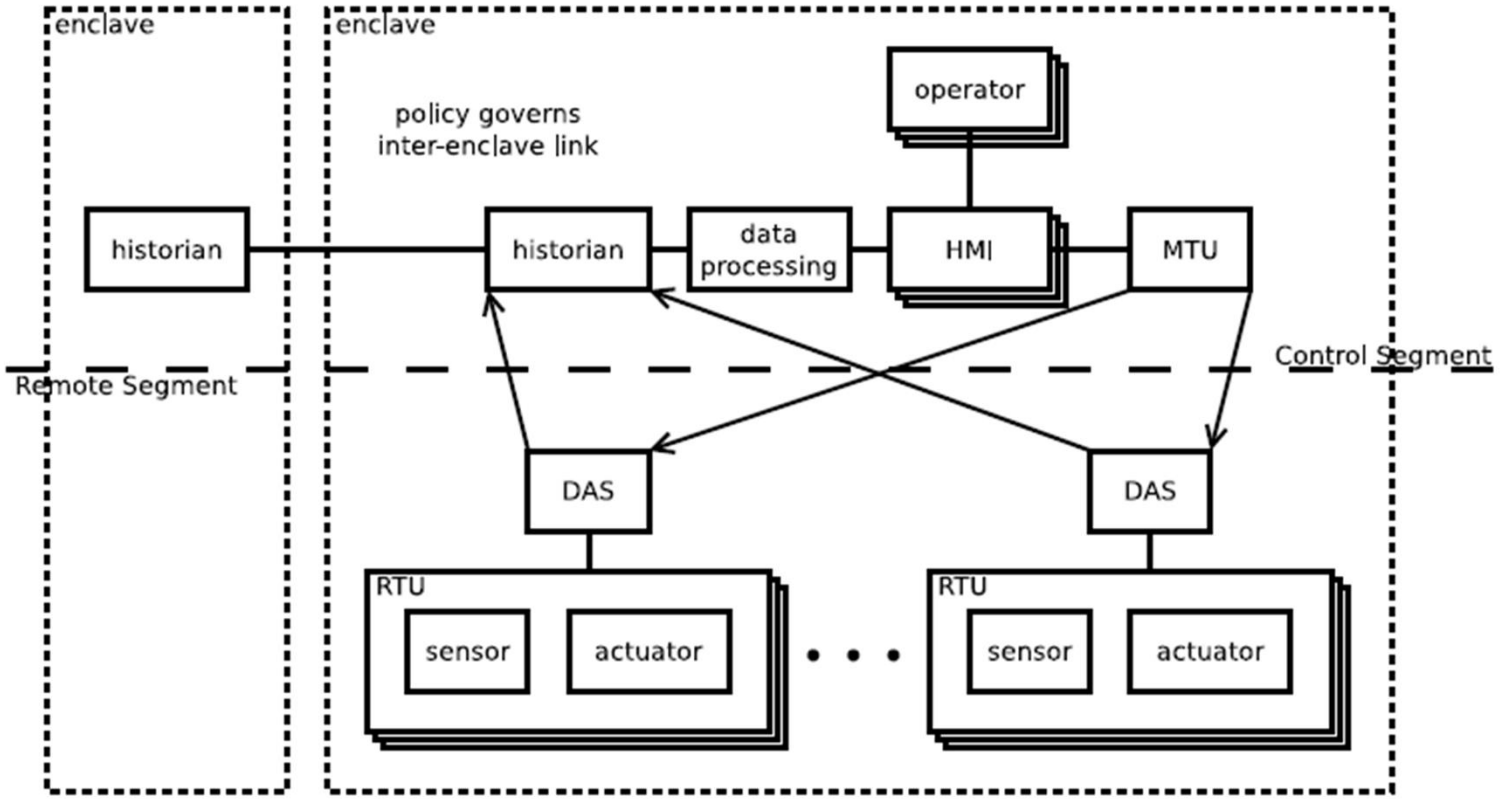
Intrusion Detection System & Firewall

S.Venkatesan

Acknowledgement: The contents, example scripts and some figures are copied from various sources.
Thanks to all authors and sources made those contents public and usable for educational purpose

Abstract Model



Core Functions - IDS

- Collecting data regarding suspects –
  - Data collection is the process by which a CPS accumulates audit data;
  - the result is one or more binary or human-readable files or databases.
  - Examples of collection are: logging system calls on the local node, recording traffic received on a network interface and gathering hearsay reputation scores.

