"FortiGate Project"

Name: Pavly George Hosny Doss

Course Name: Fortinet Cybersecurity Engineer

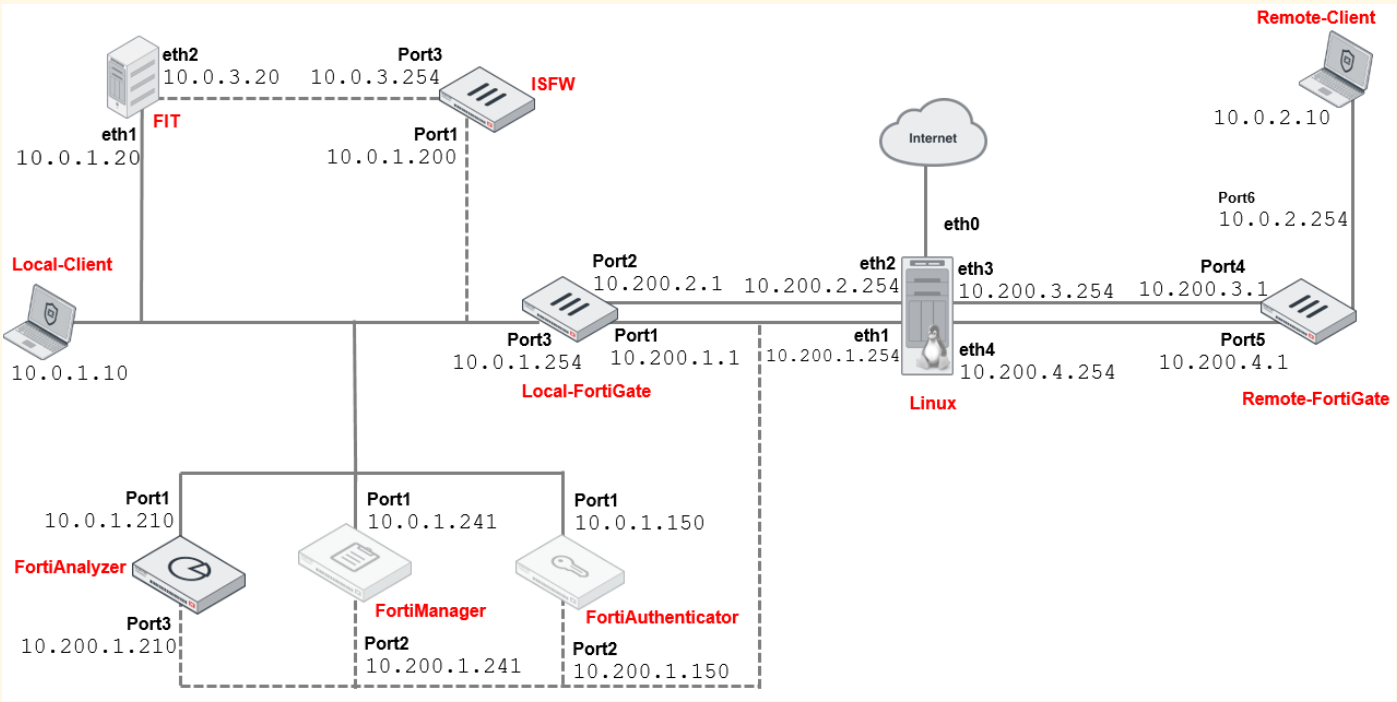
Course Code: CAI1_ISS8_S1e

Objective of the Lab

This lab demonstrates the configuration and usage of FortiGate's **application control** in both **profile-based** and **policy-based modes** to monitor, block, and manage traffic based on applications. It also teaches how to analyze application control logs.

Key Objectives:

1. Implement application control in NGFW **profile mode**.
2. Implement application control in NGFW **policy mode**.
3. Analyze logs to ensure traffic aligns with the applied policies.



Network Topology

The lab setup consists of:

- **FortiGate Device**: Configured with application control profiles and policies to manage traffic.

- **Client System (Local-Client VM)**: Used for generating traffic to test application behavior.
- **Internet**: Applications such as abc.com, Vimeo, and LinkedIn serve as targets for testing policies.

Detailed Description:

- The **FortiGate firewall** sits between the Local-Client VM and the internet.
- Outbound traffic is inspected based on application control profiles and policies.
- HTTPS traffic is deeply inspected using SSL inspection.

Visualize This: Although no image is provided here, think of a simple diagram where:

- The Local-Client VM connects to the FortiGate.
- FortiGate connects to the internet.
- Traffic flows are filtered and controlled based on policies.

