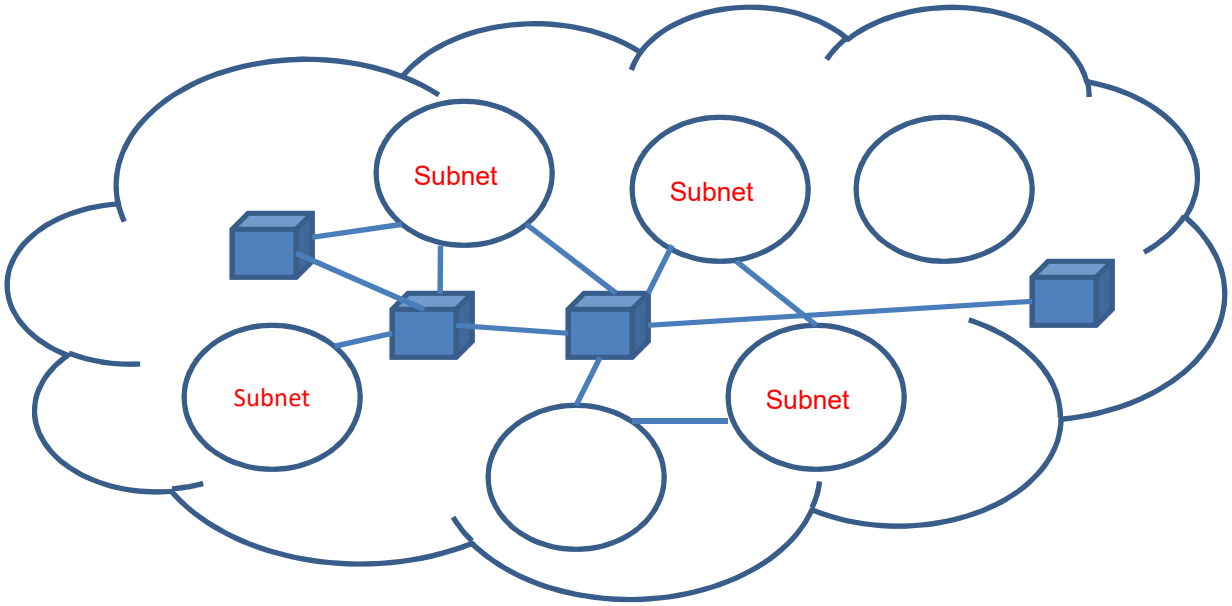
Intrusion Detection System and Firewall

S.Venkatesan
Professor
Network Security and Cryptography Lab
Department of Information Technology
Indian Institute of Information Technology, Allahabad
venkat@iiita.ac.in

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

Network

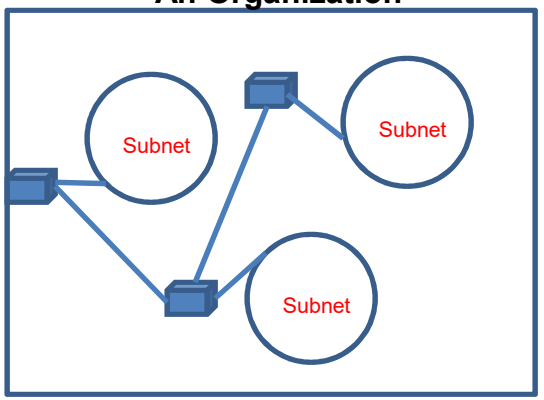


Global cyber Space

Components

- Gateway
- L2 and L3 Switch
- Router
- Access Point
- Load Balancer
- **Hub**

An Organization



Perimeter Security

- It is a practice of securing an organization's IT and OT infrastructure by establishing protective measures at the outer boundary of its network.

- The goal of perimeter defense is to prevent
  - Unauthorized Access
  - Data breaches
  - Cyber threats from entering the network.

- This is traditionally achieved through technologies like
  - Firewalls,
  - Intrusion detection and prevention systems (IDS/IPS)

Intrusion

- A network intrusion is an unauthorized penetration in your enterprise or an address in your assigned domain.

- An intrusion can be passive (in which penetration is gained stealthily and without detection) or active (in which changes to network resources are effected).

