/UDP source and destination ports

Packet filter

- Rules specify which packets are allowed through the Firewall, and which are dropped
- Rules must allow for packets in both directions
- Rules may specify source /destination IP address and source/destination TCP/UDP port numbers
- Certain (common) protocols are very difficult to support security (eg. FTP)
- Low level of security

Circuit-Level proxy

- TCP/IP proxy server
- Packet are received and go no further
- Proxy software generates new packets
- New packets go to destination

Circuit-level proxy

- Similar to packet filter, except that packets are not routed
- Incoming TCP/IP packets accepted by proxy
- Rules determine which connections will be allowed and which blocked
- Allowed connections generate new connection from Firewall to server
- Similar specification of rules as packet filter
- Low-medium level of security

Stateful packet filter

- TCP/IP packet filtering router
- Same as packet filter, except initial packets in one direction are remembered, and replies are automatically allowed for
- Simpler rules than packet filter
- Support more layer-7 protocols than a simple packet filter can

Stateful packet filter

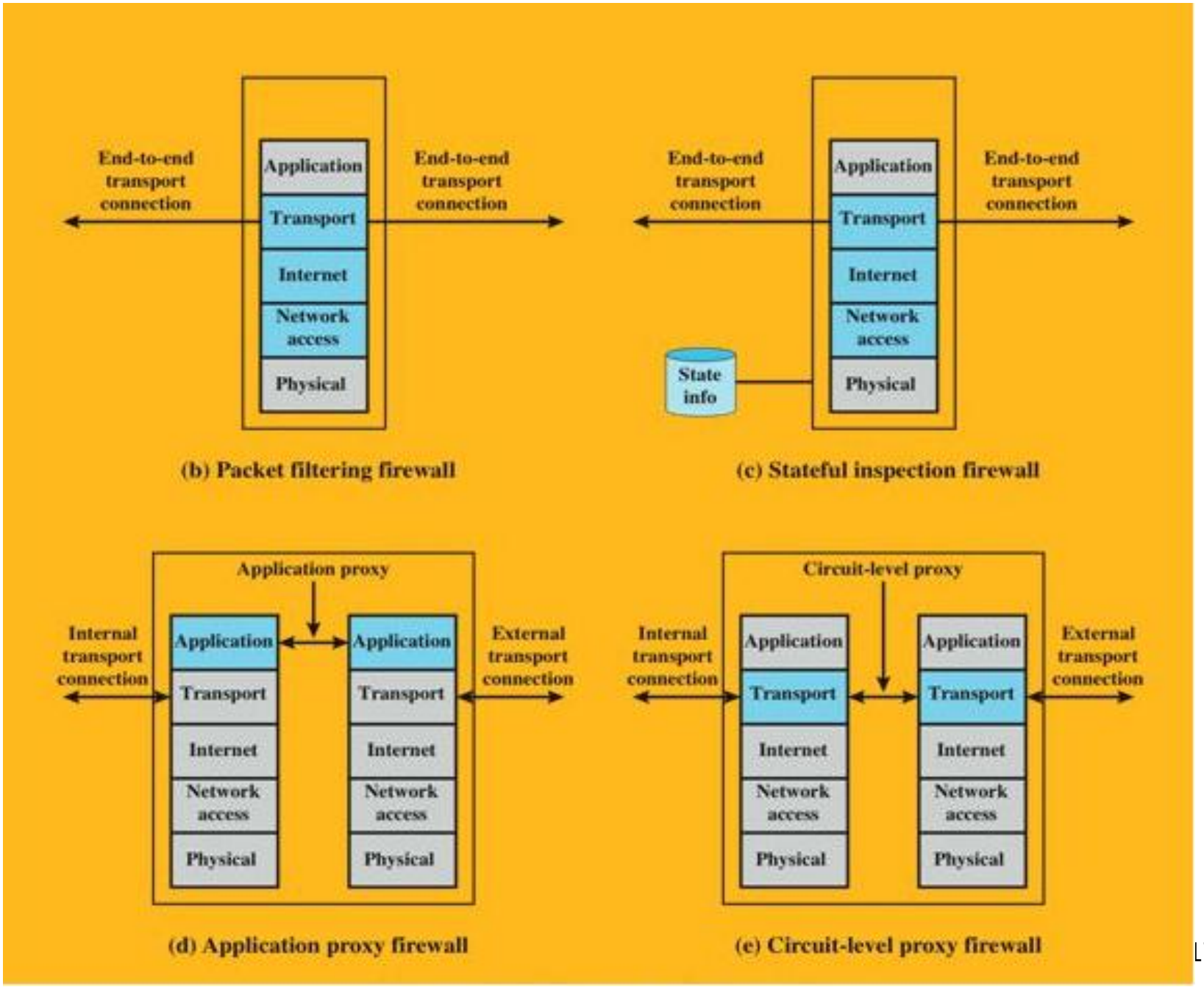
- Packet filter which understands request and replies (eg: for TCP: SYN, SYN-ACK, ACK)
- Rules need only specify packets in one direction (from client to server-the direction of the first packet in a connection)
- Replies and further packets in the connection are automatically processed
- Support wider range of protocols than simple packet filter (eg: FTP)
- Medium-High level of security