Components Used

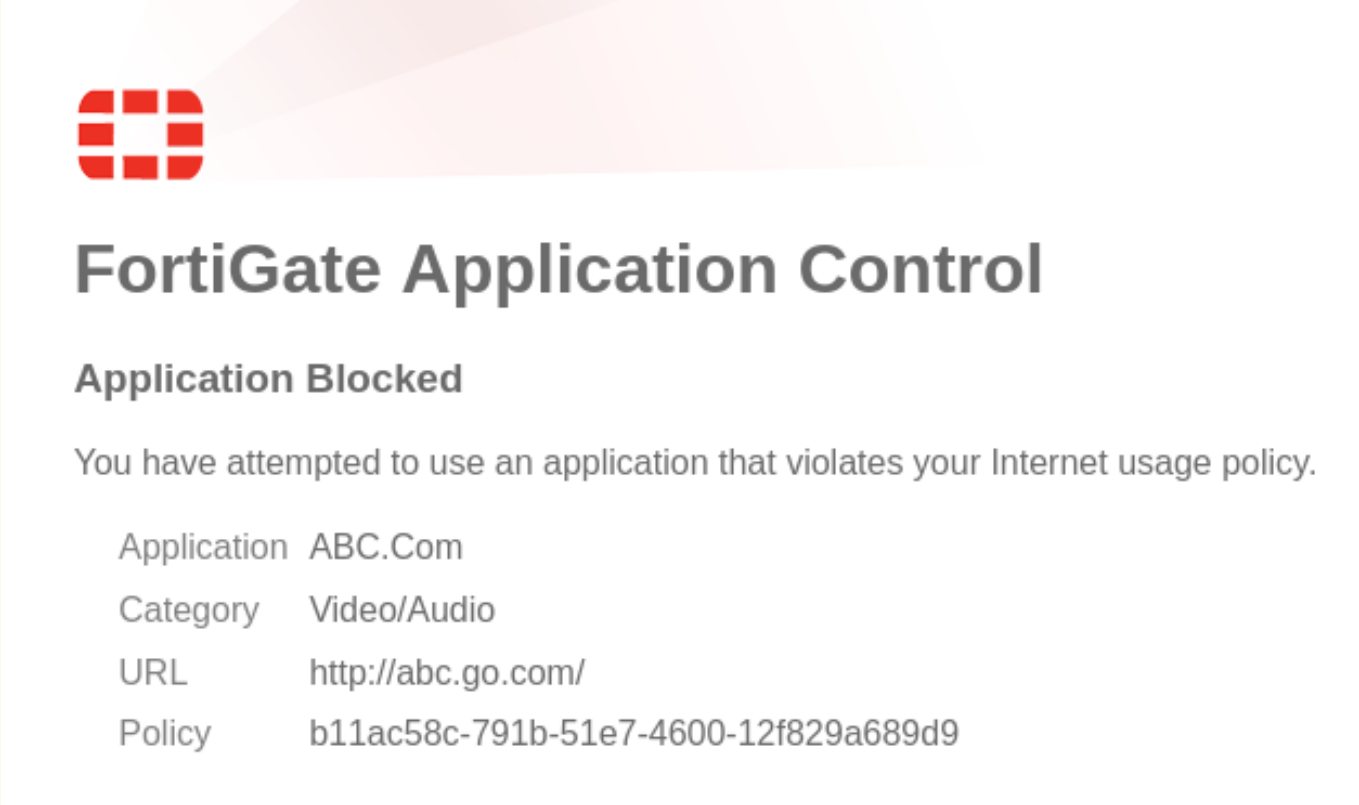
1. **FortiGate Device/VM**:
   - Functions as the application firewall.
   - Hosts predefined configuration settings from the file local-app-control.conf.
2. **Client System (Local-Client VM)**:
   - Simulates user behavior by browsing specific websites.
3. **Configuration File (local-app-control.conf)**:
   - Preloaded settings for application control, traffic shaping, and SSL inspection.

Steps of the Lab

1. Restoring Configuration

- Import the provided configuration file (local-app-control.conf) into FortiGate.
- Steps:

1. Log in to the **FortiGate GUI**.
2. Go to **Configuration > Revisions** and upload the configuration file.
3. Reboot the device to apply the configuration.



2. Exercise 1: Controlling Application Traffic

This exercise involves creating a profile-based application control setup.

1. **Modify the Default Application Control Profile**:
   - Edit the **default application control profile**.
   - Add **filter overrides** to block bandwidth-intensive applications such as abc.com.

   Configuration Steps:
   - Navigate to **Security Profiles > Application Control**.
   - Edit the default profile.
   - Under **Application and Filter Overrides,** add a new filter with:
     - Type: Filter
     - Behavior: Excessive-Bandwidth
     - Action: Block
2. **Apply the Application Control Profile**:
   - Assign the modified profile to the existing firewall policy.
   - Enable **deep inspection** in SSL/SSH settings.
3. **Testing**:
   - Open a browser on the Local-Client VM and visit http://abc.com.
   - **Expected Result**: The connection is blocked, and the browser displays a timeout or block message.

3. Exercise 2: Controlling Application Bandwidth Usage

This exercise demonstrates traffic shaping.

1. **Modify Application Overrides**:

- Edit the application control profile to monitor Vimeo traffic.
- Steps:

- Navigate to **Security Profiles > Application Control**.
- Add an override for Vimeo and set the action to Monitor.

2. **Configure Traffic Shaping**:

- Apply a **traffic shaping policy** to limit bandwidth for Vimeo.
- Key settings:

- Reverse Shaper: VIMEO_SHAPER (with low bandwidth settings).
- Target Application: Vimeo.

