Cybersecurity

Intrusion detection and prevention

Mauro Barni

University of Siena

You’d better know your enemy (goal)

- **Cybercriminals:** individuals or members of an organized crime group with a goal of financial reward. For some years, reports are quoting very large and increasing rewards.
- **Activists (hacktivists)**: individuals or members of a large group motivated by social or political causes. The aim of their attacks is often to promote and publicize their cause
- **State-sponsored organizations**: groups of hackers sponsored by governments, often associated to APTs
- **Others**: include classic hackers motivated by technical challenge or by peer-group esteem and reputation.

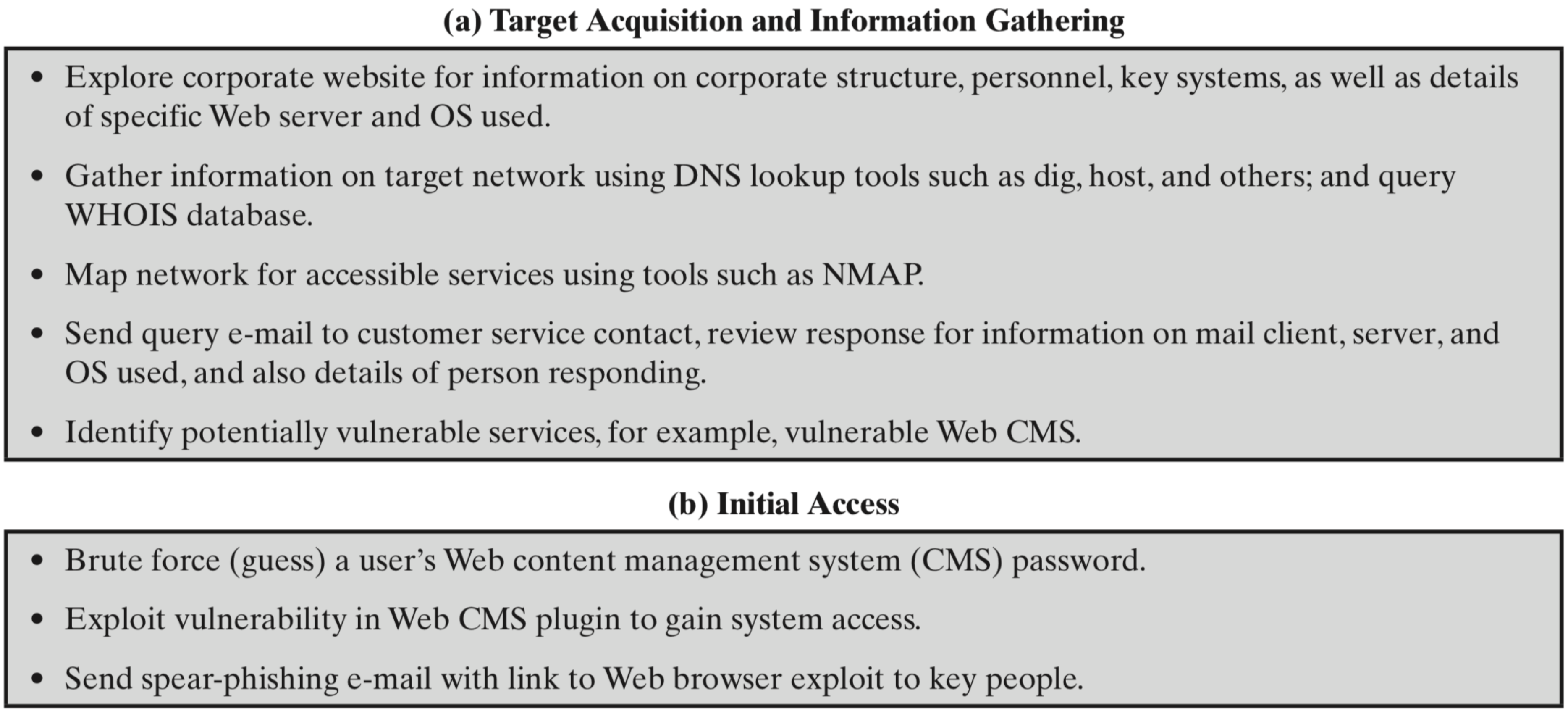
You’d better know your enemy (skills)

- **Apprentice:** hackers with minimal technical skill who primarily use existing attack toolkits. They are also known as “script- kiddies” due to their use of existing scripts (tools)
- **Journeyman**: hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities; or to focus on different target groups
- **Master**: Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities, or writing new powerful attack toolkits. Often related to APT. Defending against these attackers of the highest difficulty.

You’d better know your enemy: (behavior)

- Though attacks are generally different from each other they share common functionalities
  - Target Acquisition and Information Gathering
  - Initial Access
  - Privilege Escalation
  - Information Gathering and/or System Exploit
  - Maintaining Access
  - Covering Tracks

