Firewall :

- **Network security device OR software application.**
- **Monitors incoming and outgoing network traffic based on predetermined security rules(ACL).**
- **Barrier between trusted internal network and untrusted external network.**
- **[zero trust network ahead]**

ACL : Access Control List : here the rules to dictate which traffic is allowed are saved

Firewalls usually work on network layer and transport layer, but due to the rise of application layer protocols like “HTTP and FTP” application layer firewalls are developed to inspect traffic at the application layer.

Network layers and firewall interaction :

- **Network layer : Inspect IP packets, and filters traffic based on source and destination IP addresses, ports and protocls.**
- **Transport Layer : These may inspect even transport layer headers (TCP and UDP). Can control access based on TCP/UDP port**

numbers. [Stateful Inspection Firewalls : inspects traffic based on the connection , say 3 way handshake]

- **Application layer firewalls : also known as proxy firewalls. Explained just ahead in types of firewalls.**

Types of firewalls :

- **Packet Filtering Firewalls :**
  1. **Access Control List. Predetermined rules such as IP address, port numbers, and protocols.**
  2. **They lack features like deep packet inspection, as they inspect only headers.**
  3. **Malicious codes can be passed through from the payload.**
- **Stateful Inspection Firewall :**
  1. **Maintain a record of active connections and only allow packets that belong to established connections.**
  2. **Prevents Stateful attacks : Session Hijacking and Denial of Service attack.**
  3. **Session Hijacking : Attackers may attempt to hijack established connections by injecting malicious packets or manipulating existing sessions. Stateful inspection firewalls can detect such attempts by**

monitoring the state of connections and identifying any anomalies or unauthorized changes.

4. **Denial-of-Service (DoS) Attacks: Some DoS attacks involve overwhelming a system with a flood of connection requests or incomplete connection attempts. Stateful inspection firewalls can mitigate these attacks by only allowing packets related to legitimate, established connections, thus filtering out malicious or incomplete connection attempts.**

- **<u>Proxy Firewalls</u> :**
    1. **It inspects , filters and forwards packets oon behalf of the user.**
    2. **Acts as intermediary between internal and external network.**
    3. **Works on application layer. [chrome example]**
    4. **Masking of IP addresses of internal users.**
    5. **Latency due to extra processiong.**
- **<u>Host Based firewalls :</u> Firewalls that protect particular computer on which they are installed. A lot of antiviruses have inbuilt host based firewall.**
- **<u>Network based firewall:</u> combination of hardware and software based firewall.[house door example]**

- **Next Generation Firewalls :**
  1. **Deep Packet Inspection (DPI): NGFWs can inspect the payload of packets, not just the headers, which allows them to identify and block malicious traffic more effectively.**
  2. **Intrusion Prevention Systems (IPS): They incorporate IPS to identify and prevent attacks by examining traffic in more depth.**
  3. **Application Awareness: NGFWs recognize and control applications, regardless of the port or protocol used. This enables them to enforce security policies on a per-application basis.**
  4. **Threat Intelligence: They integrate with updated threat intelligence sources to identify and block the latest threats.**
  5. **Identity Management Integration: NGFWs can enforce policies based on users and groups by integrating with identity management systems such as Active Directory.**
  6. **Automation and Advanced Analytics: NGFWs use automation and analytics to detect patterns that may indicate a security threat.[ATP : Advanced Threat Protection]**

UTM vs NGFW :

- **UTM : firewalling, IDS/IPS, antivirus, content filtering, VPN, etc.**
- **NGFW : Deep packet filtering, application awareness, etc. everything mentioned above.**
- **Although NGFW is a part of UTM, these terms are often used interchangeably in common contexts.**

VPN :

vpn client -> vpn tunnel -> ISP -> VPN server

Web Content Filtering intuition:

Firewall majorly works on network and transport layer. But when the user does browsing in browser, the mechanism moves to application layer.
Therefore to scan user traffic on web browser level , web content filtering is used.

Major Firewall Producers : Fortinet Fortigate, Palo Alto Networks, Cisco, Juniper networks, etc.