Application-level proxy

- Layer-7 proxy server
- Client and server in a single machine
  - For every supported application protocol such as SMTP, POP3, HTTP, SSH, FTP,…
- Packet are received and processed by server
- New packets generated by client

Application level proxy

- Complete server & client implementation in one box for every protocol which can be expected through it
- Client connect to Firewall
- Firewall validate request
- Firewall connects to server
- Response comes back through Firewall and is also processed through client/server
- Large amount of processing per connection
- High level of security


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection
(b) Packet filtering firewall
End-to-end transport connection
Application
Transport
Internet
Network access
Physical
State info
End-to-end transport connection
(c) Stateful inspection firewall
Application proxy
Internal transport connection
Application
Transport
Internet
Network access
Physical
Application
Transport
Internet
Network access
Physical
External transport connection
(d) Application proxy firewall
Circuit-level proxy
Internal transport connection
Application
Transport
Internet
Network access
Physical
Application
Transport
Internet
Network access
Physical
External transport connection
(e) Circuit-level proxy firewall

How are Firewalls configured?

Allow by default, block some

- Easy to make mistakes
- If you forget something you should block, it is allowed, and you might not realise for a while
- If somebody finds a protocol is allowed, they might not tell you

Block by default, allow some

- Much more secure
- If you forget something someone will complain and you can allow the protocol

How are Firewalls configured?

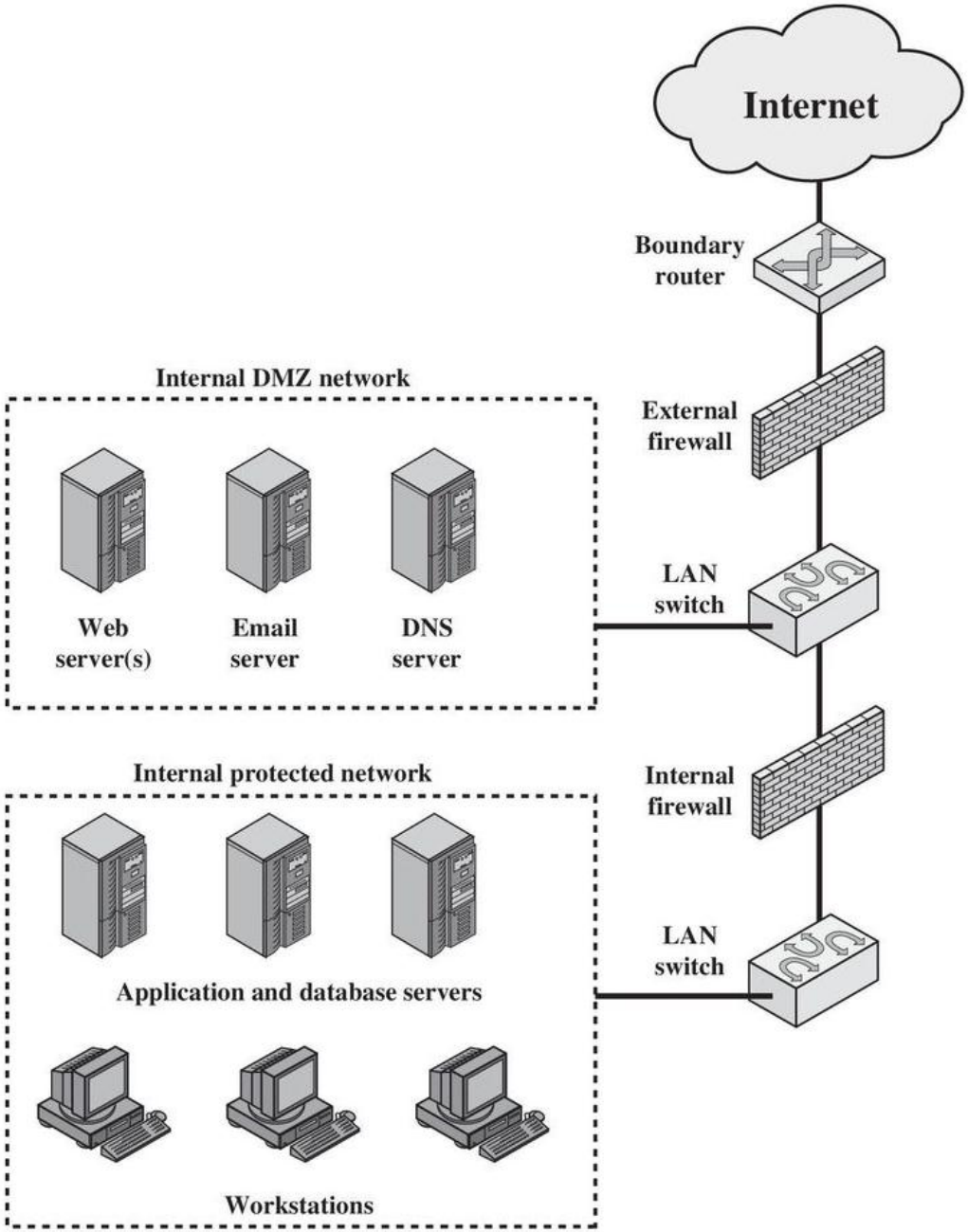
- As well as filtering out some packets, Firewalls are common locations for:
- Virtual private networking
  - All traffic passes through the Firewall
  - Convenient location to route some traffic via VPN
- Network address Translation
  - Internal machine with private addresses can be hidden behind public address
  - Public addresses can be translated to private addresses for internal servers
  - Source address is always changed by proxies

