Intrusion Detection & Firewalls

Chapters 8 & 9

Dr Naveed Khan

n.khan@ulster.ac.uk

COM398

Introduction

Intrusion and Intruders

Intrusion:

An intrusion is defined as the unauthorized use, or abuse of computer system by either authorized user or external perpetrator (person who carries harmful or illegal act.)

Intruder:

An intruder is a person who attempts to gain unauthorized access to a system or to damage that system

Classes of Intruders

- **Cyber Criminal**
- **Activist (Hacktivists)**
- **State- Sponsored Organization**
- **Others**

Classes of Intruders – Cyber Criminals

- Individuals or members of an organized crime group with a goal of financial reward
- Their activities may include:
  - Identity theft
  - Theft of financial credentials
  - Corporate espionage
  - Data theft
  - Data ransoming
- Typically they meet in underground forums to trade tips and data and coordinate attacks

Classes of Intruders – Activists

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also known as hacktivists
  - Skill level is often quite low
- The aim of their attacks is often to promote and publicize their cause typically through:
  - Website defacement
  - Denial of service attacks
  - Theft and distribution of data that results in negative publicity or compromise of their targets

Classes of Intruders – State-Sponsored Organizations

Groups of hackers sponsored by governments to conduct espionage or sabotage activities

Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class

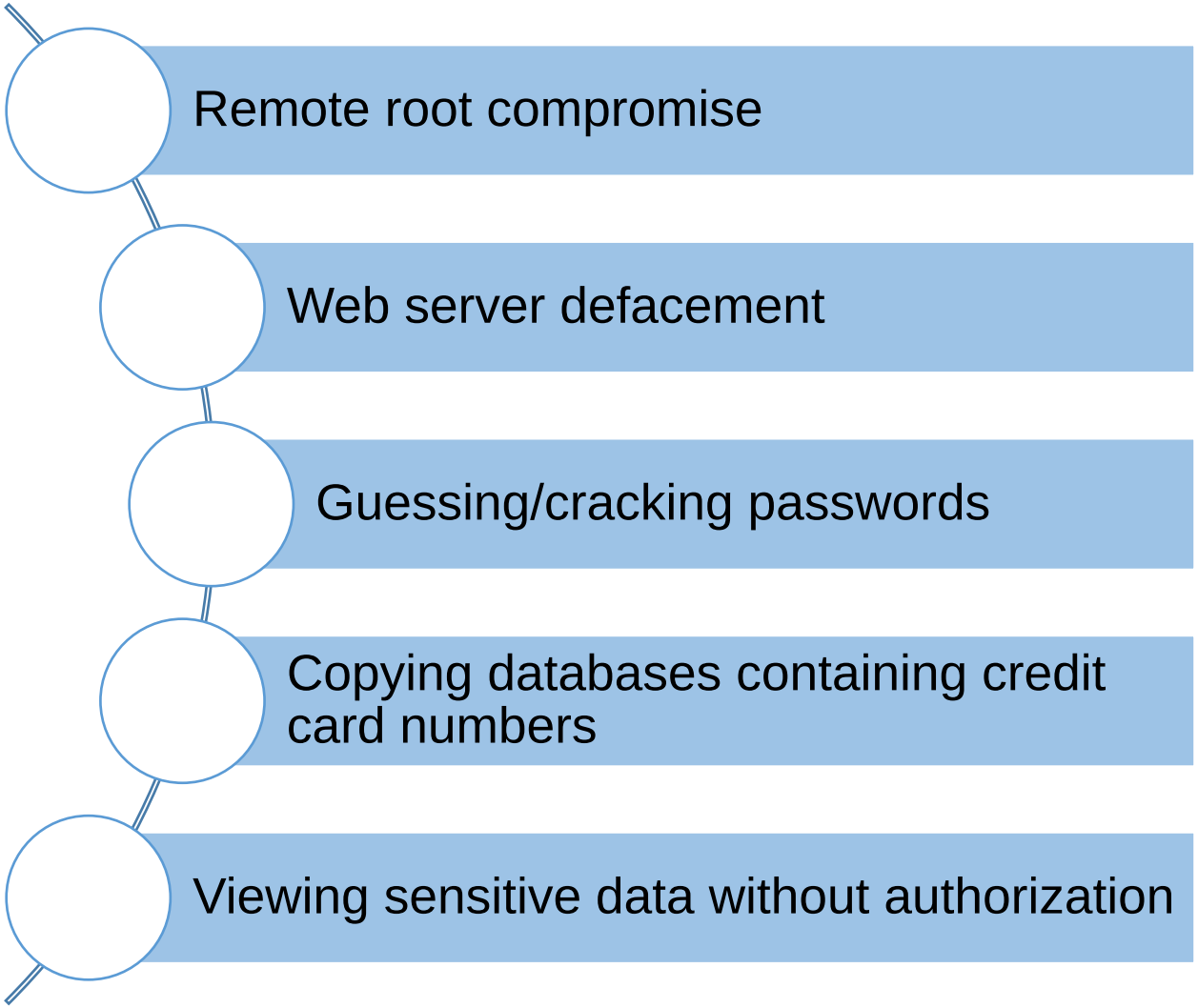
Widespread nature and scope of these activities by a wide range of countries to gain access to state secrets

