Advanced FortiGate Security Profiles

Internship Program Graduation Project

Presented to: Dr. Hussein Harb

Instructed by: Eng. Mario Aiad

Prepared by: Group A

1. Morkos Bekhit – Research and Presentation on Security Profiles
2. Youssef Tarek – Configuring and Applying Security Profiles
3. Youssef Rafeek – Implementing Monitoring and Reporting Features
4. Abdullah Ramadan – Compiling the Final Report and Presentation

Program: FortiGate Administrator Certification Internship

Organization: Digital Egypt Pioneers Initiative – Egyptian Ministry of Communications & Information Technology (MCIT)

Submission Date: Wednesday April 23, 2025

Table of Contents

---

1. Introduction

This report documents our four-week project focused on Fortinet's advanced security profiles. As recent graduates participating in the FortiGate Administrator Internship program, our objective was to understand, implement, and monitor FortiGate security profiles to improve network protection against evolving threats.

---

2. Project Plan and Timeline

Team Formation:

- The team consists of four members with designated roles.
- A team leader was appointed to ensure coordination and timely communication with the instructor.

Task Distribution:

- **Morkos Bekhit:** Security Profiles Research & Presentation
- **Youssef Tarek:** Configuration and Implementation
- **Youssef Rafeek:** Monitoring and Reporting
- **Abdullah Ramadan:** Final Report and Presentation Compilation

Execution Timeline:

- **Week 1:** Understanding Security Profiles (Morkos Bekhit)
- **Week 2:** Configuring Security Profiles (Youssef Tarek)
- **Week 3:** Monitoring and Reporting (Youssef Rafeek)
- **Week 4:** Final Report & Presentation (Abdullah Ramadan)

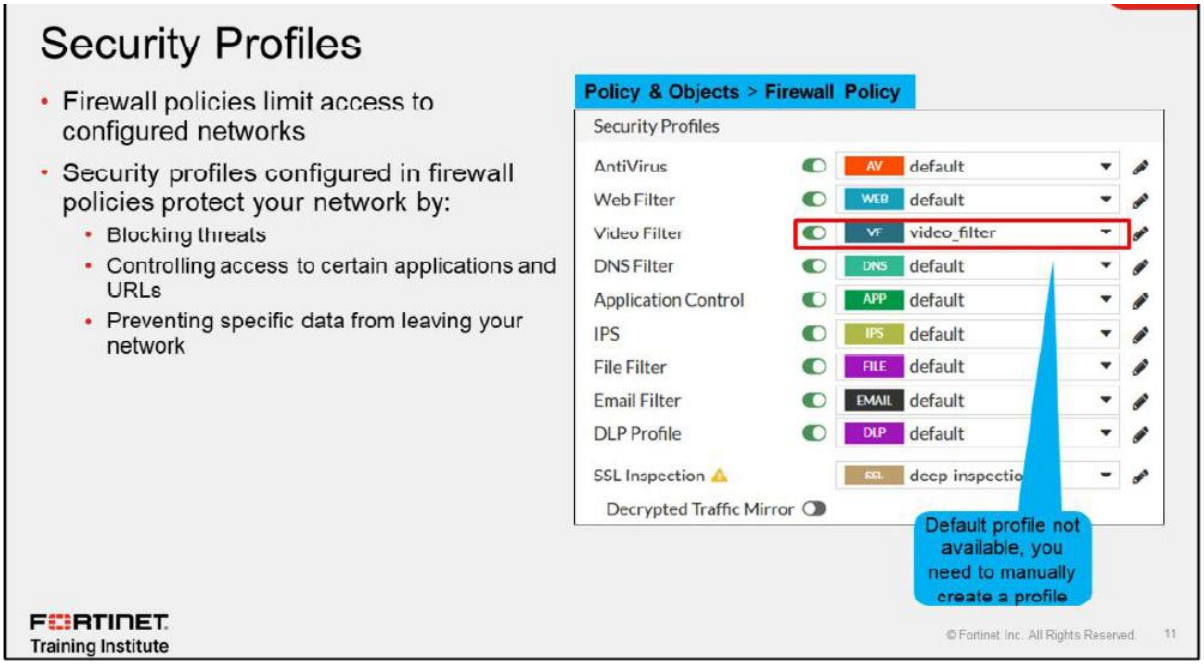
---

3. Week 1: Understanding Security Profiles

Objective: To research and understand the core FortiGate security profiles: Antivirus, Web Filtering, Application Control, IPS, and DNS Filtering, and more. Configuring security profiles to neutralize threats and misuse, including viruses, torrents, and inappropriate websites, It is one of the most important features that a firewall policy can apply, A security profile inspects each packet in the traffic flow, where the session has already been conditionally accepted by the firewall policy.

