Introduction to Network Security

- Disruption and interception attacks can be chained
- Defenses: Firewalls, IDS, IPS, Antivirus. All these rely on previous knowledge of the threat
- These defenses can be intelligent (rules, AI, machine learning, etc…)
- KPI → Key performance indicators

Network Access Control

- AAA → Authentication (identifies user), authorization (what user can do), accounting (monitors user)
- 802.1X → Network access control standard, authenticates users
- Most popular AAA protocol/service → RADIUS
- EAP is a flexible protocol used in 802.1X (802.11 is for WiFi)
- EAP has 3 phases: Discovery, Authentication, Secure Access Protocol but 802.1X only uses the Authentication phase
- RADIUS Access-request ----> ……. ←-- RADIUS Access-accept/reject

Network Flow Control

- Firewall, IPS, IDS and security compliance policies
- IDS can perform deep packet or shallow packet inspection (DPI and SPI)
- Nowadays, IDS/IPS can be mixed with AI and machine learning
- Firewalls evaluate each network packet against the policies of network security
- NAT, packet filtering, redirects, DoS detection/defense, secure communication mechanisms all run as firewalls services
- Network-Level Firewalls: Monitors packet heads and filters traffic based on them
- Circuit-Level Firewalls: Monitors the entire TCP handshake and session

- Application-Level Firewalls Analyzes application data, enforces correct application behaviour
- Stateful Firewalls: Saves state table and all previous connections. Control is based on the connection state of a flow or session.
- Network must be protected at multiple levels and locations
- Stateless firewalls: Analyzes individual packets, filters based on rules (access lists or ACLs). Good against DoS, cost-effective, very fast
- Firewall zones → Collection of interfaces/IPs/networks with different security levels/rules
- Zones can be referenced by firewall rules
- Firewalls can have different virtual instances with distinct memory and CPU cores allocated (useful when targeted by ddos)
- When failing against a ddos attack, the failing order is usually Firewalls - Servers - Routers - Links
- Routers can be directly exposed to the internet but only if doing basic routing exclusively (not any services or VPN things)
- Brute force defending with stateless firewalls is also a viable option to defend from ddos
- Load balancers are necessary to decrease processing and memory requirements of each firewall
- Load Balancing algorithms → IP Hash, Round Robin (only if synched), Least Connections, Smart (based on external info)
- Stealth firewalls don’t have IP addresses so they can’t be targeted by attacks
- Load balancers can also have virtual instances
- Load balancers should be redundant and synched, if needed
- The ideal solution is made of multi levels of defense, with redundant load balancers, stateless and stateful firewalls. Temporarily free resources on firewalls
- Build whitelists and blacklists
- Defend IP spoofing → Block IP source if comes from somewhere it’s not supposed to

- Half-Open TCP attacks are common as a DoS strategy. Reducing timeouts is a solution
- It's important to make sure hosts in your network don't participate in DDoS attacks
- Firewall Performance Evaluation → IP throughput, latency, speeds, etc..
- Linux IPTables → Filter, NAT and mangle (to manipulate packets)
- Chains → Set of rules
- Control by analysis of higher layers → Grey area in laws, deciphering SSL/TLS traffic to monitor networks
- Two possible synched firewall types: Active/Backup (outdated) or simultaneously working and synched
- Synched firewalls share the same virtual IP

Secure IP Connections

- Secure IP connections are based on tunnels, or virtual interfaces
- Tunnels can be used to force routing (without encryption)
- Tunnels are bounded to loopbacks so in case of interface failures the tunnels don't fail too
- Overlay network → Virtual network over a real network
- Full/Partial Overlay Mesh → Several tunnels connected
- Virtual networks' routing can't be the same as the underlying network, the tunnel will loop state between up and down
- Multipoint Tunnel → Single tunnel that interconnects multiple nodes
- NHRP → Next Hop Resolution Protocol, used in multipoint tunnels
- NHRP routers map IPs to Virtual IPs
- Routers talk to each other to find the next hop
- Hub-Spoke architecture → Each site is connected to a predefined central node which relays all spokes communication through himself

- Spoke-Spoke architecture → Full mesh basically, all routers are connected to each other
- IPSec → Two modes: AH and ESP (transport mode only)
- Tunnel mode → Gateways provide IPSec services to other hosts
- Transport mode → Each end host does IPSec encapsulation of its own data
- AH → Authentication Header, ensures integrity but no confidentiality
- ESP → Encapsulating Security Payload, ensures confidentiality (encryption)
- Security Associations → Describes how the IPSec security services will be used. Contains parameters such as authentication algorithm, key length, other encryption parameters, tunnel or transport mode
- ISAKMP → Used to establish security associations and cryptographic keys. Enhances IPSec by providing authentication of peers and negotiation of keys and security associations
- ISAKMP methods → Pre-shared key (PSK), Digital Signatures (RSA-SIG) and Public key encryption (RSA-ENC)
- GRE → Generic Routing Encapsulation
- VPN → Encrypted connection between private networks over a public network. Can be remote access or site-to-site
- Site-to-Site VPN → Overlay network over the internet, mostly based on IPSec
- Dynamic Multipoint VPN → Relies on NHRP and is very modular

Remote Access

- VPN servers are usually on firewalls or the DMZ
- Firewalls are ideal because they can do deep packet inspections more easily
- Nowadays a IDS or IPS is put before the VPN server in the DMZ
- But deep packet inspection is harder due to layers of encryptions
- OpenVPN UDP port 1194

Intrusion Detection and Prevention

- IDS only detects things and sends alarms (either for human or automatic intervention)
- IPS detect and also blocks/quarantines files/processes/traffic (depending if network or host based)
- Host-based → IDS/IPS deployed on a specific machine, can monitor temperature, CPU/memory usage, etc…
- Network-based → Monitors all hosts on a given network. Things such as packets and flow levels
- Signature based → Based on fingerprints of previous, known, attacks. 0-days aren't detected
- Anomaly based → Establishes a baseline behavior. Can use AI models or predefined rules too. Might detect 0-days
- IDS is connected to a network tap which reports to a network management system, which then decides to take action on the firewall
- IPS is connected to the network tap with firewall integration. IPS can talk directly to the firewall after receiving information from the tap
- Alternatively, the IPS can be inline and integrated with a firewall, reporting (or not) to the management system
- The third option would be an IPS which also is a firewall
- Not responding to packets which are rejected (treating them as unreachable) avoids giving away information to the attacker