Classes of Intruders – Others

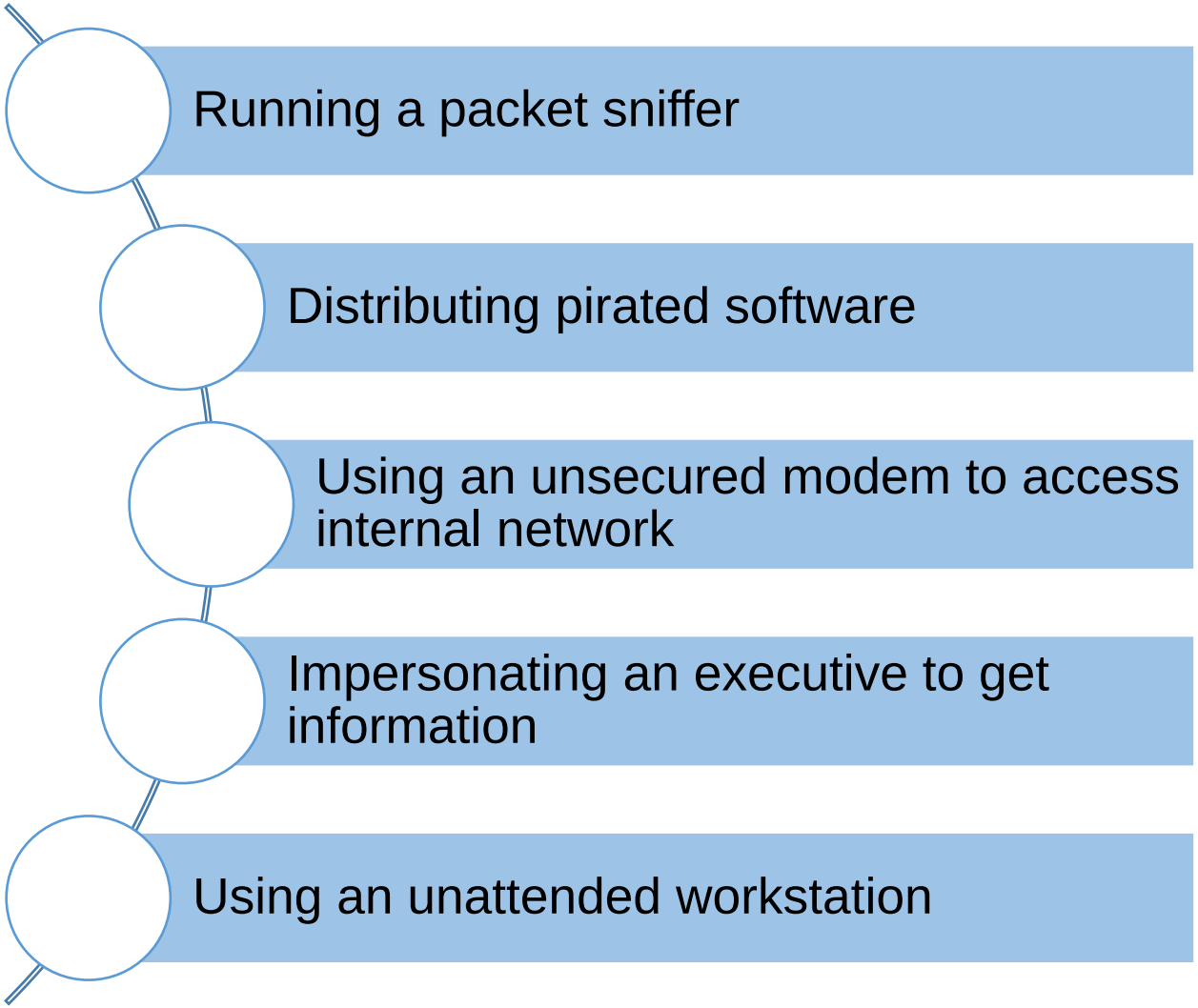
- Hackers with motivations other than those previously listed
- Include classic hackers or crackers who are motivated by technical challenges or by peer-group esteem and reputation
- Many of those responsible for discovering new categories of buffer overflow vulnerabilities could be regarded as members of this class.
- Given the wide availability of attack toolkits, there is a pool of “hobby hackers” using them to explore system and network security

Examples of Intrusion

Intruder attack from Benign to Serious



Examples of Intrusion



Intruder Behavior

Target acquisition and information gathering	**Initial access**	**Privilege escalation**
Information gathering or system exploit	**Maintaining access**	**Covering tracks**

Intrusion Techniques

- To gain access to a system or to increase the range of privileges accessible on a system.
- Most initial attacks use system or software vulnerabilities that allow a user to execute code that opens a back door into a system.
- Alternatively, the intruder attempts to acquire information that should have been protected.
- In some cases, this information is in the form of a user password.
- Typically, a system must maintain a file that associates a password with each authorized user.

Intrusion Techniques

- The password file can be protected in one of two ways.
- **One-way function**: The system stores only the value of a function based on the user's password. When the user presents a password, the system transforms that password and compares it with the stored value. In practice, the system usually performs a one-way transformation (not reversible) in which the password is used to generate a key for the one-way function and in which a fixed-length output is produced.
- **Access Control:** Access to the password file is limited to one or a very few accounts.

