University of BRISTOL

Computer System B

Dr. Alma Oracevic
alma.oracevic@bristol.ac.uk

bristol.ac.uk

University of BRISTOL

What did we learn?

- DNS attacks
- HTTP session hijacking
- TCP session hijacking
- IP spoofing
- ARP spoofing
- Jamming
- Man in the middle
- DDoS

bristol.ac.uk

University of BRISTOL

Today!

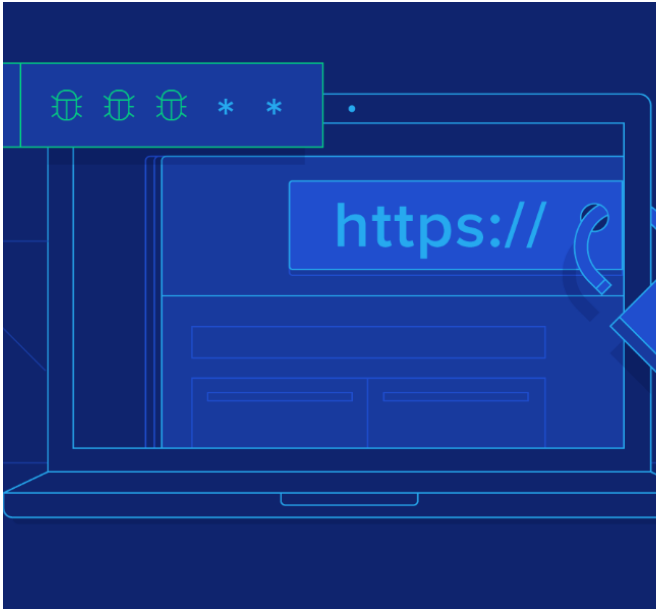
- WEB security
- Firewalls
- Intrusion Detection Systems

bristol.ac.uk

Web Security

- Web security is a broad category of security solutions that protect your
  - –users,
  - –devices, and
  - –wider network

  internet-based cyberattacks—malware, phishing, and more—that can lead to breaches and data loss.

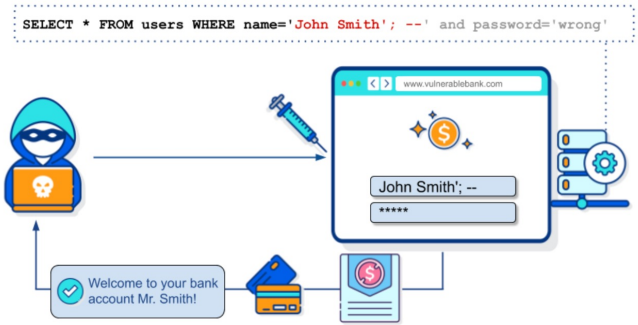


What are the top web security threats?

- Phishing.
- Ransomware.
- SQL injection.
- Cross-site scripting.
- Code injection.
- CEO fraud and impersonation.
- Viruses and worms.
- Spyware.

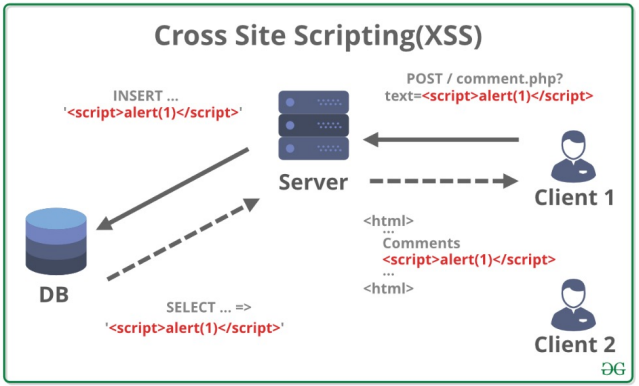
SQL injections

- An attacker can use SQL Injection to manipulate an SQL query via the input data from the client to the application, thus forcing the SQL server to execute an unintended operation constructed using untrusted input.
- A successful SQL Injection attack can result in a malicious user gaining complete access to all data in a database server

