NETWORK SECURITY

Network Security

By far the most important security area and isn't just about having a firewall

Network Security

Proper network security should also consist of security policies and practices designed to prevent and monitor unauthorized access.

Network Security

Common issues include

- Wifi
- Wireless protocols like Bluetooth, NFC
- Weak protocols like Telnet & HTTP
- MAC Address Spoofing

Network Security

Passive Threats

- Wiretapping
- Port Scanning
- Information Gathering

Network Security

Active Threats

- Malware
- DDoS
- DNS Spoofing
- Man-in-the-middle attacks

Network Security Tools

Can be categorized into the following

- Blocking
- Inspecting
- Monitoring
- Policy

Network Security

Tools for Blocking Threats

- Firewalls
- Network Access Control
- IPS & IDS

Network Security

Tools for Inspecting Threats

- Packet Capture
- Netflow Capture (network protocol developed by Cisco for collecting IP traffic information and monitoring network flow)

Network Security

Tools for Monitoring Threats

- Logs
- Network Visibility Tools e.g Wireshark

Network Security

Tools for Policy Enforcement

- Nontechnical Compliance Checking (Human Auditing)
- Contractual Compliance Checking (Employee Network Use)
- Real-time Technology Enforcement (Firewalls)
- Passive Technology Enforcement (IDS)