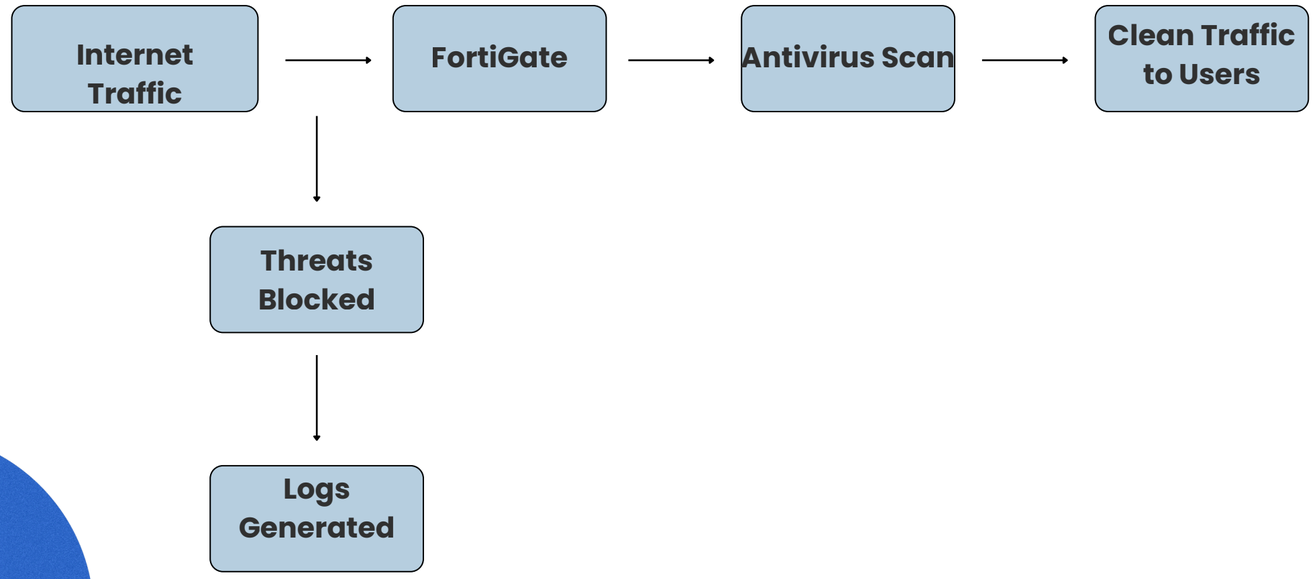
# FortiGate Security Profiles

**Project 4: Advanced FortiGate Security Profiles**

by: Nada nasr
eman moamen
Seif Wael
Ahmed Osama
shahd osama

# Week 1: Understanding Antivirus

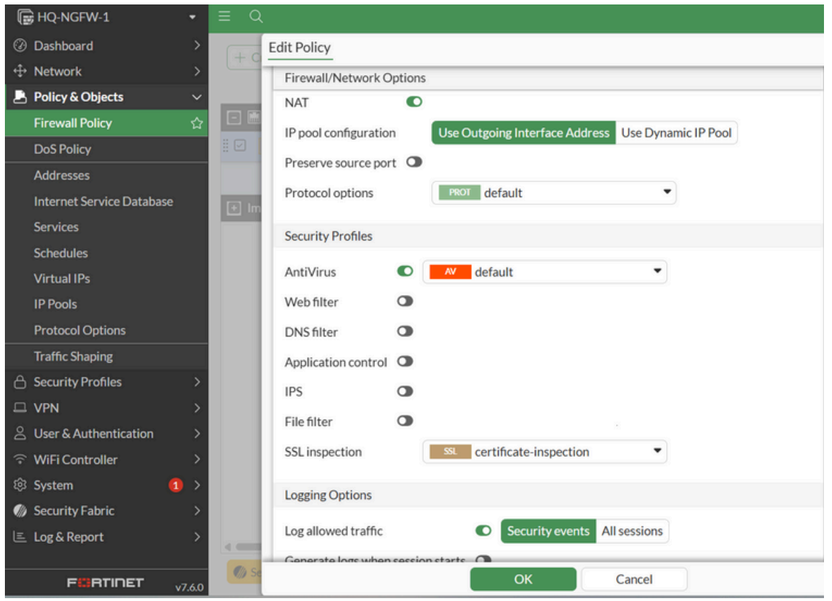
We successfully implemented FortiGate's Antivirus protection using flow-based inspection across all major protocols. The profile was integrated into our main Internet firewall policy, providing real-time scanning for all outbound traffic with automatic blocking and quarantine capabilities.