Objective:

- Corruption of Data
- Theft of Data
- Loss of Reputation
- Non-Availability

Intrusion Detection System

- IDS (Intrusion Detection System) monitors networks for suspicious and malicious activities, as well as false alarms.
- Distinguish between normal and malicious network traffic.
- Types
  - Host Based
  - Network Based

Intrusion Types

- Process
  - Signature-based Detection
  - Anomaly Based Detection

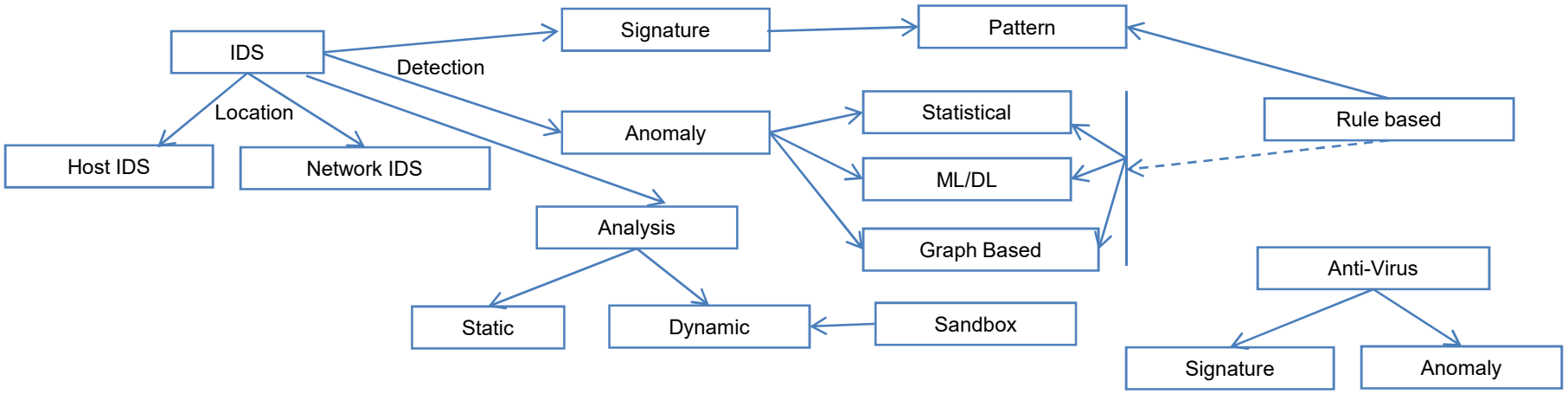
- Analysis Type
  - Static Analysis
  - Dynamic Analysis

- What about IPS?
- Where we will place IDS and IPS? Inline Vs Passive

Components

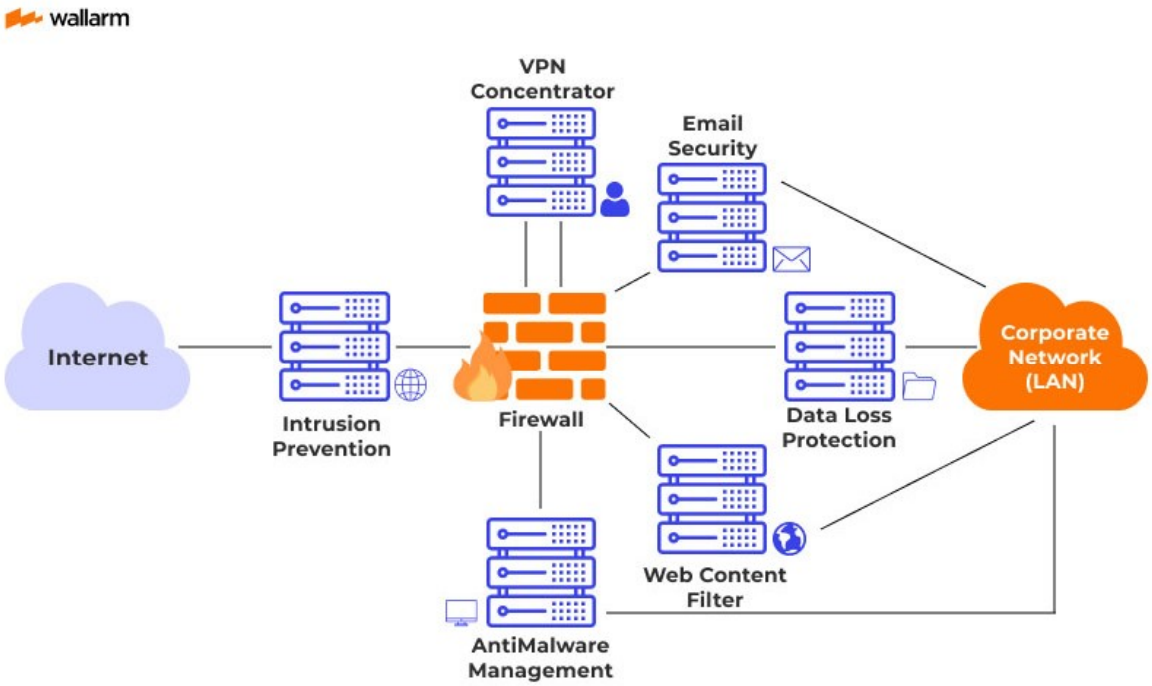
- Sensors (Data Collectors)
- Detection Engine
  - Analyzers
  - Signature/Knowledge Base
- Alert System
- Log Storage