- Data analysis is the process by
  - which a CPS audits the collected data;
  - the result can be binary (bad/good), ternary (bad/good/inconclusive) or continuous (between 0 and 100% bad probability).
  - Examples of analysis are: pattern matching, statistical analysis and data mining.

Metrics

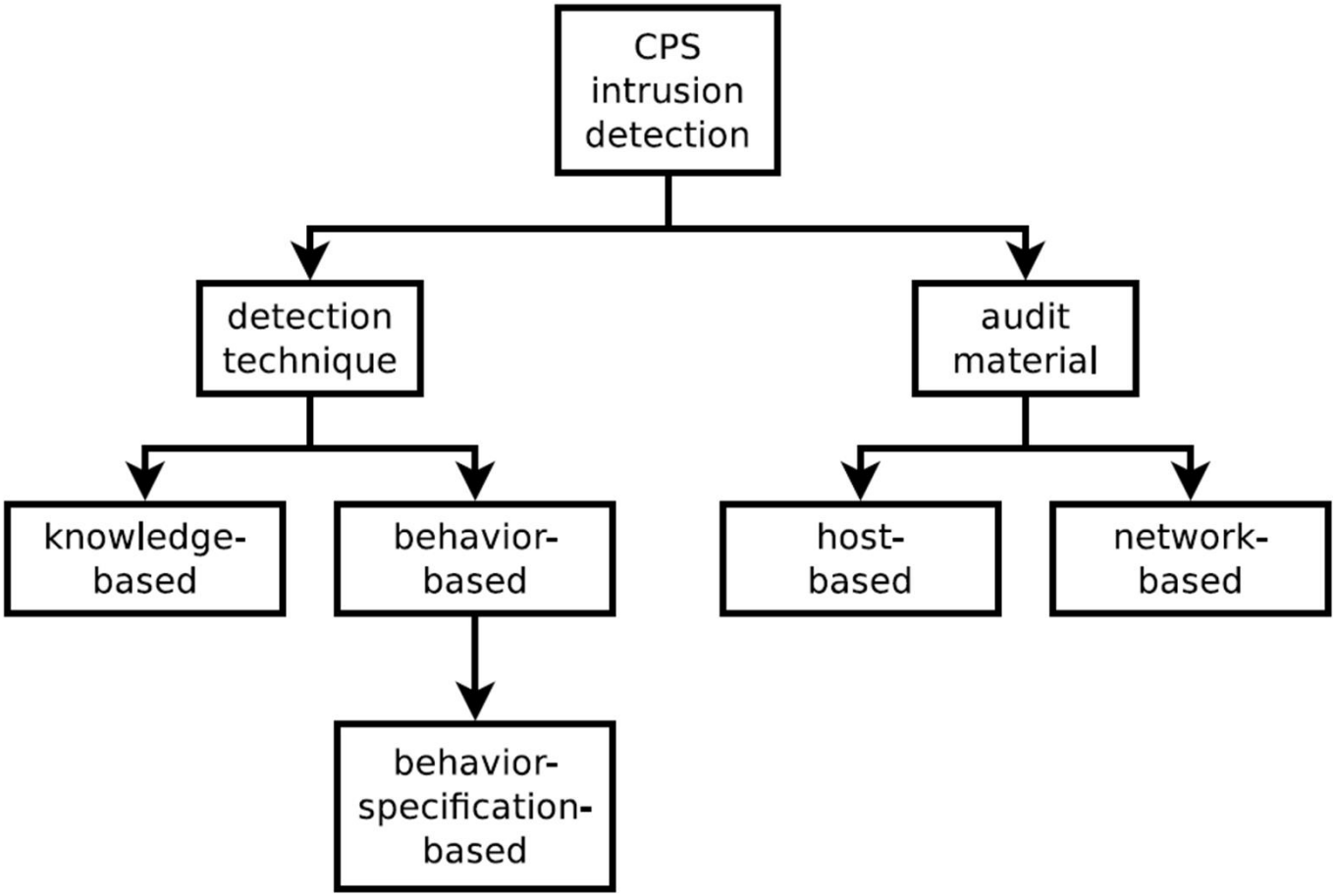
- False Positive Rate
- False Negative Rate
- True Positive/Negative Rate