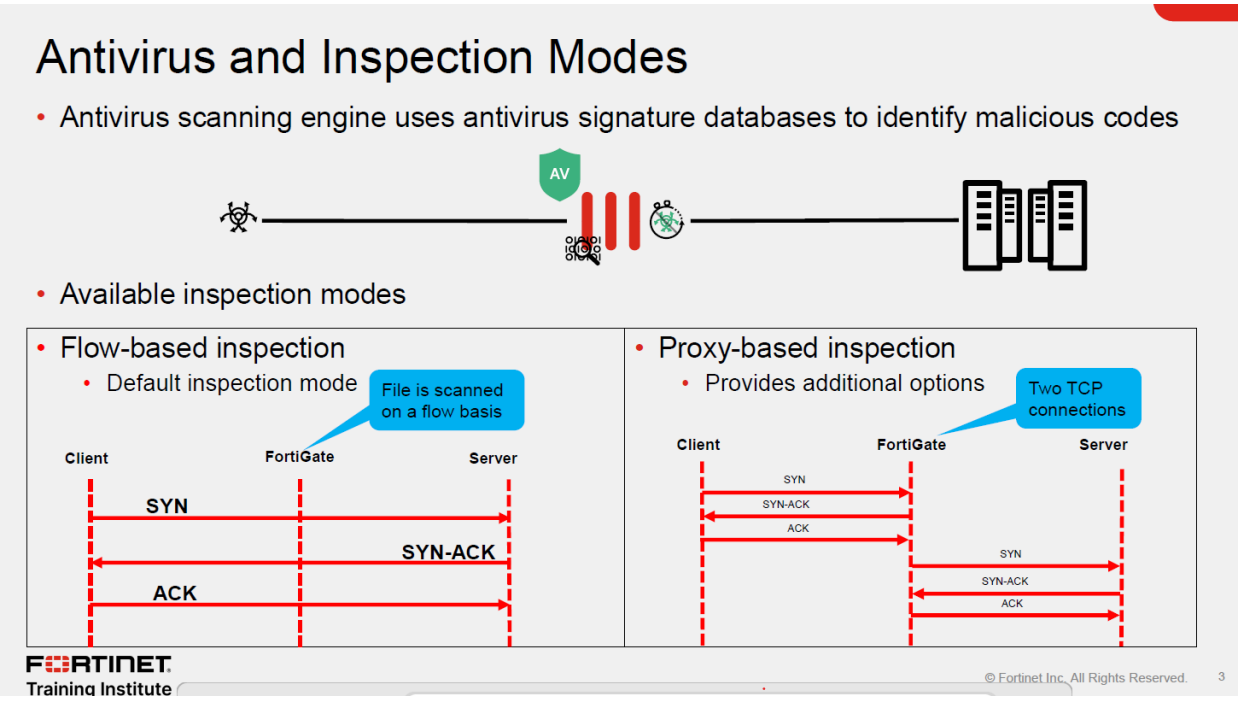
When inspecting traffic, FortiGate can use one of two methods: flow-based inspection or proxy-based inspection. Different security features are supported by each inspection type.

Note: By default, the **Video Filter**, **VOIP**, **Web Application Firewall** security profiles options are not visible on the policy page on GUI. We need to enable them on **Feature Visibility** page.