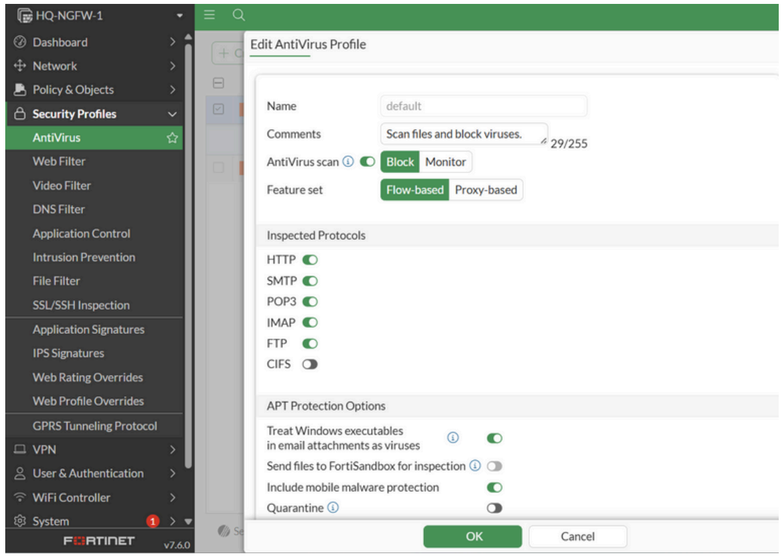



# Week 2: Configuration

Steps Taken:

- Feature verification
- profile creation
- actions / Protocols
- firewall policy

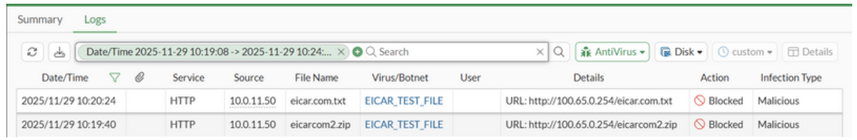



# Week 3: Monitoring

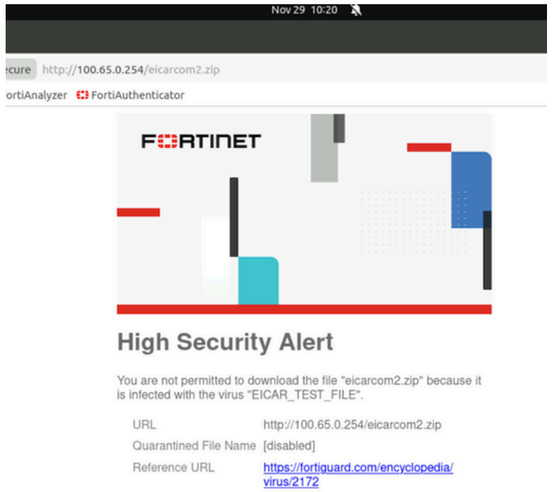
## Threat DETECTION

- EICAR test files identified
- Multiple formats detected:
  - .txt files
  - .zip archives
- Instant threat recognition



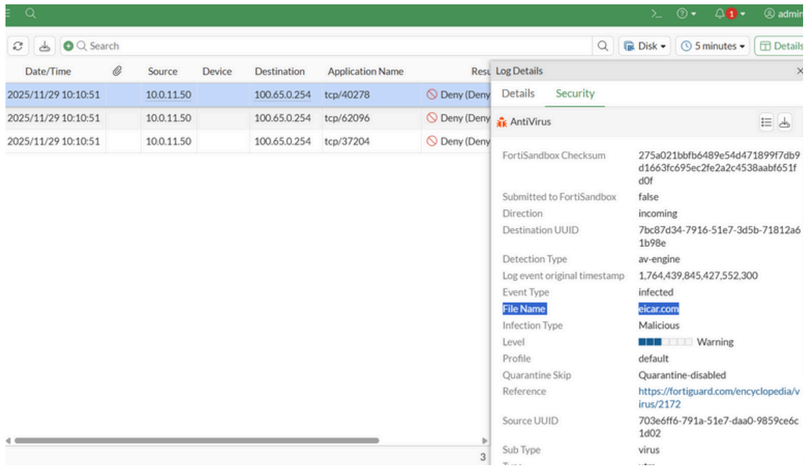

## User Protection

- Clear user block pages
- Educational messaging
- Connection termination
- Zero infections



