# LAB 7 - WEB FILTERING DOCUMENTATION

## LAB OBJECTIVE:

This lab demonstrates configuring FortiGuard Web Filtering to enforce access control, authenticate users, and customize web access through overrides. The lab emphasizes testing and troubleshooting for enterprise-grade deployments.

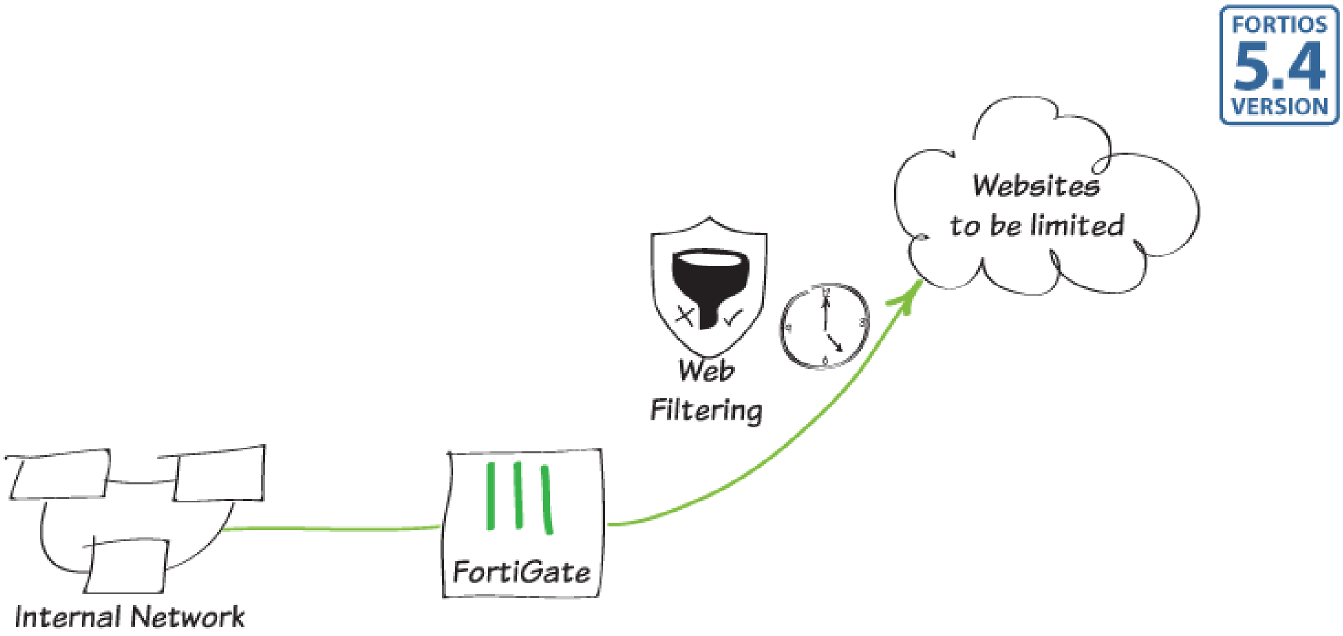
## 1. NETWORK TOPOLOGY:

### DESCRIPTION:

The network consists of:

- **FortiGate Firewall:** Central traffic control and filtering.
- **LAN Clients:** Devices requiring regulated internet access.
- **WAN Connectivity:** External internet access filtered by FortiGate

### DIAGRAM:



## 2. EQUIPMENT/COMPONENTS:

### HARDWARE:

- FortiGate Firewall (FG-VM64 or equivalent).
- Client Machines: Test devices.

### SOFTWARE:

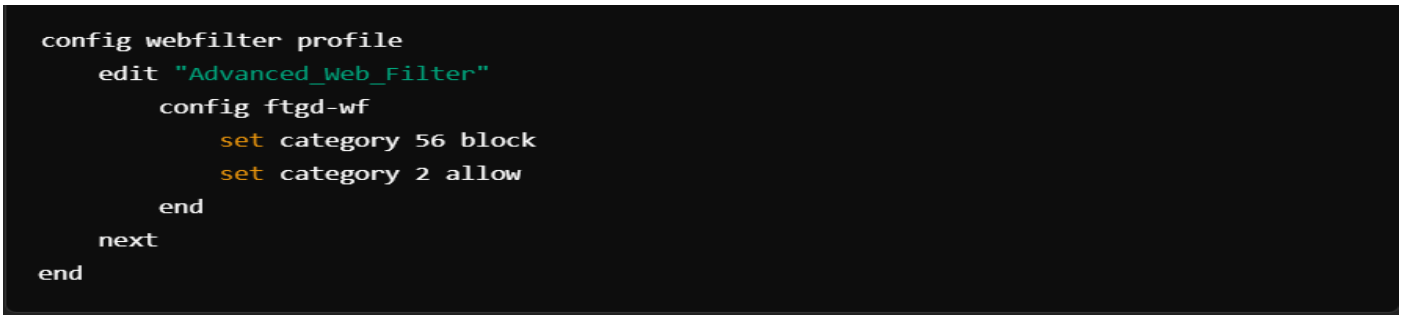
- FortiOS 7.2 or higher.
- FortiGuard Web Filtering Subscription.

