Operational Observation of a WAF / IDS Detection and Enforcement Pipeline

AstroPema AI LLC

March 6, 2026

Abstract

This document presents a brief operational observation of a production web security pipeline consisting of a reverse proxy, web server, detection layer, and automated enforcement mechanism. The system processes incoming web traffic, classifies requests using deterministic rules, and applies blocking decisions through a Rust-based `ipset` enforcement component integrated with the Linux firewall.

The figure shown below captures two synchronized terminal monitoring windows operating simultaneously. One window displays detection and classification events derived from analyzed HTTP requests, while the other shows enforcement actions applied by the automated blocking mechanism. Together they illustrate the relationship between traffic analysis and active defensive response within the system.

The observations indicate that reconnaissance attempts targeting common web application paths are detected and blocked while legitimate traffic continues to pass without interruption. The absence of false positives or unintended enforcement actions suggests that the defensive pipeline is operating as intended.

1 System Architecture Context

The defensive pipeline follows a layered structure designed to maintain visibility into incoming traffic while enabling automated response:

```
Internet
   ↓
NGINX Reverse Proxy
   ↓
Apache Web Server
   ↓
Detection Engine
   ↓
Traffic Classification
   ↓
Rust ipset Enforcement
   ↓
iptables Firewall
```

This architecture allows the detection system to analyze web requests before the enforcement component applies deterministic blocking rules.

2 Observed Monitoring Output

Figure 1 shows the operational monitoring output captured from the production environment. The screenshot contains two terminal panes running simultaneously.

The left pane displays activity generated by the Rust-based enforcement component responsible for inserting malicious sources into the `ipset` block list. Entries such as:

```
BLOCKED <IP> into bad_ips
BACKFILL_BLOCKED <IP> into bad_ips
```

indicate that IP addresses previously identified as suspicious have been added to the firewall blocking set. The presence of `BACKFILL_BLOCKED` entries indicates that the enforcement system can replay prior detections and apply retroactive blocking when required.

The right pane shows the detection and classification output derived from analyzed HTTP requests. Requests are categorized using several classifications including:

- **CLEAN_PREML** – traffic determined to be benign
- **ALLOW** – requests explicitly permitted by whitelist logic
- **SUSPICIOUS** – requests matching deterministic attack patterns

Many suspicious entries correspond to automated probes targeting well-known WordPress administrative paths such as:

```
/wp-admin/setup-config.php
/wp-admin/install.php
/wp-login.php
```

These requests are characteristic of automated scanning behavior commonly observed across internet-facing infrastructure.

3 Operational Observations

The monitoring output demonstrates a healthy defensive posture. Suspicious requests are detected through deterministic rules and immediately trigger enforcement actions through the automated blocking system. Legitimate requests such as root page access, favicon retrieval, and other standard web traffic remain unaffected.

The system also demonstrates protective safeguards including the explicit exclusion of private address ranges from enforcement actions, ensuring that internal infrastructure and monitoring systems are not inadvertently blocked.

Equally important is the absence of anomalous behavior. No evidence of false positive blocking, enforcement loops, or instability within the detection pipeline was observed during the monitoring period.

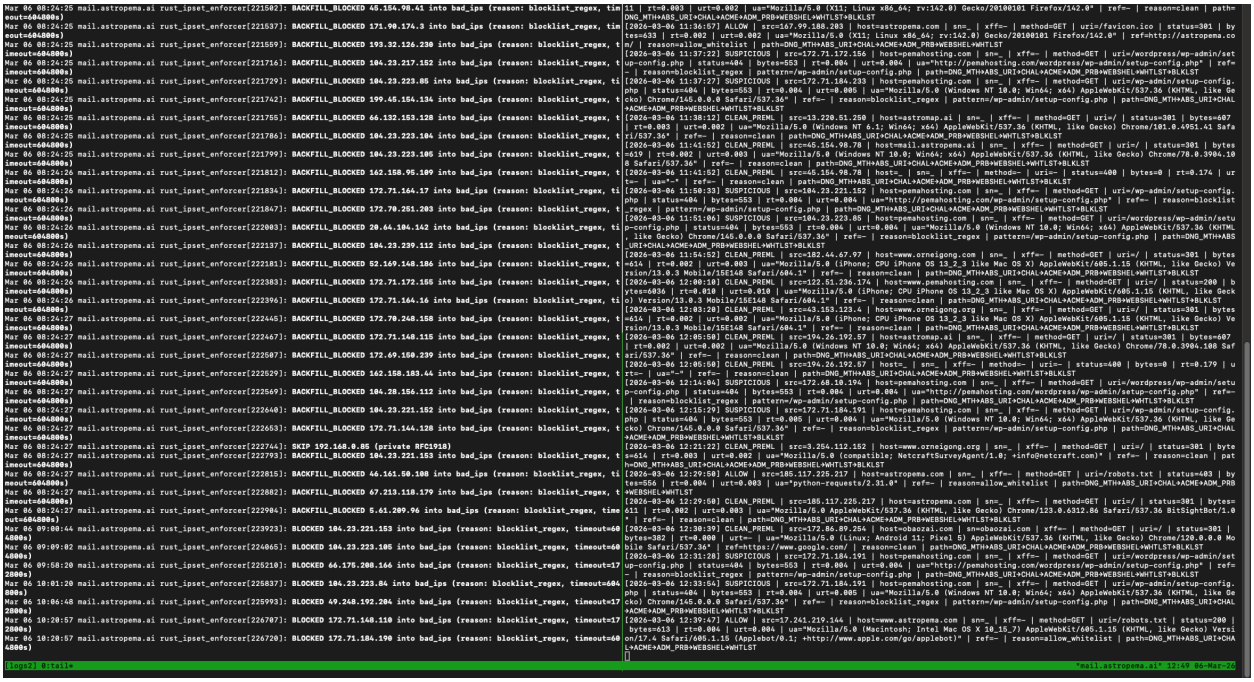

Figure 1: Simultaneous monitoring of detection and enforcement components within the WAF / IDS pipeline. The right pane shows request classification events, while the left pane displays automated firewall enforcement actions.

4 Conclusion

The screenshot presented in this document illustrates the normal operational state of a layered web application firewall and intrusion detection system. Automated reconnaissance activity is detected and mitigated while legitimate traffic continues to pass without disruption.

Telemetry produced by this system provides valuable data for further analysis and future enrichment using standardized threat intelligence frameworks such as MITRE ATT&CK. Such integration will allow detected events to be mapped to adversarial techniques and incorporated into broader security analytics workflows.