Classification



False Positive and False Negative – Important consideration

UTM



Copied from https://www.wallarm.com/what/unified-threat-management

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

Malware Analysis

- HIDS for Malware Detection
  - File integrity
  - System logs
  - Process activity
  - User actions
  - Network connections originating from the host

- Anti-Virus
  - Scan files

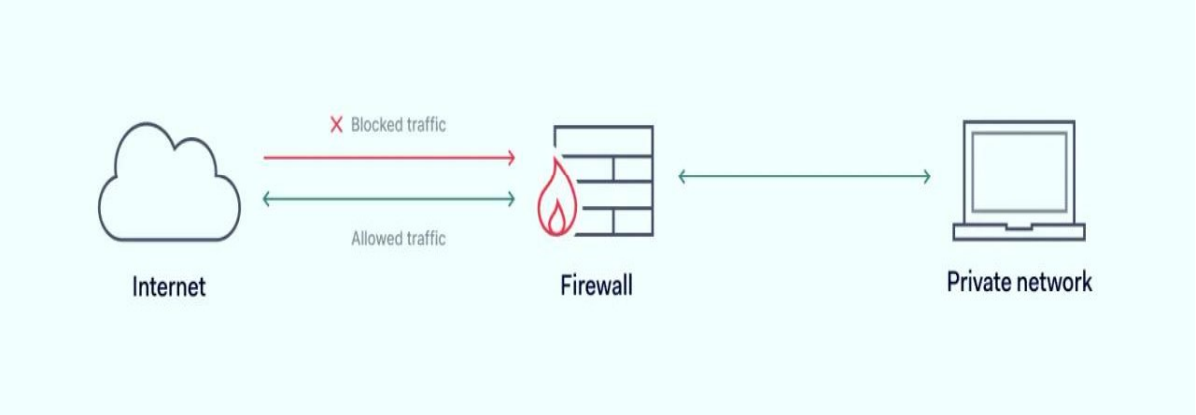
YARA Rules

- **YARA** is a **tool and language for pattern matching** used mainly in **malware research and detection**

```
rule ExampleMalware {
    meta:
        description = “Malware”
    strings:
        $a = "malicious_code"
        $b = { 6A 40 68 00 30 00 00 }
    condition:
        $a or $b
}
```

Firewall

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



Firewall

- Inspects each individual “packet” of data as it arrives at either side of the firewall
- Inbound to or outbound from your computer/network
- Determines whether it should be allowed to pass through or if it should be blocked

Allow – traffic that flows automatically because it has been deemed as “safe”

Block/Reject – traffic that is blocked because it has been deemed dangerous to your computer

Ask – asks the user whether or not the traffic is allowed to pass through

Firewall 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

- IP address
- Port
- Circuit Level Firewall[Session]

Inspection Types

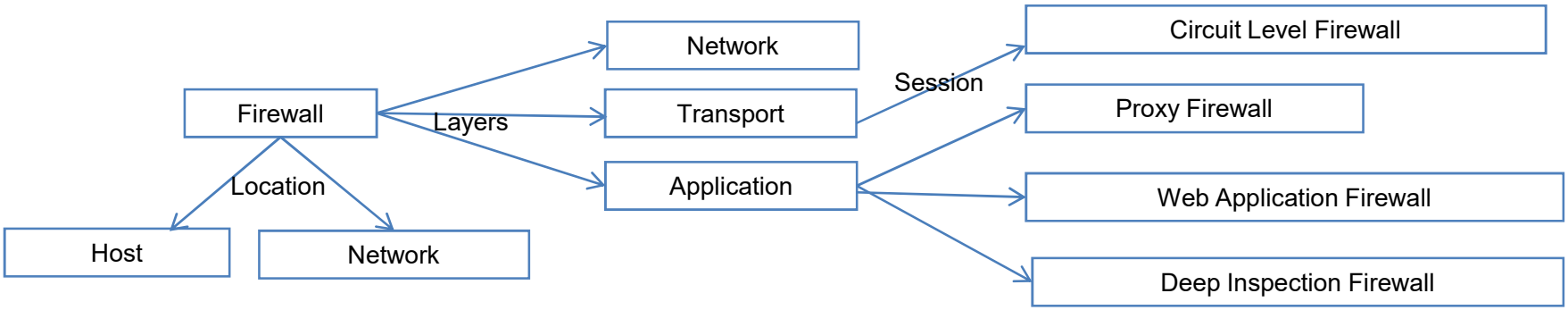
- Stateful inspection
- Static packet-filtering firewalls, also known as stateless inspection firewalls