Examples

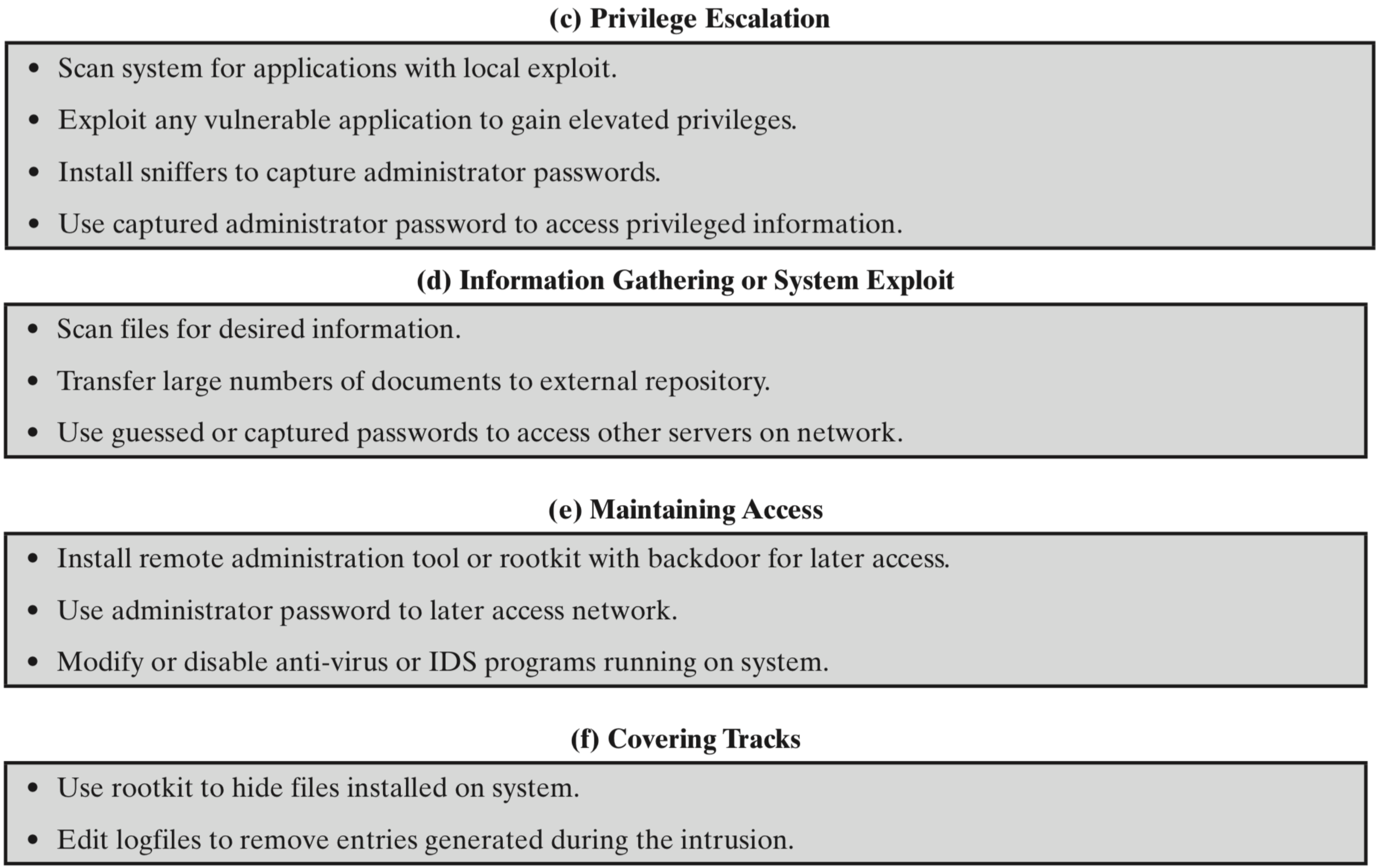


(a) Target Acquisition and Information Gathering

- Explore corporate website for information on corporate structure, personnel, key systems, as well as details of specific Web server and OS used.
- Gather information on target network using DNS lookup tools such as dig, host, and others; and query WHOIS database.
- Map network for accessible services using tools such as NMAP.
- Send query e-mail to customer service contact, review response for information on mail client, server, and OS used, and also details of person responding.
- Identify potentially vulnerable services, for example, vulnerable Web CMS.

(b) Initial Access

- Brute force (guess) a user's Web content management system (CMS) password.
- Exploit vulnerability in Web CMS plugin to gain system access.
- Send spear-phishing e-mail with link to Web browser exploit to key people.



(c) Privilege Escalation

- Scan system for applications with local exploit.
- Exploit any vulnerable application to gain elevated privileges.
- Install sniffers to capture administrator passwords.
- Use captured administrator password to access privileged information.

(d) Information Gathering or System Exploit

- Scan files for desired information.
- Transfer large numbers of documents to external repository.
- Use guessed or captured passwords to access other servers on network.

(e) Maintaining Access

- Install remote administration tool or rootkit with backdoor for later access.
- Use administrator password to later access network.
- Modify or disable anti-virus or IDS programs running on system.

(f) Covering Tracks

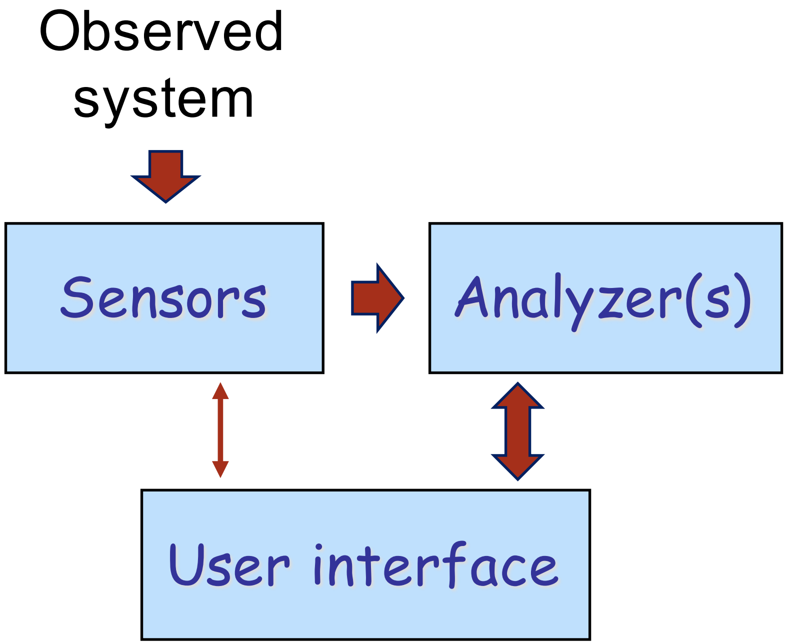
- Use rootkit to hide files installed on system.
- Edit logfiles to remove entries generated during the intrusion.

Intrusion detection systems

Intrusion detection

- **Intrusion detection system:** A hardware or software function that gathers and analyzes information from various areas within a computer or a network to identify possible security intrusions
- **Security intrusion:** Unauthorized act of bypassing the security mechanisms of a system.

