Security Platform Comparison
Custom ML-Driven WAF/IDS Architecture vs Fortinet Rugged 70F

AstroPema AI LLC

2026

Purpose

This document compares two approaches to network security monitoring and protection:

- Custom ML-driven WAF/IDS platform built on Linux infrastructure
- Fortinet FortiGate Rugged 70F industrial firewall appliance

The comparison evaluates:

- architecture
- operational capabilities
- transparency
- cost structure
- advantages and limitations

1 Architecture Overview

1.1 Custom Security Platform

Typical architecture:

```
Internet
  ↓
NGINX Reverse Proxy
  ↓
Detection Engine (Rust)
  ↓
Apache Application Layer
  ↓
Event Pipeline
  ↓
PostgreSQL Telemetry Database
  ↓
SOC Analytics / ML Detection
```

Core components include:

- NGINX reverse proxy
- Apache backend services
- Rust-based detection engine
- Machine learning detection models (CNN-GRU)
- PostgreSQL event storage
- Structured logging pipelines
- SOC analysis notebooks
- MITRE ATT&CK mapping
- Automated audit report generation

The design philosophy emphasizes transparent, data-driven security analysis.

1.2 FortiGate Rugged 70F

Typical architecture:

```
Internet
  ↓
FortiGate Appliance
  ↓
Protected Network
```

Core components include:

- FortiOS operating system
- proprietary DPI inspection engines
- firewall policy engine
- IPS signatures
- antivirus scanning
- application control

Additional components commonly required:

- FortiAnalyzer (logging and analytics)
- FortiManager (centralized management)
- FortiGuard subscription (threat intelligence)

The design philosophy prioritizes turnkey deployment and vendor-managed security.

2 Functional Capabilities

Capability	Custom Platform	Rugged 70F
Firewall filtering	Yes	Yes
Web application firewall	Yes	Limited
Intrusion detection	Yes	Yes
ML anomaly detection	Yes	No
Detection engineering	Full control	Vendor controlled
Event telemetry database	Yes	External system required
MITRE ATT&CK mapping	Yes	No
SOC reporting	Native	Requires FortiAnalyzer
Research experimentation	Yes	No
Custom rule development	Yes	Limited

3 Transparency

3.1 Custom Platform

Advantages:

- full access to logs
- full control over detection logic
- full control over ML models
- transparent analytics
- reproducible security analysis

Disadvantages:

- requires engineering expertise
- requires system maintenance

3.2 Rugged 70F

Advantages:

- vendor maintained
- standardized deployment
- simplified management

Disadvantages:

- closed detection logic
- limited telemetry access
- limited customization
- reliance on vendor updates

4 Cost Comparison

4.1 FortiGate Rugged 70F

Typical costs:

- Hardware appliance: \$3,000 – \$5,000
- FortiGuard subscriptions: \$1,000 – \$2,000 per year
- Additional systems: FortiAnalyzer, FortiManager

Estimated five-year operational cost:

$$\$10,000 - \$15,000+$$

Additional infrastructure often required:

- VPN tunnels
- centralized management infrastructure
- proprietary analytics platforms

4.2 Custom Security Platform

Typical infrastructure:

- commodity Linux server
- open-source software stack

Example hardware:

- modern CPU server
- 64 GB RAM
- NVMe storage

Estimated hardware cost:

$$\$2,000 - \$4,000$$

Operational costs:

- no licensing fees
- no vendor subscriptions
- open-source software ecosystem

Additional advantages:

- no tunnel licensing
- no proprietary analytics platforms
- no vendor lock-in

5 Security Telemetry Capability

5.1 Custom Platform

Produces structured security datasets including:

- behavioral detection events
- machine learning scoring metrics
- network activity telemetry
- forensic datasets

This enables:

- SOC investigations
- research and experimentation
- forensic analysis
- compliance documentation

5.2 Rugged 70F

Telemetry model relies primarily on vendor logging systems.

Deep analysis often requires:

- FortiAnalyzer
- external SIEM platforms

6 Operational Model

6.1 Custom Platform

Best suited for:

- research environments
- security engineering teams
- detection engineering
- ML security experimentation
- forensic analysis

6.2 Rugged 70F

Best suited for:

- industrial networks
- turnkey deployments
- standardized enterprise environments

7 Advantages and Disadvantages

7.1 Custom Platform

Advantages:

- full transparency
- ML detection capability
- customizable detection logic
- integrated analytics
- lower long-term cost
- no vendor lock-in

Disadvantages:

- requires engineering expertise
- requires operational maintenance
- lacks vendor certification

7.2 Rugged 70F

Advantages:

- turnkey deployment
- vendor support
- enterprise certifications
- deterministic packet inspection

Disadvantages:

- closed architecture
- higher long-term cost
- limited detection flexibility
- dependence on proprietary ecosystem

8 Conclusion

Both approaches provide network protection but follow different architectural philosophies.

The FortiGate Rugged 70F represents a closed, vendor-managed appliance optimized for ease of deployment.

The custom ML-driven platform represents a transparent, extensible architecture enabling advanced detection engineering, telemetry analysis, and research-driven security capabilities at a lower long-term cost.