Definitions

- **Security Intrusion**

  Unauthorized act of bypassing the security mechanisms of a system

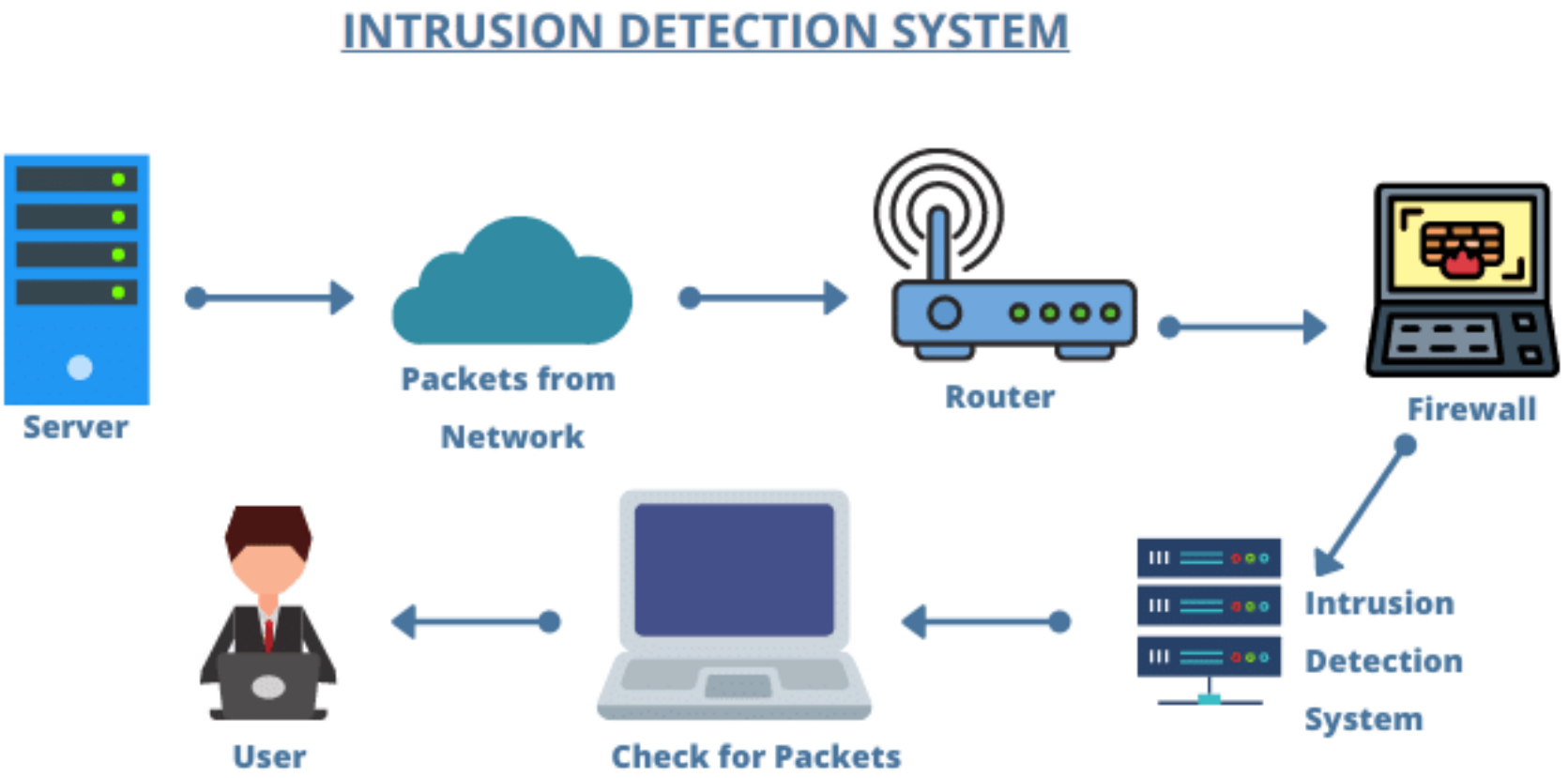
- **Intrusion Detection**

  A hardware or software function that gathers and analyzes information from various areas within a computer or a network to identify possible security intrusions

Intrusion Detection System (IDS)

- An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered.
- Some intrusion detection system are capable of taking actions when malicious activity or anomalous traffic is detected.
- It may include blocking traffic sent form suspicious Internet Protocol (IP) addresses. This system called as Intrusion Prevention System (IPS).

Intrusion Detection System (IDS)



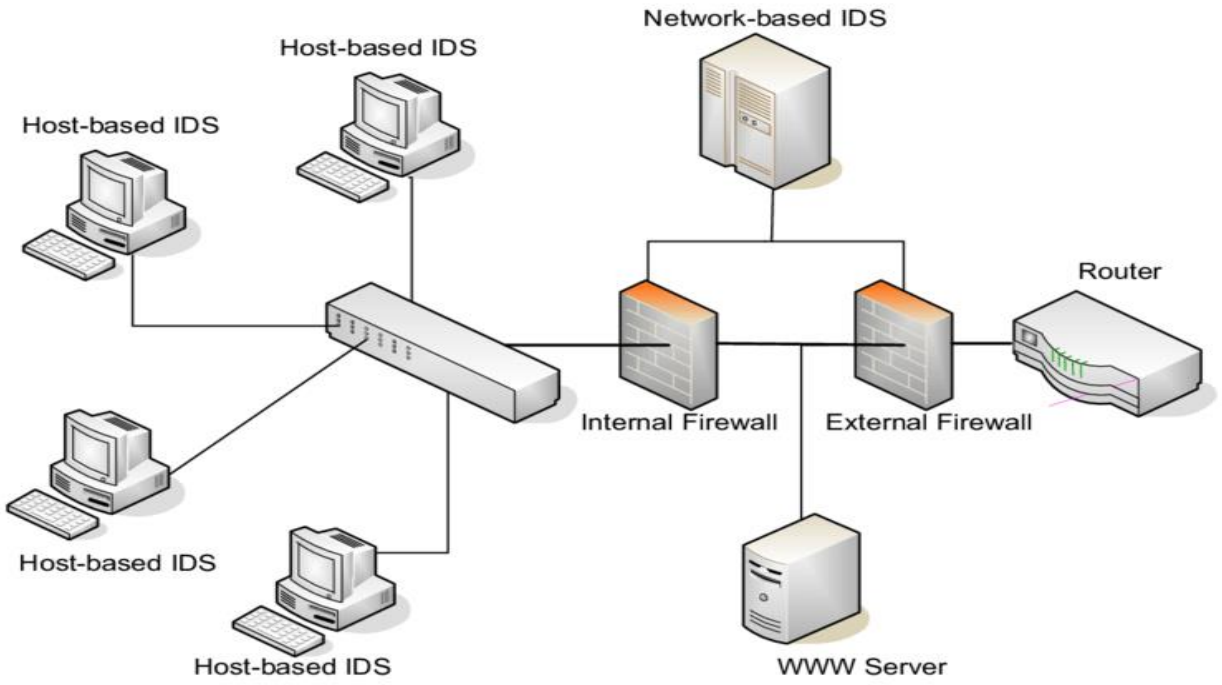
www.networksimulationtools.com

Intrusion Detection System (IDS)

- **IDS logical components**
  - **Sensors**
    - collect data (e.g., network packets, log files, and system call traces)
  - **Analyzer**
    - Determine if intrusion has occurred
  - **User Interface**
    - View output or control system behavior.