Fortinet Fortigate firewall solutions for dic=verse needs :

- **Entry-Level (30-90 Series) : for small offices or branch**
- **Mid-Range (100-900 Series): caters to mid-sized businesses**
- **High-End (1000-3000 & 6000 Series): Designed for large enterprises and data centers**
- **Chassis-Based (5000 & 7000 Series): high-density solutions are ideal for service providers and large organizations**
- **Software-Based (FortiGate VMs): virtualized firewalls for deployment within cloud environments**

FORTINET FORTIGATE NEXT GENERATION FIREWALL VERSION 30E :

- **All the features of NGFW and UTM discussed above and some are below.**
- **Secure SD-WAN (Software Defined Wide Area Network): SD-WAN lets you combine multiple connections, It intelligently routes your data traffic across the best performing connection.**
- **Wired Connectivity: Includes multiple Gigabit Ethernet ports for LAN and WAN connections.**

- **SSL (Secure Sockets Layer): Establishes a secure connection between a web server and a browser. Encrypts data transfer, protecting sensitive information like credit card details or login credentials.**
- **1 WAN and 4 LAN ports**
- **1 USB port for configuration backup and external storage.**
- **Firewall Throughput: Up to 950 Mbps**
- **IPS Throughput: Up to 300 Mbps**
- **NGFW Throughput: Up to 200 Mbps**
- **Cloud based analytics for centralised visibility and reporting.**

Fortigate 30E 2 varients :

1. **Fortinet-30E : it has all above features**
2. **Fortinet-30E-3G4G-GBL : Support building cellular connectivity or wireless connectivity for regions, where wired connections are not feasible.**

Security features by Fortigate 30E :

- **Up-to-date security protection**
- **Continuous threat intelligence**
- **Advanced threat protection capabilities**
- **SD-WAN features :**

1. **Dynamic Traffic Routing : Dynamically route traffic across multiple WAN connections, ensuring high availability and performance.**
2. **Latency and cost improvements : Improves latency and reduces WAN cost through efficient traffic management.**

CVE (Common Vulnerabilities and Exposures)

CVE-2023-27997 :

- **Affecting SSL VPN pre-authenication process**
- **How it takes place :**
    1. **Overflow: During the SSL-VPN pre-authentication stage, a vulnerability allows attackers to send excessive data exceeding the allocated memory buffer.**
    2. **Heap Corruption: This overflows into adjacent memory blocks within the device's heap, a dynamic memory allocation area.**
    3. **Code Execution: The attacker can potentially overwrite memory in the heap with malicious code.**
    4. **Control Seized: If successful, the attacker's code can be executed, potentially granting them unauthorized access and control over the device.**

- **Description: Heap buffer overflow vulnerability in the SSL VPN preauthentication module allowing potential remote code execution (RCE).**
- **Existing Controls: May include firewalls, intrusion detection/prevention systems (IDS/IPS), and Multi-Factor Authentication (MFA).**
- **Patch Availability: Yes (reduces likelihood over time) [patch means a fix or update released by company over vulnerability]**

CVE-2013-1414 :

- **Cross Site Request Forgery Attack (CSRF) :**
  1. **You click the link and your phone automatically sends a request to social media (because you're already logged in).**
  2. **This request might be something you didn't intend, like posting something embarrassing or changing your password to something the hacker can guess.**
- **Threat Actor: Malicious attacker with some knowledge of the target network and potential social engineering techniques.**
- **Attack Method: Social engineering to trick a legitimate user into clicking a malicious link or**

visiting a website crafted to exploit the CSRF vulnerability

- **Description: Multiple CSRF vulnerabilities in the FortiOS web-based management interface allowing unauthorized modification of system settings, firewall policies, or potentially complete takeover of the firewall.**
- **Patch is available here also.**

CVE-2012-4948 :

- **Type: Improper Certificate Validation**
- **Attack Method: exploiting the use of the same Certification Authority (CA) certificate and private key across multiple FortiGate deployments.**
- **Description: Improper certificate validation in the default configuration. The FortiGate UTM appliances use the same CA certificate and private key by default.**
- **An attacker could exploit this by creating a fake certificate that appears to be from a trusted source.**
- **If your device connects to the attacker's fake server, the attacker could potentially intercept the communication and steal information like login credentials.**

- **Same key and certificate to authenticate other servers and self-authentication.**

LIMITATIONS AND PERFORMANCE BOTTLENECKS :

Performance Scalability

- **The FortiGate 30E is designed for small to medium-sized businesses (SMBs) but may struggle with the demands of rapidly growing businesses or those expanding online services. Upgrading to more capable models is advised for businesses experiencing growth.**

Wired Connectivity Only

- **Lacking built-in Wi-Fi, the FortiGate 30E necessitates separate wireless access points, complicating network management and increasing IT overhead. Planning for wireless hardware integration is essential due to the increasing reliance on wireless communication.**