Common Firewall networking

- A firewall can only filter traffic which goes through it
- Where to put for example a mail server?
- Requires external access to receive mail from the Internet
  - Should be on the outside of the Firewall
- Requires internal access to receive mail from the internal network
  - Should be on the inside of the firewall
- Solution: use a perimeter network (DMZ)

Common Firewall networking

- Perimeter network
- Uses to locate servers which require (selective) access from both inside and outside of Firewall
  - eg: mail server
  - Web server
  - Name server (DNS)
- Firewall can have many interfaces
  - Multiple internal departments
  - Multiple client networks eg: for ISP


Internet
Boundary router
External firewall
Internal DMZ network
Web server(s)
Email server
DNS server
LAN switch
Internal firewall
Internal protected network
Application and database servers
LAN switch
Workstations

What problems do Firewalls introduce?

- Some services do not work because they are blocked
  - People complain
- Network diagnostic may be harder
- Some protocols are hard to support
  - FTP
  - IRC
  - H.323

What do not Firewalls do?

- Packet filtering Firewalls do not provide any content-based filtering
  - If email allowed through, then emails containing viruses are allowed through
  - If Web access is permitted, then pornographic Websites can be accessed
- Encrypted traffic cannot be examined/filtered
  - https
  - SSH

What do not Firewalls do?

- Packet filters do not check content
- Even Application-Proxy Firewalls may not perform thorough checks on content
  - An increasing number of services are being offered across the Internet using TCP port 80, (HTTP) no longer just Web page access
  - This makes it increasingly difficult for Firewalls to allow or block access to different services
- Well-established dilemma:
  - Security versus convenience

What do not Firewalls do?

Encrypted data is a problem for Firewalls

- Encryption is becoming more widespread
  - Privacy
  - Ecommerce
- SSH, TLS etc are end-to-end client to server
- Any system in between cannot decode data
- Users can visit unknown Websites
  - Non-productive business time
- Download cannot be anti-virus checked

How do you get round Firewalls?

- Modem or other external link
- If traffic does not go through the Firewall the Firewall cannot block it
- Poor configuration
  - eg: Allow access to any machine, inside or outside, on TCP/UDP port 53
- Protocol tunnelling

Firewalls in context

- Firewalls protect against network threats, no understanding of Operating System or Application vulnerably.

- Firewall must be between the good guy and the bad guy if they are to be any help.

- A good Firewall is good for network security. A strong Firewall needs to be supported by strong security elsewhere, such as Network Intrusion Detection systems, Internal and external detectors.