Intrusion Detection System (IDS)

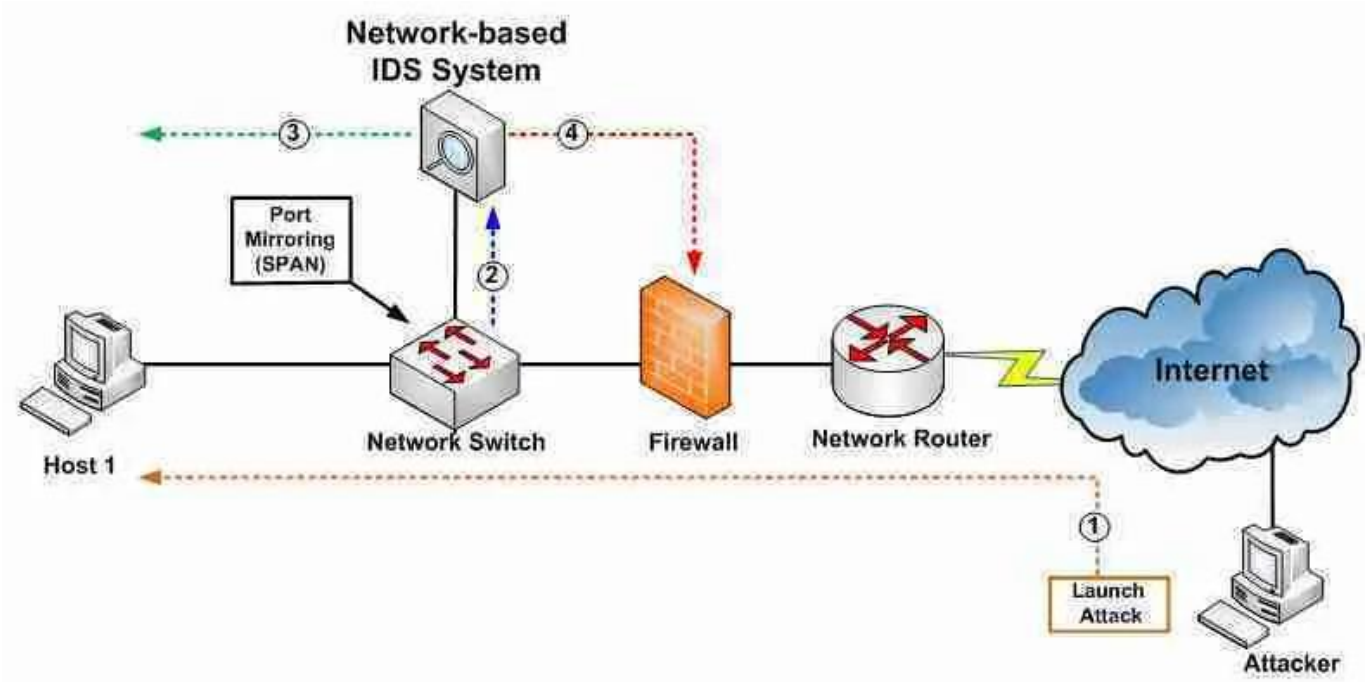
- **Host-based IDS (HIDS)**
  - Monitors the characteristics of a single host for suspicious activity



https://www.liquidweb.com/blog/host-based-intrusion-detection-system/

Intrusion Detection System (IDS)

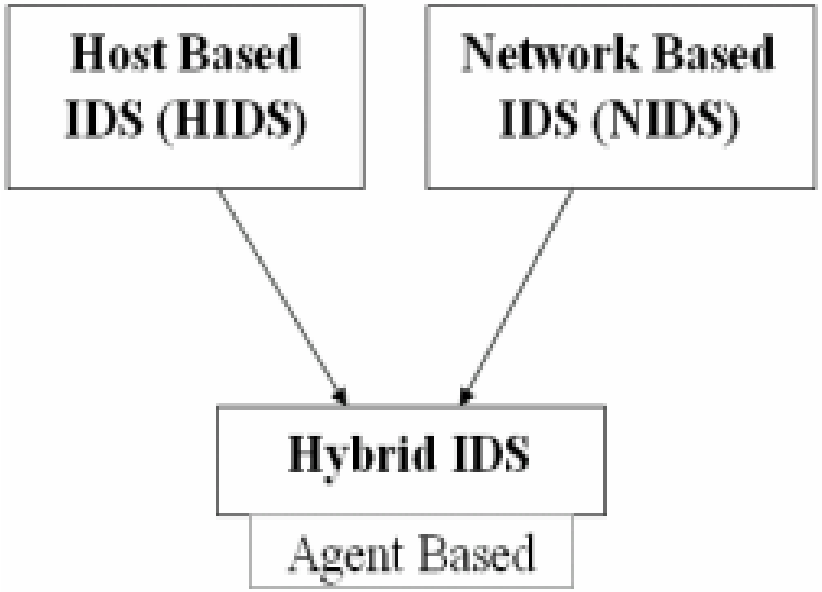
- **Network-based IDS (NIDS)**
  - Monitors network traffic and analyzes network, transport, and application protocols to identify suspicious activity



https://www.researchgate.net/figure/Architecture-of-network-based-intrusion-detection-system-NIDS_fig1_357153369

Intrusion Detection System (IDS)

- **Distributed or hybrid IDS**
  - Combines information from a number of sensors, often both host and network based, in a central analyzer that is able to better identify and respond to intrusion activity



https://arxiv.org/ftp/arxiv/papers/1312/1312.2052.pdf

IDS Requirements

Run continually	Be fault tolerant	Resist subversion
Impose a minimal overhead on system	Configured according to system security policies	Adapt to changes in systems and users
Scale to monitor large numbers of systems	Provide graceful degradation of service	Allow dynamic reconfiguration

Analysis Approaches

Anomaly detection

- Involves the collection of data relating to the behavior of legitimate users over a period of time
- Current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or that of an intruder

Signature/Heuristic detection

- Uses a set of known malicious data patterns or attack rules that are compared with current behavior
- Also known as misuse detection
- Can only identify known attacks for which it has patterns or rules

Signature or Heuristic Detection

Signature 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 need to be large enough to minimize the false alarm rate, while still detecting a sufficiently large fraction of malicious data

Widely used in anti-virus products, network traffic scanning proxies, and in NIDS