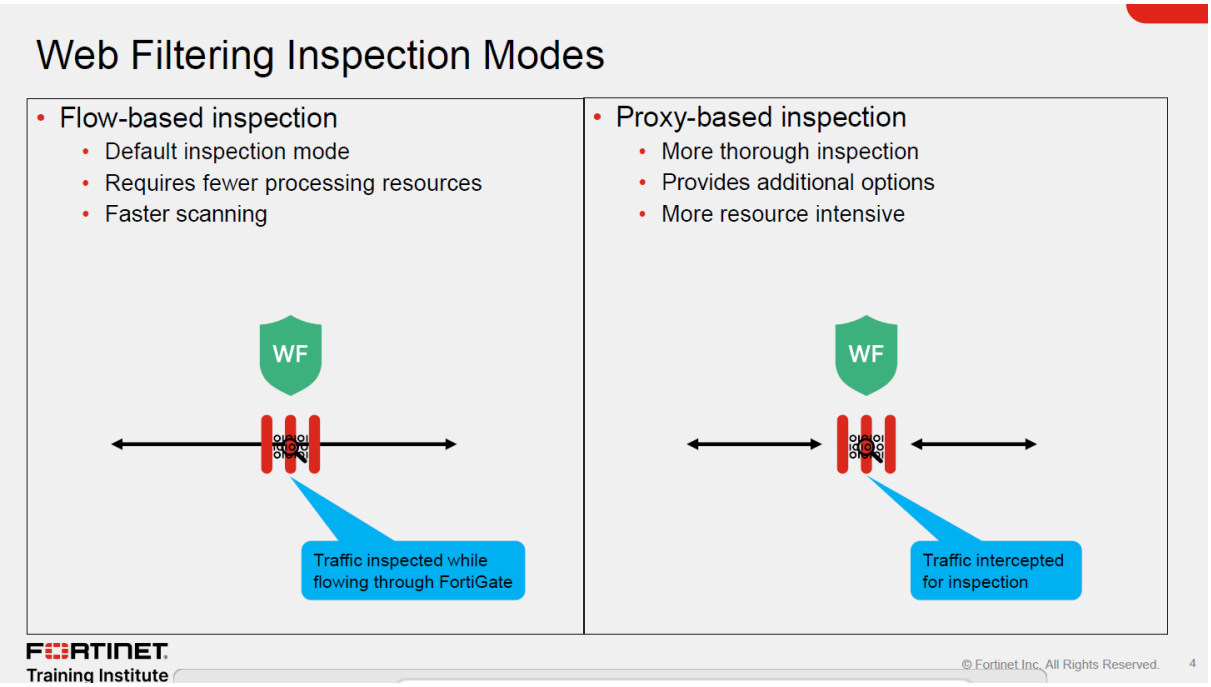


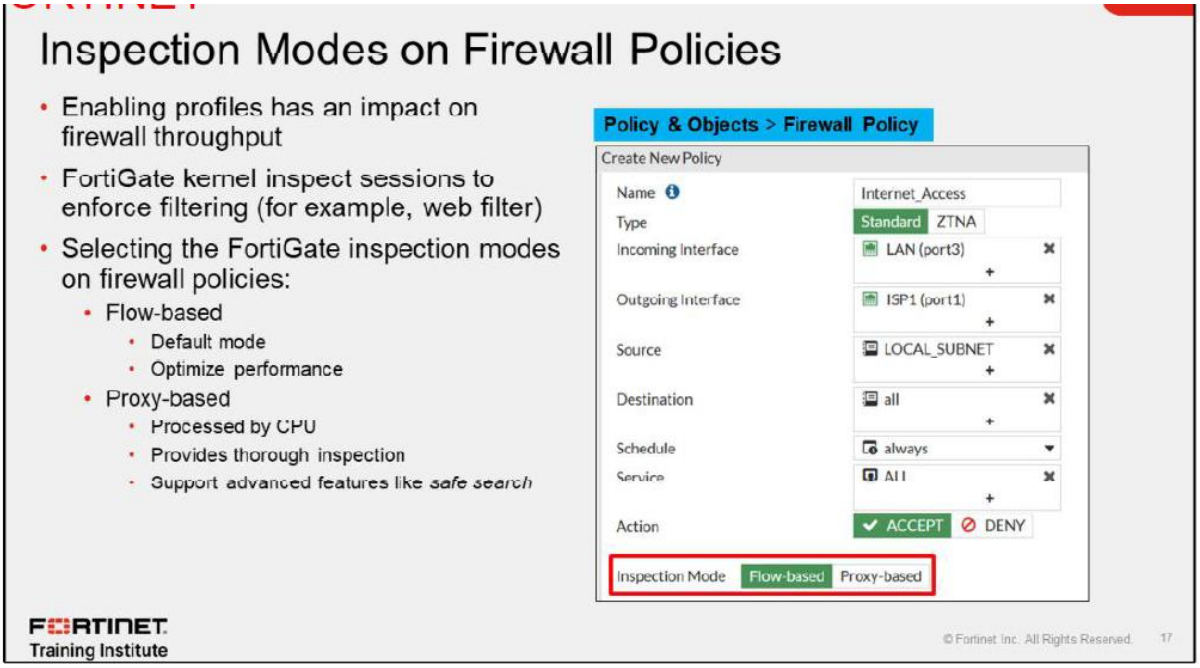
Key Concepts:

- **Antivirus:** Scans traffic for viruses, malware, and spyware.

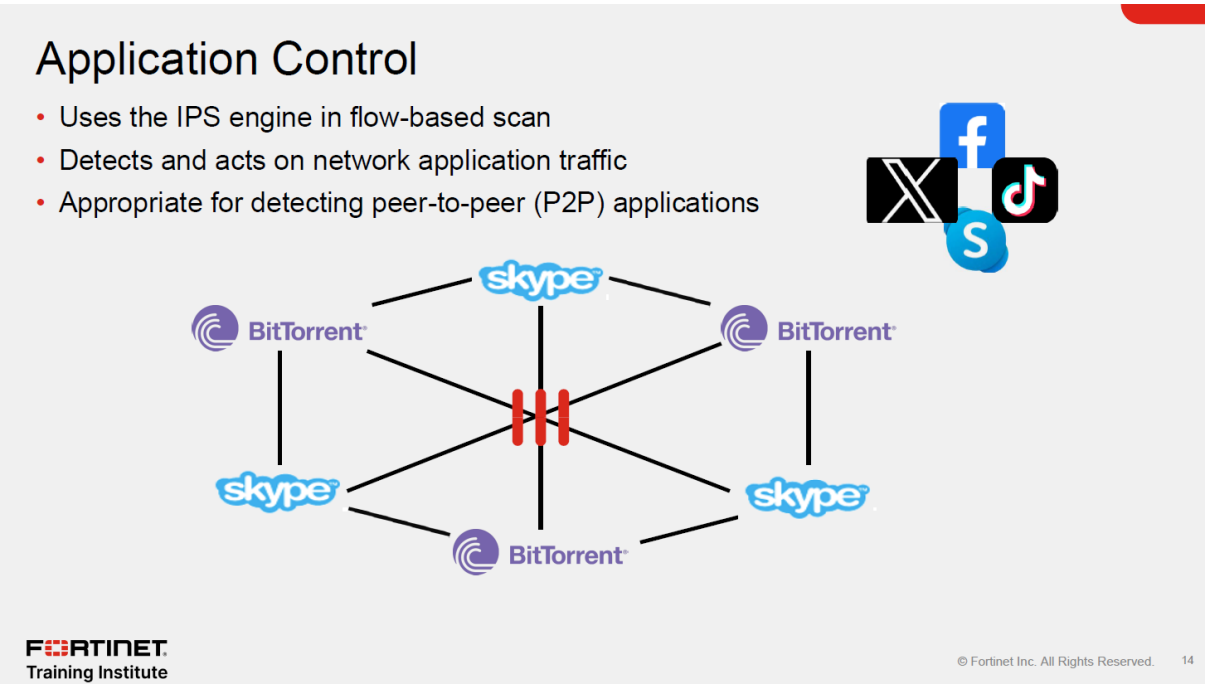


- **Web Filtering:** Controls access to web content by category or URL.

