WEB FILTERING PROJECT

1. Objective of the project

The objective of this project is to:

- Implement web filtering using FortiGate’s FortiGuard Web Filtering feature

.

- Block or allow website access based on predefined categories.

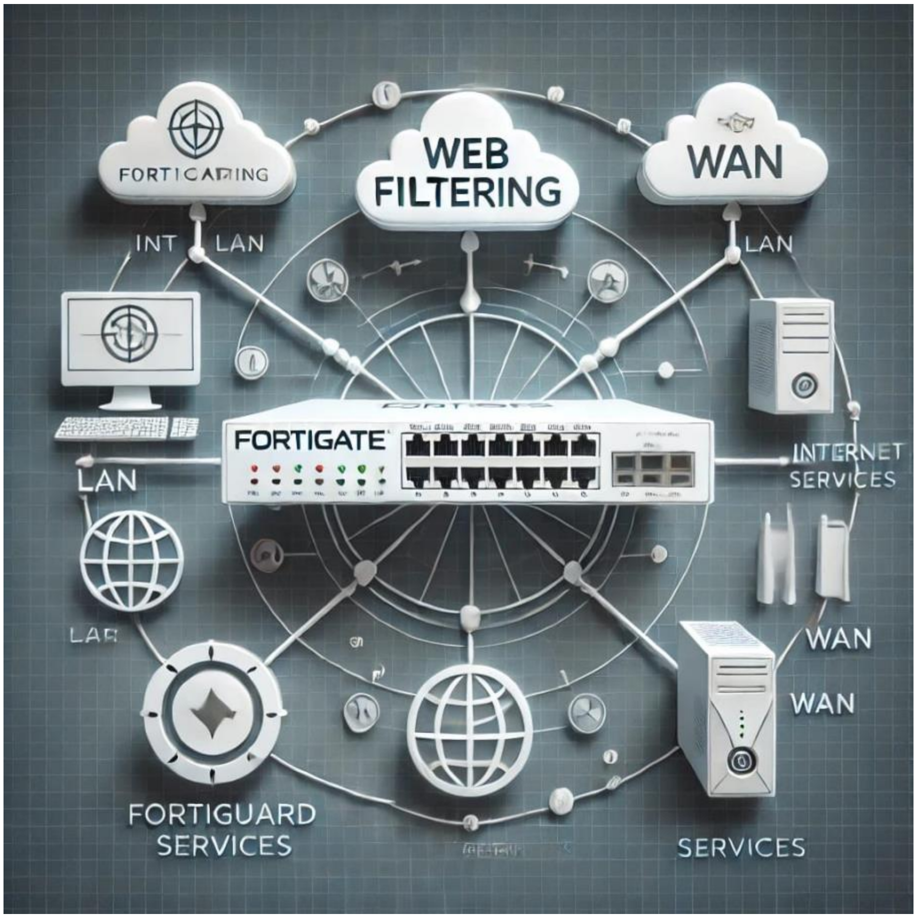
- Apply advanced configurations such as Web Rating Overrides and user authentication for more granular control.

- Ensure network security and productivity by managing internet access effectively.

2. Network Topology

The network setup includes:

1. **FortiGate Firewall** – Configured to manage traffic between the internal network (LAN) and the internet.
2. **Internal Client Machine** – Used to test web filtering rules.
3. **External Internet Services** – Websites categorized as blocked (e.g., Social Media) or allowed (e.g., Educational).



3. Components Used

1. **FortiGate Firewall** running FortiOS 7.2.
2. **Client devices** for testing (e.g., desktop or laptop).
3. **Web Browser** (e.g., Chrome, Firefox) for testing website access.
4. **Test URLs** categorized into blocked and allowed groups.
5. **Administrative Access** to the FortiGate GUI for configuration and management.

4. Steps of the Lab

Step 1: Configure FortiGuard Web Filtering

- Log in to the FortiGate GUI.
- Navigate to **Security Profiles > Web Filter**.
- Create a new web filter profile named WebFilter_Profile.
- Define category-based filtering rules:
  - Block Social Media (Category ID: 52).
  - Allow Educational Sites (Category ID: 18).
  - Leave other categories at their default settings.

Step 2: Apply Web Filter Profile to a Firewall Policy

- Navigate to **Policy & Objects > Firewall Policy**.
- Create a new policy:
  - Incoming Interface: port3 (LAN).
  - Outgoing Interface: port1 (WAN).
  - Action: Accept.
  - Enable Web Filter and assign the profile WebFilter_Profile.

Step 3: Test Access to Websites

- From the client device, attempt to visit:
  - Blocked websites such as Facebook and Twitter (expected result: access denied).
  - Allowed websites such as educational platforms like Coursera or Khan Academy (expected result: access granted).

Step 4: Configure and Test Web Rating Overrides

- Override the default rating of a specific URL (e.g., categorize YouTube as "Educational").
- Test by attempting to access the overridden URL.

Step 5: Enable Web Filtering Authentication

- Configure user groups and authentication on the FortiGate.
- Apply policies that enforce web filtering based on user roles.
- Test access to confirm policies work per user group.

5. Testing the Lab

Testing involves:

1. **Blocked Websites**
   - Attempt to visit Facebook or other social media platforms.
   - Ensure the connection is blocked with a message indicating restricted access.
2. **Allowed Websites**
   - Visit educational or business-related websites.
   - Confirm they are accessible without restrictions.
3. **Overrides**
   - Access URLs that were overridden and confirm they are categorized correctly.
4. **Logs**
   - Review logs for detailed tracking of web access attempts and enforcement of policies.

6. Results

The lab results demonstrate:

- Successful implementation of category-based web filtering.
- Accurate blocking of unauthorized websites while allowing access to approved ones.
- Effective application of Web Rating Overrides.
- User activity is logged for detailed analysis.

7. Configuration on the FortiGate Devices

Web Filter Profile Configuration

```
config webfilter profile
    edit "WebFilter_Profile"
        config web
            set category 52 block  # Blocks Social Media
            set category 18 allow  # Allows Educational Sites
        end
    next
end
```

Firewall Policy Configuration

```
config firewall policy
    edit 1
        set name "WebFilteringPolicy"
        set srcintf "port3"
        set dstintf "port1"
        set action "accept"
        set webfilter-profile "WebFilter_Profile"
        set schedule "always"
    next
end
```

Web Rating Overrides

```
config webfilter urlfilter
    edit 1
        set url "youtube.com"
        set type "simple"
        set action "allow"
        set category 18  # Categorized as Educational
    next
end
```

Additional Notes

- **Log Analysis**: Ensure that logs are enabled in the firewall policy to track all activities.
- **Customization**: Policies and profiles can be adjusted based on organizational needs.
- **Advanced Features**: Consider integrating FortiAnalyzer for centralized log analysis and reporting.