Limited Physical Interfaces

- **The limited number of ports on the FortiGate 30E can constrain network design and scalability for businesses expecting to add wired devices or needing extensive connectivity. Advanced planning and potential investment in additional networking hardware may be required.**

Limited Physical Security

- **The desktop form factor of the FortiGate 30E is vulnerable to unauthorized access, tampering, or theft, especially in less secure environments. Enhancing physical security measures and carefully considering device placement are critical.**

Single Point of Failure

- **Relying on a single FortiGate 30E for network security poses a risk of network exposure if the device fails or is compromised. Implementing High Availability configurations to provide failover support is crucial for maintaining continuous network protection and availability.**

VULNERABILITIES :

Notable CVEs

- **Awareness of specific vulnerabilities, like CVE-2023-27997 and CVE-2012-4948, is crucial. Quick patching and mitigation efforts are necessary to reduce exploitation risks.**

Supply Chain Attacks

- **Assessing the security practices of vendors, including Fortinet, is important to mitigate supply chain attack risks. Verifying device integrity from reputable suppliers is essential.**

Zero-Day Exploits

- **Defending against zero-day exploits requires a layered security strategy and a proactive incident response plan due to the absence of immediate patches.**

Default Configuration Risks

- **Avoiding default configurations and tailoring settings to specific needs enhances security. Changing default passwords and disabling unused services are key hardening steps.**

Insider Threats

- **Mitigating insider threats involves strict access controls, monitoring user activities, and enforcing a principle of least privilege to limit access based on roles.**

Social Engineering Attacks

- **Counteracting social engineering, including CSRF attacks, emphasizes the importance of user education on recognizing and defending against phishing and similar tactics.**

ADDITIONAL CONSIDERATIONS :

End-of-Life Planning

- **Preparing for the FortiGate 30E's eventual end-of-life is crucial for maintaining network security integrity. This involves staying updated with Fortinet's lifecycle announcements and devising a replacement strategy that meets security and operational needs.**

Security Logging and Monitoring

- **Setting up extensive security logging and monitoring is key for early detection of security issues. Using a centralized SIEM system with the FortiGate 30E improves network visibility and facilitates swift responses to anomalies.**

Penetration Testing

- **Conducting regular penetration tests assesses the network's security strength and the FortiGate 30E's attack resilience. These tests help uncover vulnerabilities and inform ongoing enhancements to security protocols.**

EMERGING NGFW TRENDS THAT COULD ENHANCE FUTURE VERSIONS :

AI and Machine Learning (ML) Integration

- **Future versions could utilize AI and ML for advanced anomaly detection and predictive analytics, significantly improving threat detection and response times.**

Zero Trust Network Architecture (ZTNA) Support

- **Integrating ZTNA principles to offer refined access controls and security policies, ensuring more secure and granular network access management.**

Enhanced Cloud Integration

- **Providing more comprehensive integration with cloud platforms to ensure uniform security policies across both on-premises and cloud environments.**

Automation and Orchestration

- **Strengthening automation and orchestration for more efficient security policy management, quicker incident response, and streamlined maintenance processes.**

Increased Focus on User and Entity Behavior Analytics (UEBA)

- **Incorporating UEBA to better identify unusual behaviors and potential insider threats, enhancing overall security posture by monitoring for anomalies more effectively.**

RECOMMENDATIONS FOR DEPLOYMENT AND USAGE:

Regular Firmware Updates

- **Keep the firmware of the device up-to-date to fix vulnerabilities and add new security features, prioritizing these updates as a key part of the maintenance routine.**

Physical Security Measures

- **Place the device in secure, restricted-access areas to prevent unauthorized physical access and employ measures to detect any tampering attempts.**

Leverage High Availability Configurations

- **Utilize High Availability (HA) setups in critical network segments to eliminate single points of failure, enhancing network resilience.**

Customize Default Configurations

- **Adjust the default settings and passwords to fit the specific needs of the organization, reinforcing the device's security against generic exploit attempts.**

Comprehensive Security Training

- **Conduct regular security training sessions for users, focusing on the creation of strong**

passwords and the identification of phishing and other malicious activities.

Plan for Future Needs

- **Anticipate the future expansion of the network and evolving security challenges, ensuring that the deployment of the FortiGate 30E is scalable and adaptable.**

Integration with a Broader Security Ecosystem

- **Integrate the FortiGate 30E within a larger security framework that includes endpoint protection, intrusion detection, and centralized security management for a more robust defense.**