Rule-based heuristic identification

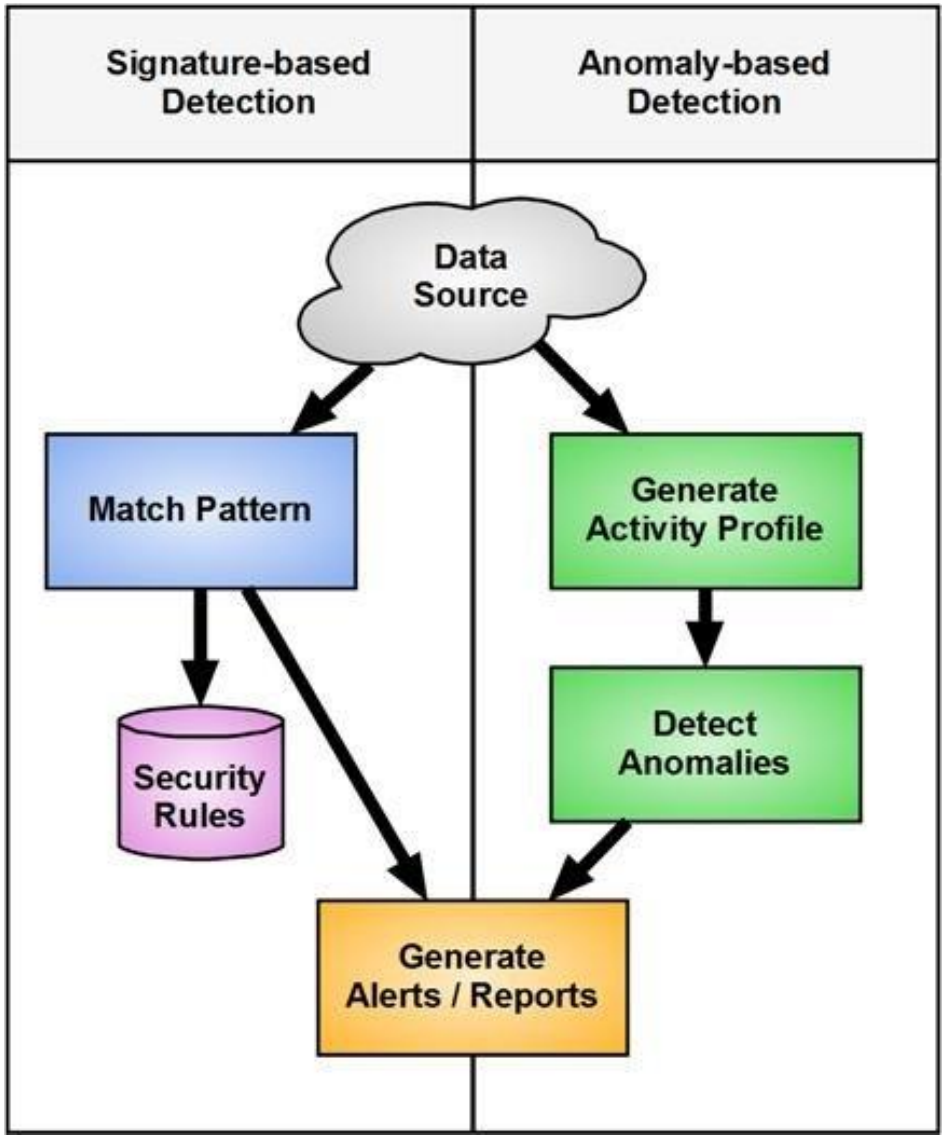
Involves the use of rules for identifying known penetrations or penetrations that would exploit known weaknesses

Rules can also be defined that identify suspicious behavior, even when the behavior is within the bounds of established patterns of usage

Typically rules used are specific

SNORT is an example of a rule-based NIDS

Analysis Approaches



https://www.researchgate.net/publication/297171228_Intrusion_Detection_and_Prevention_Systems_Overview_of_Snort_and_Suricata

Anomaly Detection

A variety of classification approaches are used:

Statistical	Knowledge based	Machine-learning
• Analysis of the observed behavior using univariate, multivariate, or time-series models of observed metrics	• Approaches use an expert system that classifies observed behavior according to a set of rules that model legitimate behavior	• Approaches automatically determine a suitable classification model from the training data using data mining techniques

Network-Based IDS (NIDS)

Monitors traffic at selected points on a network

Examines traffic packet by packet in real or close to real time

May examine network, transport, and/or application-level protocol activity

Comprised of a number of sensors, one or more servers for NIDS management functions, and one or more management consoles for the human interface

Analysis of traffic patterns may be done at the sensor, the management server or a combination of the two

Network-Based IDS (NIDS)

