Date: 13/06/2024 to 14/06/2024

➢ Firewall Setup and Their Configuration and Licensing

Objective: To provide a comprehensive report on the setup, configuration, and license approval process for the firewall to ensure robust network security at BVM Schools.

1. Firewall Selection and Licensing

Firewall Selection: Choosing a suitable firewall involves evaluating several factors including security features, performance, scalability, and cost. For BVM Schools, a Fortinet firewall has been selected due to its comprehensive security features, ease of use, and reliability.

License Approval:

- **License Type:** Fortinet offers various licensing options based on the features and duration required. For BVM Schools, an annual subscription with advanced security features is recommended.
- **Approval Process:**
    - Obtain approval from the school administration and IT department.
    - Contact Fortinet or an authorized reseller to purchase the license.
    - Ensure the license includes content filtering, intrusion prevention, and anti-virus capabilities.

2. Firewall Hardware and Initial Setup

Hardware Installation:

- **Placement:** Install the firewall device in the server room under the stairs.
- **Connections:** Connect the firewall to the network's core switch and ensure it has a direct connection to the internet gateway.

Initial Setup:

1. **Power On:** Power up the firewall and connect a laptop/PC to the firewall’s management port.
2. **Access Management Interface:** Open a web browser and enter the default IP address to access the management interface.
3. **Login:** Use default login credentials to access the setup wizard.

3. Firewall Configuration

Step-by-Step Configuration:

1. **Basic Settings:**
    - **Change Default Admin Password:** Immediately change the default password for security reasons.
    - **Configure Hostname:** Set a meaningful hostname (e.g., BVM-Firewall).
2. **Network Settings:**
    - **LAN and WAN Interfaces:** Configure IP addresses for the LAN and WAN interfaces.
    - **DNS Settings:** Set up primary and secondary DNS servers. If using a separate DNS within the firewall, configure it accordingly.
3. **Security Policies:**

    - **Create Security Zones:** Define different security zones (e.g., LAN, WAN, DMZ).
    - **Define Firewall Policies:**
        - **Admin Policy:** Full access to all resources.
        - **Teacher Policy:** Block access to social networks.
        - **Student Policy:** Block all social sites and allow access only to specific educational websites.
4. **Content Filtering:**
    - **Web Filtering:** Enable web filtering and configure categories to block social networking and other inappropriate content.
    - **Application Control:** Block specific applications and websites as per the policies.
5. **User Authentication:**
    - **Configure User Groups:** Create user groups for administrators, teachers, and students.
    - **Authentication Methods:** Set up authentication methods (e.g., LDAP, RADIUS) for user verification.
6. **NAT Configuration:**
    - **Setup NAT Rules:** Configure NAT rules to translate internal IP addresses to a public IP address for internet access.
    - **Port Forwarding:** If required, set up port forwarding rules for specific services.
7. **VPN Configuration (if needed):**
    - **Setup VPN:** Configure VPN settings for secure remote access by teachers and administrators.
8. **Logging and Monitoring:**
    - **Enable Logging:** Configure logging to monitor network traffic and firewall activities.
    - **Set Alerts:** Set up alerts for suspicious activities and security breaches.

4. License Activation

Activate License:

1. **Access Licensing Portal:** Log in to the Fortinet licensing portal.
2. **Enter License Key:** Input the license key provided at the time of purchase.
3. **Activate License:** Follow the prompts to activate the license.
4. **Verify Activation:** Check the firewall's status to ensure the license is active and all subscribed features are enabled.

5. Testing and Validation

Testing:

- **Connectivity Tests:** Verify internet connectivity and access to internal resources.
- **Policy Tests:** Ensure that the firewall policies are correctly enforced.
- **Content Filtering Tests:** Test access to blocked and allowed sites to confirm content filtering is working as expected.

Validation:

- **Security Audit:** Conduct a security audit to ensure the firewall is properly configured and secure.
- **Performance Monitoring:** Monitor the performance to ensure the firewall is not introducing significant latency or bottlenecks.

Fig 1: Fortinet FortiGate 40F Firewall Front View

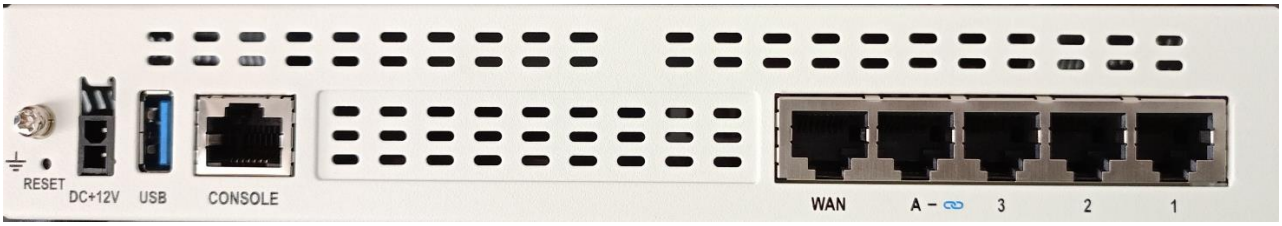

Fig 2: Fortinet FortiGate 40F Firewall Rear View