ICT vs CPS IDS

ICT	CPS
An ICT IDS monitors host- or network-level user/machine activity (e.g., an HTTP request or a web server).	A CPS IDS monitors the physical processes (and hence laws of physics) which govern behavior of physical devices that make certain behaviors more likely to be seen more than others.
An ICT IDS monitors user-triggered activities, leading to unacceptably high false positive rates due to the unpredictability of user behaviors.	A CPS IDS monitors activities which are frequently automated and time-driven in a closed-loop setting, thus providing some regularity and predictability for behavior monitoring.
An ICT IDS deals with mostly non-zero-day attacks, rendering knowledge-based detection effective.	A CPS IDS deals with zero-day or highly sophisticated attacks, rendering knowledge-based detection ineffective.
An ICT IDS often does not have to deal with legacy components, making behavior specification of the physical processes governing legacy components unnecessary.	A CPS IDS often must deal with legacy technology, making behavior-specification-based detection an effective technique by precisely specifying the physical processes governing behavior of legacy components.

ICT IDS also focuses on the Zero-Day attacks

IDS Classification



Types

- Knowledge Based – Low false positive rate
- Behavior Based - They do not look for something specific
  - Classify behavior-based approaches into conventional statistics-based approaches and non-parametric methods. A conventional statistics-based approach may test if a sensor reading or actuator setting is within some number of standard deviations of a mean.
  - Data clustering and support vector machines (SVMs) are examples of non-parametric methods. A feature is a component of a multivariate dataset (e.g., start time, end time, data source, data sink and position).
- Behavior Specific Based - advantage of behavior specification-based intrusion detection is a low false negative rate
  - Major advantage of behavior-specification-based intrusion detection is the system is immediately effective because there is no training/profiling phase.
  - The key disadvantage of behavior-specification-based intrusion detection is the effort required to generate a formal specification.

Types

- Host Based – Advantage
  - Distributed Control
  - well-defined host-specific knowledge to detect intruders

- Disadvantage
  - One major disadvantage of host-based auditing is each node has to perform additional work to collect, if not analyze, their audit data. This is relevant in resource constrained applications like smart grids.
  - Another major disadvantage of this technique is that a sophisticated attacker can cover their tracks by modifying the audit data on the captured node.
  - A third disadvantage of this technique is that it can be OS or application specific (depending on the particular content of the logs).

- *Network-Based Audit –*
  - key advantage regarding resource management is that individual nodes are free of the requirement to maintain or analyze their logs.
  - The key disadvantage regarding data collection is that the visibility of the nodes collecting audit data limits the effectiveness of a network-based technique.
  - it is challenging to arrange network-based audit sensors to get complete intracell and intercell pictures of network activity.

Security incidents

- In 2012, Qatar's Ras-Gas oil company was attacked by a virus that brought down all the computers of the company and caused a complete system shutdown for hours until recovery

- In 2010, The Stuxnet worm that attacked the Iranian nuclear power plant caused long-term damage to Iran's nuclear centrifuges and physically degraded many machines.