Firewall Types (Contd.)

- 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

  - What happens if data Encrypted?



Filter Location

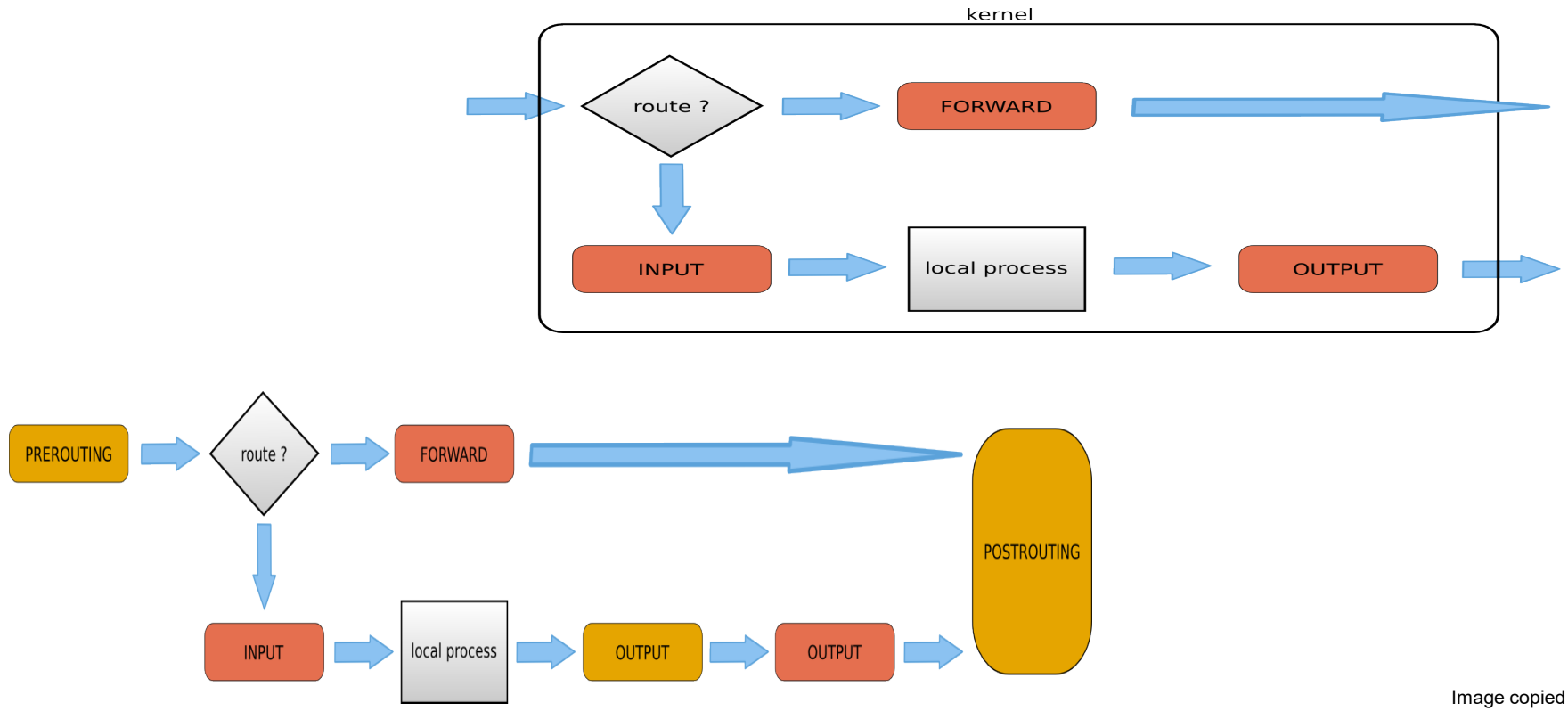


Image copied

Comparison

Parameters	HIPS	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 except malware scanning. 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.

Thank You