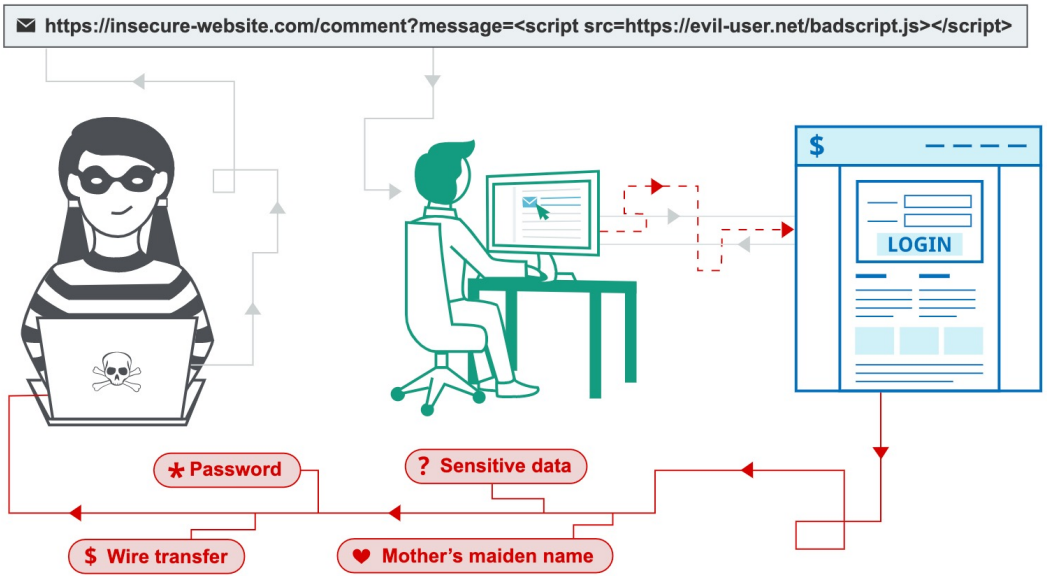


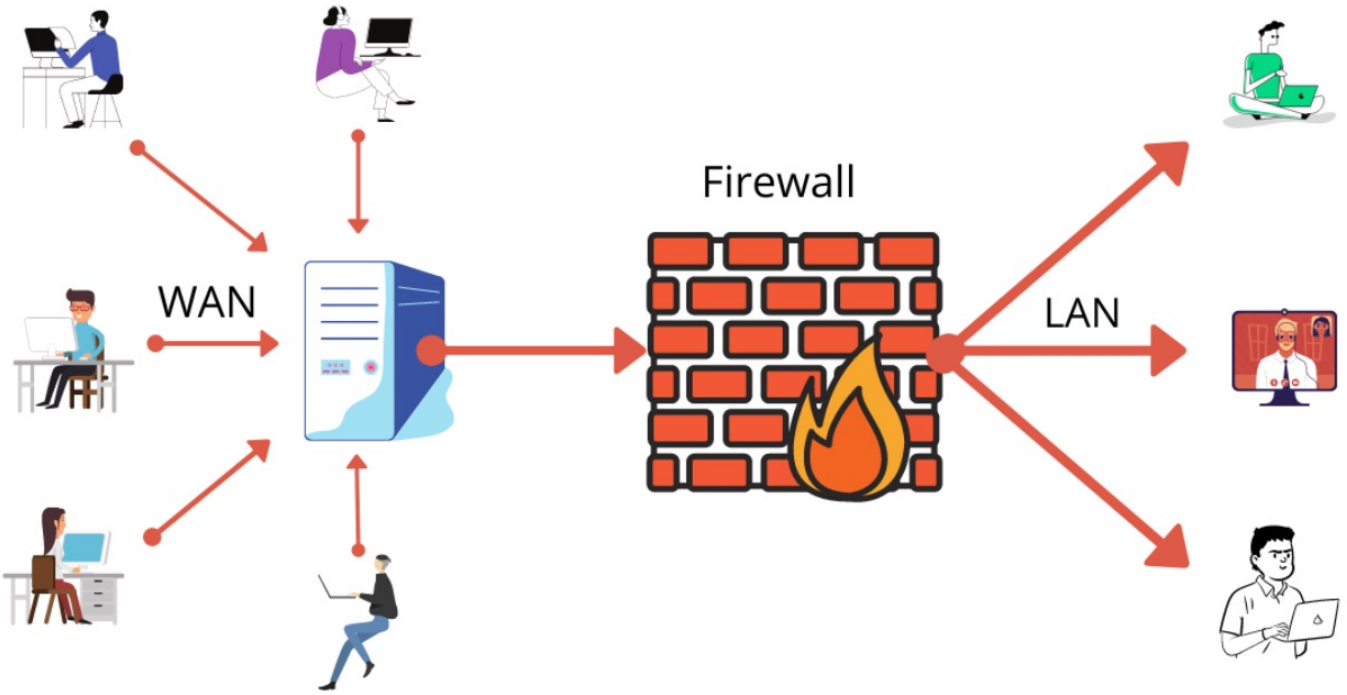
Cross-site scripting XSS

- An attacker sends on input JavaScript tags to your web application. When this input is returned to the user unsanitized, the user's browser would execute it.
- This is a fairly widespread input sanitization failure, essentially a subcategory of injection flaws.
- CSS can be as simple as crafting a link and persuading a user to click it, or it can be something much more sinister.
  - For example, on page load, the script would run and be used to post your cookies to the attacker.



Cross-site scripting XSS




Firewall
WAN
LAN

Firewalls

- A firewall is a device that filters all traffic between a protected or "inside" network and a less trustworthy or "outside" network.
  - Usually a firewall runs on a dedicated device because it is a single point through which traffic is channeled, performance is important
    - Non-firewall functions should not be done on the same machine.
  - Firewall code usually runs on a proprietary or carefully minimized operating system
    - More code means more security problems
  - The purpose of a firewall is to keep "bad" things outside a protected environment.
    - firewalls implement a security policy that is specifically designed to address what bad things might happen
    - determining security policies is challenging!

Firewalls

- People in the firewall community (users, developers, and security experts) disagree about how a firewall should work.
  - the community is divided about a firewall's default behavior
  - two schools of thought
    - “that which is not expressly forbidden is permitted" (default permit)”
    - “that which is not expressly permitted is forbidden" (default deny)”.

Firewall's (in)capabilities

Firewall's (in)capabilities

✓ Provide a focal point for monitoring.

Firewall's (in)capabilities

✓ Provide a focal point for monitoring.

✓ Provide a central point for access control (who can do what).