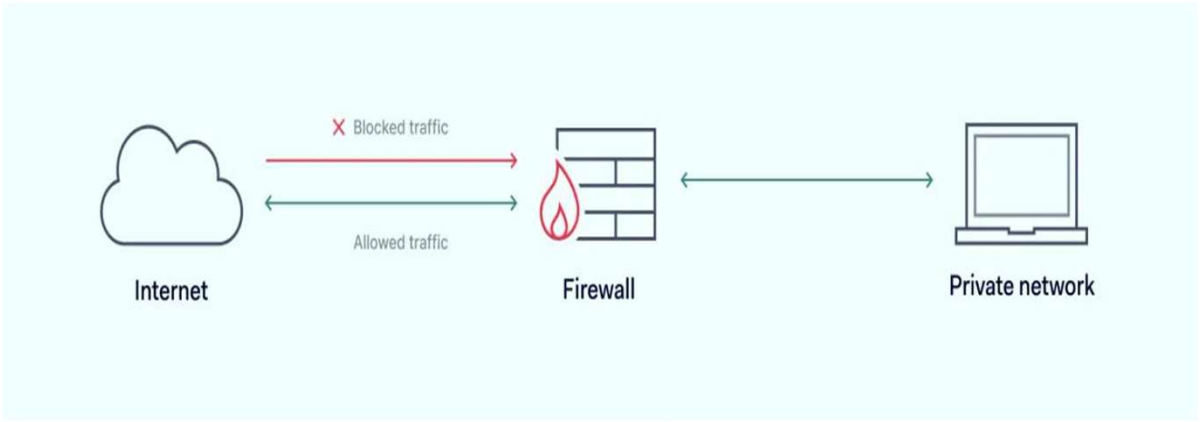
- DDoS BlackEnergy Malware that targeted the Ukrainian Powergrids for political motives in 2015 causing a complete power out-age.

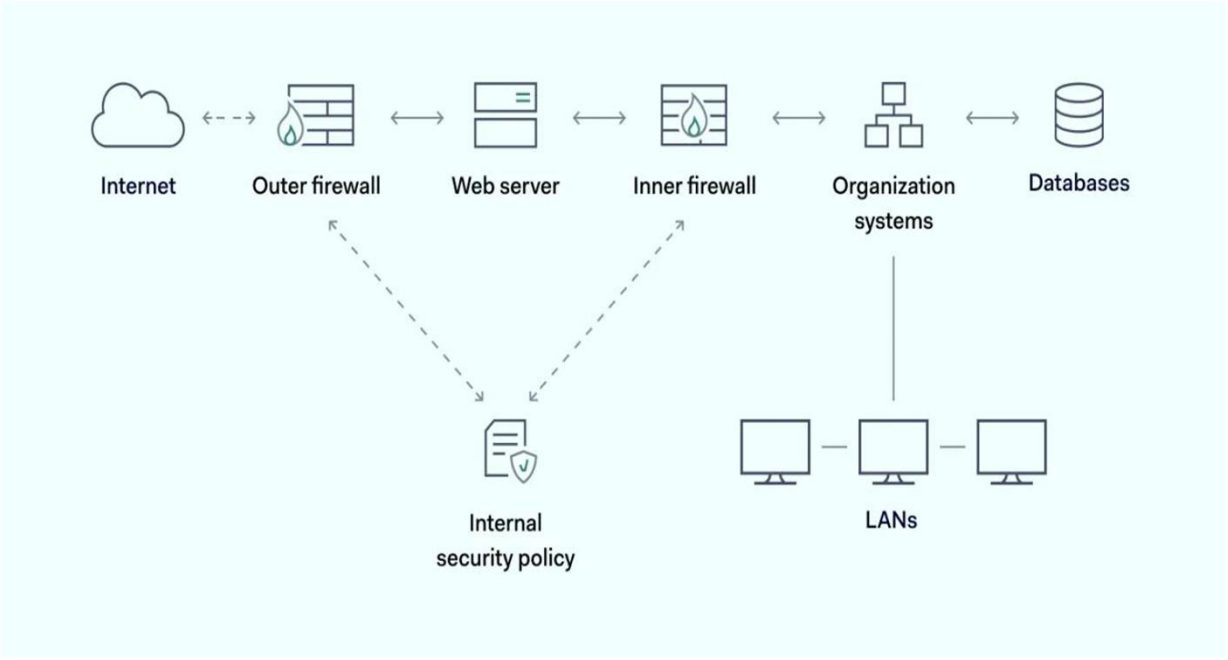
- Shamoon worm attack targeted the Saudi Arabia oil production plant in 2012, which erased all computer hard drives clean.