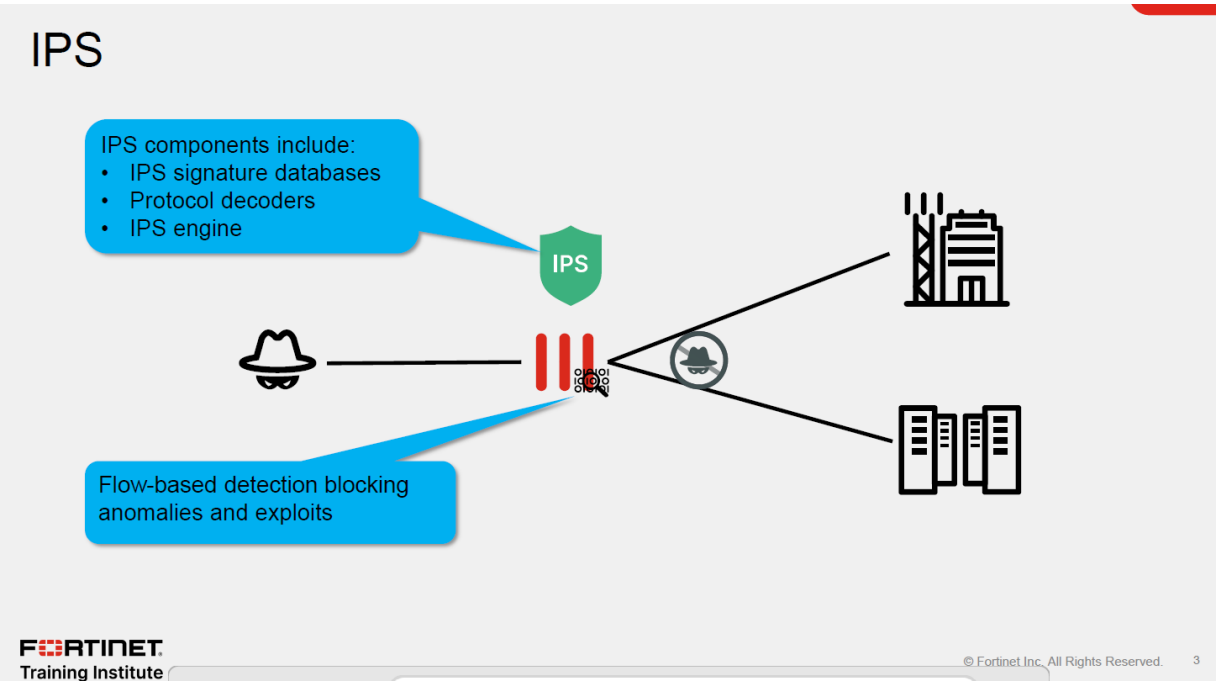




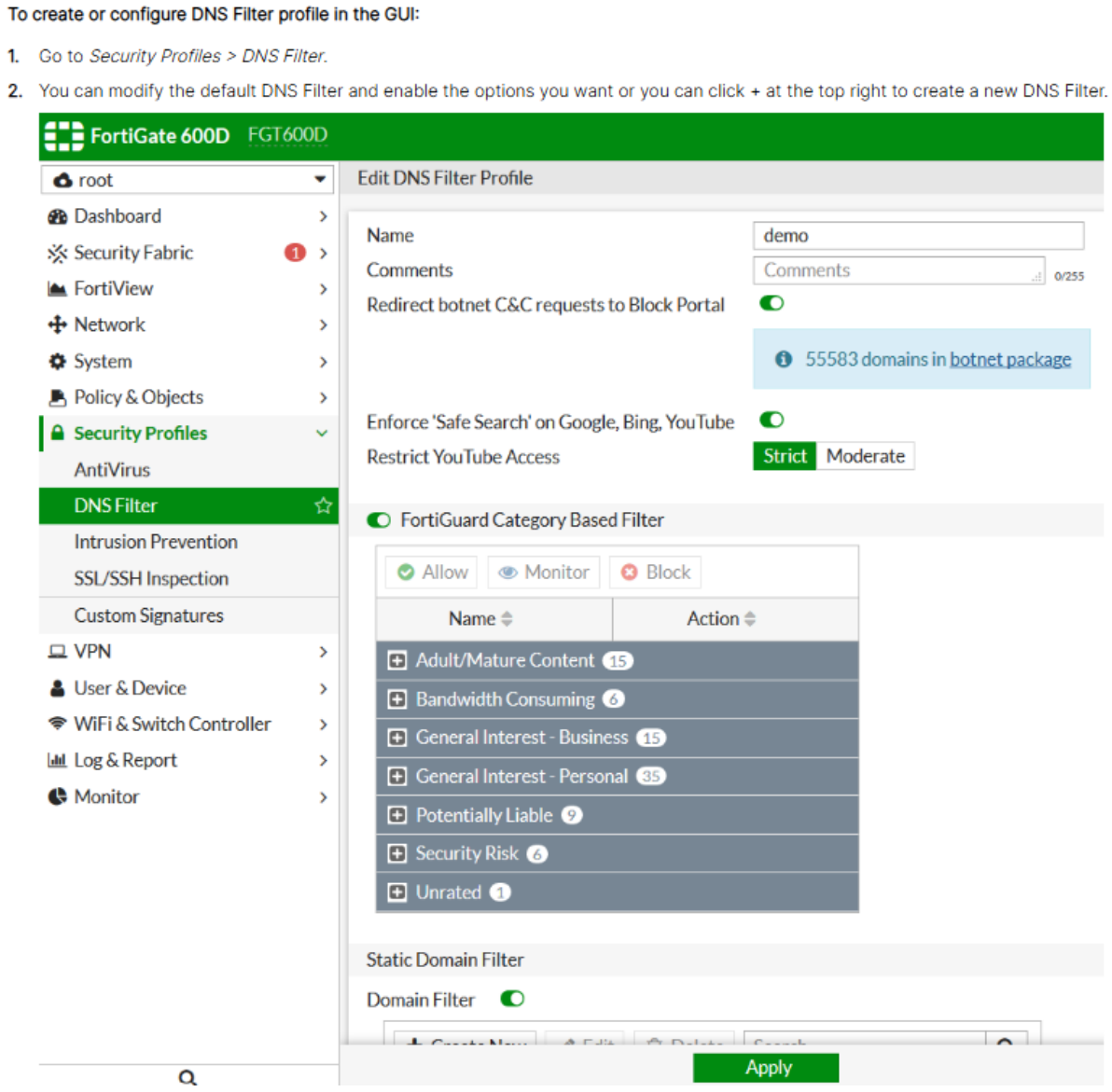
- **Application Control:** Identifies and manages applications by behaviour and protocol.



- **Intrusion Prevention System (IPS):** Detects and blocks exploits, buffer overflows, and known vulnerabilities.



- **DNS Filtering:** Prevents access to malicious or inappropriate domains.



---

4. Week 2: Configuring Security Profiles

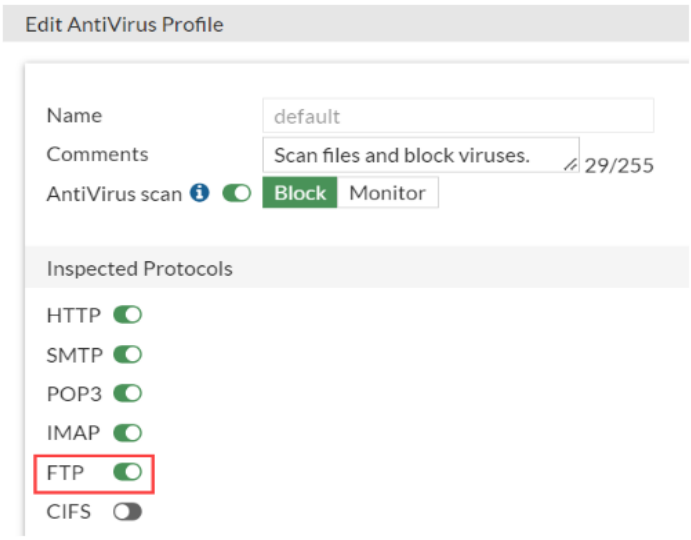
Objective: To configure and apply various security profiles within the FortiGate firewall.

