Amr Ahmed Ahmed Nasser ID=21034091

Project Documentation: Application Control and Traffic Shaping using FortiGate Firewall

1.Project Overview

1.1 Objective

The objective of this project was to implement and configure **Application Control** and **Traffic Shaping** on a **FortiGate firewall** to manage network traffic, improve bandwidth efficiency, and enforce security policies based on applications. This project focused on:

- Controlling the access and bandwidth usage of specific applications, such as LinkedIn, YouTube, Facebook, and Vimeo.
- Ensuring proper inspection and filtering of encrypted traffic using **SSL Inspection**.
- Implementing **traffic shaping** policies to guarantee quality of service (QoS) for critical applications while limiting bandwidth for non-essential services.

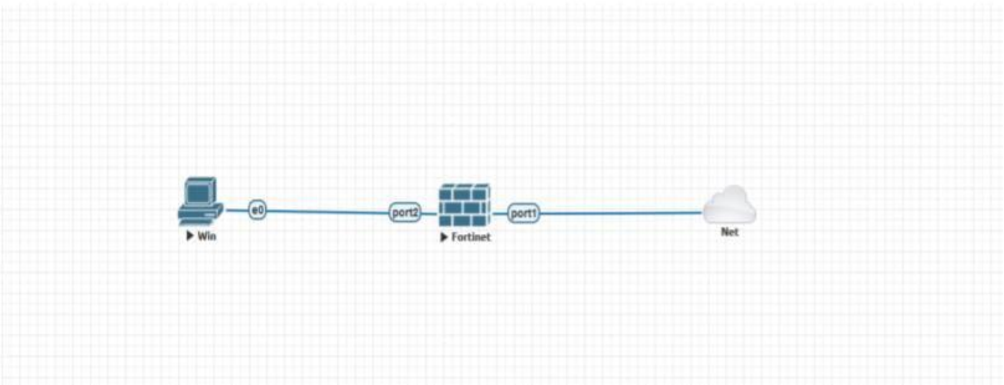
1.2 Project Scope

- Configuration of a FortiGate firewall to apply application control and traffic shaping on the network.
- Configuration of SSL inspection profiles to decrypt and inspect encrypted traffic.
- Creation and enforcement of security policies to allow/deny specific applications and manage bandwidth utilization.
- Testing the setup by simulating traffic from client machines to verify policy enforcement.

2. Network Topology

2.1 Network Diagram

The network topology consists of a **FortiGate firewall** placed between the internal clients and the external network. The firewall is configured to manage and control application traffic, enforce bandwidth policies, and inspect SSL traffic.



- **Client Machine(s)**: Simulate user traffic for testing.
- **FortiGate Firewall**: The primary security device that controls traffic.
- **Internet**: External network accessed by the firewall.

2.2 Components Used

- **FortiGate 60F**: The firewall appliance used for application control, traffic shaping, and SSL inspection.
- **Client Machines**: Devices used to simulate web traffic, including social media and video streaming sites.
- **Forti OS Version**: Forti OS 7.4.1
- **Web Applications**: Websites such as LinkedIn, YouTube, Facebook, and Vimeo were tested for access and bandwidth restrictions.

3. Configuration Steps

3.1 Initial Setup

1. **Connect and Configure the FortiGate Firewall**:
   - The **FortiGate firewall** was physically connected between the internal network (LAN) and the external network (WAN).
   - Basic settings for the interfaces were configured, including IP addresses for LAN and WAN interfaces, and routing settings to ensure the firewall could access the internet.
2. **Access the FortiGate Admin Console**:
   - The **FortiGate GUI** was accessed via a web browser using the firewall's IP address.
   - Basic connectivity to the internet was verified.

3.2 Application Control Configuration

1. **Create an Application Control Profile**:
   - In the GUI, navigate to **Security Profiles > Application Control**.
   - A new **Application Control Profile** was created, which included applications like LinkedIn, YouTube, Vimeo, and Facebook.
   - Specific **Application Overrides** were applied to block Facebook and limit YouTube traffic.
2. **Apply the Application Control Profile to Security Policies**:
   - Security policies were created in **Policy & Objects > IPv4 Policy** to apply the application control profile.
   - Policies were defined to allow or deny access to the applications based on the profile.