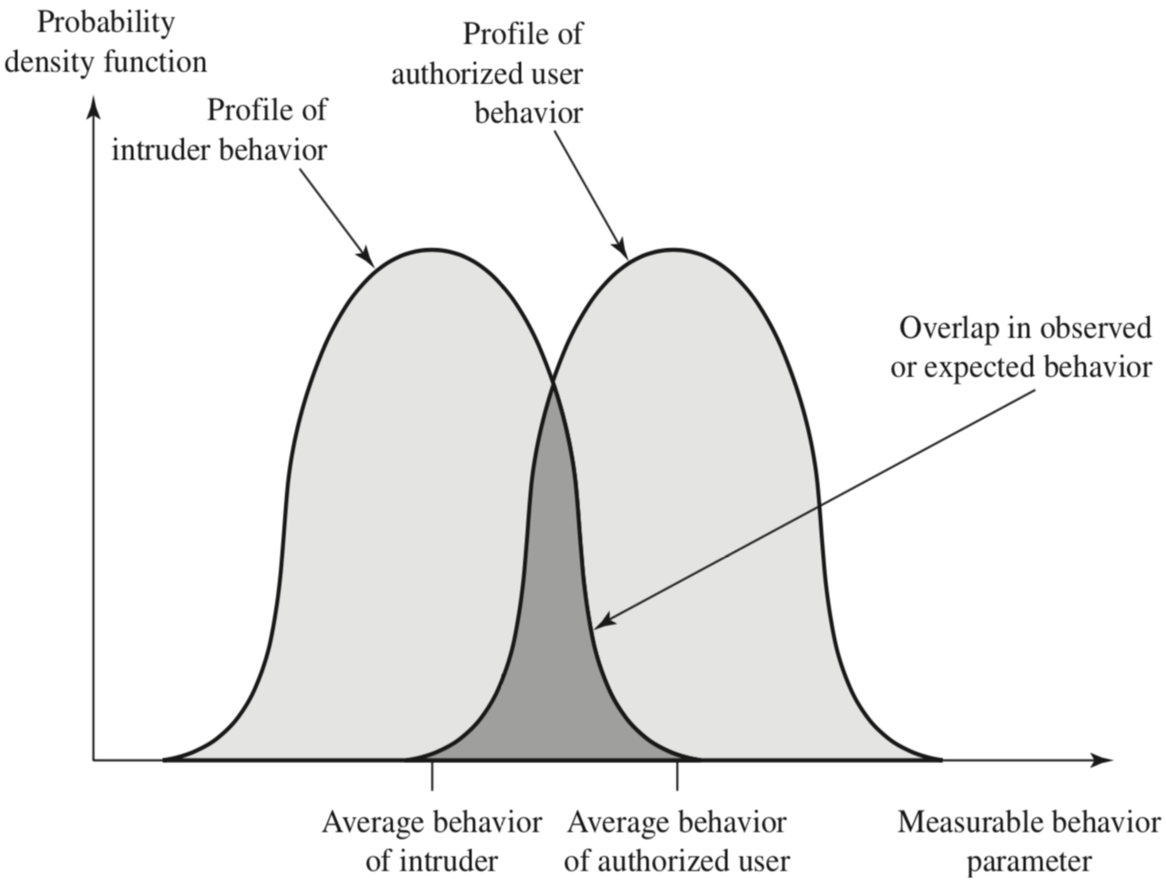
Intrusion detection: main components



- Sensors gather information about: log files, network packets, system call traces
- The analyser detects intrusions, identify kind of intrusions, provides evidence of intrusion, suggests remedies

Host-based IDS (HIDS) vs Network-based IDS (NIDS) vs Hybrid/Distributed IDS

Base-rate fallacy


Probability density function
Profile of intruder behavior
Profile of authorized user behavior
Overlap in observed or expected behavior
Average behavior of intruder
Average behavior of authorized user
Measurable behavior parameter

- ID is a typical Hypothesis testing problem
- Trade-off between false alarm and missed detection rates
- Lack of statistical models makes the problem difficult (even in a Neyman Pearson sense)

Two approaches to ID

- **Anomaly detection**: Involves the collection of data relating to the behavior of legitimate users over a period of time. Then, current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or alternatively that of an intruder
- **Signature or Heuristic detection**: Uses a set of known malicious data patterns (signatures) or attack rules (heuristics) that are compared with current behavior to decide if it is that of an intruder. It is also known as misuse detection. This approach can only identify known attacks for which it has patterns or rule (problems with zero-day attacks)

Systems based on anomaly-detection

- **Statistical methods:** Analysis of the observed behavior using univariate, multivariate, or time-series models
  - data gathering
  - feature extraction
  - statistical HT based on NP criterion
- **Knowledge based methods:** use an expert system that classifies observed behavior according to a set of rules
  - requires definition of rules and human intervention
- **Machine-learning methods:**
  - feature based vs deep learning
  - problems in gathering enough training data and with generalization

Signature-based and heuristic methods

- Complementary advantages and disadvantages of anomaly-based detection
  - characterize observations under the alternate hypothesis
  - works well for known intrusions
- **Signature-based** approaches match a large collection of known patterns of malicious data against data stored on a system or in transit over a network. The signatures must be large enough.
- **Rule-based** approaches are based on rules for identifying known penetrations or penetrations. Rules can also be defined that identify suspicious behavior. The most fruitful approach to developing such rules is to analyze attack tools and scripts collected on the Internet.