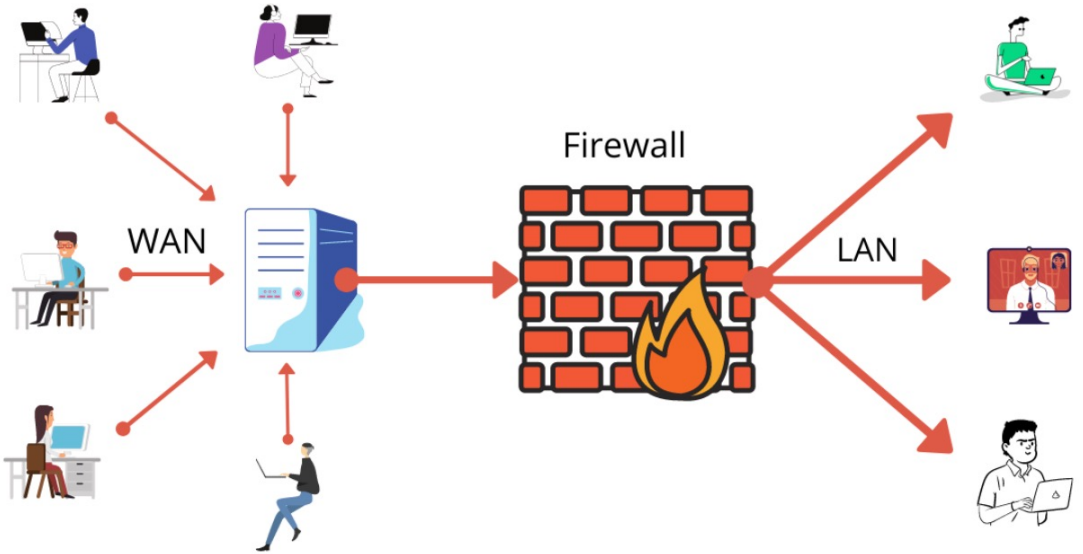
Firewall's (in)capabilities

- ✓ Provide a focal point for monitoring.
- ✓ Provide a central point for access control (who can do what).
- ✓ Limit the damage that a network security problem can do to the overall network.

Firewall's (in)capabilities

- ✓ Provide a focal point for monitoring.
- ✓ Provide a central point for access control (who can do what).
- ✓ Limit the damage that a network security problem can do to the overall network.
- ✓ Protect against malicious insiders.
- ✓ Protect a connection that doesn't go through it!!
- ✓ Protect against completely new threats.
- ✓ Protect against viruses, Trojans etc.

Firewall Deployment



Firewall Deployment

- All traffic from inside to outside, and vice versa, must pass through the firewall.

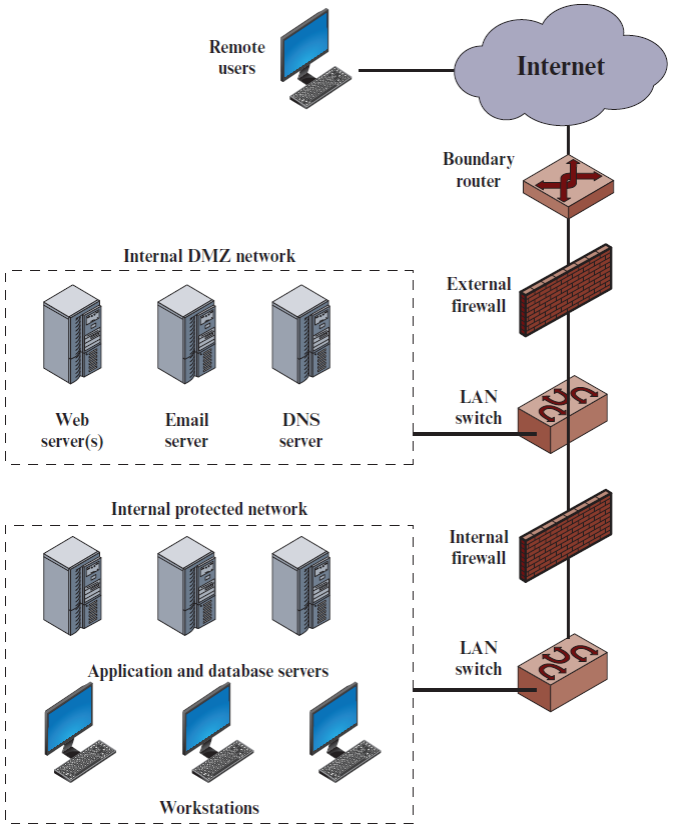
Firewall Deployment

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass

Firewall Deployment

- All traffic from inside to outside, and vice versa, must pass through the firewall.
- Only authorized traffic, as defined by the local security policy, will be allowed to pass
- Ideal Assumption: The firewall itself is immune to penetration.
    - E.g. Cisco iOS vulnerabilities, Juniper Junos vulnerabilities.

Typical Deployment



Generic Techniques for Enforcing policy

Generic Techniques for Enforcing policy

- Service control: Determines the types of Internet services that can be accessed.

Generic Techniques for Enforcing policy

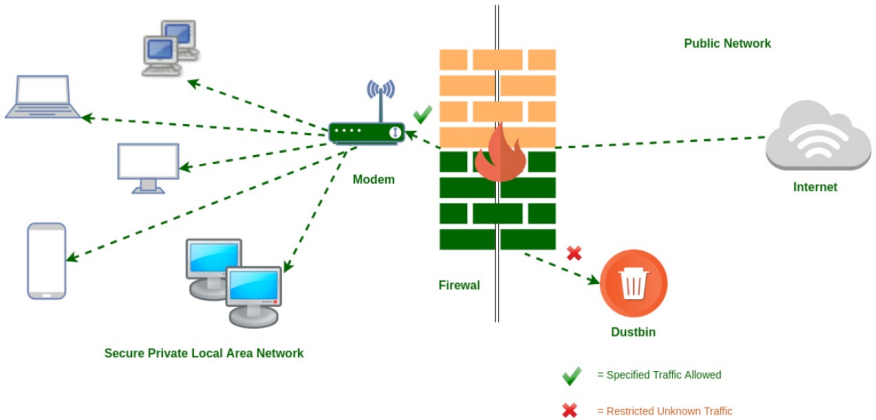
- Service control: Determines the types of Internet services that can be accessed.
- Direction control: Determines the direction in which particular service requests are allowed.

