Fortinet Fortigate Next Generation Firewall (Version 30E)

Information Security Audit and Assurance

Saurabh Sunil Mishra

Roll No: 2023201034

Table of Contents

1. Introduction to Firewalls
2. Firewall Interaction with Network Layers
3. Types of Firewalls
4. UTM vs NGFW
5. VPN and Web Content Filtering
6. Major Firewall Producers
7. Fortinet Fortigate Solutions
8. Fortinet Fortigate NGFW Version 30E
9. Variants and Security Features of Fortigate 30E
10. Common Vulnerabilities and Exposures (CVEs)
11. Limitations and Performance Bottlenecks
12. Vulnerabilities
13. Emerging NGFW Trends
14. Recommendations for Deployment and Usage

Introduction to Firewalls

- **Definition:** Network security device or software application that monitors traffic.
- **Function:** Acts as a barrier between trusted internal network and untrusted external network.
- **ACL:** Utilizes Access Control Lists to dictate permitted traffic.

Firewall Interaction with Network Layers

- **Network Layer:** Filters traffic based on IP addresses, ports, and protocols.
- **Transport Layer:** Inspects TCP/UDP headers, controls access by port numbers.
- **Application Layer:** Proxy firewalls work here, inspecting content like HTTP and FTP.

Types of Firewalls

- **Packet Filtering:** Use ACLs, but lack deep packet inspection.
- **Stateful Inspection:** Monitor active connections, prevent session hijacking and DoS attacks.
- **Proxy Firewalls:** Act as an intermediary, can mask IP addresses.
- **Host-Based vs Network-Based:** Installed on individual hosts or networks respectively.
- **NGFW - Next Generation Firewalls:** Incorporate advanced features for enhanced security:
  1. Deep Packet Inspection (DPI)
  2. Intrusion Prevention Systems (IPS)
  3. Application Awareness
  4. Threat Intelligence
  5. Identity Management Integration
  6. Automation and Advanced Analytics

UTM vs NGFW

- **Unified Threat Management (UTM):** Includes firewalling, IDS/IPS, antivirus, content filtering, and VPN.
- **NGFW:** In addition to UTM functions, emphasizes deep packet filtering and application awareness.

VPN and Web Content Filtering

- **VPN:** Secure tunnel between a client and a server over an ISP.
- **Web Content Filtering:** Scans user traffic at the web browser level, crucial for application-layer filtering.

Major Firewall Producers

- **Market Leaders:** Leaders include Fortinet Fortigate, Palo Alto Networks, Cisco, and Juniper Networks.

Fortinet Fortigate Solutions

- **Entry-Level (30-90 Series):** For small offices or branches.
- **Mid-Range (100-900 Series):** Suits mid-sized businesses.
- **High-End (1000-3000 & 6000 Series):** Designed for large enterprises and data centers.
- **Chassis-Based (5000 & 7000 Series):** Ideal for service providers and large organizations.
- **Software-Based (FortiGate VMs):** Virtual firewalls for cloud environments.

Fortinet Fortigate NGFW Version 30E

- **Combines NGFW and UTM Features:** Incorporates both next-generation firewall and unified threat management functionalities.
- **Secure SD-WAN:** Integrates software-defined wide area networking for optimal data routing across multiple connections.
- **Wired Connectivity:** Features multiple Gigabit Ethernet ports for LAN and WAN connections.
- **SSL Encryption:** Utilizes Secure Sockets Layer to safeguard data transfer, protecting sensitive information.
- **Connectivity Ports:** Includes 1 WAN and 4 LAN ports, plus 1 USB port for configuration backups and external storage.
- **Throughput Rates:** Offers up to 950 Mbps firewall throughput, 300 Mbps IPS throughput, and 200 Mbps NGFW throughput.
- **Cloud Analytics:** Provides cloud-based analytics for centralized visibility and reporting.

Variants and Security Features of Fortigate 30E

- **Fortinet 30E (Standard Model):** Includes all core NGFW features with options for cloud analytics.
- **Fortinet-30E-3G4G-GBL :** Provides cellular connectivity for remote or mobile deployments.
- **Security Features:** Offers continuous threat intelligence and advanced threat protection.
- **SD-WAN:** Features dynamic traffic routing and cost-effective WAN management.

Common Vulnerabilities and Exposures (CVEs)

- **CVE-2023-27997:** Vulnerability in SSL VPN pre-authentication allowing remote code execution.
- **CVE-2013-1414:** CSRF vulnerabilities allowing unauthorized system changes.
- **CVE-2012-4948:** Default certificate validation issues leading to potential man-in-the-middle attacks.

Limitations and Performance Bottlenecks

- **Performance Scalability:** Designed for SMBs, might struggle with rapidly growing business demands.
- **Wired Connectivity Only:** Requires additional wireless access points, increasing IT complexity.
- **Limited Physical Interfaces:** Few ports can constrain network design and scalability.
- **Limited Physical Security:** Desktop form factor vulnerable to unauthorized access or theft.
- **Single Point of Failure:** Reliance on one unit poses a risk of network exposure if compromised.

Vulnerabilities

- **Notable CVEs:** Awareness and quick mitigation crucial for CVE-2023-27997 and CVE-2012-4948.
- **Supply Chain Attacks:** Importance of assessing vendor security practices, including Fortinet.
- **Zero-Day Exploits:** Requires a layered security strategy and proactive incident response.
- **Default Configuration Risks:** Enhancing security by avoiding defaults and customizing settings.
- **Insider Threats:** Strict access controls and monitoring to mitigate risks.
- **Social Engineering Attacks:** Emphasizing user education against phishing and similar tactics. [Cross Site Request Forgery Attack (CSRF)]
- **End-of-Life Planning:** Staying updated with lifecycle announcements for timely replacements.

Emerging NGFW Trends

- **AI and ML Integration:** For improved threat detection and response.
- **Zero Trust Network Architecture (ZTNA) Support:** For refined access controls and security policies.
- **Enhanced Cloud Integration:** Ensuring uniform security policies across environments.
- **Automation and Orchestration:** Streamlining security policy management and incident response.
- **Increased Focus on UEBA:** Monitoring for anomalies more effectively.

Recommendations for Deployment and Usage

- **Regular Firmware Updates:** Keeping the device firmware up-to-date.
- **Physical Security Measures:** Securing the device in restricted-access areas.
- **Leverage High Availability Configurations:** To eliminate single points of failure.
- **Customize Default Configurations:** Adjusting settings to fit organizational needs.
- **Comprehensive Security Training:** Educating users on security best practices.
- **Plan for Future Needs:** Ensuring scalability and adaptability for future expansion.
- **Integration with a Broader Security Ecosystem:** For a more robust defense.

Conclusion

Thank you for your attention!
Are there any questions?