2. Intrusion Detection System (IDS)

- What is Intrusion Detection ?
- Why Intrusion Detection and Vulnerability Assessment ?
- Implementation of IDS
  - Knowledge-based IDS
    - Network based
    - Host based
  - Behaviour-based IDS
    - Statistical anomaly detection

Assumption

- Perimeter security devices (e.g. Firewalls) and computer security mechanisms (e.g. application and OS security) can only offer best effort at preventing attacks.
- They may fail to do so:
  - a Firewall may be mis-configured,
  - a password may be sniffed off the network,
  - a new attack type may emerge. (cf. Zero-day attacks)
- They do not detect when an attack is underway or has taken place.
- And they do not react to attacks.

Intrusion Detection Systems (IDS)

- An Intrusion Detection System (IDS) is a network security system designed to identify intrusive or malicious behaviour via monitoring of network activity.

- The IDS identifies suspicious patterns that may indicate an attempt to attack, break in to, or otherwise compromise a system.

- An IDS can be network-based or host-based, passive or reactive, and can rely on either misuse detection or anomaly detection.

IDS vs Firewalls

- Firewalls specify policies about what traffic may or may not enter a particular computer network.

- An IDS monitors patterns of traffic and signals an alert once it deems that an attack has taken place.

Knowledge-based IDS

- ALL commercial IDS look for attack signatures:
  - specific patterns of network traffic or activity in log files that indicate suspicious behaviour.
- Called a knowledge-based or misuse detection IDS
- Example signatures might include:
  - a number of recent failed login attempts on a sensitive host;
  - a certain pattern of bits in an IP packet, indicating a buffer overflow attack;
  - certain types of TCP SYN packets, indicating a SYN flood DoS attack.

Knowledge-based IDS

- Knowledge-based IDS uses information such as:
  - Security policy;
  - Known vulnerabilities of particular OS and applications;
  - Known attacks on systems.
- They are only as good as the information in the database of attack signatures:
  - new vulnerabilities not in the database are constantly being discovered and exploited;
  - vendors need to keep up to date with latest attacks and issue database updates; customers need to install these;
  - large number of vulnerabilities and different exploitation methods, so effective database difficult to build;
  - large database makes IDS slow to use.

Behaviour-based IDS

- Statistical Anomaly Detection (or behaviour-based detection) is a methodology where statistical techniques are used to detect penetrations and attacks.
- Begin by establishing base-line statistical behaviour: what is normal for this system?
- Then gather new statistical data and measure the deviation from the base-line.
- If a threshold is exceeded, issue an alarm.

Behaviour-based IDS

- Example: monitor the number of failed login attempts at a sensitive host over a period;
  - if a burst of failures occurs, an attack may be under way;
  - or maybe the admin just forgot his password!
- This raises the issue of false positives (an attack is flagged when one was not taking place – a false alarm) and false negatives (an attack was missed because it fell within the bounds of normal behaviour).
- This issue does also apply to knowledge-based systems.

Behaviour-based IDS

- IDS does not need to know about security vulnerabilities in a particular system
  - the base-line defines normality;
  - don’t need to know the details of the construction of a buffer overflow packet.

- Normal behaviour may overlap with forbidden behaviour.
  - Legitimate users may deviate from the base-line, causing false positives (e.g. user goes on holiday, or works late in the office, or forgets password, or starts to use new application).
  - If the base-line is adjusted dynamically and automatically, a patient attacker may be able to gradually shift the base-line over time so that his attack does not generate an alarm.

Host-based and Network-based IDS

- When an IDS looks for attack signatures in network traffic, it is called a network-based IDS (NIDS).
- When an IDS looks for attack signatures in log files of hosts, it is called a host-based IDS (HIDS).
- Naturally, the most effective Intrusion Detection System will make use of both kinds of information.