3.3 Traffic Shaping Configuration

1. **Create Traffic Shaping Profiles**:
   - Under **Traffic Shaping** in **Policy & Objects**, shaping profiles were created to limit bandwidth for non-essential applications such as YouTube and Vimeo.
   - **Maximum Bandwidth** was defined for each application, such as limiting YouTube to 2 Mbps while providing full bandwidth for LinkedIn.
2. **Apply Traffic Shaping Policies**:
   - Security policies were created to apply traffic shaping profiles to the respective applications.
   - For example, YouTube traffic was limited to 2 Mbps, while LinkedIn had no bandwidth restrictions.

3.4 SSL Inspection Configuration

1. **Enable Deep SSL Inspection**:
   - In **Security Profiles > SSL/SSH Inspection**, **Deep SSL Inspection** was enabled to decrypt and inspect SSL traffic, ensuring that HTTPS traffic for LinkedIn and other applications could be analyzed for security threats.
2. **Configure SSL Inspection Policies**:
   - Firewall policies were configured to ensure SSL traffic from applications like LinkedIn and Facebook was inspected.

3.5 Create Security Policies

1. **Policy Creation**:
    - Security policies were created for each application (LinkedIn, Facebook, YouTube) to:
        - Allow or deny access based on the application control profile.
        - Apply traffic shaping profiles to manage bandwidth.
        - Enable SSL inspection for HTTPS traffic.
    - Policies were defined to control traffic from LAN to WAN interfaces.

4. Testing the Configuration

4.1 Application Control Tests

1. **LinkedIn Access Test**:
    - LinkedIn was accessed from a client machine.
    - LinkedIn was successfully accessible with no bandwidth restrictions.
    - The logs confirmed that the **Application Control** profile was applied correctly.
2. **Facebook Block Test**:
    - Facebook was accessed from a client machine.
    - Facebook access was blocked as per the security policy.
    - The logs confirmed that traffic was blocked according to the policy.

4.2 Traffic Shaping Tests

1. **YouTube Bandwidth Test**:
    - YouTube was accessed and the bandwidth was verified to be limited to 2 Mbps as per the traffic shaping policy.
    - The bandwidth was measured using network monitoring tools, and logs confirmed the traffic shaping was applied.
2. **Vimeo Bandwidth Test**:
    - Vimeo was accessed and the bandwidth was shaped according to the defined policy.
    - The bandwidth was monitored to ensure proper shaping.

4.3 SSL Inspection Test

1. **SSL Inspection for LinkedIn**:
    - LinkedIn was accessed over HTTPS and SSL inspection was verified to be active.

   - Logs showed SSL inspection events, confirming that encrypted traffic was decrypted and inspected.

2. **Encrypted Traffic Test**:
   - Encrypted traffic from LinkedIn and Facebook was inspected for any security issues.
   - SSL inspection was confirmed to be working for these services.

5. Project Results and Analysis

5.1 Expected Results

- **LinkedIn**: Successfully accessible, no bandwidth restrictions, and SSL inspection applied.
- **Facebook**: Access blocked as per the security policy.
- **YouTube**: Bandwidth limited to 2 Mbps.
- **Vimeo**: Bandwidth shaped as per the defined policy.

5.2 Actual Results

- **LinkedIn**: Successfully accessible, no bandwidth restrictions, and SSL inspection applied.
- **Facebook**: Blocked as expected, access was denied.
- **YouTube**: Bandwidth was limited to 2 Mbps.
- **Vimeo**: Bandwidth shaping applied as expected.

5.3 Challenges

- SSL Inspection required additional configuration steps to ensure proper decryption and inspection of encrypted traffic.
- Fine-tuning traffic shaping profiles was needed to ensure that bandwidth limits were enforced without causing congestion.

6. Conclusion

6.1 Summary

This project involved the successful configuration of a **FortiGate firewall** to implement **Application Control**, **Traffic Shaping**, and **SSL Inspection**. These configurations ensured that critical applications like LinkedIn had sufficient bandwidth, while non-essential services like Facebook and YouTube were either blocked or limited in bandwidth.

6.2 Recommendations

- It is recommended to periodically review and update the application control profiles to accommodate new applications or changes in network usage patterns.
- The traffic shaping profiles should be adjusted based on ongoing usage patterns to ensure optimal bandwidth utilization.