- German steel factory in 2014, an attack which caused massive physical damages to the system because the plant was unable to perform the safety shutdown procedures.

Firewall

Firewalls can be viewed as gated borders or gateways that manage the travel of permitted and prohibited activity in a private network.





Types

- Based on System
  - Hardware: **Independent of the devices they protect**
  - Software: **Installed on the devices being protected**

- **Based on Location**
  - **Network Firewall**
  - **Host Firewall**

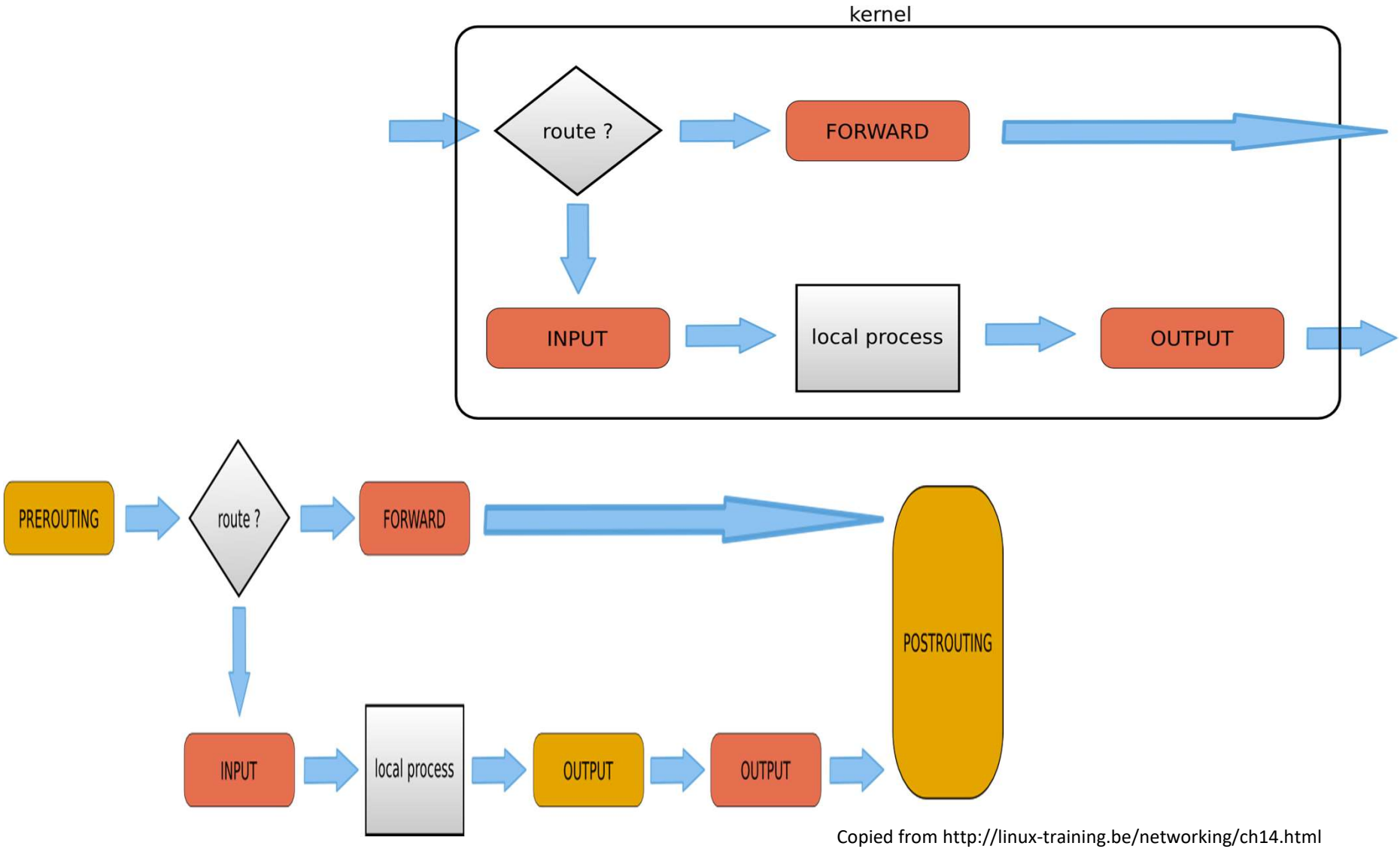
Packet filtering

- IP address
- Port
- Data Transfer Protocol [Circuit Level Firewall]

