Advanced FortiGate Security Profiles Project

1. Introduction

This report presents the full implementation, configuration, monitoring, and evaluation of FortiGate Security Profiles completed over four weeks. The goal of the project was to gain a comprehensive understanding of core FortiGate security capabilities—including Antivirus, Web Filtering, and Application Control—and to deploy them in a virtual lab environment to simulate real-world network protection.

FortiGate Security Profiles serve as the primary line of defense within Fortinet's security ecosystem. They deliver deep inspection of traffic, actively block malicious activity, and enforce network usage policies. Throughout the project, hands-on testing was performed to examine how each profile responds to threats, unwanted applications, and inappropriate web content. Monitoring tools such as FortiView, event logs, and traffic dashboards were used to verify the effectiveness of the deployed controls.

This report consolidates the work done across Weeks 1, 2, and 3, followed by the final evaluation and recommendations in Week 4. The result is a full security implementation cycle—from research and deployment to monitoring, documentation, and optimization.

---

2. Week 1 – Understanding FortiGate Security Profiles

The objective of Week 1 was to research and understand the role of various FortiGate Security Profiles. These profiles provide layered protection and are essential for modern network security.

2.1 Overview of Security Profiles

Security Profiles are applied to firewall policies to inspect traffic at Layer 7 (application layer). Their purpose is to prevent malware infections, block malicious or inappropriate content, and regulate the use of applications inside the network. The profiles studied include:

- **Antivirus** – Scans files and traffic to detect malware, viruses, worms, and suspicious files using signature-based and heuristic detection.

- **Web Filtering** – Controls access to websites using categories, URL filters, content filters, and reputation analysis.
- **Application Control** – Detects and controls applications based on deep packet inspection (DPI), even when traffic uses non-standard ports.
- **IPS (Intrusion Prevention System)** – Detects and blocks network exploits and intrusions.
- **DNS Filtering** – Blocks malicious domains before a connection is established.
- **Email Filtering** – Filters spam, phishing, and malicious email attachments.
- **SSL/SSH Inspection** – Decrypts encrypted traffic for deep inspection.
- **Sandbox Integration** – Sends suspicious files to a virtual sandbox for analysis.

2.2 Key Takeaways

Through the research conducted in Week 1, the following insights were obtained:

- Modern threats frequently use encryption; therefore, SSL Deep Inspection is crucial.
- Application Control can identify apps even when users attempt to bypass controls through proxies or encrypted channels.
- Web Filtering is effective in enforcing acceptable-use policies such as blocking social media or gambling websites.
- Antivirus provides essential protection but is more effective when combined with sandboxing and IPS.
- Security Profiles benefit from working together—no single profile provides complete protection.

This understanding laid the foundation for the practical configurations in Week 2.

---

3. Week 2 – Configuration and Implementation of Security Profiles

The focus of Week 2 was to configure three primary security profiles—Antivirus, Web Filtering, and Application Control—and apply them to the main LAN-to-WAN firewall policy.

3.1 Lab Environment

A virtual environment was created using VMware Workstation:

- **FortiGate Firewall** installed as the virtual security appliance.
- **Kali Linux** used as the test device for browsing and application testing.
- The Kali VM was connected to the same LAN segment as the FortiGate internal interface.

All traffic from Kali passed through FortiGate for inspection.

3.2 Web Filtering Configuration

The Web Filter profile was configured to block several high-risk and non-productive categories:

- Gambling
- Dating
- Social Media
- Malicious Websites
- Proxy Avoidance (set to *Warning*)

Testing Results:

- Before applying the Web Filter, Kali Linux could access all websites freely, including gambling and dating sites.
- After applying the profile, attempts to access restricted categories resulted in a **FortiGate block page**, confirming successful enforcement.
- Proxy avoidance websites triggered security warnings as configured.

3.3 Application Control Configuration

A custom Application Control profile was created with the specific goal of blocking:

- **ABC.com** (categorized under Video/Audio)

Testing Results:

- Before applying the profile, ABC.com was accessible.
- After deployment, the connection was blocked, and the session was logged in the Application Control logs.
- SSL Deep Inspection enabled the firewall to decrypt HTTPS and accurately identify the application.