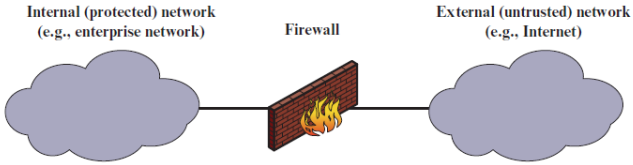
Generic Techniques for Enforcing policy

- Service control: Determines the types of Internet services that can be accessed.
- Direction control: Determines the direction in which particular service requests are allowed.
- User control: Controls access to a service according to which user is attempting to access it. IP based filtering or authentication with IPSec.

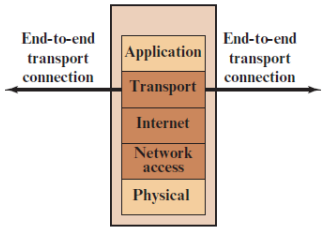
Types of firewalls

- Packet Filtering Firewall (works at the network layer, IP)
- Circuit-level gateway (works at the transport layer, TCP)
- Stateful Inspection Firewall
- Application Level Gateway (works at higher layers)

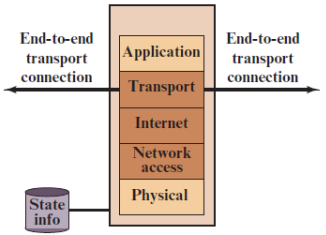




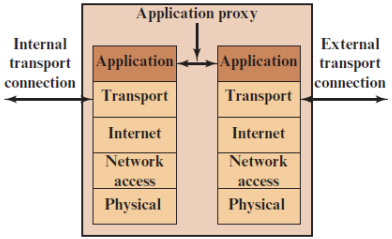
(a) General model



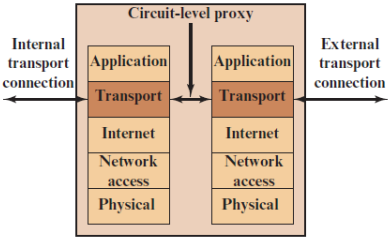
(b) Packet filtering firewall



(c) Stateful inspection firewall

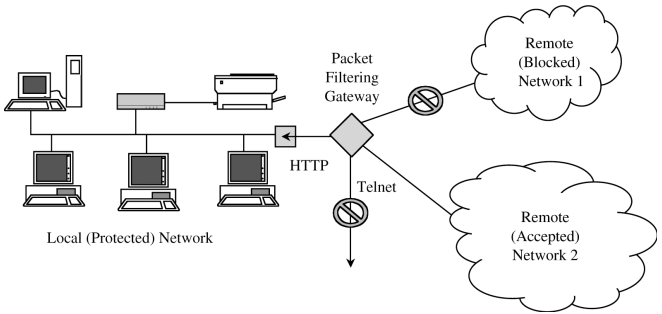


(d) Application proxy firewall



(e) Circuit-level proxy firewall

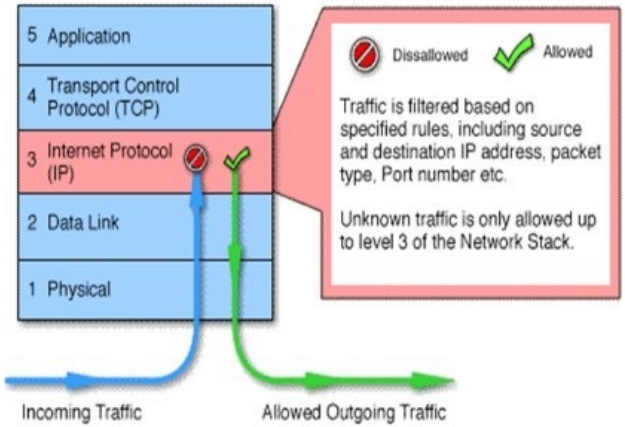
Packet Filtering Gateway



- the simplest, and in some situations, the most effective type of firewall
  - controls access to packets on
    - the basis of packet address (source or destination)
    - or specific transport protocol type (such as HTTP web traffic).

Packet filters

- Works at most up to transport layer, but at individual packet level.
- Stateless
- Fast processing



Example packet filters

Rule Set A

action	Ourhost	port	theirhost	port	comment
block	*	*	SPIGOT	*	we don't trust these people
allow	OUR-GW	25	*	*	connection to our SMTP port

Rule Set B

action	Ourhost	port	theirhost	port	comment
block	*	*	*	*	default

Rule Set C

action	Ourhost	port	theirhost	port	comment
allow	*	*	*	25	connection to their SMTP port

Rule Set D

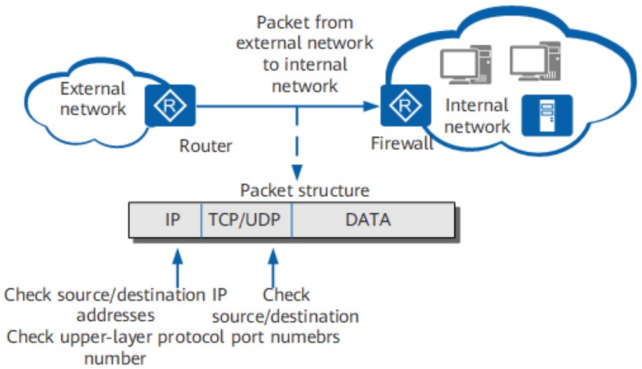
action	Src	port	dest	port	flags	comment
allow	{our hosts}	*	*	25		our packets to their SMTP port
allow	*	25	*	*	ACK	their replies

Rule Set E

action	Src	port	dest	port	flags	comment
allow	{our hosts}	*	*	*		our outgoing calls
allow	*	*	*	*	ACK	replies to our calls
allow	*	*	*	>1024		traffic to nonservers