Inspection Types

- Stateful inspection
- Static packet-filtering firewalls, also known as stateless inspection firewalls

IP table filter



Copied from http://linux-training.be/networking/ch14.html

Deep Packet Inspection Firewall

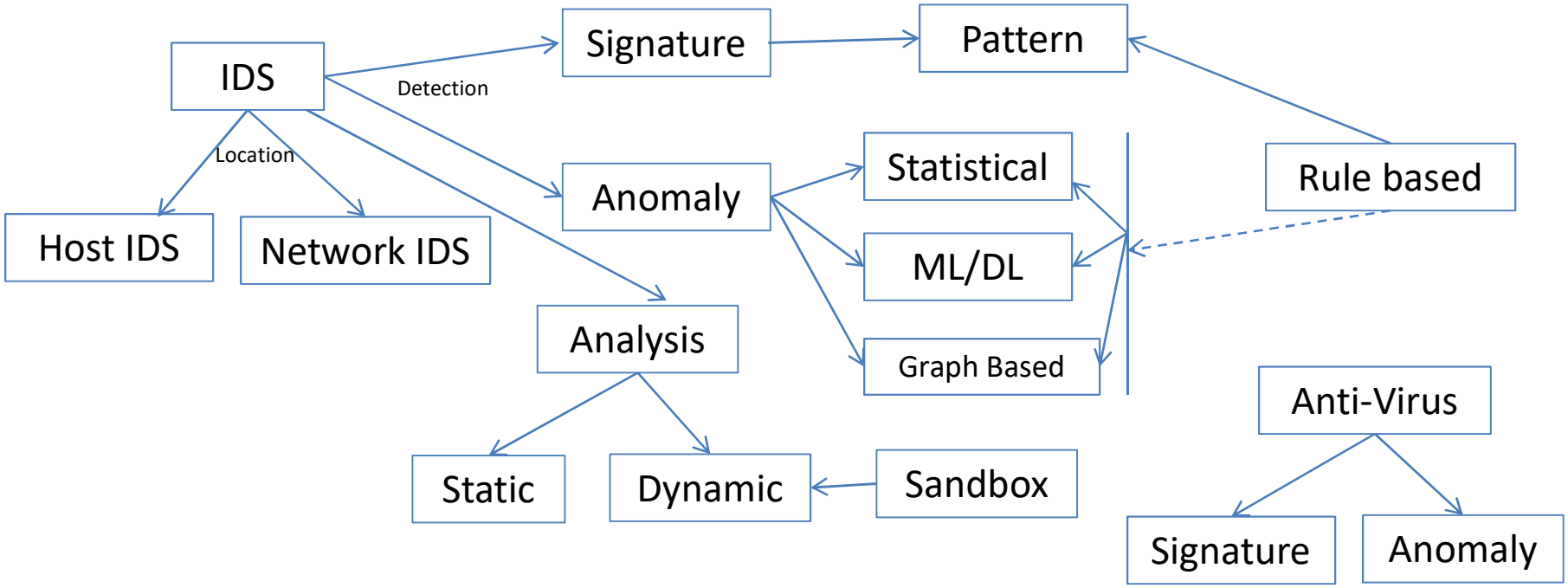
- Deep packet inspection (DPI), also known as packet sniffing, is a method of examining the content of data packets as they pass by a checkpoint on the network.