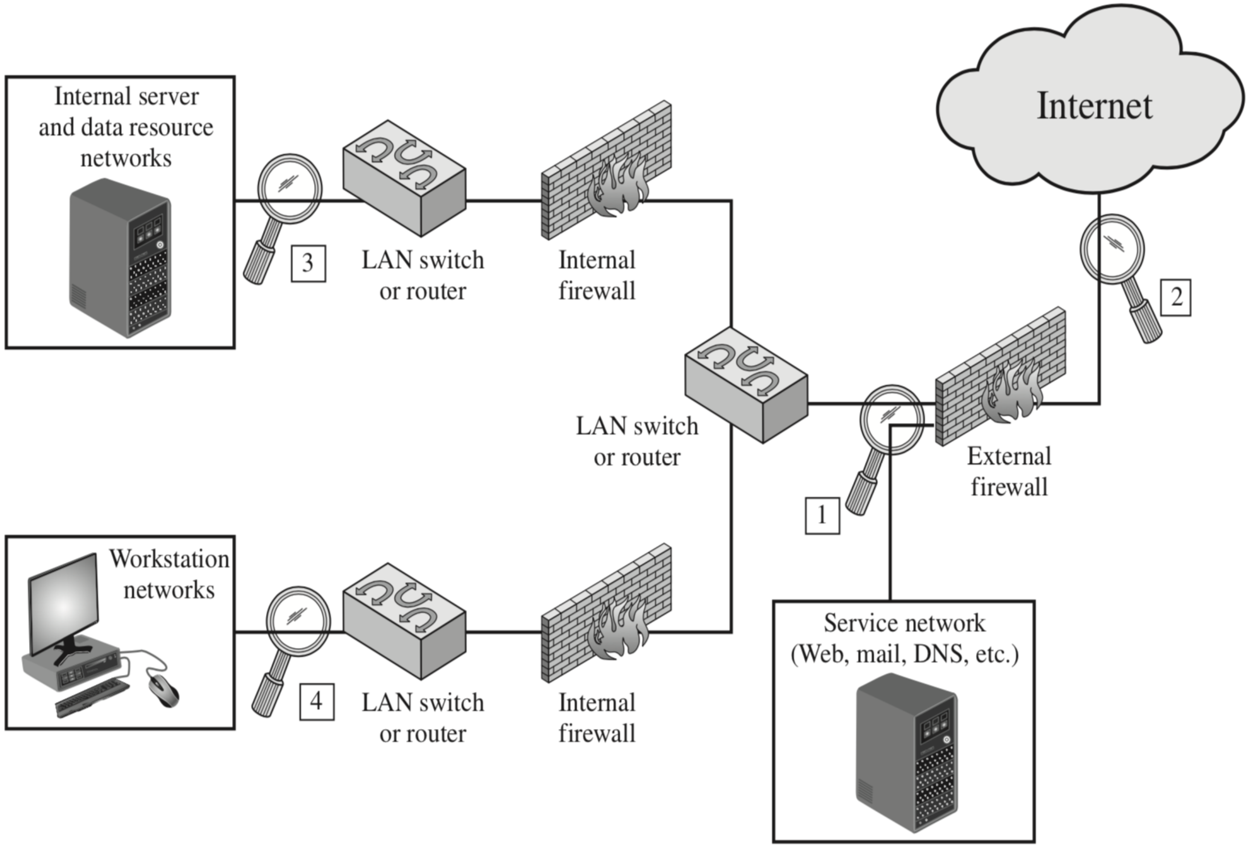
Host-based IDS

- Data collected by sensors
  - **System call traces:** A record of the sequence of systems calls by processes on a system. It works well on Unix and Linux systems, they are problematic on Windows systems (DLL)
  - **Audit (log file) records**: Most modern operating systems include accounting software that collects information on user activity.
  - **File integrity checksums**: periodically scan critical files for changes from the desired baseline.
  - **Registry access**: An approach used on Windows systems is to monitor access to the registry, given the amount of information and access to it used by programs on these systems.

Network-based IDS

- Data collected by sensors
  - **Packets and packets statistics:** all kinds of packets can be analyzed, network-, transport-, and/or application-level packets
  - Problems with encrypted traffic
- Deployment of sensors
  - Inline vs passive sensors
  - Position of NIDS within large organizations must be designed carefully

Deployment of sensors in NIDS

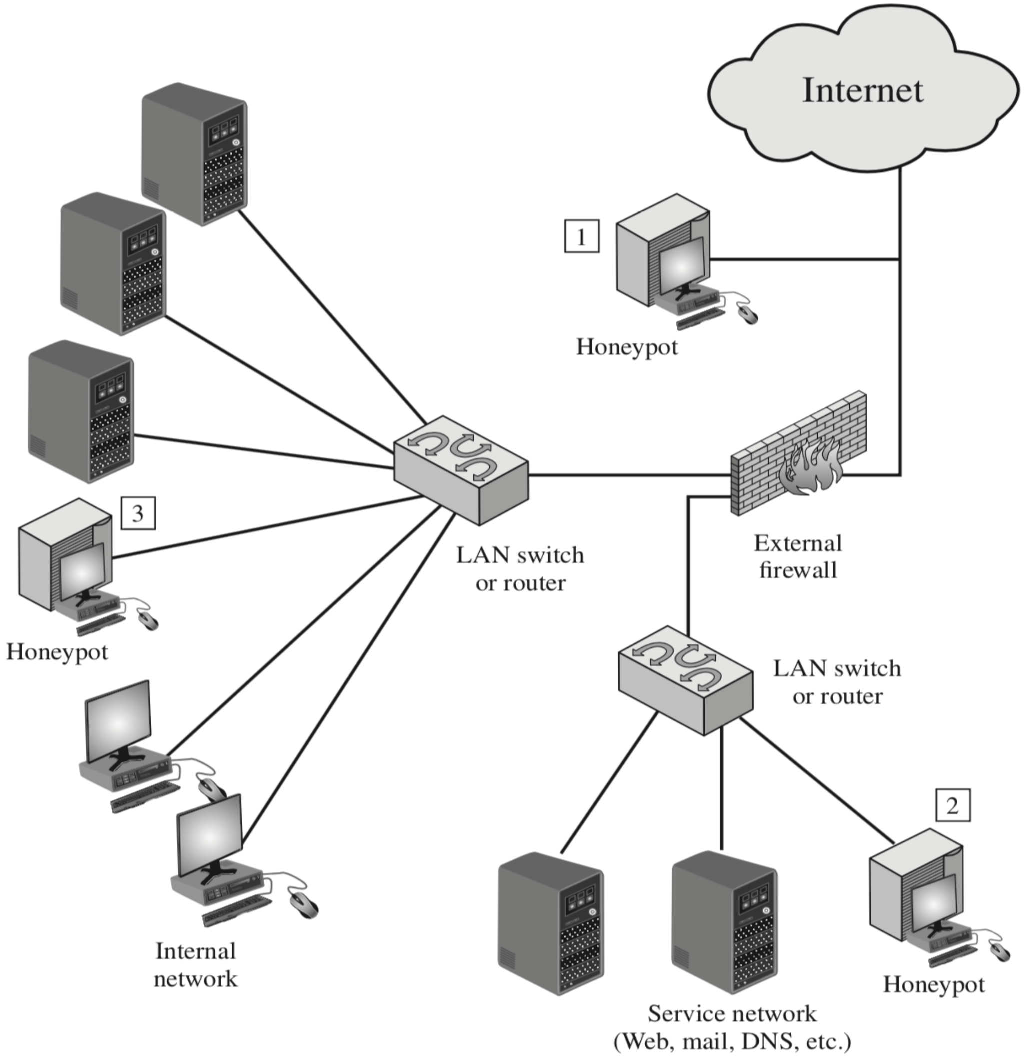


1. Focuses only on attacks that passes the firewall
2. Higher workload, it can document all kinds of (external) attacks
3. Can detect internal attacks, can focus on more specific attacks
4. Similar to 3.