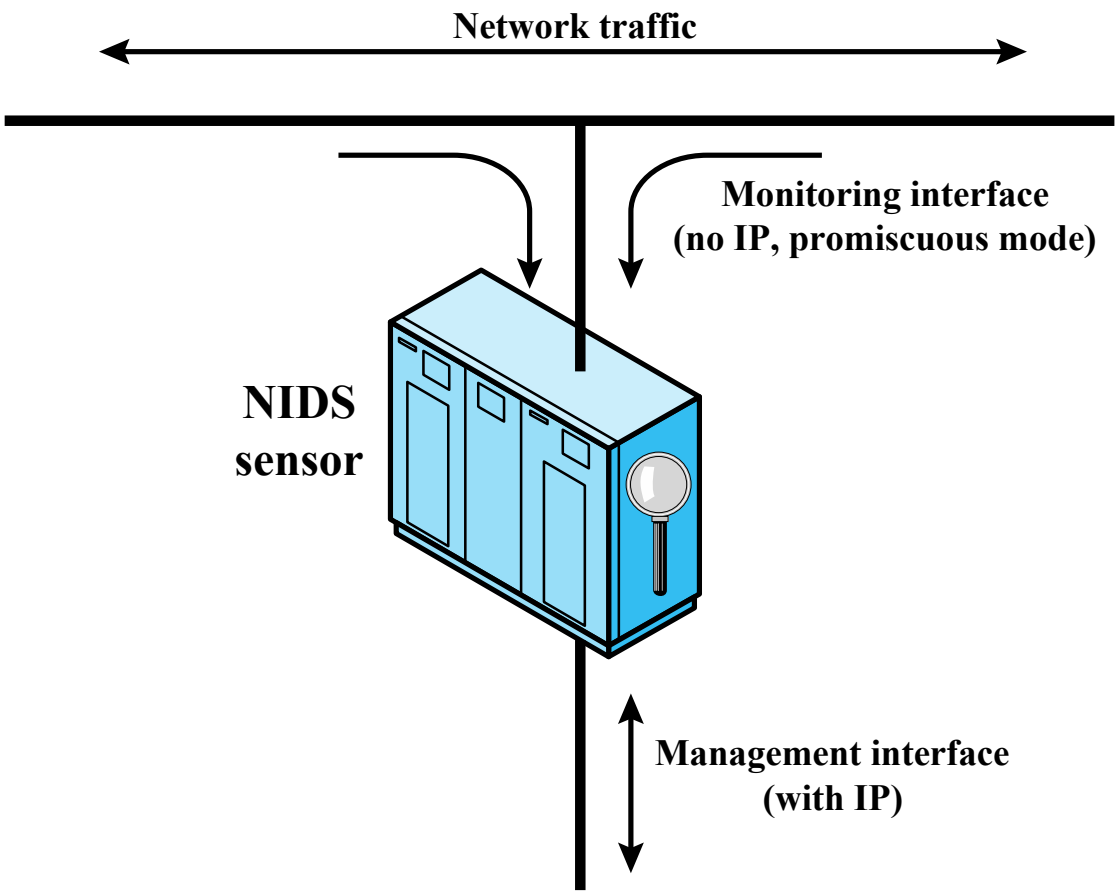


Figure 8.4 Passive NIDS Sensor

Stateful Protocol Analysis (SPA)

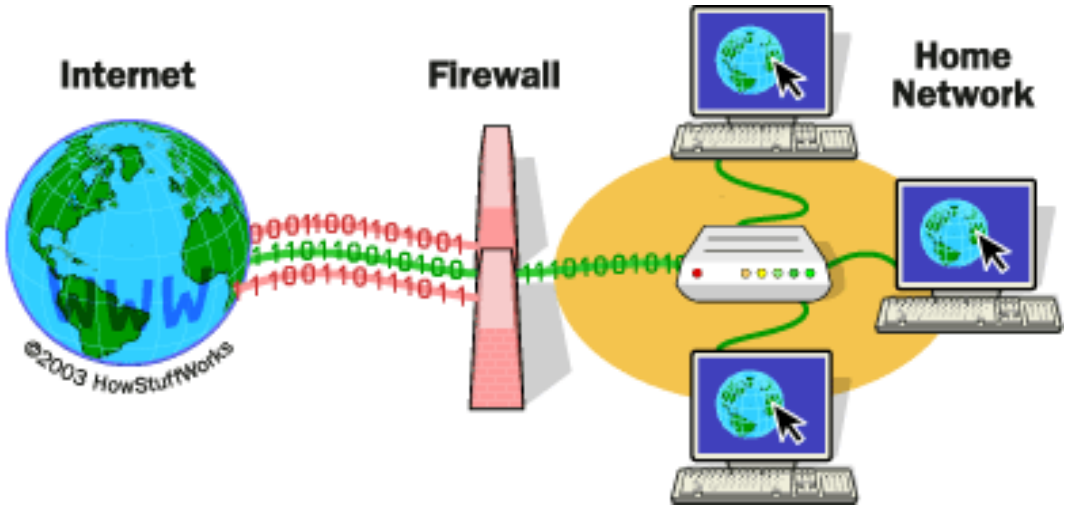
- Subset of anomaly detection that compares observed network traffic against predetermined universal vendor supplied profiles of benign protocol traffic
    - This distinguishes it from anomaly techniques trained with organization specific traffic protocols
- Understands and tracks network, transport, and application protocol states to ensure they progress as expected
- A key disadvantage is the high resource use it requires

Honeypots

- Decoy systems designed to:
  - Lure a potential attacker away from critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond
- Systems are filled with fabricated information that a legitimate user of the system wouldn't access
- Resources that have no production value
  - Therefore, incoming communication is most likely a probe, scan, or attack
  - Initiated outbound communication suggests that the system has probably been compromised

Firewall ?

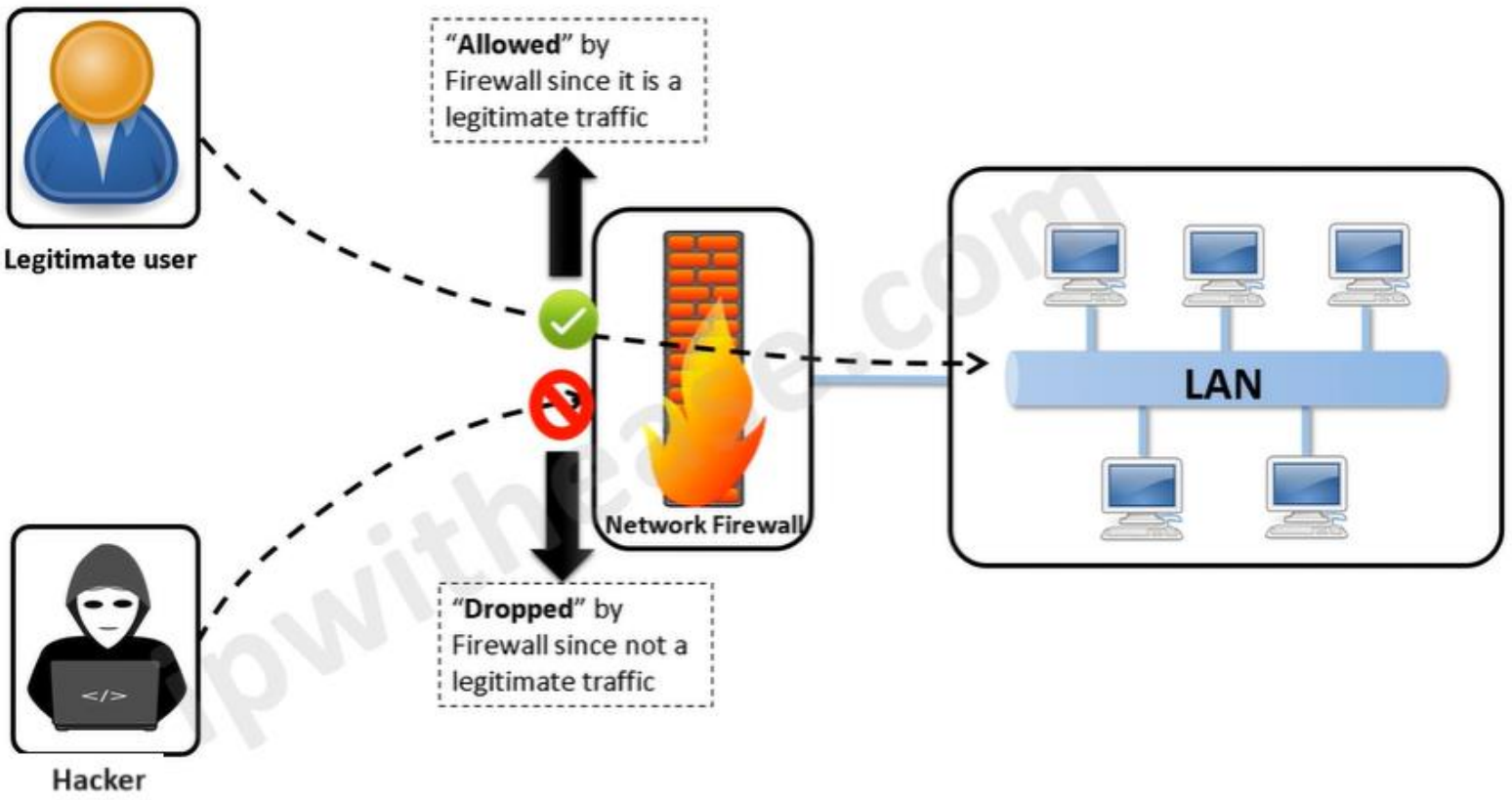
- A network security device that monitors and filters incoming and outgoing network traffic
- Based on an organization's previously established security policies.
- A barrier that sits between a private internal network and the public Internet.



