NETWORK SECURITY:

FIREWALL, NAT, IDS

FIREWALL

→ is a security measure designed to prevent unauthorized electronic access to a networked comp. system

→ prevents malicious actions from the internet AND local network

→ applies a set of rules called 'firewall policies' to allow/deny the traffic

- Blocklist — Allow-by-default
- Allowlist — Deny-by-default

TYPES OF FIREWALL

LEAST EFFECTIVE

1) Packet Filters [Stateless] → may have to be fairly restrictive in order to prevent most attacks

→ If a packet matches the packet filter's set of rules, the packet filter will drop/accept it

2) Stateful Filters → Hence, stateful firewalls can allow only inbound TCP packets tht. are in response to a connection initiated from within the internal network

→ It maintains records of all connections passing through it and can determine if a packet is either the start of a new connection, a part of an existing connection or an invalid packet

3) Application Layer → simulates the effects of an application

MOST EFFECTIVE

→ works like a 'proxy'; it can 'understand' certain apps and protocols

→ may inspect the contents of the traffic, blocking what it views as inappropriate content (i.e. websites, viruses, ...)

↳ Effectively a protective MiTM tht. screens info. at an app. layer

PERSONAL FIREWALL

→ runs on workstation that it protects

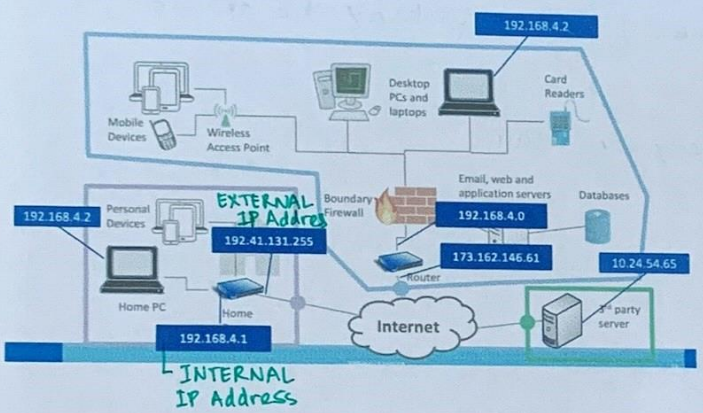
→ provides basic protection

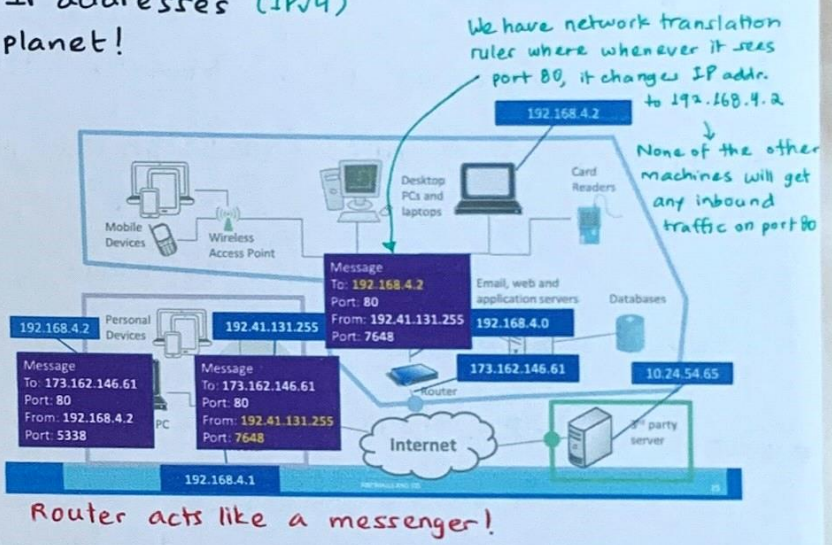
→ HOWEVER, any rootkit type software can disable the firewall

NETWORK ADDRESS TRANSLATION (NAT)

→ remaps an IP address into another by modifying network address info. in the IP header of packets while they are in transit across a routing device

→ REASON FOR THIS → We do not have enough IP addresses (IPv4) for every device on the planet!





→ enables IoT; raises the issue: convenience vs. security

INTRUSION DETECTION SYSTEMS (IDS)

→ Firewalls are preventative measures, while IDS detects a potential incident in progress

→ Alarms can be sounded or not:

	Intrusion Attack	No attack
Alarm Sounded	TP	FP
No alarm	FN	TN

1) RULE-BASED IDS

→ Rules identify the types of actions tht. match certain known intrusion attack; Rule encode a signature for such an attack

→ This requires you to anticipate patterns of the attack in advance

→ (−): Attacker may test attack on common signatures
(−): Impossible to detect new type of attack

→ ↑ACCURACY, ↓FP

2) STATISTICAL IDS

system needs to warm up to new behavior

→ Dynamically build a statistical model of acceptable behavior and flag anything that does not match; Admin does not need to anticipate potential attacks

→ ↑FP, ↓ACCURACY