Honeypots

- Honeypots are decoy systems that are designed to divert potential attacker away from critical systems
- Honeypots are designed to:
  - Divert an attacker from accessing critical systems
  - Collect information about the attacker’s activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
- Honeypot have no production value. Thus, any attempt to communicate with the system is most likely a probe, scan, or attack. If a honeypot initiates outbound communication, the system has probably been compromised.

Deployment of honeypots

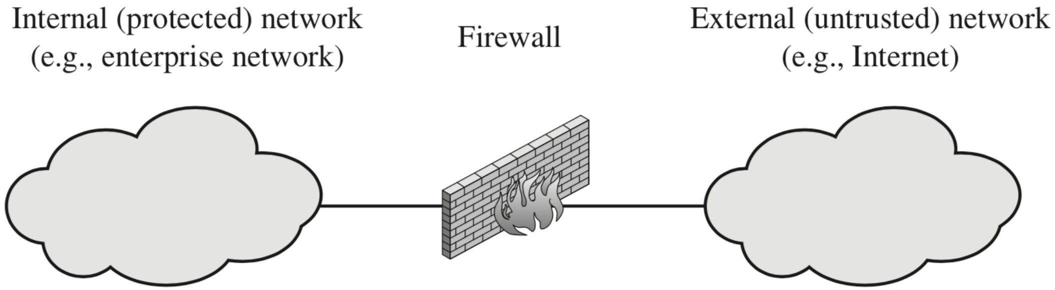


1. High visibility, less risky (an infected honeypot does not risk to compromise the rest of the system)
2. Less visible (firewall must let some traffic to pass in), more risky. Can attract internal attacks
3. Fully internal honeypots. Can catch internal attacks, but it is risky

Intrusion prevention Firewalls

Need and role of firewalls

- Internet connectivity is no longer optional for most organizations
- Internet access enables the outside world to reach and interact with local network assets raising new threats
- Host-based security only may not possible, for sure it is not practical
- The firewall is inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter: most security features are moved from hosts to the perimeter


Internal (protected) network
(e.g., enterprise network)
Firewall
External (untrusted) network
(e.g., Internet)

What a firewall does

- Single check point keeping unauthorized users out of the protected network
- Provides a location for monitoring security-related events.
- Convenient platform for several Internet functions that are not security related
- Platform for IPSec. The firewall can be used to implement virtual private networks.

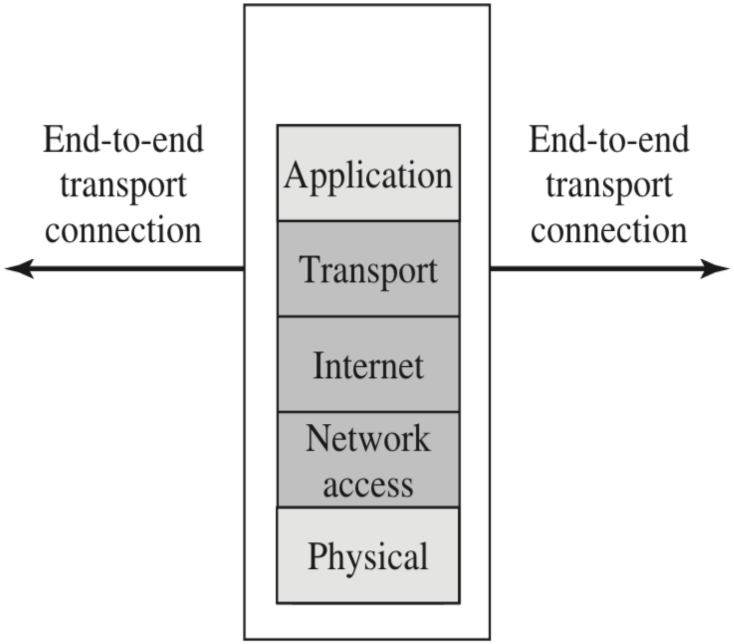
What a firewall doesn’t do

- Cannot protect (completely) against internal threats
- Cannot protect against attacks that bypass the firewall, e.g. systems with wired or mobile broadband capability to connect to an ISP
- Protect against laptops, PDA, or other portable storage device used and infected outside network, then attached and used internally

Types of filtering

- **IP Address and Protocol Values**: Controls access based on the source or destination addresses and port numbers, and other network and transport layer characteristics
- **Application Protocol**: Controls access on the basis of authorized application protocol data.
- **User Identity**: Controls access based on the users identity, (IPSec)
- **Network Activity**: Controls access based on considerations such as the time or request, rate of requests, or other activity patterns.

Packet filtering firewalls


End-to-end transport connection
Application
Transport
Internet
Network access
Physical
End-to-end transport connection

Filter is applied at the packet level. Possible rules include:

- Source IP address
- Destination IP address
- Source and destination transport-level address (the transport-level (TCP or UDP) port number, which defines applications such as SNMP or HTTP)