https://computer.howstuffworks.com/firewall.htm

The Need For Firewalls

- Internet connectivity is essential
  - However, it creates a threat
- Effective means of protecting LANs
- Inserted between the premises network and the Internet to establish a controlled link
  - Can be a single computer system or a set of two or more systems working together
- Used as a perimeter defense
  - Single choke point to impose security and auditing
  - Insulates/protect the internal systems from external networks


"Allowed" by Firewall since it is a legitimate traffic
Legitimate user
Network Firewall
LAN
"Dropped" by Firewall since not a legitimate traffic
Hacker

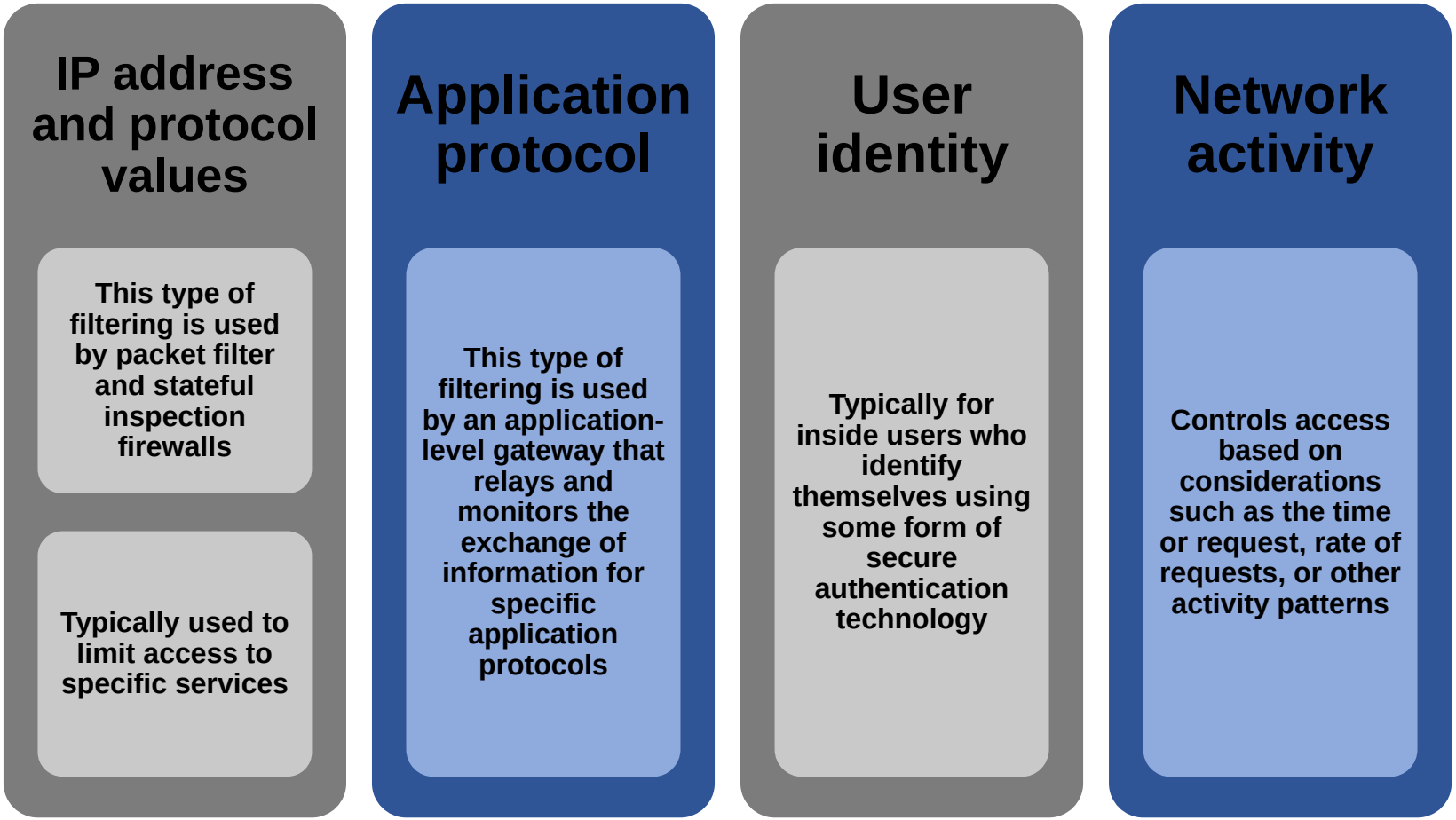
Firewall

Firewall Access Policy

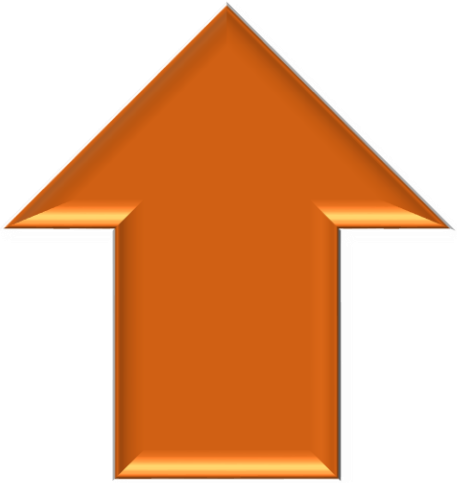
- A critical component in the planning and implementation of a firewall is specifying a suitable access policy
  - This lists the types of traffic authorized to pass through the firewall
  - Includes address ranges, protocols, applications and content types
- This policy should be developed from the organization's information security risk assessment and policy
- Should be developed from a broad specification of which traffic types the organization needs to support
  - Then refined to detail the filter elements which can then be implemented within an appropriate firewall topology

Firewall Filter Characteristics

- Characteristics that a firewall access policy could use to filter traffic include:

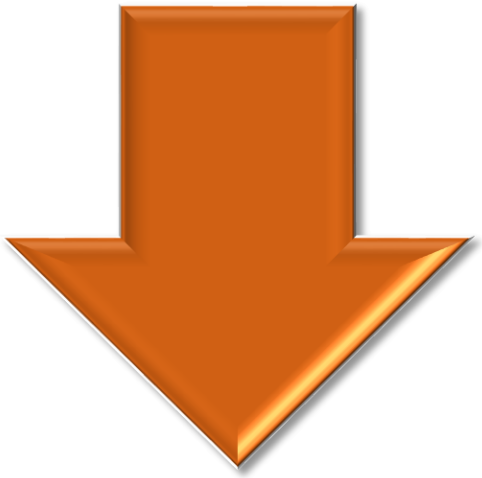


Firewall Capabilities And Limits



Capabilities

- Defines a single choke point
- Provides a location for monitoring security events
- Convenient platform for several Internet functions that are not security related
- Can serve as the platform for IPSec



Limitations

- Cannot protect against attacks bypassing firewall
- May not protect fully against internal threats