Tasks Completed:

- Created custom Antivirus and Web Filtering profiles
- Applied security profiles to existing firewall policies
- Configured Application Control to block P2P and proxy apps

To verify the antivirus profile

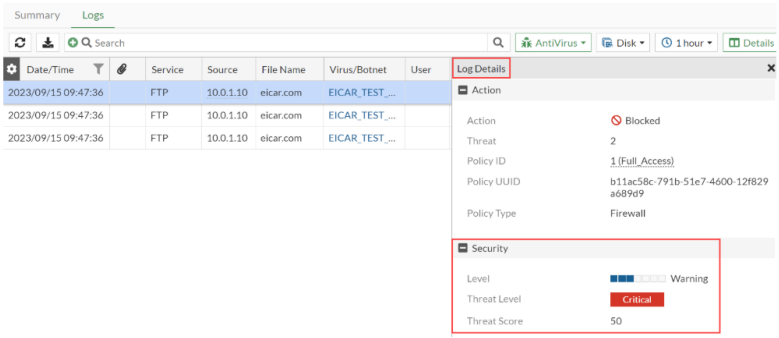
1. Connect to the Local-FortiGate GUI, and then log in with the username
2. Click **Security Profiles** > **AntiVirus**.
3. Right-click the **default** antivirus profile, and then click **Edit**.
4. In the **Inspected Protocols** section, verify that **FTP** is enabled.



Best Practices:

- Assign different profiles to internal and guest networks
- Use custom categories for specific business policies

2. Locate the antivirus log message from when you tried to access the file using FTP, and then double-click the log entry to view the security details.



---

5. Week 3: Monitoring and Reporting

Objective: To monitor traffic logs and generate reports to evaluate the effectiveness of applied security profiles. Security Profiles help to provide appropriate security for network. Proper logging configuration can also help us to analyze, diagnose, and resolve common network issues.

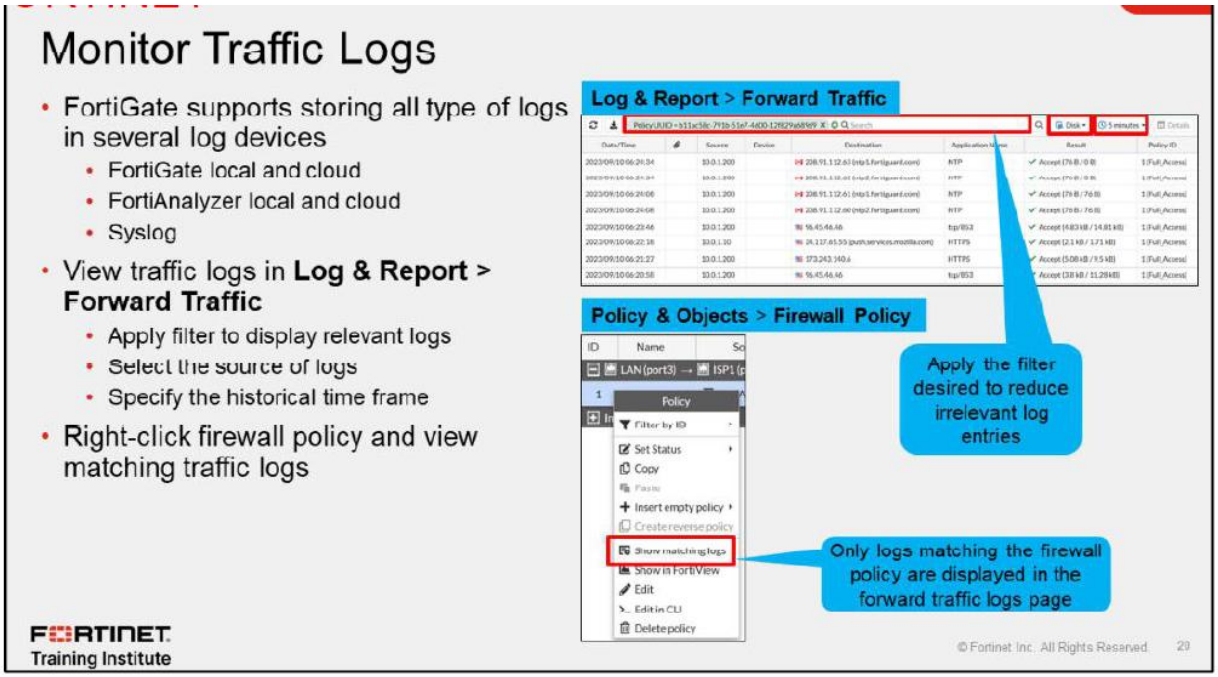
Monitoring Tools Used:

- FortiView
- Log & Report > Application Control, Web Filter Logs

- Custom report generation in FortiAnalyzer (if available)