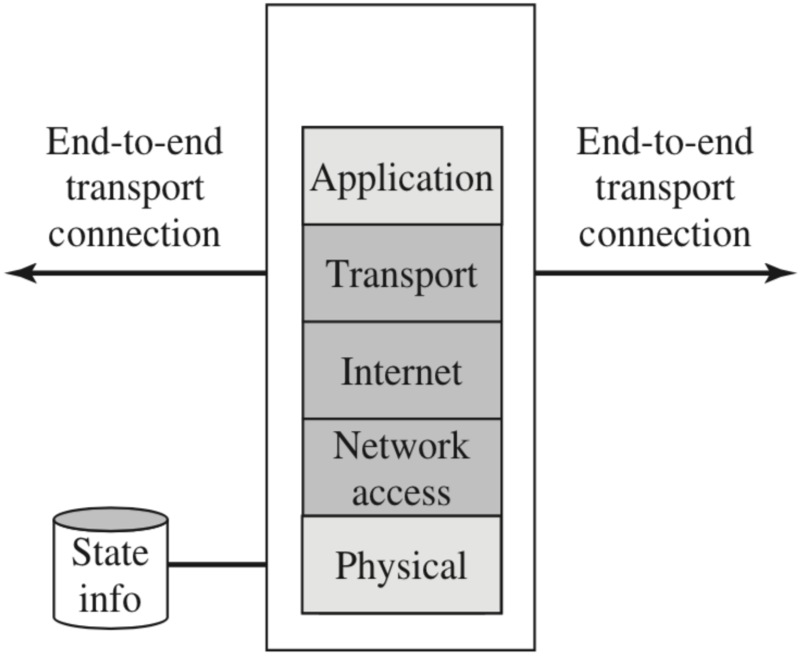
Default = discard: what is not expressly permitted is prohibited

Default = forward: what is not expressly prohibited is permitted.

Limits of packet filtering

- Cannot prevent attacks that **employ application-specific vulnerabilities** or functions.
- Most packet filter firewalls **do not support advanced user authentication schemes**.
- Vulnerable to attacks based on **address spoofing**
- **Improper configurations**: it is easy to accidentally configure a packet filter firewall to allow traffic types, sources, and destinations that should be denied based on an organization's information security policy.

Statefull packet filtering

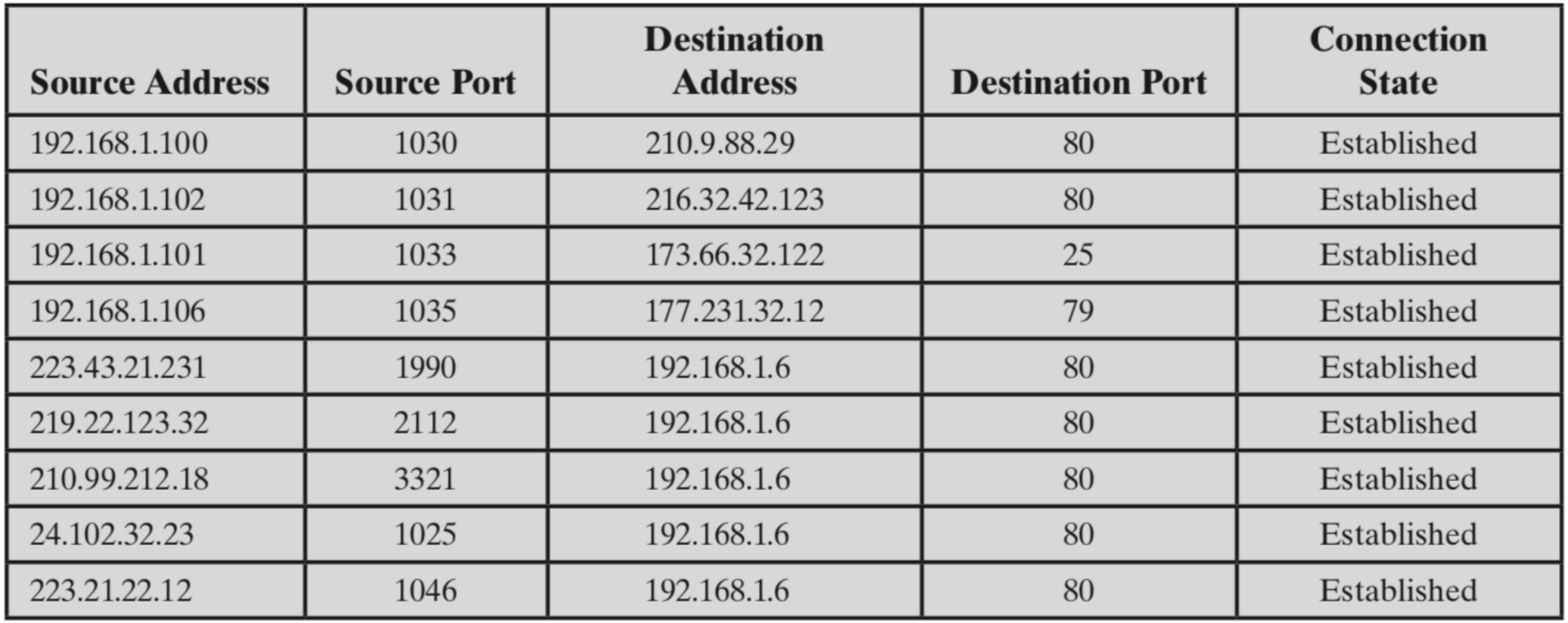


Example: port numbers < 1024 are dedicated to known services, port numbers > 1024 are used on the fly when connections are created

Without state information the firewalls must either block all or no packets coming from ports > 1024.

A stateful packet inspection firewall reviews the same packet information as a packet filtering firewall, but also records information about TCP connections.