3. **Testing**:

- Visit http://vimeo.com and play a video.
- **Expected Result**: The video buffers slowly due to bandwidth limitations.

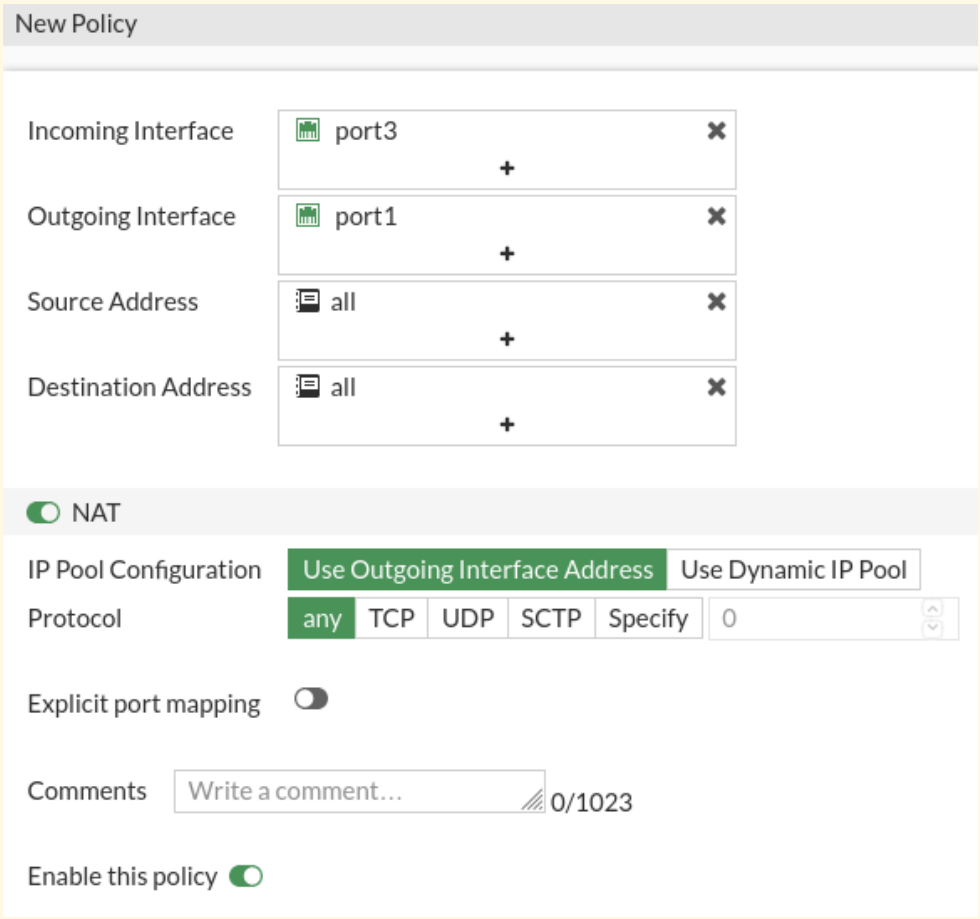
Additional Insight:

- Check the **Traffic Shaping** section in the FortiGate GUI to monitor bandwidth usage and dropped packets for Vimeo.

4.Exercise 3: Implementing Application Control in NGFW Policy-Based Mode

This exercise involves switching to **policy-based mode** and configuring policies at the NGFW level.

1. **Enable NGFW Policy-Based Mode**:
   - Change the mode under **System > Settings**.
   - Note: Switching modes deletes existing firewall policies.
2. **Create Security Policies**:
   - Configure a policy to allow only LinkedIn traffic.
   - Steps:
     - Navigate to **Policy & Objects > Security Policy**.
     - Create a new policy with:
     - Application: LinkedIn
     - Action: Accept
   - Block all other applications using the implicit deny policy.
3. **Testing**:
   - Open a browser on the Local-Client VM:
     - Visit http://linkedin.com: **Access allowed**.
     - Visit http://facebook.com: **Access blocked**.



Testing the Lab

1. **Blocked Applications**:
   - Confirm that abc.com and Facebook are blocked.
2. **Bandwidth Shaping**:
   - Verify that Vimeo traffic experiences bandwidth throttling.
3. **Allowed Applications**:
   - Ensure that only LinkedIn is accessible.

Results

1. **Traffic Management**:
   - Successfully blocked unwanted applications (abc.com and Facebook).
   - Allowed specific applications (LinkedIn).
2. **Bandwidth Control**:
   - Restricted Vimeo bandwidth using traffic shaping policies.
3. **Application Logs**:
   - Verified traffic matches in the logs under **Security Events**.

Details Observed in Logs:

- Application Name: Matched to specific overrides (e.g., LinkedIn, Vimeo).
- Action Taken: Allowed/Blocked.
- Bandwidth Utilization: Logged for Vimeo.

Configuration Done on Devices

- **Application Control Profiles**:
  - Filter overrides for Excessive-Bandwidth.
  - Application overrides for abc.com and LinkedIn.
- **Traffic Shaping Policies**:
  - Limited bandwidth for Vimeo.
- **Policy-Based Mode**:
  - Explicit policies created for LinkedIn while blocking others.