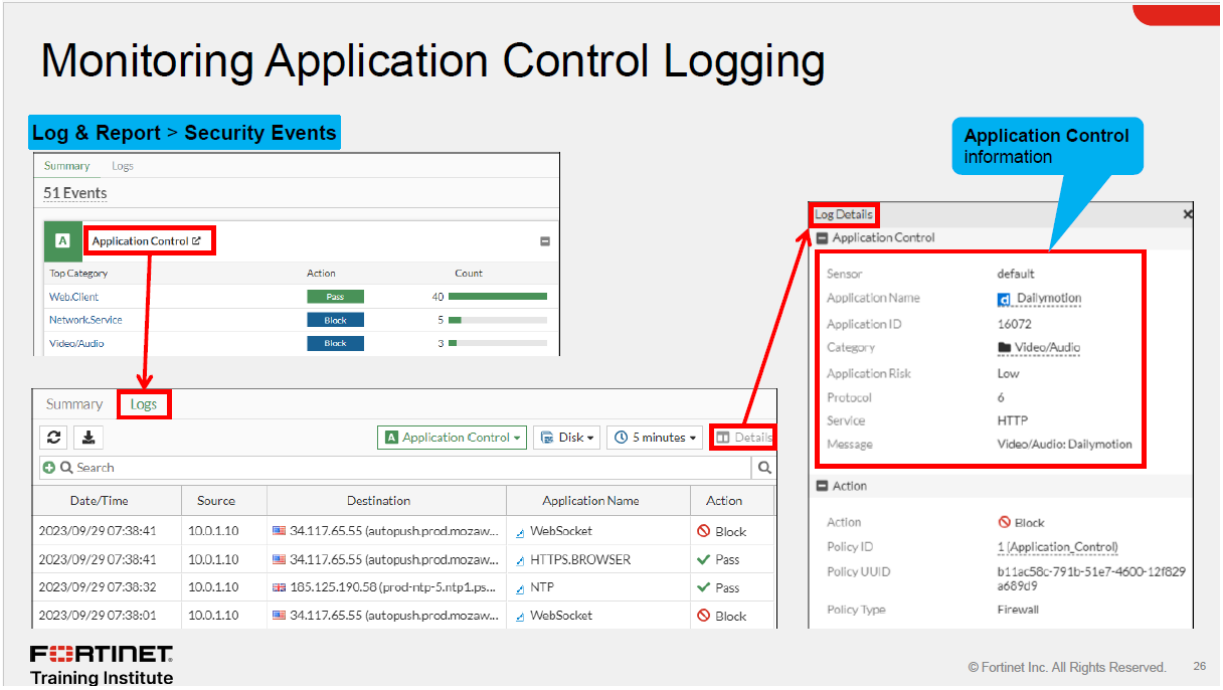
Logging on FortiGate records the traffic that passes through, start from, or end on FortiGate. It records the actions during the traffic scanning process. FortiGate supports sending all log types to several log services including its local storage which is subject to the disk available on different FortiGate models.

We can view traffic logs in **Logs & Reports** > **Forward Traffic**. Apply the filter needed to display the logs and then enter the Policy UUID in the filter field to display records that match the firewall policy. Select the source of the logs the historical time frame to reduce irrelevant log entries.



Observations:

- Malware downloads blocked by Antivirus profile
- High-risk websites blocked under Web Filtering
- Unauthorized proxy apps blocked through App Control



---

6. Week 4: Final Presentation and Report

Objective: Compile all tasks and findings into a final report and presentation.

Actions Taken:

- Integrated research, configuration, and monitoring content
- Formatted slides and designed visuals for clarity
- Reviewed the report against project requirements

Deliverable: Final PDF Report and PowerPoint Presentation

---

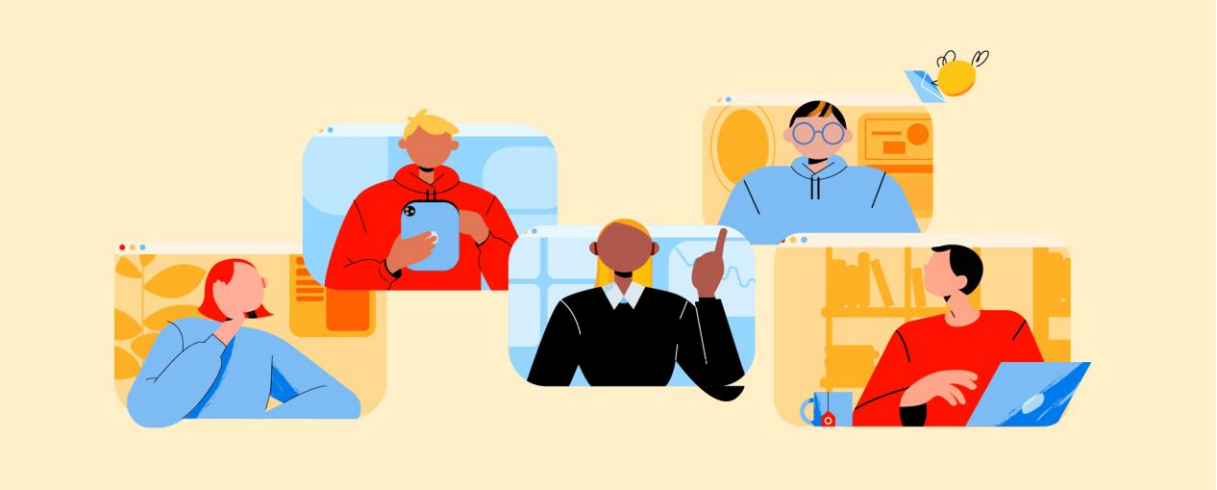
7. Risk Management and Communication

Risk Management:

- **Delay in configuration setup:** Assigned a backup member to assist
- **Lack of understanding of FortiGate settings:** Referred to Fortinet course documentation/labs and online resources
- **Ineffective coordination:** Regularly team check-ins and clear role assignments resolved this

Communication Strategy:

- Used Microsoft Teams, What's App and Google Drive for Docs collaboration
- Regularly virtual meetings to track progress



---

8. Summary and Recommendations

Summary:
Over four weeks, the team effectively:

- Understood FortiGate security profiles
- Configured and applied real use-case scenarios
- Monitored their effectiveness with Fortinet tools

Recommendations:

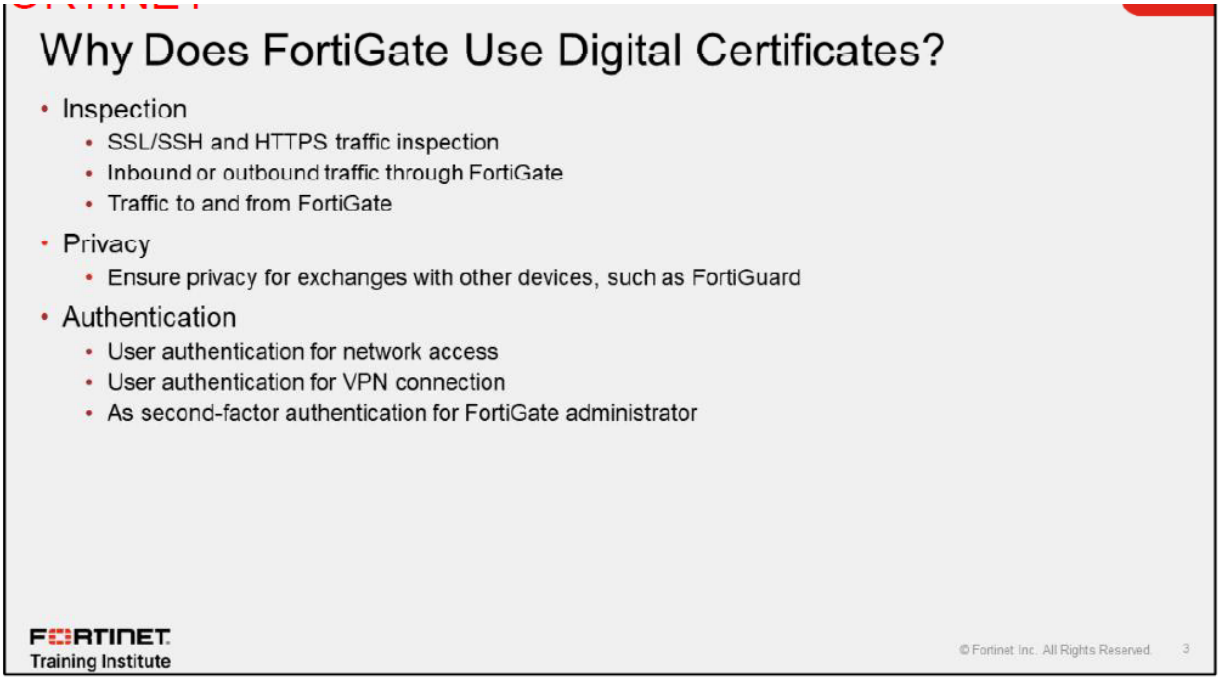
- Enable SSL deep inspection for full content visibility
- Use FortiAnalyzer (if available) for detailed insights and history
- Automate log backup and periodic report generation

---

9. Certificate Operations Overview

Although not the central focus, certificate management plays a crucial role in securing advanced FortiGate features such as SSL deep inspection and secure web filtering.

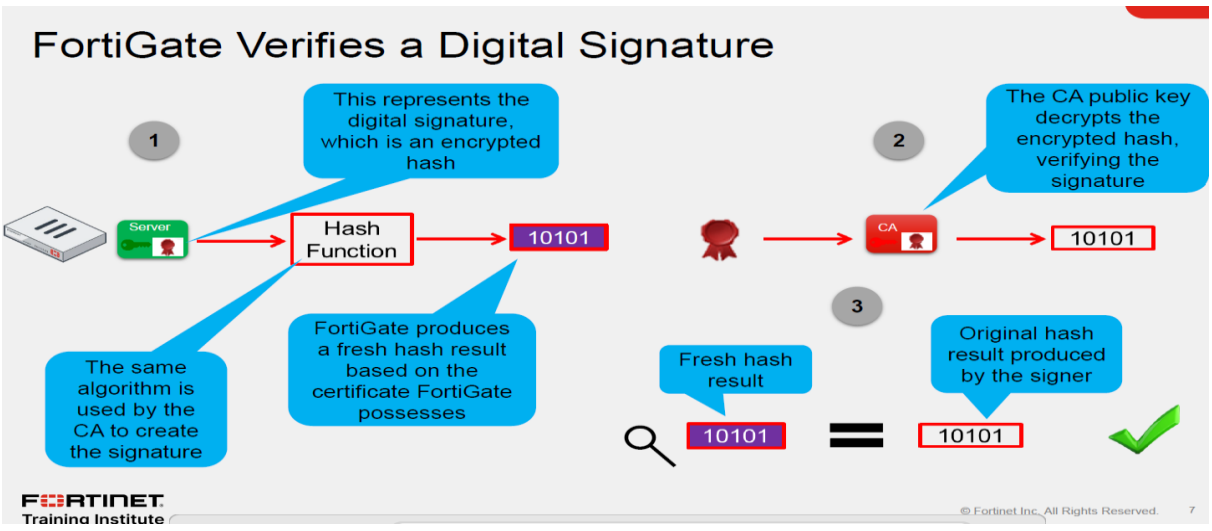
FortiGateUses digital Certificates for inspections, mainly outbound or inbound traffic inspection, if FortiGate trusts the certificate, it permits the connection. But if FortiGate dies not trust the certificate, it can prevent the connection, FortiGate also inspect certificates to identify people and devices, before it permits a person or device to make a full connectio to the enity that it is protecting.