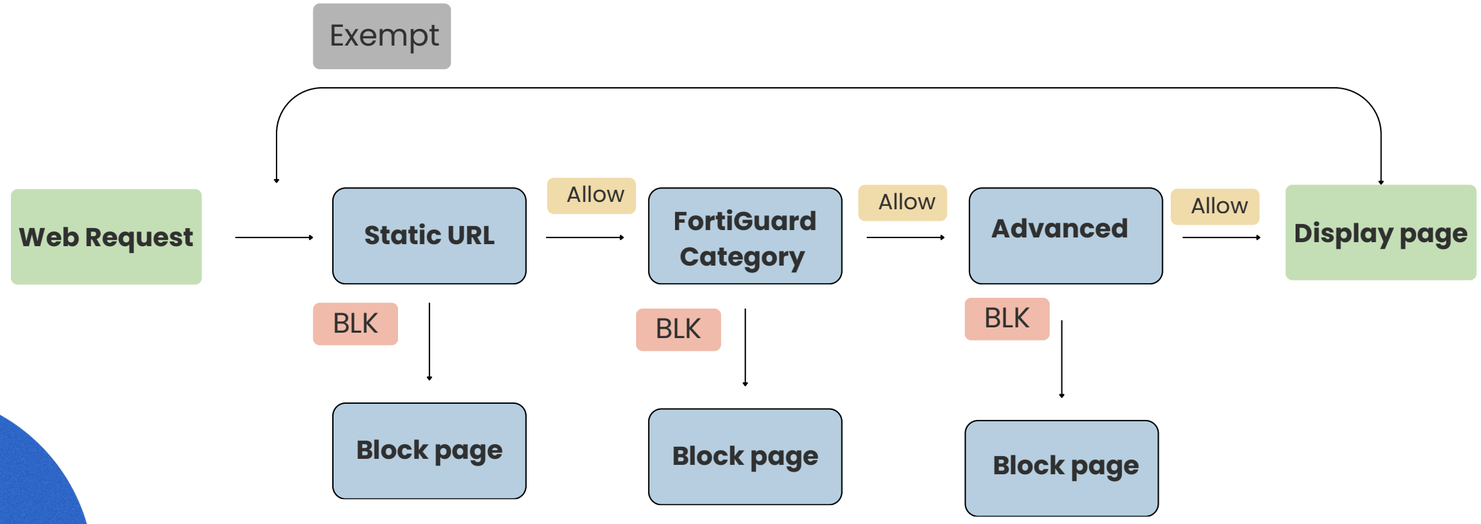

## COMPLETE LOGGING

- All events documented
- Policy enforcement recorded
- Session details captured
- Compliance ready



# Week 1: Understanding Webfilter

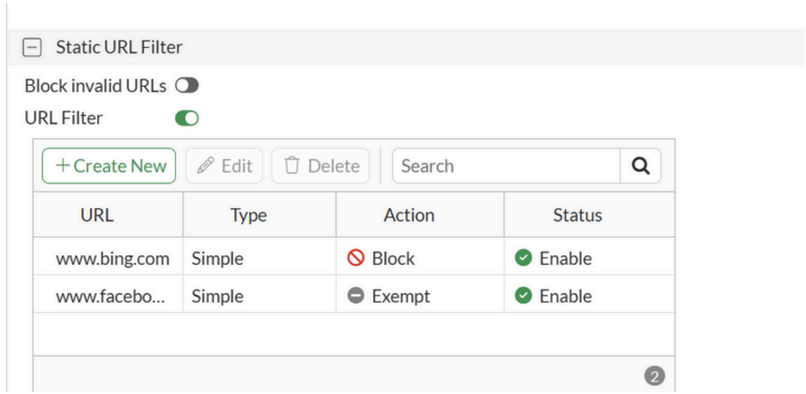
We implemented a multi-layered web filtering solution using FortiGuard categories, static URL rules, and quota management. The system provides granular control over internet access while maintaining user productivity through features like rating overrides and error handling

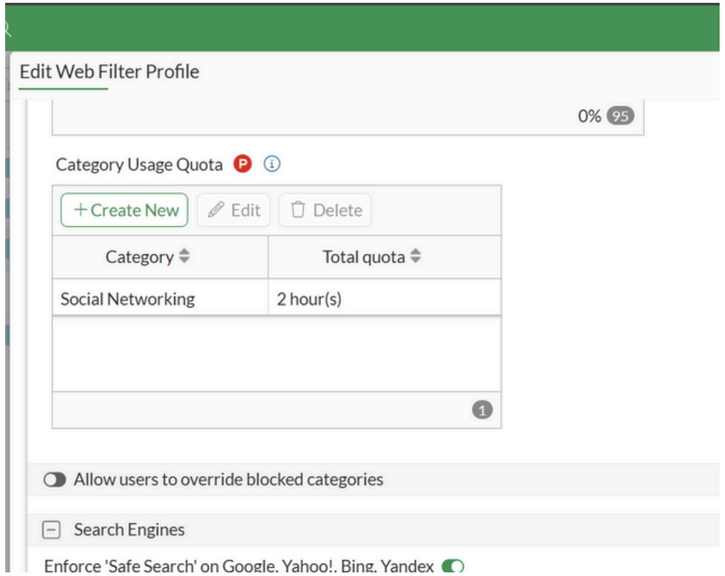


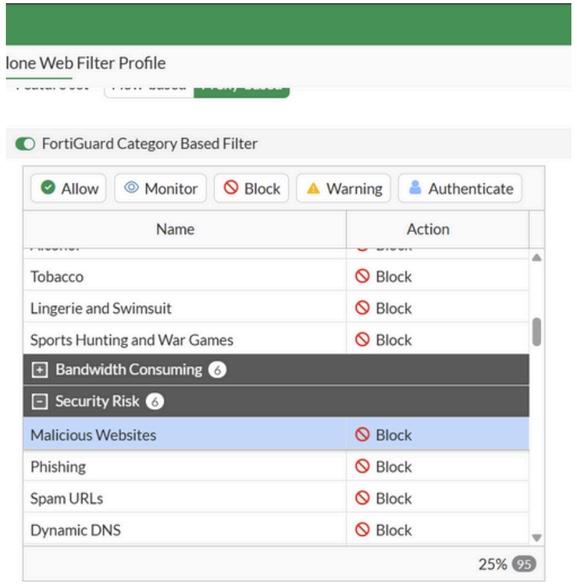

# Week 2: Configuration

Steps Taken:

- Feature verification
- profile creation
- categories/actions
- firewall policy



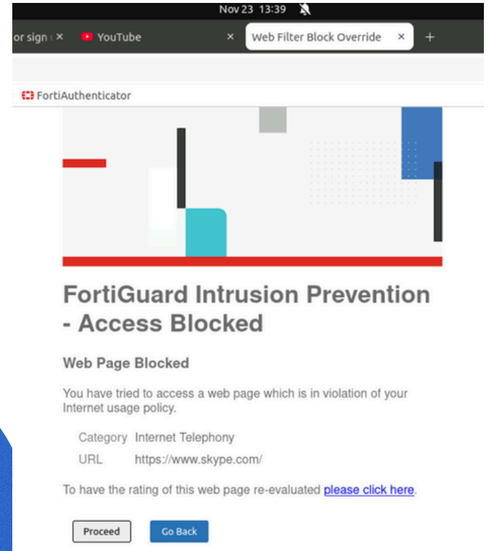




# Week 3: Monitoring

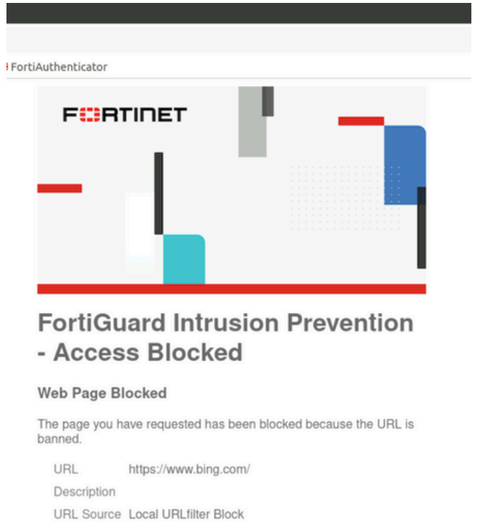
## CATEGORY ENFORCEMENT

- Social Networking: Blocked
- Internet Telephony: Warned
- Malicious Websites: Blocked
  - Clear policy messaging



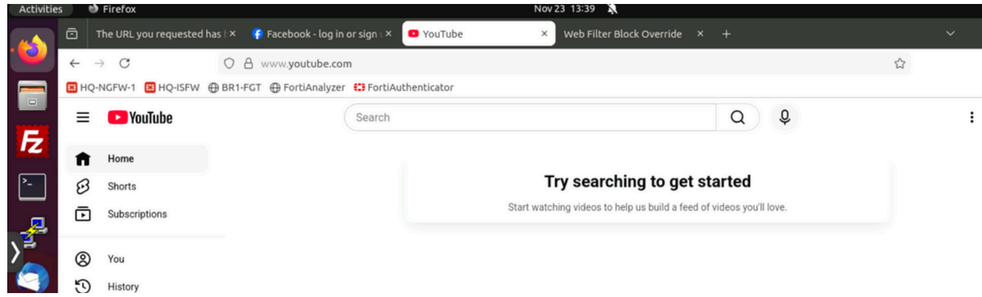

## Static URL Control

- Bing.com: Double-blocked
  - Malicious category
  - Static URL filter
- Facebook.com: Exempted




## Balanced Access

- YouTube: Accessible
- Search Engines: Allowed
- Job Sites: Permitted
- Legitimate work enabled