3.4 Antivirus Configuration

Antivirus settings included:

- Real-time malware inspection
- Flow-based scanning for performance
- Logging all malware-related events
- Inspection of HTTP/HTTPS downloads

Though no real malware files were tested, logs confirmed that Antivirus inspection was active.

3.5 Firewall Policy Integration

All profiles were attached to a single LAN → WAN firewall policy:

- Web Filter
- Application Control
- Antivirus
- SSL Deep Inspection

This integration ensured that every outbound connection was scanned according to the configured policies.

---

4. Week 3 – Monitoring and Reporting

The purpose of Week 3 was to validate the effectiveness of the implemented security profiles using FortiGate’s monitoring and reporting tools.

4.1 Logging Configuration

Logging was enabled for:

- UTM events
- Forward traffic
- Denied traffic
- Application events
- Web Filter events

This ensured complete visibility.

4.2 Web Filter Monitoring Results

Logs from the *Web Filter* section confirmed:

- Multiple blocked attempts to gambling and dating sites
- “UTM Blocked” actions displayed
- Domain categories correctly identified
- FortiView dashboards showed repeated attempts categorized by site and user

4.3 Application Control Monitoring

The Application Control logs showed:

- Multiple blocked sessions related to **ABC.com**
- Traffic classified under “Video/Audio”
- DPI successfully detected the target application
- FortiView displayed bandwidth usage attempted by blocked apps

4.4 Antivirus Monitoring

The Antivirus monitoring panel confirmed:

- All HTTP/HTTPS traffic was being inspected
- No malware detected during testing, but logging was functional
- Profile effectiveness validated through scanning statistics

4.5 Observations

The monitoring phase confirmed:

- Policies and profiles were functioning correctly
- All events were logged with precise timestamps
- Blocked content matched the security policy rules
- SSL Deep Inspection played a crucial role in detecting encrypted apps
- FortiView provided clear visualization of threats and usage attempts

---

5. Week 4 – Final Evaluation, Summary, and Recommendations

Week 4 consisted of preparing the final report, presentation, and addressing the overall effectiveness of the deployed security solution.

5.1 Project Achievements

The following goals were successfully accomplished:

- Researched and understood FortiGate Security Profiles
- Configured Web Filtering, Application Control, and Antivirus
- Applied profiles to the LAN-to-WAN policy
- Tested each profile before and after configuration
- Collected and analyzed real monitoring data
- Prepared technical documentation and visualization

5.2 Security Improvements

The network now benefits from:

- **Meaningful content control** through Web Filter
- **Application-level enforcement** via Application Control
- **Threat prevention** through Antivirus scanning
- **Visibility into encrypted traffic** through SSL Deep Inspection
- **Comprehensive logging and reporting**

5.3 Challenges Encountered

Some challenges and their solutions:

Challenge	**Solution**
SSL Inspection caused browser warnings	Install FortiGate CA on client machine
Some apps used encrypted bypass methods	Deep Inspection allowed correct identification
Category misclassification during tests	Used Web Rating Overrides feature

5.4 Recommendations for Future Enhancements

To increase security and visibility, the following recommendations are proposed:

- **Integrate FortiAnalyzer** for advanced analytics and automated reporting.
- **Enable FortiSandbox** for zero-day threat detection.
- Deploy **DNS filtering** to block malicious domains at the DNS layer.
- Expand Application Control rules to include more risky or bandwidth-heavy apps.
- Configure **advanced IPS protections**, especially virtual patching.

---

6. Conclusion

This project demonstrated the complete life cycle of deploying FortiGate Security Profiles—from initial research to hands-on implementation, testing, monitoring, and reporting. The configured profiles successfully blocked unauthorized websites, regulated application usage, and inspected traffic for potential threats.

The monitoring logs confirmed that security events were accurately detected and recorded, and the firewall enforced the configured rules precisely as intended. Through this deployment, the network's security posture significantly improved in terms of threat protection, traffic visibility, and user control.

Overall, the project showcased the importance of layered security and the powerful capabilities of FortiGate's integrated security architecture. By combining Security Profiles with consistent monitoring and analysis, the environment is now better prepared to detect, block, and respond to modern cybersecurity threats.