Certificate Operations Summary:

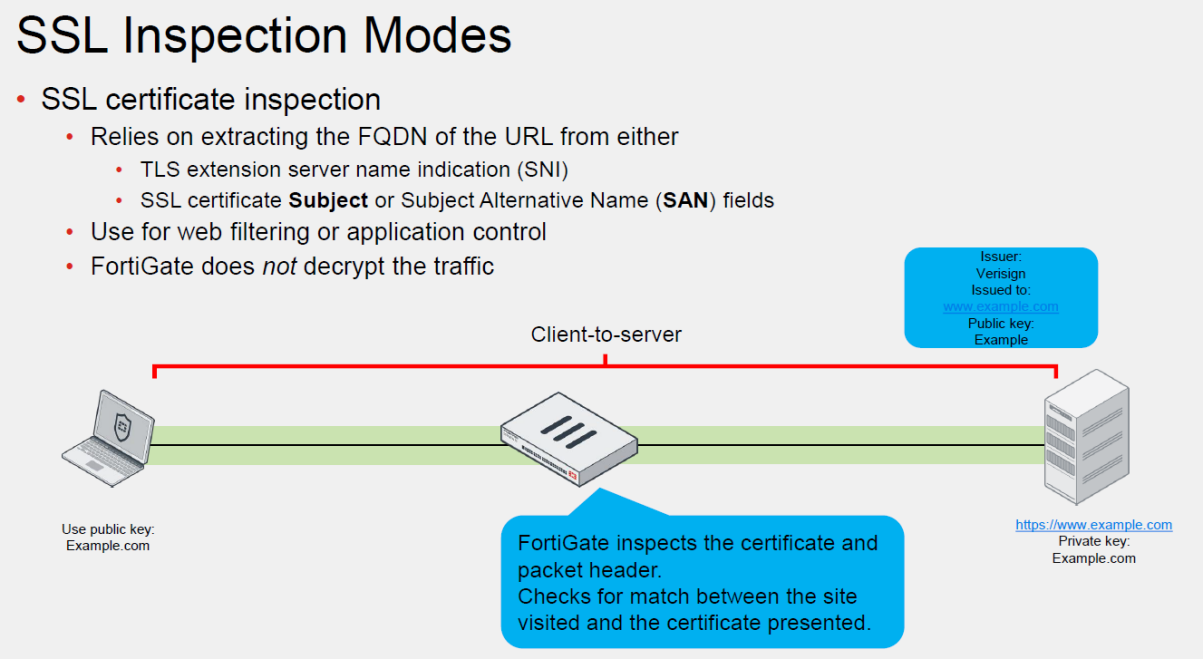
- Uploaded and installed SSL certificates to FortiGate for web filtering and VPN inspection
- Applied certificates to SSL inspection profiles
- Validated certificate trust on endpoint devices to prevent browser security alerts

FortiGate Uses SSL to ensure that data remains private when connecting with servers, such as FortiGaurd, and with clients, such as a web browser. Another Feature of SSL is that FortiGate can use it to identify one or both parties using certificates.



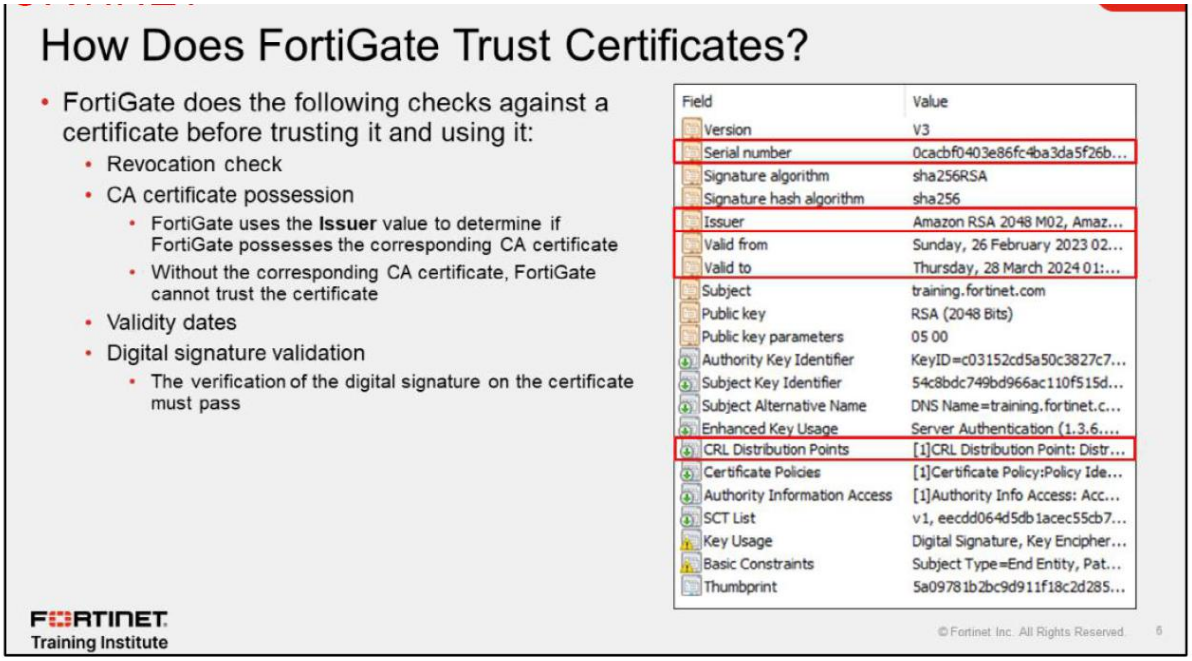
Example Tasks Performed:

- Generated and imported a local certificate into FortiGate
- Assigned the certificate to a deep inspection profile
- Tested browsing behaviour to verify SSL decryption and re-encryption



Example Screenshot:

Certificates enhance the accuracy of threat inspection, ensuring encrypted traffic can be scanned while maintaining user trust.



10. Appendix

FortiOS Version: [V7.0.x - v7.4.x]
Device Model: FortiGate Administration (Lab Environment)

Sample Policy Configuration:

```
config firewall policy
  edit 10
    set name "Secure-Access"
    set srcintf "lan"
    set dstintf "wan1"
    set srcaddr "all"
    set dstaddr "all"
    set action accept
    set schedule "always"
    set service "ALL"
    set utm-status enable
    set av-profile "AV-Custom"
    set webfilter-profile "WF-Strict"
    set application-list "App-Control-1"
  next
end
```

Teamwork Members:
Morkos Bekhit – Security Profiles Research
Youssef Tarek – Configuration & Testing
Youssef Rafeek – Monitoring & Logging
Abdullah Ramadan – Reporting & Documentation

Thank you for your time,