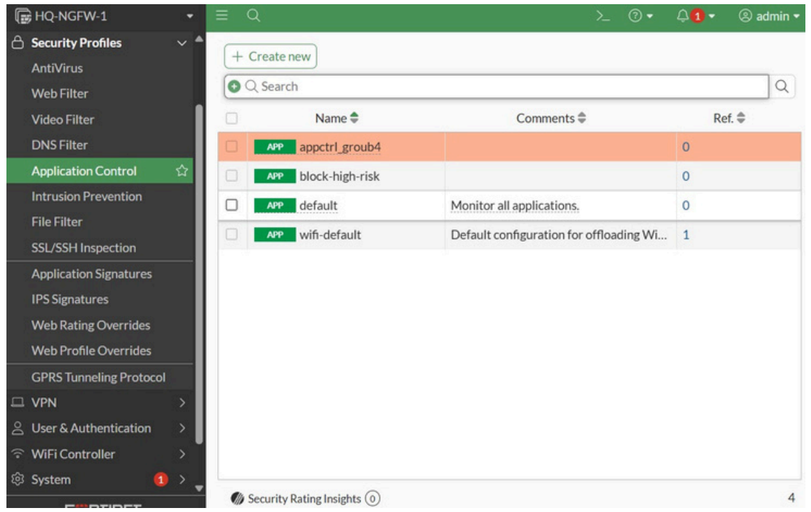
رواد مصر الرقمية

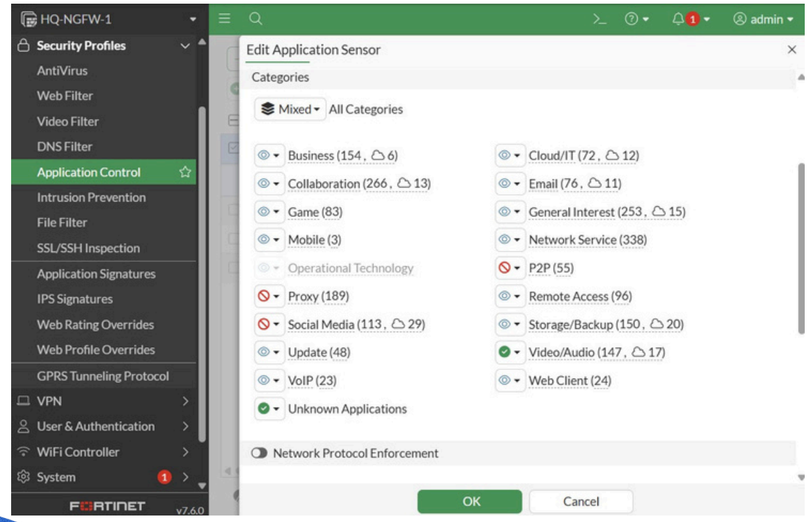
FORTINET

# Week 1 : Understanding Application Controll

- Definition
- Purpose
- How it works
- Use Cases

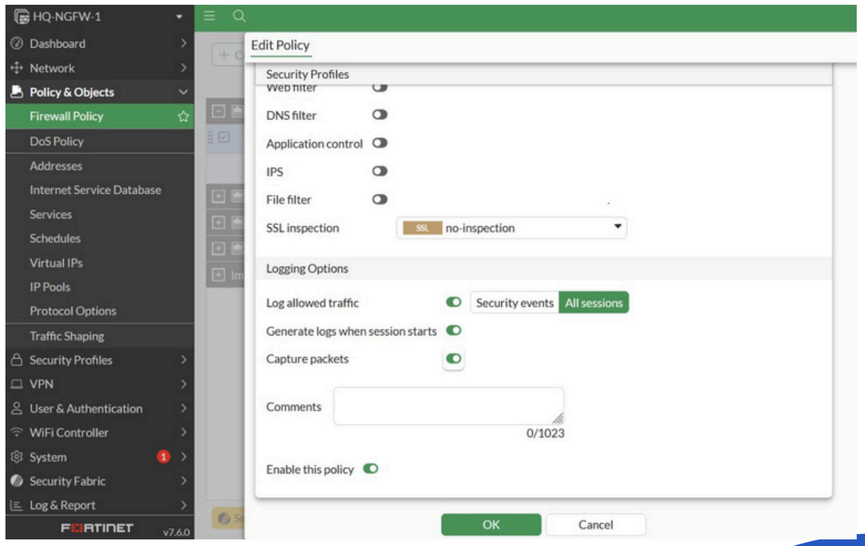
# Week 2 : Configuration



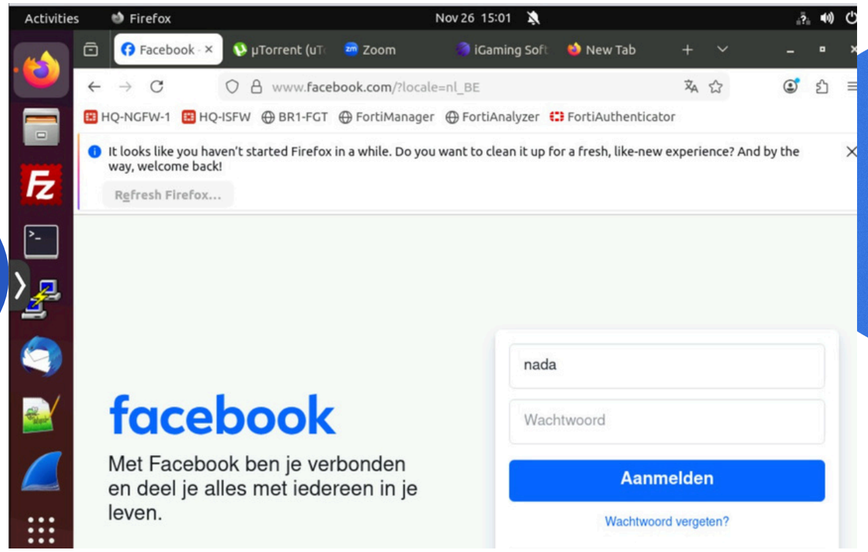

Steps Taken:

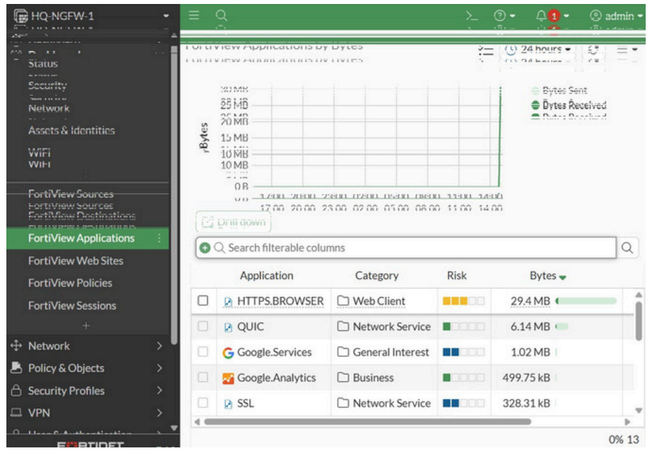
- Feature verification
- profile creation
- categories/actions
- firewall policy

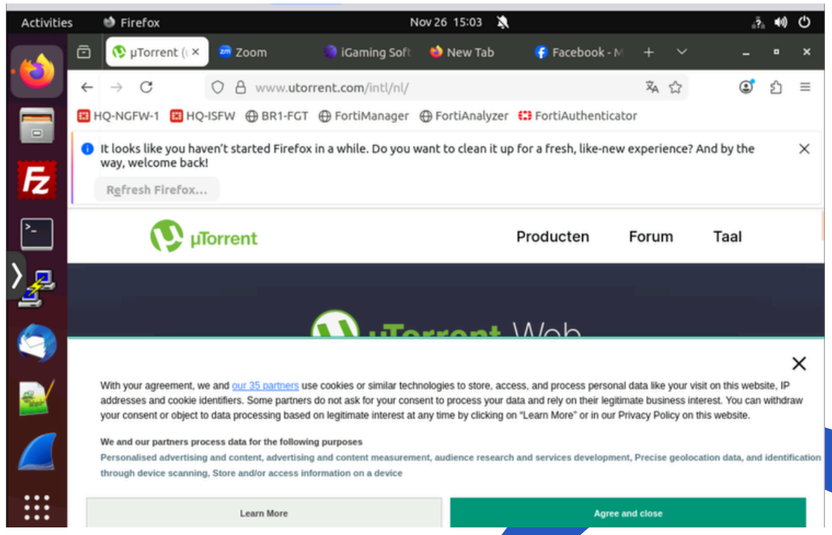


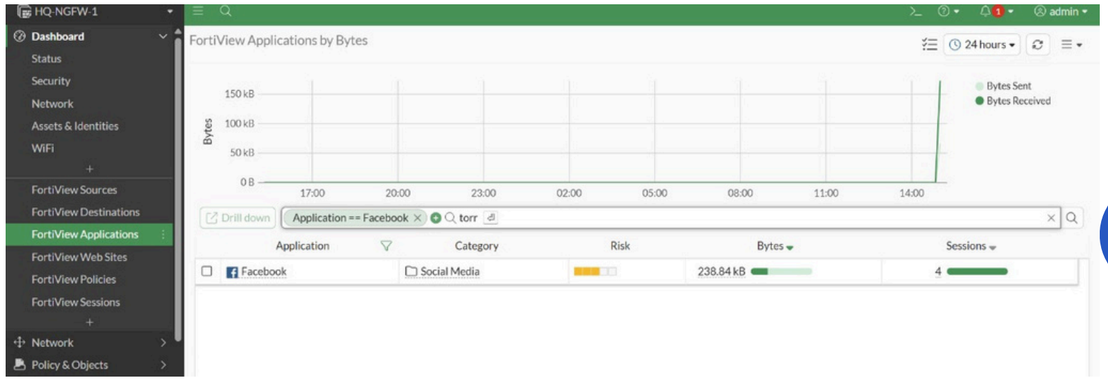
# Week 3 : Testing & Monitoring

- Test Traffic
- Results
- Analysis



# Application Control Summary & Transition

Key Takeaways from Application Control

- Application Control was successfully configured and applied on FortiGate.
- Traffic logging and monitoring were enabled using FortiView.
- Policy enforcement depends heavily on Firewall Policy Priority.
- Full visibility of application traffic was achieved.