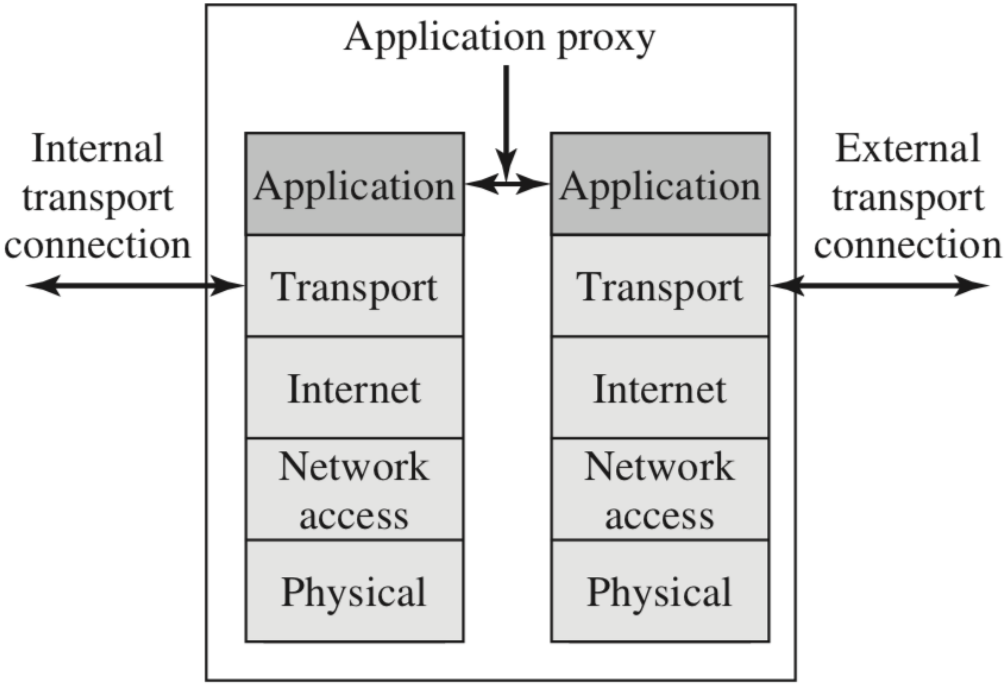
Statefull packet filtering



Source Address	Source Port	Destination Address	Destination Port	Connection State
192.168.1.100	1030	210.9.88.29	80	Established
192.168.1.102	1031	216.32.42.123	80	Established
192.168.1.101	1033	173.66.32.122	25	Established
192.168.1.106	1035	177.231.32.12	79	Established
223.43.21.231	1990	192.168.1.6	80	Established
219.22.123.32	2112	192.168.1.6	80	Established
210.99.212.18	3321	192.168.1.6	80	Established
24.102.32.23	1025	192.168.1.6	80	Established
223.21.22.12	1046	192.168.1.6	80	Established

Outbound packets generated from ports > 1024 are accepted only for destination ports and addresses for which a valid connection has been established

Application proxy firewalls



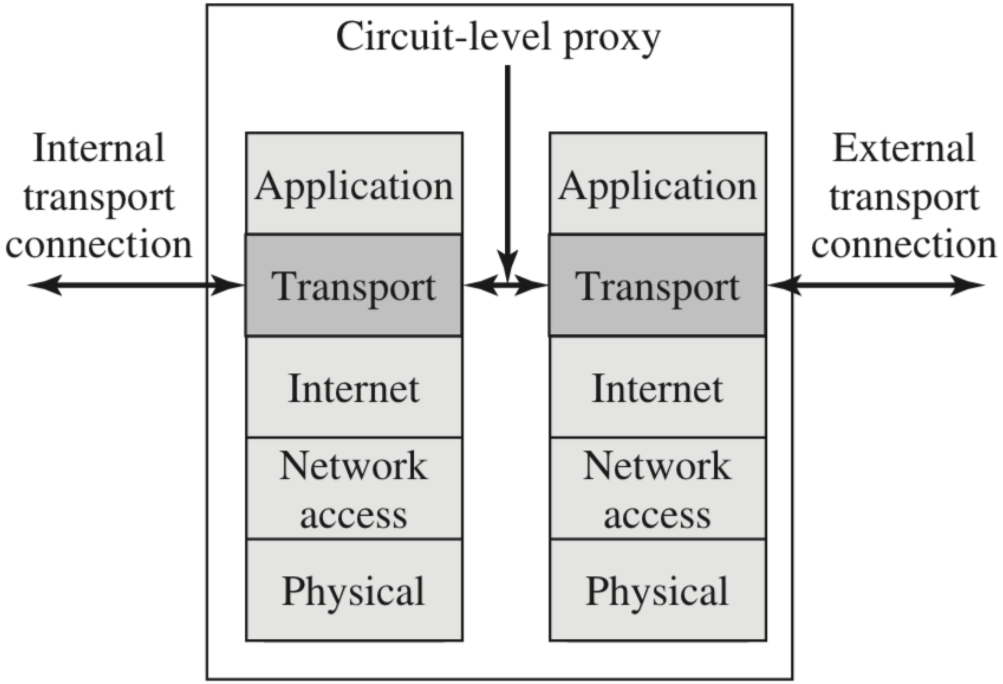
Proxy firewalls are more secure than packet-based firewalls, the price to pay being a computational overhead.

Logging and monitoring at application level can also be implemented easily at the proxy

The user contact the proxy asking to establish an application level connection with a system inside the firewall. The gateway dispatches the packets by running the proxy code

Circuit-level proxy firewalls

If the system administrator trusts internal users the gateway can be configured to support application-level or proxy service on inbound connections and circuit-level functions for outbound connections.