# 3. CONFIGURATION STEPS:

**Step 1: Configure Web Filtering**

1. Navigate to Security Profiles > Web Filter.
2. Create a profile:
   - **Name:** Advanced_Web_Filter.
   - Enable **Category-Based Filtering.**
   - Set actions:
     - **Block:** Social Media, Adult Content, Streaming Media
     - **Monitor:** Shopping.
     - **Allow:** Business, Education.

**CLI configuration:**



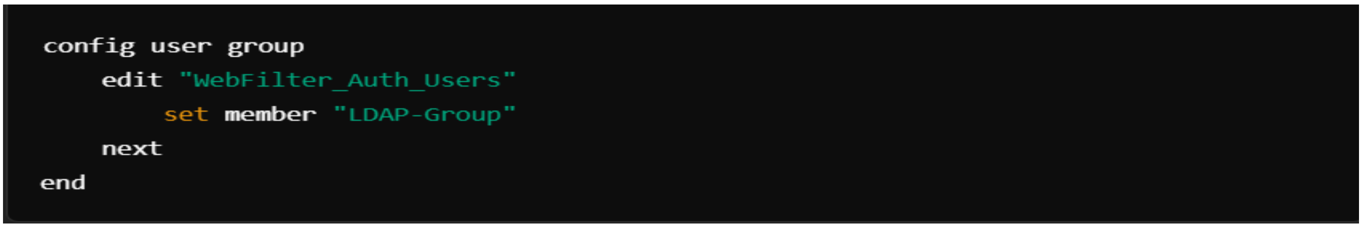
```
config webfilter profile
    edit "Advanced_Web_Filter"
        config ftgd-wf
            set category 56 block
            set category 2 allow
        end
    next
end
```

**Step 2: Apply Web Filter to a Policy**

1. Navigate to Policy & Objects > IPv4 Policy.
2. Create a policy:
   - Incoming Interface: LAN.
   - Outgoing Interface: WAN.
   - Source: all
   - Destination: all
   - Schedule: always
   - Service: ALL
3. Under Security Profiles, select the created Web Filter profile (Advanced_Web_Filter).
4. Save changes.

**Step 3: Set Up Authentication**

1. Navigate to User & Authentication > User Groups and create a group for authenticated users.
2. Configure LDAP/Active Directory settings if external authentication is used:



```
config user group
    edit "WebFilter_Auth_Users"
        set member "LDAP-Group"
    next
end
```

3. Modify the web filter policy:
   - Action: Authenticate.
   - Link the policy to the created user group.

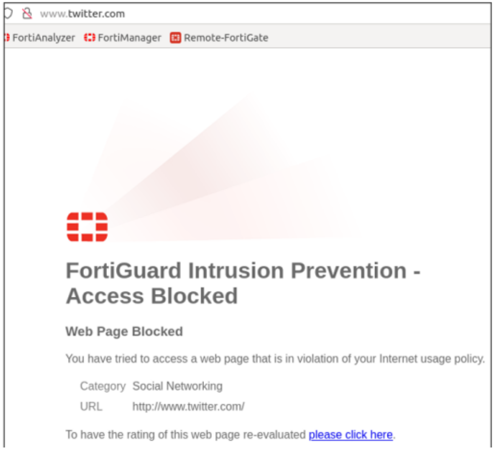
**Step 4: Add Web Rating Overrides**

1. Navigate to Security Profiles > Web Rating Overrides.
2. Add an override:
   - URL: example.com
   - Action: Allow
   - Category: Assign a custom category (e.g., Business).
3. Save and apply changes.

# 4. TESTING AND VALIDATION:

**Test Case 1: Blocked Categories**

- Attempt to access twitter.com.
- **Expected Result:** Block page appears.



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

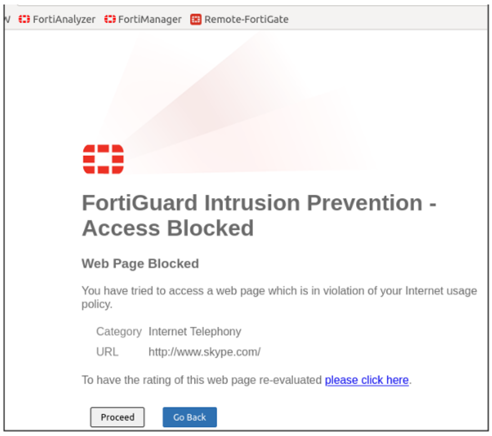
You have tried to access a web page that is in violation of your Internet usage policy.

| | |
|---|---|
| Category | Social Networking |
| URL | http://www.twitter.com/ |

To have the rating of this web page re-evaluated please click here.