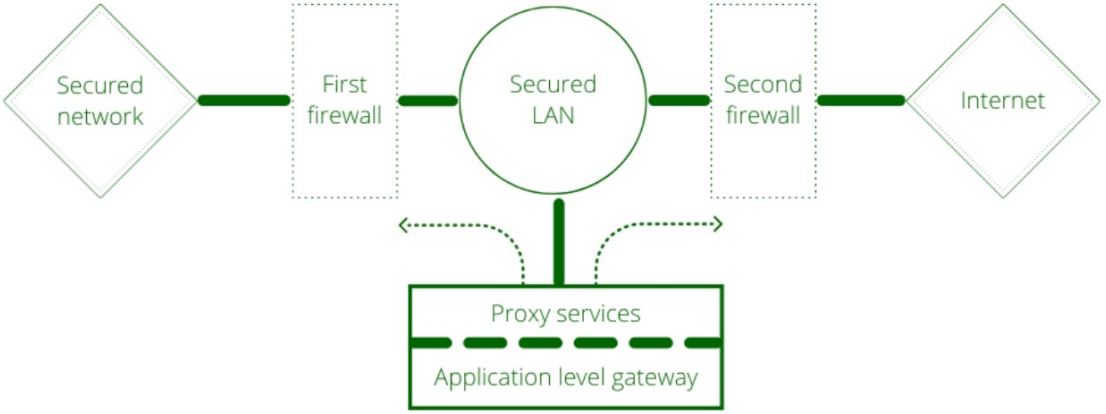
Problems with Packet filters

- Lack of upper-layer functionality;
- Do not support advanced user authentication schemes;
- Cannot block specific application commands: either the application is disallowed, or all its functions are permitted;



Pros:
• Simple;
• Transparent for users;
• Very fast.

Application-Level Gateway

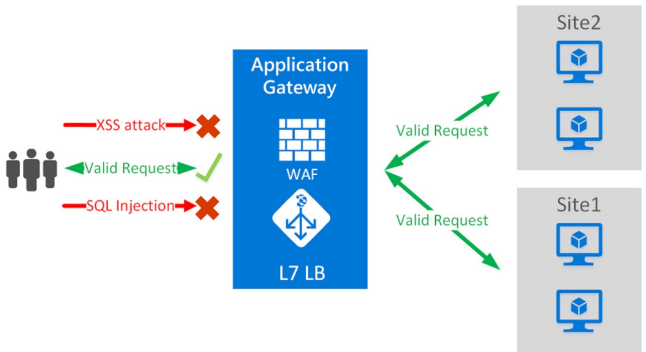


Application level gateway

Application-Level Gateway

- Also called an *application proxy*
- Acts as a relay of application-level traffic
- Tend to be more secure than packet filters
  - Rather than trying to deal with the numerous possible combinations that are to be allowed and forbidden at the TCP and IP level, the application-level gateway need only scrutinize a few allowable applications
- A prime disadvantage of this type of gateway is the additional processing overhead on each connection
  - In effect, there are two spliced connections between the end users, with the gateway at the splice point, and the gateway must examine and forward all traffic in both directions

Application gateway (aka Proxy)



- Filters traffic at application layer
- Specific to applications which are configured.
- Works at client-server mode
- Offer High level of security
- Have impact on network performance

Stateful Inspection Firewall

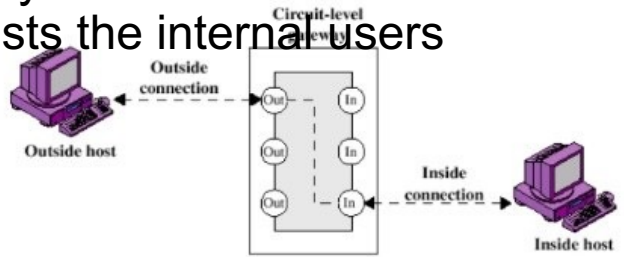
- Filtering firewalls work on packets one at a time, accepting or rejecting each packet and moving on to the next.
  - They have no concept of "state" or "context" from one packet to the next.
- A **stateful inspection firewall** maintains state information from one packet to another in the input stream.
- One classic approach used by attackers is to break an attack into multiple packets
  - forcing some packets to have very short lengths so that a firewall cannot detect the signature of an attack split across two or more packets

Stateful Inspection Firewall

- Remember that with the TCP protocols, packets can arrive in any order
  - the protocol suite is responsible for reassembling the packet stream in proper order before passing it along to the application
- A stateful inspection firewall would track the sequence of packets and conditions from one packet to another to thwart such an attack.

Circuit Level gateway

- A fourth type of firewall is the circuit-level gateway or *circuit-level proxy*
- Can be a stand-alone system or it can be a specialized function performed by an application-level gateway for certain applications
- A circuit-level gateway does not permit an end-to-end TCP connection
- The security function consists of determining which connections will be allowed
- A typical use of circuit-level gateways is a situation in which the system administrator trusts the internal users