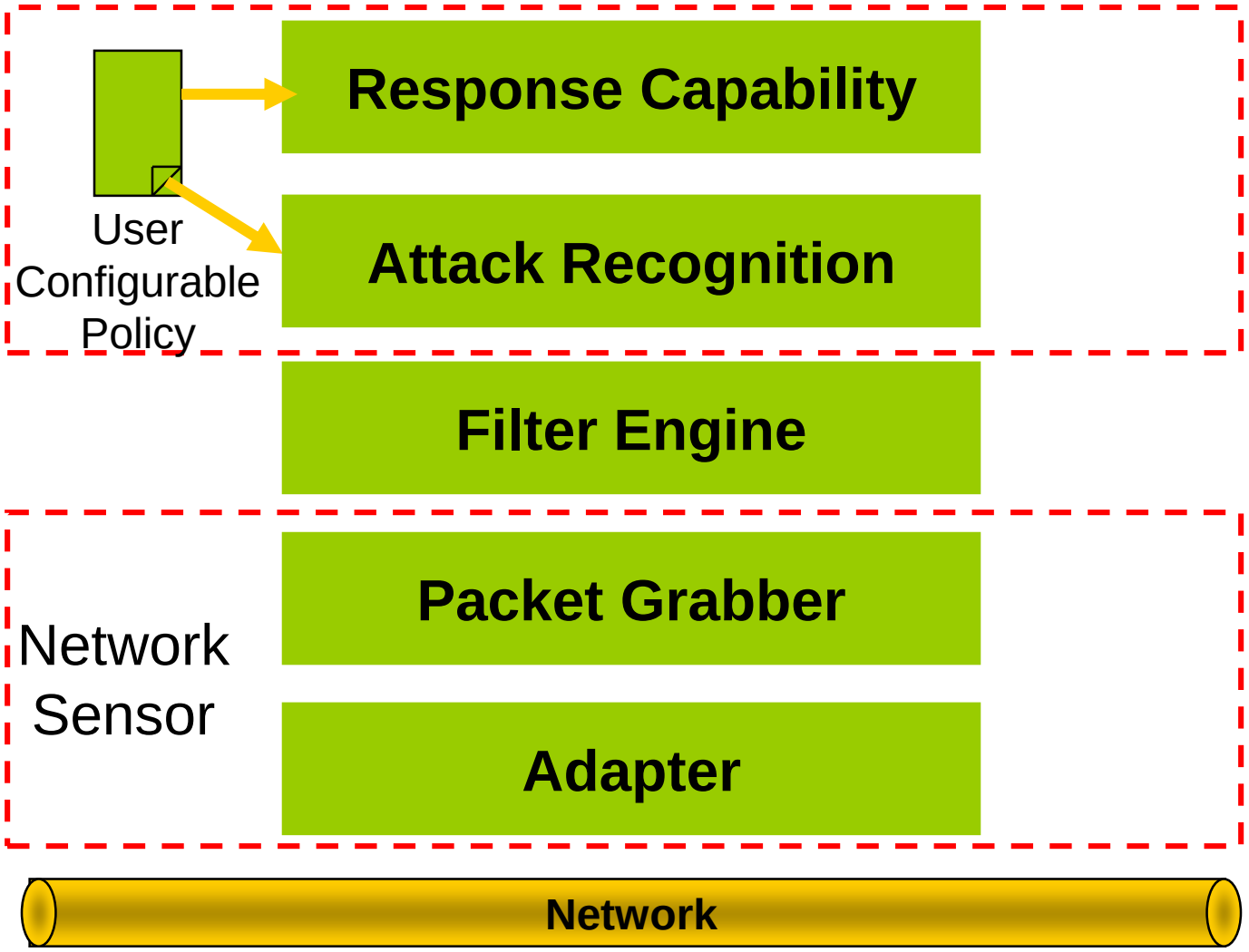
IDS Architecture

- Distributed set of sensors – either located on hosts or on network – to gather data.
- Centralised console to manage sensor network, analyse data, report and react.
- Ideally:
  - Protected communications between sensors and console;
- Protected storage for signature database/logs;
  - Secure console configuration;
  - Secured signature updates from vendor;
  - Otherwise, the IDS itself can be attacked and manipulated.

Network-based IDS

- Uses network packets as the data source.
- Typically utilises a network adapter running in promiscuous mode to monitor and analyse all traffic in real-time as it travels across the network (Network sniffer) .
- The attack recognition module uses three common techniques to recognise attack signatures:
  - Pattern, expression or byte code matching;
  - Frequency or threshold crossing (eg detect port scanning activity);
  - Correlation of lesser events (in reality, not much of this in commercial systems).