**Test Case 2: Authentication Prompt**

- Access example.org under an authenticated policy.
- **Expected Result:** Prompt appears for credentials.
-



FortiGuard Intrusion Prevention - Access Blocked

Web Page Blocked

You have tried to access a web page which is in violation of your Internet usage policy.

| | |
|---|---|
| Category | Internet Telephony |
| URL | http://www.skype.com/ |

To have the rating of this web page re-evaluated please click here.

**Test Case 3: Web Rating Override**

- Access example.com and ensure the URL adheres to the override action.
- **Expected Result:** Allowed based on override.

**Logs Validation**

- Navigate to Log & Report > Web Filter Logs.
- Verify entries for blocked and allowed traffic, including overrides.

---

# 5. RESULTS

**Configuration Success:**

- Web filter effectively enforced category-based restrictions.
- Authentication prompts were functional and responsive.
- Web rating overrides worked as expected.

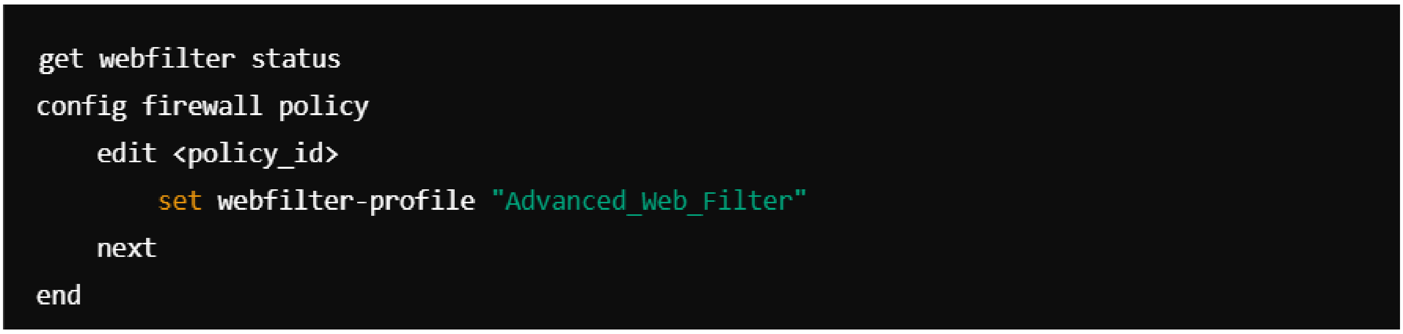
**Key Observations:**

- Logs accurately captured actions and matched policies.

## 6. TROUBLESHOOTING:

**Blocked Pages Not Displayed:**

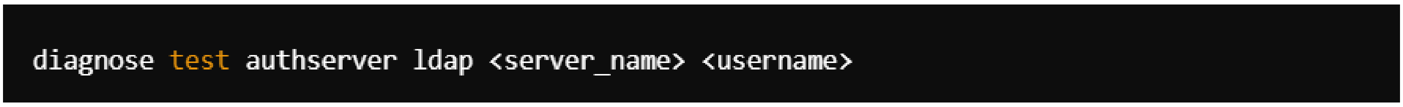
- **Cause:** Incorrect profile or FortiGuard issue.
- **Resolution:**



```
get webfilter status
config firewall policy
    edit <policy_id>
        set webfilter-profile "Advanced_Web_Filter"
    next
end
```

**Authentication Fails:**

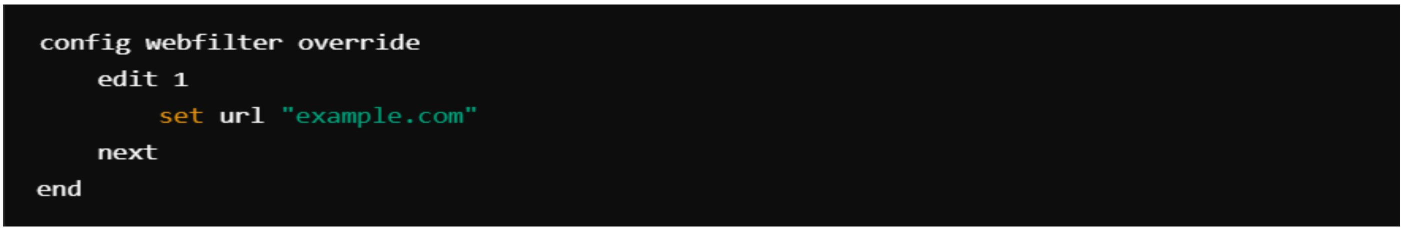
- **Cause:** LDAP misconfiguration.
- **Resolution:**



```
diagnose test authserver ldap <server_name> <username>
```

**Override Not Working:**

- **Cause:** Incorrect URL.
- **Resolution:**



```
config webfilter override
    edit 1
        set url "example.com"
    next
end
```

---

## 6. CONCLUSION:

This lab demonstrates configuring and testing FortiGuard Web Filtering with a focus on advanced troubleshooting. Proper implementation ensures compliance and security in enterprise environments.