- Proxy Firewall

Web Application Firewall

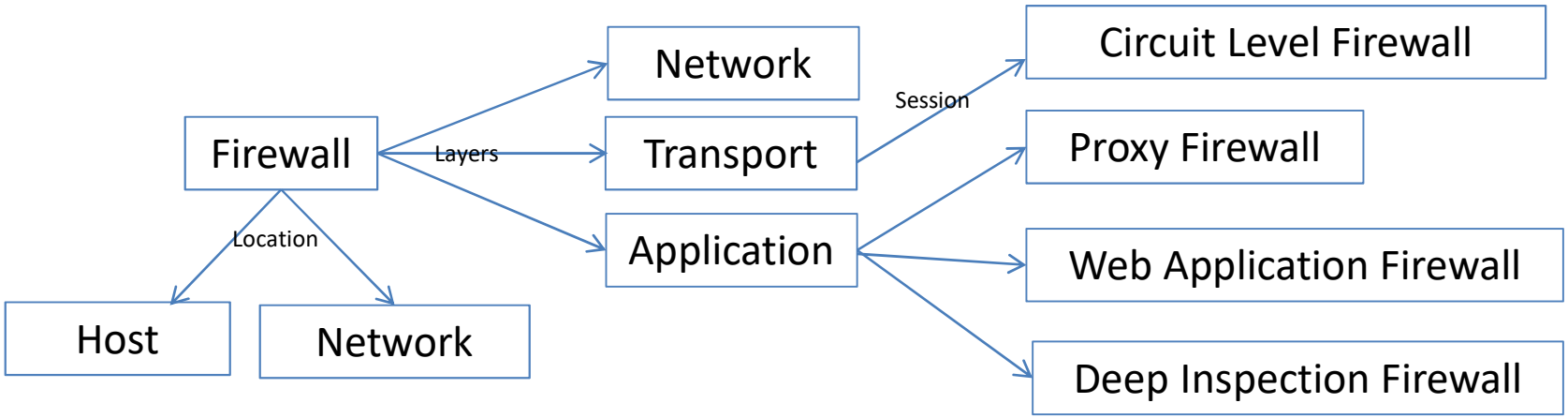
- A WAF or web application firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