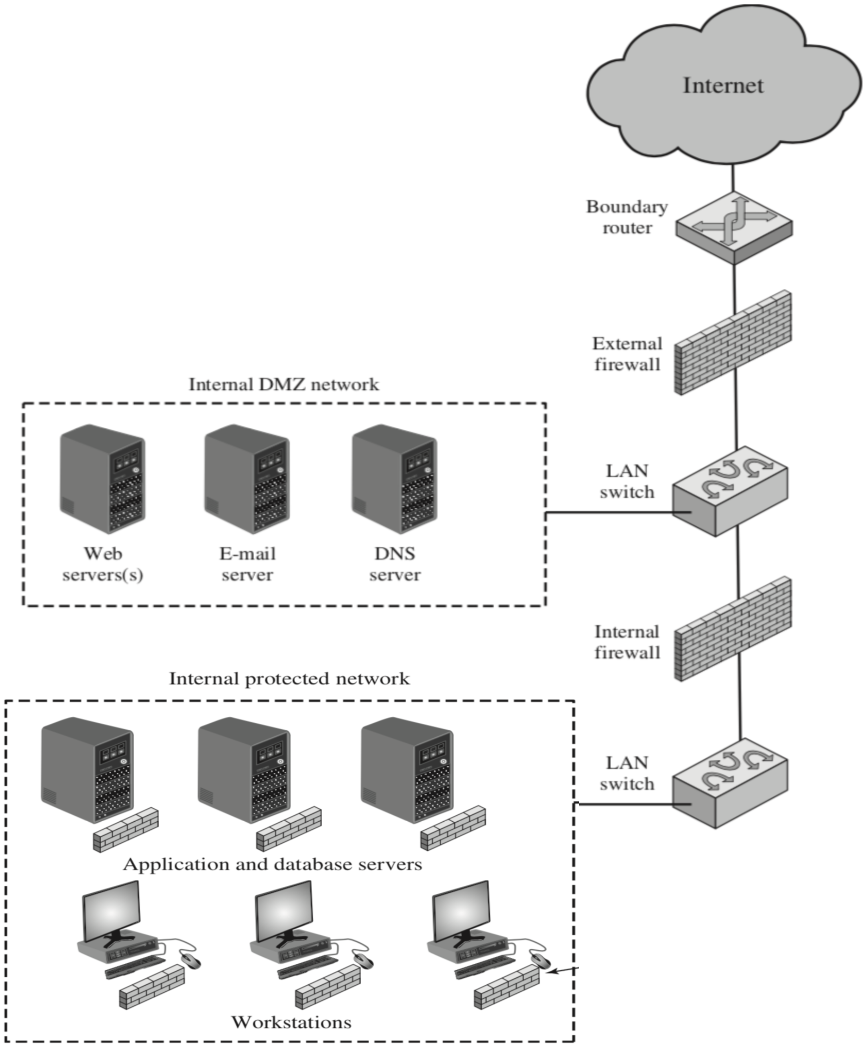


Similar to the application proxy, however when a connection is established between a server and a client, no further application-level control is made

Where do firewalls reside

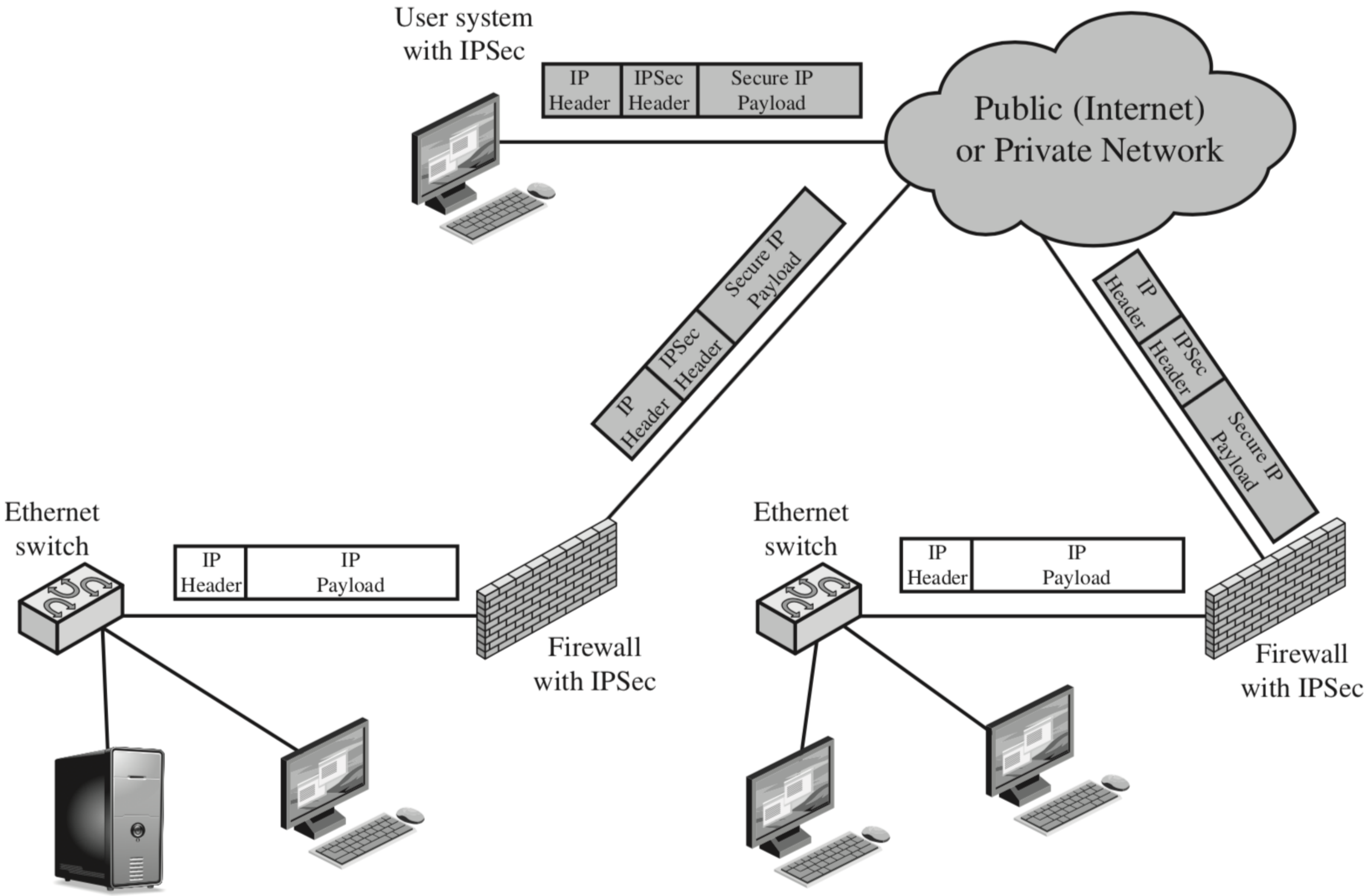
- **Bastion host**
  - typically serves as a platform for application-level or circuit-level gateways, or to support IPSec
  - usually running a hardened operating system
  - runs only essential services
  - maintains detailed audit information
- **Host based firewalls**
  - server firewalls
  - personal
- **Network device firewalls**
- **Virtual firewalls**

Where do firewalls reside



- In medium or large corporate networks several firewall-levels coexist
- The DMZ network may include e-mail servers, corporate websites, DNS
- Internal firewalls protect also from attacks generated from the DNZ and directed to the DMZ from the internal networks

Virtual Private Networks (VPNs)



Intrusion Detection and Prevention

- **IDS + firewall functionalities**
  - An IDS that after detection tries to prevent the intruder to carry out its payload
  - A firewall that filters packets according to the result of an IDS analysis
- **Positioning and strategies are similar to those described for IDS and firewalls**

References

- W. Stallings, L. Brown, “*Computer security: principles and practices”,* Pearson, 4-th edition. Chapters 8 and 9
- Lectures notes (these slides)