Firewalls

1. **Stateful multilayer**
   - traditional firewall.
2. **UTM** (Unified Threat Management), 2000s, integrates:
   - Web Proxy,
   - Spam Filter,
   - Antivirus,
   - Intrusion Detection.
3. **NGFW** (Next Generation Firewall), 2008, Palo Alto Networks, awareness of:
   - applications,
   - user identity,
   - supports encrypted traffic via SSL/TLS.
4. **Proactive NGFW**
   - machine learning involved,
   - identifying variations of known attacks.

Techniques

1. DPI (Deep Packet Inspection) inspects in detail the data being processed, used for
   - baselining application behavior,
   - analyzing network usage
   - troubleshooting network performance,
   - ensuring that data is in the correct format,
   - checking malicious code,
   - eavesdropping,
   - internet censorship, …
2. IDS/IPS (Intrusion Detection/Prevention Systems)
   - signature-based detection (recognizing bad patterns, such as malware),
   - anomaly-based detection (deviations from model of “good” traffic) – machine learning,
   - reputation-based detection – based on reputation scores.

SSL/TLS deep inspection? How?

1. Implementation:
   - **NGFW,** or
   - **proxy** (two separate connections between endpoints, and **re-encryption**)
2. Proxy approach (example based on Fortinet’s docs):
   - firewall works as a **subordinate CA** to **sign certificates on the fly**,
   - the SSL traffic gets re-encrypted at firewall,
   - users (browsers) have to **trust** the subordinate CA installed on firewall.

Citation (from Fortinet docs):

*To implement seamless deep inspection, **users must trust the certificate** that is **signed** by the **FortiGate**, and there must be certificate chain back to the trusted root CA that is installed on the user's endpoint. If the root certificate is not installed, the user receives a certificate warning every time they access a website that is scanned by the FortiGate using deep inspection. Administrators should provide the CA certificate to the end users if deep inspection will be used.*

*Users should be made aware that their communication is subject to these security measures, and that their privacy while protected by a FortiGate that is performing deep inspection cannot be guaranteed. Performing **deep inspection** might be **undesirable** when users are accessing certain web categories, such **banking** or **personal health related sites**. When creating SSL/SSH inspection profiles that use full SSL inspection, the Finance and Banking, Health and Wellness, and Personal Privacy categories are **exempt from inspection by default**. Administrators can customize these categories, enable Reputable websites, and add individual addresses to the SSL exemptions as required.*