Personal Firewalls

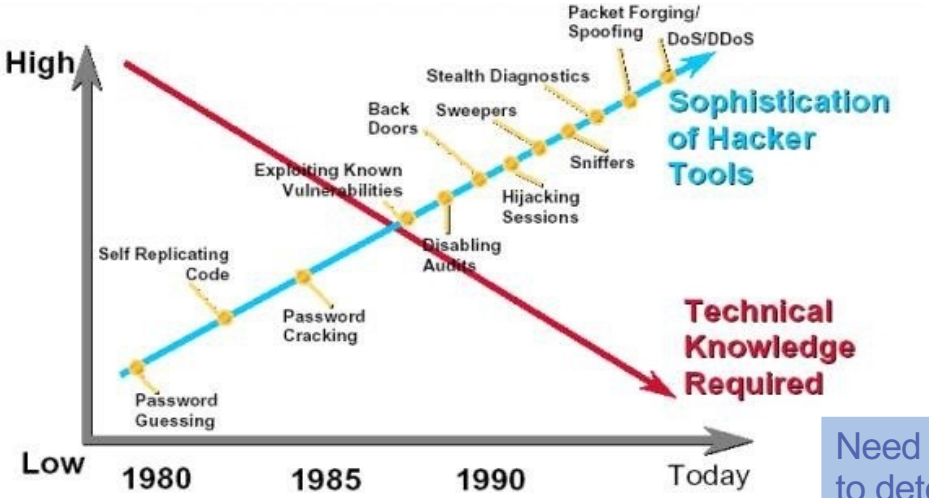
- A **personal firewall** is an application program that runs on a workstation to block unwanted traffic
  - can complement or compensate for the lack of a regular firewall
- Commercial implementations of personal firewalls include Norton Personal Firewall from Symantec, McAfee Personal Firewall, and Zone Alarm from Zone Labs (now owned by CheckPoint).
- The personal firewall is configured to enforce some policy.
  - computers on the company network, are highly trustworthy, but most other sites are not.
- Personal firewalls can also generate logs of accesses

Intrusions

- DARPA IDS Evaluation Project 1998 attack categories[1]:
  - Probes (e.g. port scanning, fingerprinting)
  - Denial of Service (DoS) (e.g. packet flooding, crash)
  - Remote to Local (R2L)
  - User to Root (U2R)

http://www.ll.mit.edu/mission/communications/cyber/CSTcorpora/ideval/docs/attackDB.html

Attacker's Picture

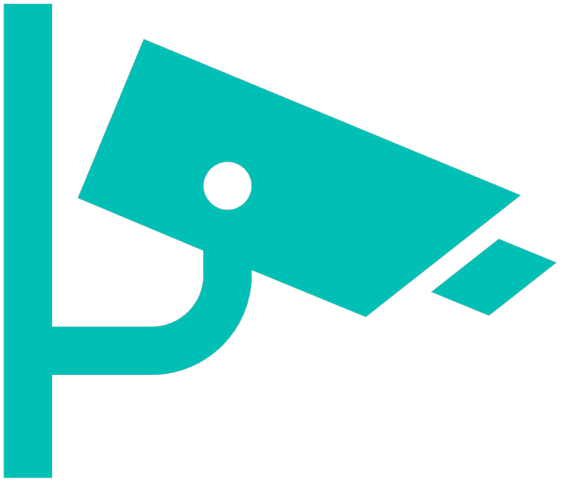


Need of automatic ways to detect them!

Curtsey: Internet source

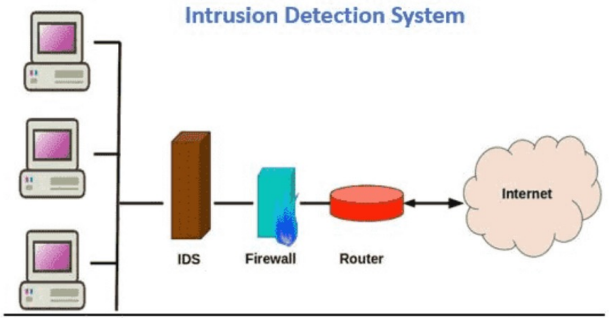
Intrusion Detection Systems

- **What is intrusion detection?**



Intrusion Detection Systems (IDS)

- Intrusion detection systems complement these preventive controls as the next line of defense
- An **intrusion detection system (IDS**) is a device, typically another separate computer, that monitors activity to identify malicious or suspicious events.
  - An IDS is a sensor, like a smoke detector, that raises an alarm if specific things occur.



Intrusion Detection Systems (IDS)

- IDSs perform a variety of functions:
  - monitoring users and system activity
  - auditing system configuration for vulnerabilities and misconfigurations
  - assessing the integrity of critical system and data files
  - recognizing known attack patterns in system activity
  - identifying abnormal activity through statistical analysis
  - managing audit trails and highlighting user violation of policy or normal activity
  - correcting system configuration errors
  - installing and operating traps to record information about intruders
- No one IDS performs all of these functions. Let us look more closely at the kinds of IDSs and their use in providing security.

Some (intended) General characteristics

Some (intended) General characteristics

- The ability to react in a timely fashion to prevent substantive damage – by automatic or manual intervention.

Some (intended) General characteristics

- The ability to react in a timely fashion to prevent substantive damage
  - – by automatic or manual intervention.
- The ability to identify which is the precursor of more serious attacks.

Some (intended) General characteristics

- The ability to react in a timely fashion to prevent substantive damage
  - by automatic or manual intervention.
- The ability to identify which is the precursor of more serious attacks.
- The ability to identify a perpetrator.

Some (intended) General characteristics

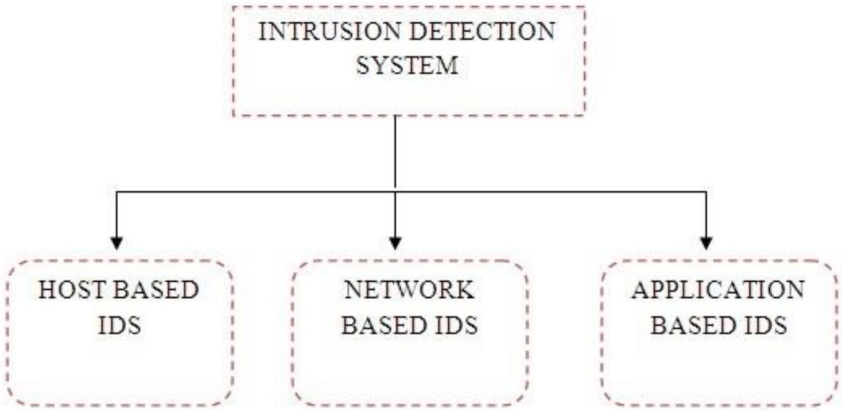
- The ability to react in a timely fashion to prevent substantive damage
  - by automatic or manual intervention.
- The ability to identify which is the precursor of more serious
- attacks.
- The ability to identify a perpetrator.
- The ability to discover new attack patterns.