- Improperly secured wireless LAN can be accessed from outside the organization
- Laptop, PDA, or portable storage device may be infected outside the corporate network then used internally

Packet Filtering Firewall

- Applies rules to each incoming and outgoing IP packet
  - Typically a list of rules based on matches in the IP or TCP header
  - Forwards or discards the packet based on rules match

Filtering rules are based on information contained in a network packet
• Source IP address • Destination IP address • Source and destination transport-level address • IP protocol field • Interface

- Two default policies:
  - Discard - prohibit unless expressly permitted
  - More conservative, controlled, visible to users
- Forward - permit unless expressly prohibited
  - Easier to manage and use but less secure

Table 9.1- Packet-Filtering Examples

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

Packet Filter
Advantages And Weaknesses

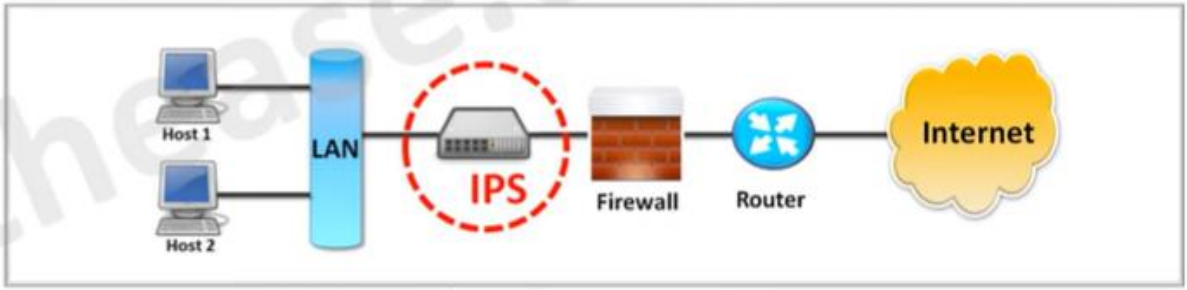
- Advantages
  - Simplicity
  - Typically transparent to users and are very fast
- Weaknesses
  - Cannot prevent attacks that employ application specific vulnerabilities or functions
  - Limited logging functionality
  - Do not support advanced user authentication
  - Vulnerable to attacks on TCP/IP protocol bugs
  - Improper configuration can lead to breaches

Intrusion Prevention Systems (IPS)

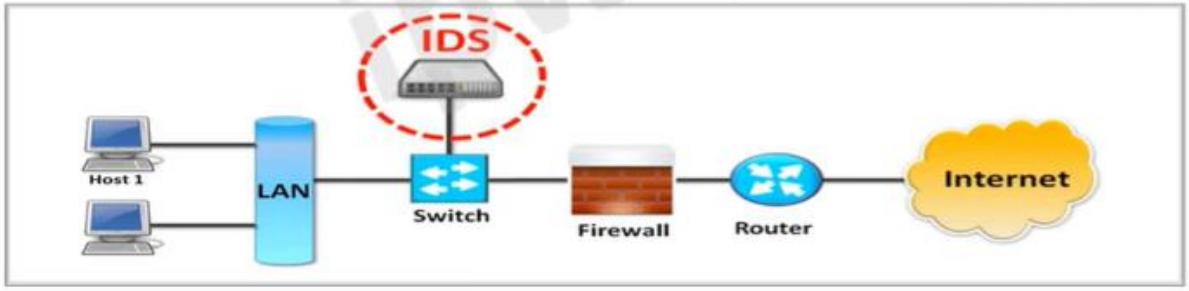
- Also known as Intrusion Detection and Prevention System (IDPS)
- Is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity
- Can be host-based, network-based, or distributed/hybrid
- Can use anomaly detection to identify behavior that is not that of legitimate users, or signature/heuristic detection to identify known malicious behavior can block traffic as a firewall does, but makes use of the types of algorithms developed for IDSs to determine when to do so

Firewall vs IPS vs IDS

VS



VS



Thanks!