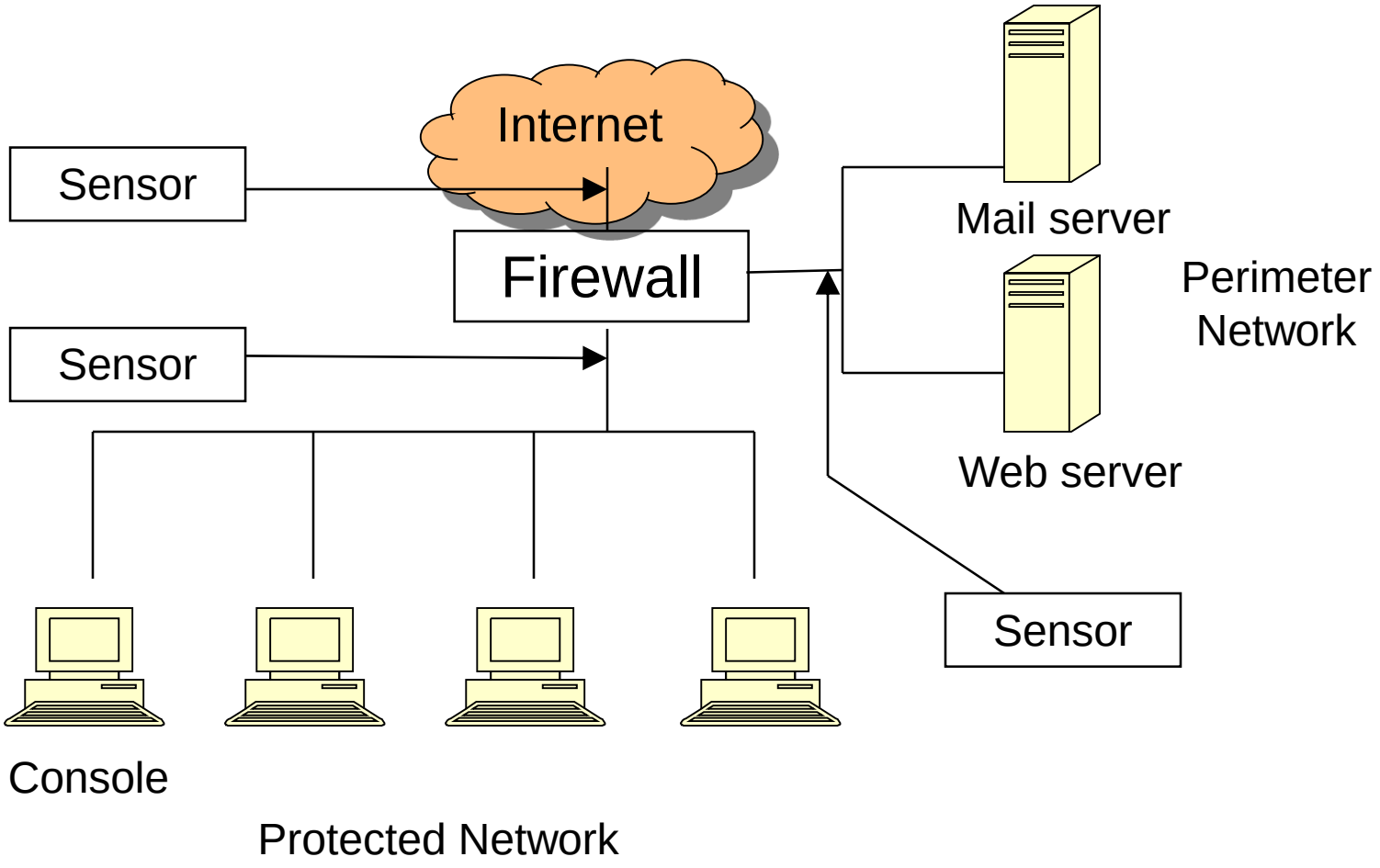
Network-based IDS



Placement of Network-based IDS

- Deployment options:
  - Outside Firewall
  - Just inside Firewall
    - Combination of both will detect attacks getting through Firewall and may help to refine Firewall rule set.
  - Behind remote access server
  - Between Business Units
  - Between Corporate Network and Partner Networks