Some (intended) General characteristics

- The ability to react in a timely fashion to prevent substantive damage
  - by automatic or manual intervention.
- The ability to identify which is the precursor of more serious
- attacks.
- The ability to identify a perpetrator.
- The ability to discover new attack patterns.
- The ability to produce evidence.

Type of IDS

Type of IDS


INTRUSION DETECTION SYSTEM
HOST BASED IDS
NETWORK BASED IDS
APPLICATION BASED IDS

Types of IDSs

- The two general types of intrusion detection systems are signature based and heuristic
  - **Signature-based** intrusion detection systems perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type
  - **Heuristic** intrusion detection systems, also known as **anomaly-based**, build a model of acceptable behavior and flag exceptions to that model
- Intrusion detection devices can be **network-based** or **host-based**.
  - A **network-based** IDS is a stand-alone device attached to the network to monitor traffic throughout that network
  - a **host-based** IDS runs on a single workstation or client or host, to protect that one host.

Signature-Based Intrusion Detection

- Signature for a known attack types
  - series of TCP SYN packets sent to many different ports in succession and at times close to one another, as would be the case for a port scan.
  - Of course, signature-based IDSs cannot detect a new attack for which a signature is not yet installed in the database
  - And, an attacker will try to modify a basic attack in such a way that it will not match the known signature of that attack
- Signature-based intrusion detection systems tend to use **statistical analysis**.
  - To obtain sample measurements of key indicators (such as amount of external activity, number of active processes, number of transactions)
  - to determine whether the collected measurements fit the predetermined attack signatures.

Heuristic Intrusion Detection

- Instead of looking for matches, heuristic intrusion detection looks for behavior that is out of the ordinary.
- The original work in this area focused on the individual, trying to find characteristics of that person that might be helpful in understanding normal and abnormal behavior.
  - For example, one user might always start the day by reading e-mail, write many documents using a word processor, and occasionally back up files.
  - This user does not seem to use many administrator utilities.
  - If that person tried to access sensitive system management utilities, this new behavior might be a clue that someone else was acting under the user's identity.

Goals for Intrusion Detection Systems

- Ideally, an IDS should be fast, simple, and accurate, while at the same time being complete.
  - It should detect all attacks with little performance penalty.
- An IDS could use some (or all) of the following design approaches:
  - Filter on packet headers
  - Filter on packet content
  - Maintain connection state
  - Use complex, multipacket signatures
  - Use minimal number of signatures with maximum effect
  - Filter in real time, online
  - Hide its presence
  - Use optimal sliding time window size to match signatures

Responding to Alarms

- Whatever the type, an intrusion detection system raises an alarm when it finds a match.
- What are possible responses?
  - The range is unlimited and can be anything the administrator can imagine
- In general, responses fall into three major categories (any or all of which can be used in a single response):
  - Monitor, collect data, perhaps increase amount of data collected
    - watch the intruder, to see what resources are being accessed or what attempted attacks are tried
    - record all traffic from a given source for future analysis
  - Protect, act to reduce exposure
    - increasing access controls and even making a resource unavailable (for example, shutting off a network connection or making a file unavailable).
    - may be very visible to the attacker
  - Call a human

False Results

- Intrusion detection systems are not perfect, and mistakes are their biggest problem
  - raising an alarm for something that is not really an attack (called a false positive, or type I error in the statistical community)
    - Too many false positives means the administrator will be less confident of the IDS's warnings, perhaps leading to a real alarm's being ignored.
  - or not raising an alarm for a real attack (a false negative, or type II error).
    - mean that real attacks are passing the IDS without action.
- We say that the degree of false positives and false negatives represents the sensitivity of the system.
  - Most IDS implementations allow the administrator to tune the system's sensitivity, to strike an acceptable balance between false positives and negatives.

Measuring the effectiveness

- Obviously, not every attack can be detected by an IDS and not every alert by an IDS is an attack!

Actual ↓ / Reported →	Attack	Not-attack
Attack	True positive (TP)	False negative (FN)
Not- attack (benign)	False positive (FP)	True negative (TN)

Measuring the effectiveness

- Obviously, not every attack can be detected by an IDS and not every alert by an IDS is an attack!

Actual ↓ / Reported →	Attack	Not-attack
Attack	True positive (TP)	False negative (FN)
Not- attack (benign)	False positive (FP)	True negative (TN)

$$DR = \frac{TP}{TP + FN}$$

DR: detection rate (*aka* ***Recall***).
Precision: What proportion of positive identifications was actually correct?

$$Precision = \frac{TP}{TP + FP}$$

Measuring the effectiveness

- Obviously, not every attack can be detected by an IDS and not every alert by an IDS is an attack!