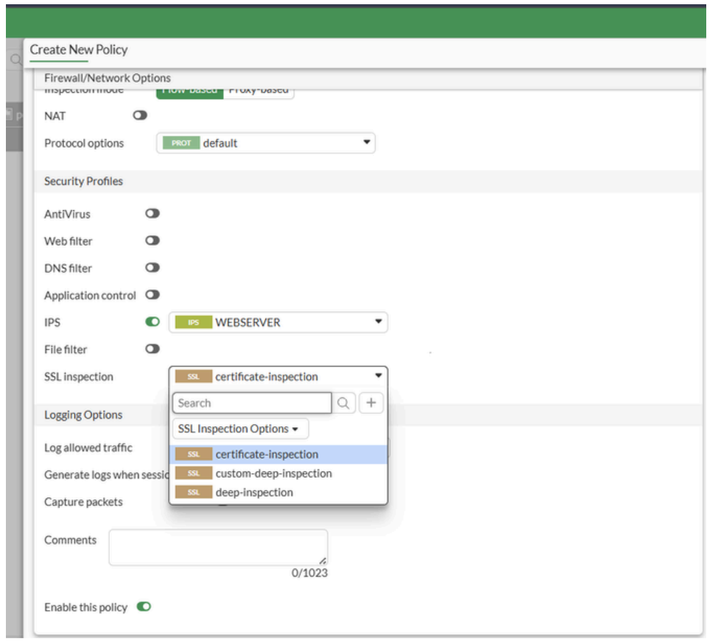
رواد مصر الرقمية

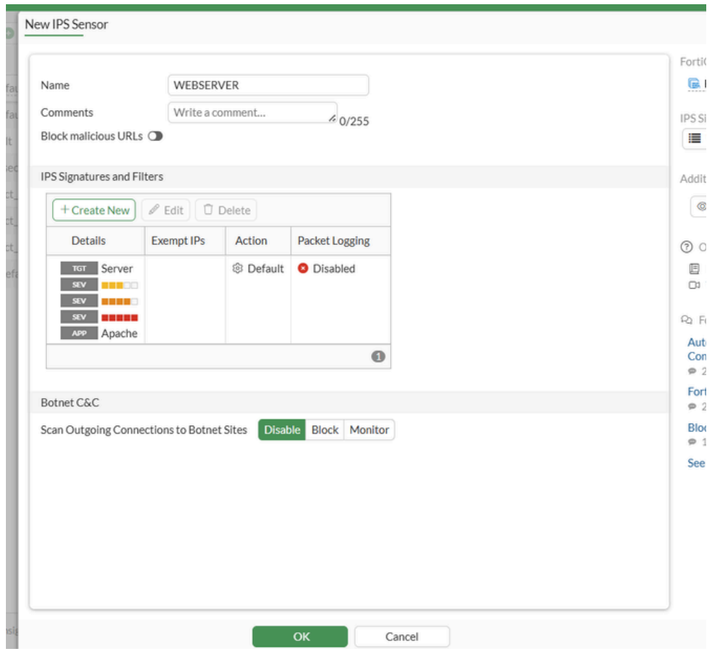
FORTINET

# Week 1 : Understanding IPS

- Definition
- Purpose
- How it works
- Use Cases

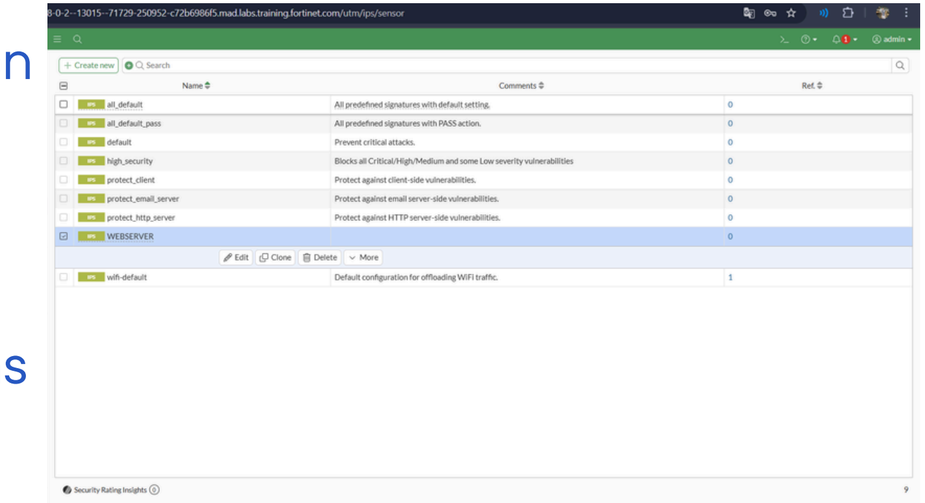
# Week 2 : Configuration



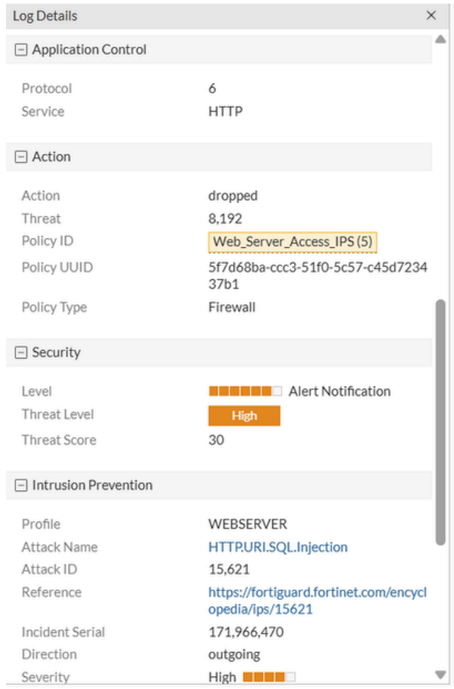

Steps Taken:

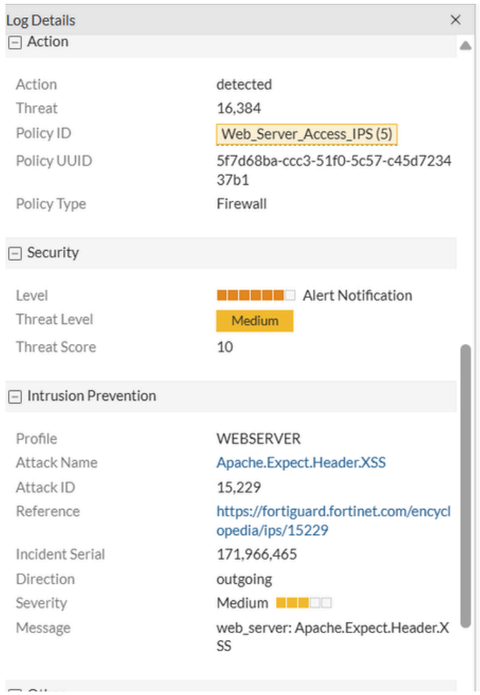
- Feature verification
- profile creation
- categories/actions
- firewall policy

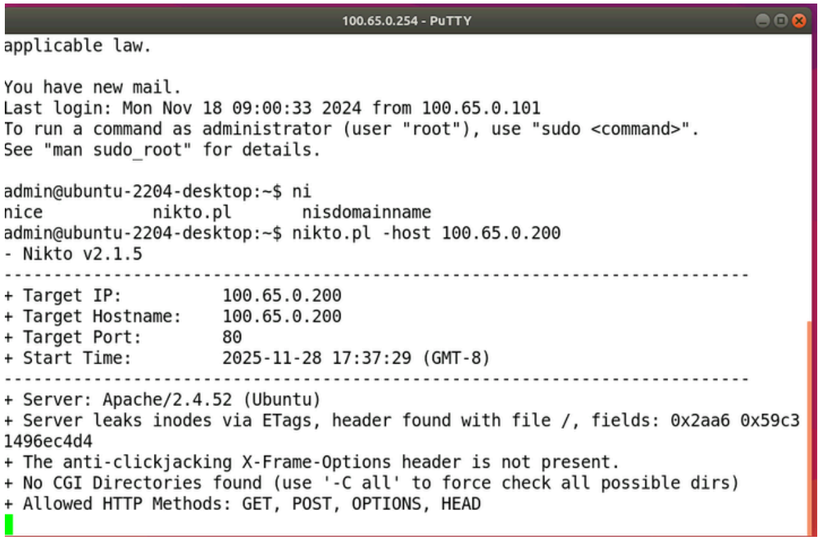


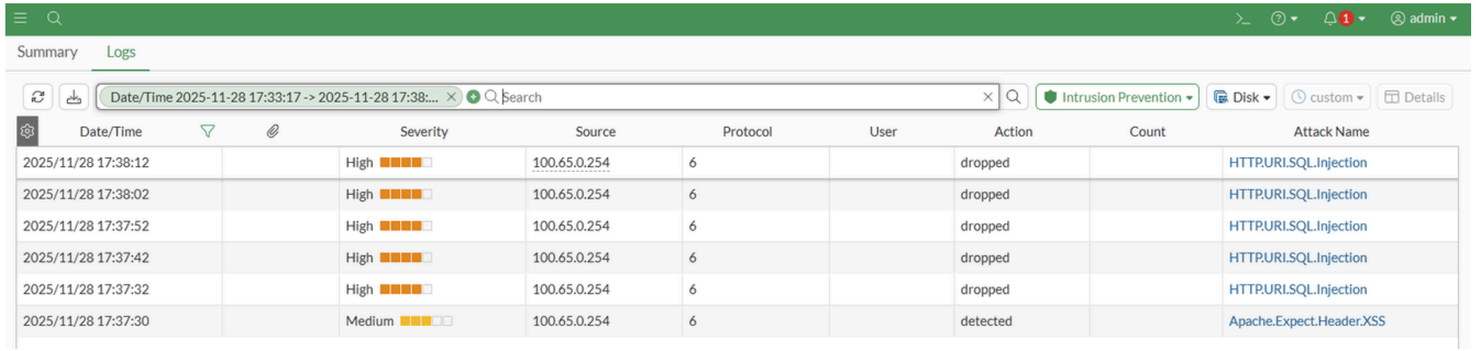
# Week 3 : Testing & Monitoring

- Simulated Attack
- Results
- Analysis



# IPS Summary & Transition

**Key Takeaways from IPS**

- IPS was successfully configured and applied on FortiGate.
- Threat detection and prevention were verified through FortiView.
- IPS actions (Block, Reset, Monitor) were tested.
- Clear visibility of attacks and signatures was achieved.

# Conclusion

Throughout our project, we've demonstrated that FortiGate Security Profiles are much more than just individual features - they form a cohesive security framework that provides comprehensive protection.

Security Profiles are not just features - they're the foundation of modern network security, providing the intelligent, adaptive protection essential in today's threat landscape.