# Name: Thomas Saad Tawfik

# Lab: Configuring and Monitoring Firewall Policies on FortiGate

## Objective of the Lab

* Configure IPv4 firewall policies.
* Monitor traffic logs from firewall policies.
* Choose and apply inspection modes for firewall policies.

## Topology

**Network Layout:** The topology includes a FortiGate firewall, with various zones or interfaces (incoming and outgoing), user devices, and internet services for real-world traffic testing.

**Connections:**

* Incoming interfaces represent traffic from internal networks or devices.
* Outgoing interfaces represent traffic towards external networks or services.

## Components Used

* **FortiGate Firewall:** Central security appliance for traffic management.
* **Administrative Tools:** FortiGate GUI and CLI for policy configuration and monitoring.
* **Logging Platforms:** FortiGate local/cloud storage, FortiAnalyzer, or Syslog servers for traffic log monitoring.

## Steps of the Lab

### 1. ****Understanding Firewall Policies****

Firewall policies control traffic by:

* Matching criteria such as source, destination, service, and schedule.
* Applying the first policy match in the top-down order.
* Enforcing implicit deny if no match is found.

### 2. ****Components of Firewall Policies****

**Objects Used in Policies:**

* + Interfaces and zones.
  + Address, user, and internet service objects.
  + Service definitions and schedules.
  + NAT rules and security profiles.

**Policy Types:**

* + IPv4/IPv6 Firewall Policies.
  + Local-in and DoS Policies.
  + Proxy and Traffic Shaping Policies.

### 3. ****Configuring Firewall Policies****

#### Create Policies via GUI:

1. Assign a mandatory policy name (or allow unnamed policies).
2. Specify source and destination criteria:
   * IP address/range, subnet, or FQDN.
   * Source users/groups or internet service databases.
3. Define services (e.g., HTTP, SSH, PING) and schedules.
4. Set actions to **ACCEPT** or **DENY**.
5. Enable logging (e.g., All Sessions or Security Events).
6. Select NAT and apply security profiles as needed.

#### Adjust Policy Order:

* Use drag-and-drop to reorder policies in the list.
* Ensure specific policies are placed above more general ones.

### 4. ****Selecting Inspection Modes****

* **Flow-Based:** Optimized for performance; enforces basic filtering.
* **Proxy-Based:** CPU-intensive but provides in-depth inspection for advanced features like:
  + Inline CASB.
  + Web Application Firewall.
  + Data Leak Prevention (DLP).

### 5. ****Monitoring Traffic Logs****

* Navigate to **Log & Report > Forward Traffic** in the GUI.
* Apply filters for relevant logs by source, destination, or policy.
* View live or historical logs based on time frame.
* Right-click a firewall policy to view matching traffic logs.

## Testing the Lab

### 1. ****Policy Matching:****

* Test various traffic scenarios to confirm matching policies.
* Verify that FortiGate applies the first matching policy in top-down order.

### 2. ****Log Monitoring:****

* Generate traffic (e.g., web browsing, pings).
* Confirm logs are generated for accepted and denied traffic.
* Use logs to troubleshoot and refine policies.

### 3. ****Reordering Policies:****

* Move specific policies above general policies.
* Test traffic behavior before and after reordering.

## Results

* **Traffic Control:** Confirmed that policies correctly accepted or denied traffic based on configurations.
* **Logs:** Logs showed detailed information on allowed and denied traffic.
* **Policy Refinement:** Adjusted policy order improved traffic matching accuracy.

## Configuration Done on the Devices

### Example Configuration: IPv4 Firewall Policy (ACCEPT):

config firewall policy

edit 1

set name "Internet\_Access"

set srcintf "port3"

set dstintf "port1"

set srcaddr "LOCAL\_SUBNET"

set dstaddr "all"

set schedule "always"

set service "HTTP" "HTTPS" "DNS"

set action "accept"

set logtraffic "all"

set nat enable

next

end

### Example Configuration: IPv4 Firewall Policy (DENY):

config firewall policy

edit 2

set name "Block\_FTP"

set srcintf "port3"

set dstintf "port1"

set srcaddr "LOCAL\_SUBNET"

set dstaddr "all"

set service "FTP"

set action "deny"

set logtraffic "all"

next

end

## Best Practices

* Test new policies in a maintenance window before applying them to production.
* Configure policies to be as specific as possible for better security.
* Regularly monitor logs to detect anomalies and refine policies.
* Apply security profiles only when necessary to balance performance and security.