Actual ↓ / Reported →	Attack	Not-attack
Attack	True positive (TP)	False negative (FN)
Not- attack (benign)	False positive (FP)	True negative (TN)

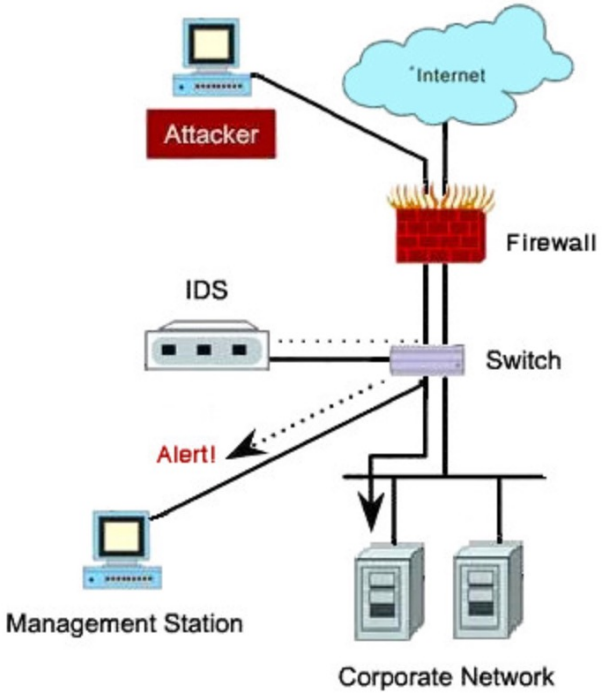
$$DR = \frac{TP}{TP + FN}$$

DR: detection rate (*aka* ***Recall***).
Precision: What proportion of positive identifications was actually correct?

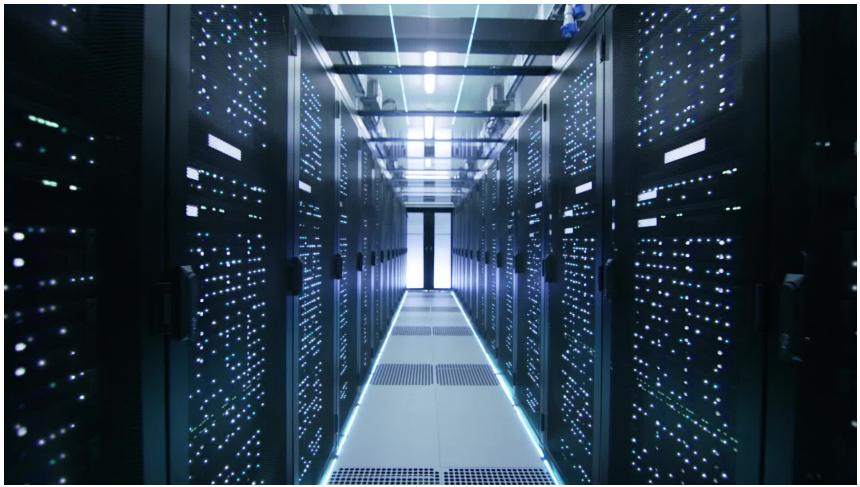
$$Precision = \frac{TP}{TP + FP}$$

Ideally, one would like to have 0 FP and 0 FN

Deploying NIDS

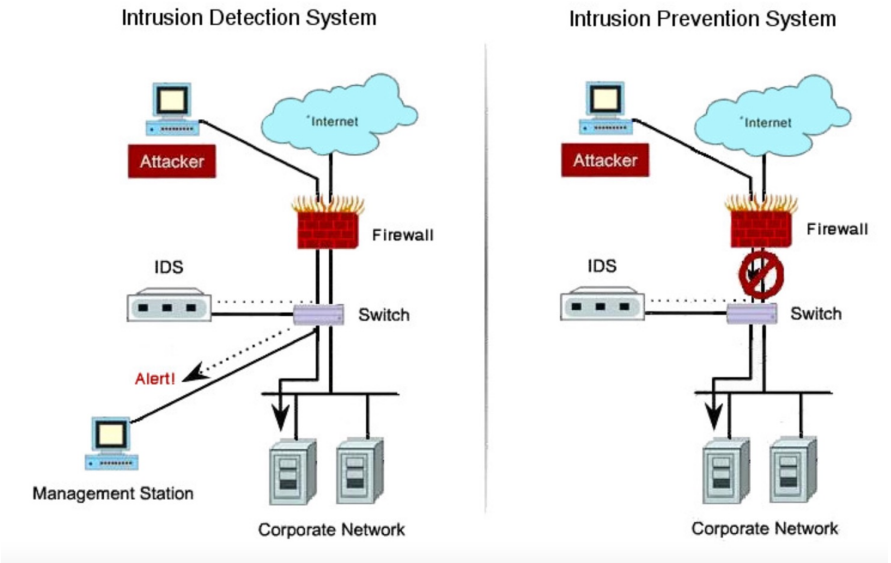


Intrusion Prevention System

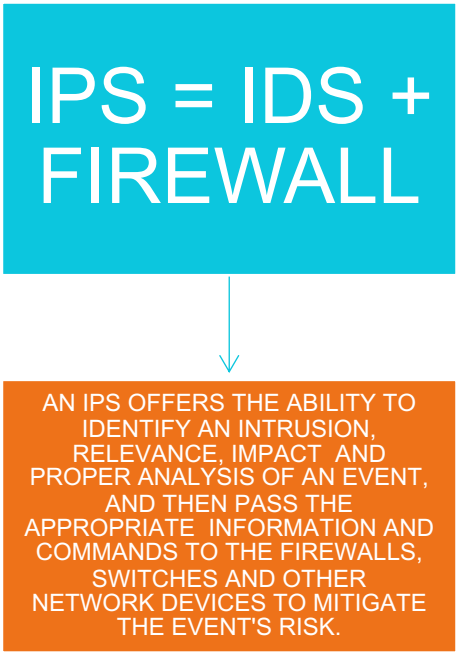


Intrusion Prevention System

- IPS = IDS + Firewall



Intrusion Prevention System



Network security!

Firewalls

IDS/IPS

What did we learn today?

- The role of firewalls as part of a computer and network security strategy
- List the key characteristics of firewalls
- The basic principles of and requirements for intrusion detection

bristol.ac.uk