IDS

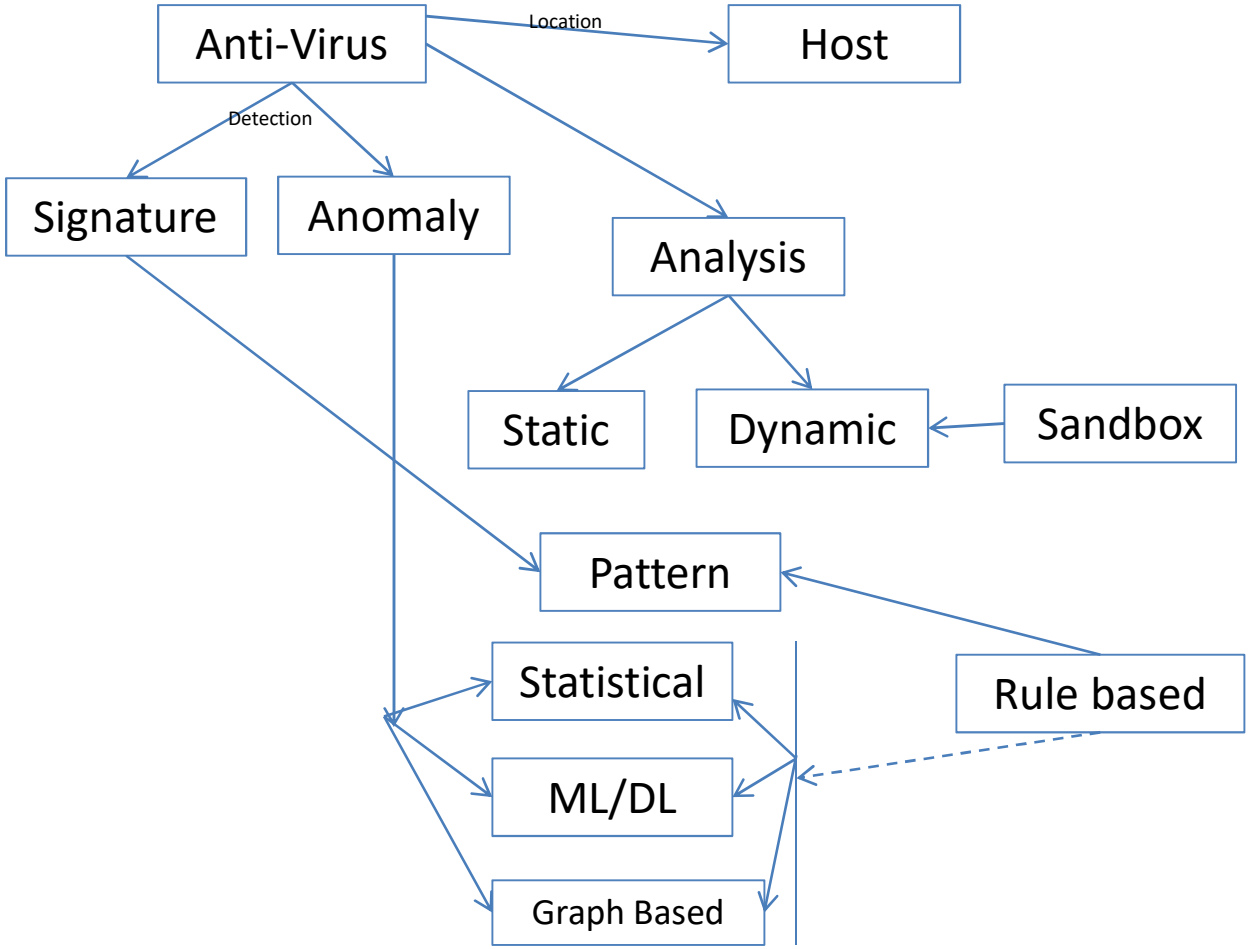


False Positive and False Negative – Important consideration

Firewall


Firewall
Layers
Location
Host
Network
Network
Transport
Application
Session
Circuit Level Firewall
Proxy Firewall
Web Application Firewall
Deep Inspection Firewall

Anti-Virus


Anti-Virus
Location
Host
Detection
Signature
Anomaly
Analysis
Static
Dynamic
Sandbox
Pattern
Statistical
Rule based
ML/DL
Graph Based

Difference

Parameters	HIDS	Anti-Virus	Layer 7 Firewall
Scope	Look into the internal process	Look into the internal process	Only at the Interface
Coverage	Network Packets, Files, Settings or Configurations	Files	Packet header and payload
Policy	Handle	Cannot Handle	Not Applicable

Q1. Do we need HIDS/HIPS and Anti-Virus for our device?

Ans: The Modern Anti-Virus is also having the features of HIDS/HIPS. Otherwise HIDS/HIPS is better than Anti-Virus. However, cost impacts.

Q2. Do we need HIDS/HIPS and Firewall for our device?

Ans: Even though HIDS performs task similar and more than the Firewall, the earlier filtering increase the performance of HIDS/HIPS.

Indicators of Compromise

- Indicates a system may have been infiltrated by a cyber threat.
  - Unusual inbound and outbound network traffic
  - Anomalies in privileged user account activity
  - Other login red flags
  - Swells in database read volume
  - HTML response sizes
  - Large numbers of requests for the same file
  - Mismatched port-application traffic
  - Suspicious registry or system file changes
  - DNS request anomalies
  - Geographical irregularities
  - Virus Signature
  - Unexpected Software Installations
  - Large amounts of compressed files or data bundles in incorrect or unexplained locations

Indicators of Attack are active in nature and focus on identifying a cyber attack that is in process.

References- https://www.fortinet.com/resources/cyberglossary/indicators-of-compromise
https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/

References

- http://linux-training.be/networking/ch14.html
- https://nordlayer.com/learn/firewall/what-is-firewall/
- https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/
- Robert Mitchell and Ing-Ray Chen. 2014. A survey of intrusion detection techniques for cyber-physical systems. ACM Computing Survey, Vol. 46, 4, Article 55 (April 2014), 29 pages. https://doi.org/10.1145/2542049