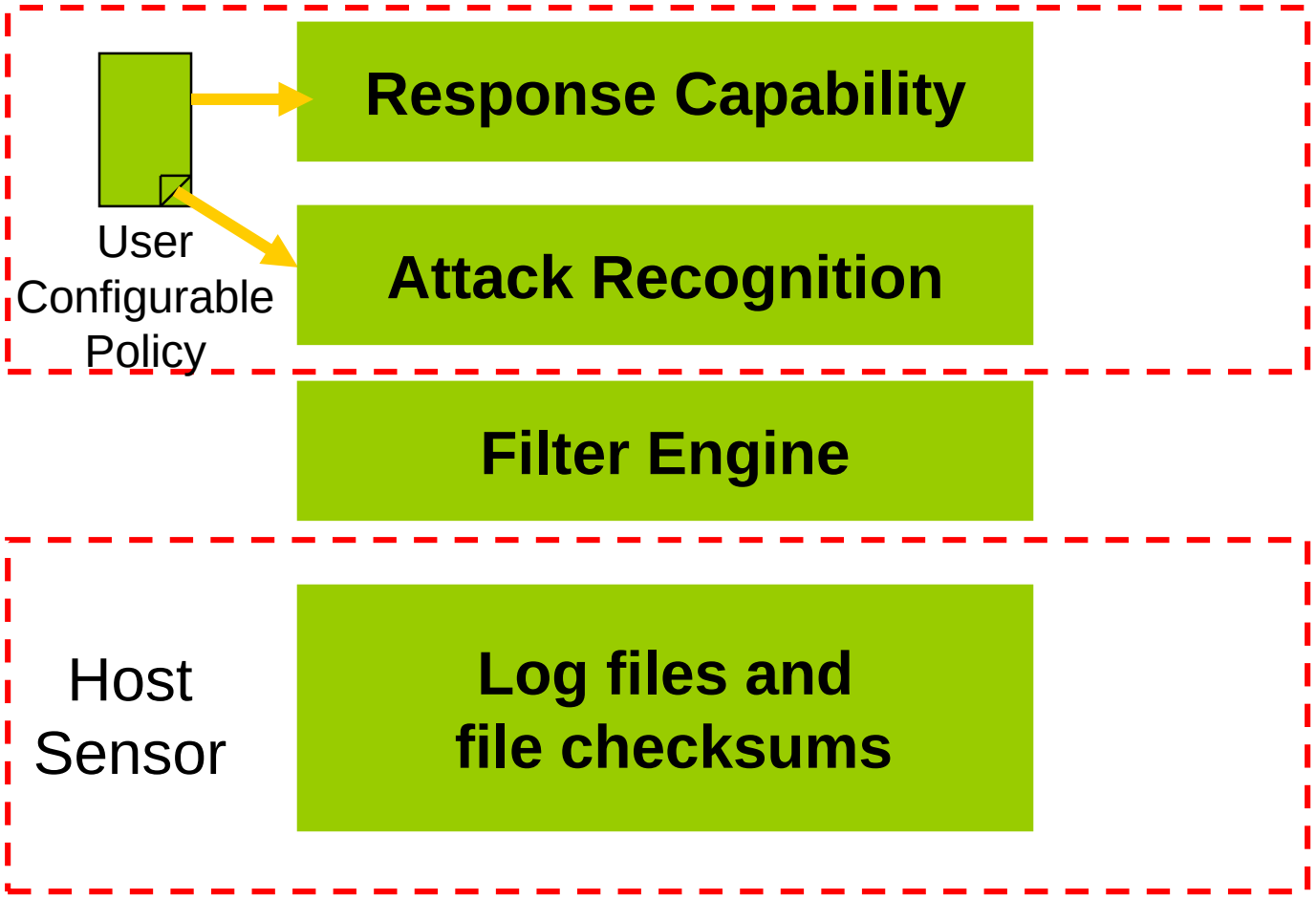
Placement of Network-based IDS



Host-based IDS

- Typically monitors system, event, and security logs on Windows and syslog in Unix environments.
- Checks key system files and executable via checksums at regular intervals for unexpected changes.
- Some products can use regular-expressions to refine attack signatures (e.g. passwd program executed AND .rhosts file changed).
- Some products listen to port activity and alert when specific ports are accessed

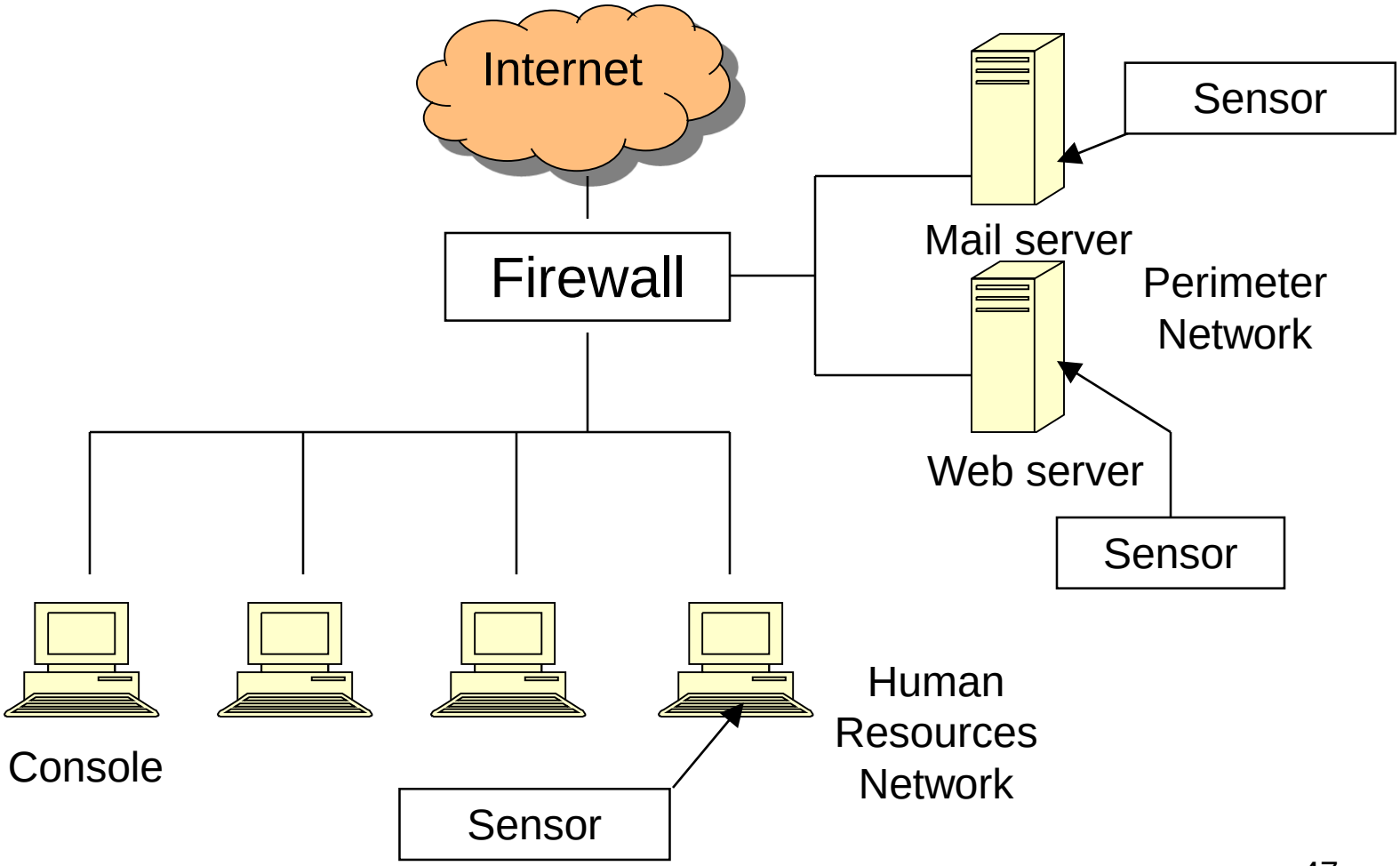
Host-based IDS



Placement of Host-based IDS

- Deployment options:
  - Key servers that contain mission-critical and sensitive information;
  - Web servers;
  - FTP and DNS servers;
  - E-commerce database servers, etc.

Placement of Host-based IDS



IDS as a Response Tool

- Given the (near) real-time nature of IDS alerts, an IDS can be used as a response tool as well as for detection.

- NIDS and HIDS have different response capabilities – because they detect different attacks, or the same attacks but in different ways.

HIDS and NIDS

- There are attack types that a HIDS can detect but a NIDS cannot:
  - Trojan login script, walk up to unattended keyboard attack, encrypted traffic,…

There are attack types that a NIDS can detect but a HIDS cannot:

- IP Spoofing, denial-of-service attacks, arp cache poisoning, DNS name corruption, and man-in-the-middle attacks

For more reliable detection, combine both types of IDS.

IDS Response Options

	Network-based	Host-based
Notification	**Alarm to console**	**Alarm to console**
	E-Mail notification	**E-Mail notification**
	SNMP trap	**SNMP trap**
	View active session	
Storage	**Log summary**	**Log summary**
	Log raw network data	
Active	**Kill connection (TCP Reset)**	**Terminate user login**
	Re-configure firewall	**Disable user account**
		Restore index.html

IDS Response Options

- Dangers of automated response:
  - Attacker tricks IDS to respond, but response aimed at innocent target (say, by spoofing source IP address);
  - Users locked out of their accounts because of false positives;
  - Repeated e-mail notification becomes a denial of service attack on sysadmin's e-mail account;
  - Repeated restoration of index.html from CD reduces website availability.