EN

CrowdSec and fail2ban with OPNsense

Collaborative IDS/IPS and SSH Protection

OPNSENSE ENTERPRISE STACK — POST 5

Mars 2026

Table of Contents

1. Why CrowdSec + fail2ban?

The OPNsense firewall blocks attacks at the perimeter. But servers behind it — open SSH, Nginx as reverse proxy — remain permanent targets. The combination:

- **CrowdSec**: collaborative IDS/IPS. Analyzes logs, detects malicious behavior, blocks IPs at OPNsense firewall level via the bouncer.
- **fail2ban**: local protection via log analysis. Bans IPs that fail too many times (SSH, Nginx...) via iptables/nftables.
- **Integration**: fail2ban reports IPs to CrowdSec, which propagates them to the OPNsense bouncer and the global community.

2. Prerequisites

- OPNsense operational — see Post 1: blog.botum.ca/installer-opnsense-proxmox/
- OPNsense exposed to internet (WAN with public IP or DDNS)
- Linux servers behind OPNsense (Ubuntu/Debian) with SSH enabled
- SSH admin access to backend servers
- Free account at app.crowdsec.net

3. Install CrowdSec Plugin on OPNsense

OPNsense offers the official os-crowdsec plugin via its plugin manager:

```
# OPNsense GUI:
# System -> Firmware -> Plugins
# Search: crowdsec
# Find: os-crowdsec
# Click "+" to install
# After installation: reload page
# New menu: Services -> CrowdSec

# Verification via SSH OPNsense (System -> Shell):
cscli version
# CrowdSec version: v1.x.x
cscli machines list
```

Services -> CrowdSec -> Overview: verify that daemon and bouncer are Running.

4. Configure the Firewall Bouncer

The bouncer translates CrowdSec decisions into OPNsense firewall rules (pf mode):

```
# Services -> CrowdSec -> Bouncers
# "crowdsec-firewall-bouncer" Status: Running

# Bouncer config file:
# /usr/local/etc/crowdsec/bouncers/crowdsec-firewall-bouncer.yaml
api_url: http://127.0.0.1:8080/
api_key: <automatically generated>
mode: pf
blacklists_ipv4: crowdsec_blacklists
blacklists_ipv6: crowdsec6_blacklists

# Check active decisions:
cscli bouncers list
cscli decisions list
# IP              Reason               Duration  Source
# 185.220.x.x    crowdsecurity/ssh-bf  4h        CrowdSec CTI
```

5. Enroll in the CrowdSec Console

The app.crowdsec.net console centralizes alerts and provides access to premium blocklists:

```
# 1. Create an account at app.crowdsec.net (free)
# 2. Security Engines -> Add -> Copy the enrollment command

# On OPNsense (SSH / System -> Shell):
cscli console enroll <your-enroll-key>
# Output: Machine enrolled successfully

# 3. In console: Security Engines -> Pending -> Accept

# 4. Verify:
cscli console status
# Enrollment: OK
```

6. Install fail2ban on Backend Servers

```
# Ubuntu/Debian:
sudo apt update && sudo apt install fail2ban -y

sudo systemctl status fail2ban
# Active: active (running)

# Do NOT modify jail.conf directly:
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

7. Create Custom Jails (SSH + Nginx)

SSH Jail

```
# /etc/fail2ban/jail.local

[DEFAULT]
bantime  = 3600     # 1 hour ban
findtime = 600      # 10-minute window
maxretry = 5        # max 5 attempts
backend  = systemd

[sshd]
enabled  = true
port     = ssh
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 3        # SSH stricter
bantime  = 86400    # 24h ban
```

Nginx Jail

```
[nginx-http-auth]
enabled  = true
port     = http,https
filter   = nginx-http-auth
logpath  = /var/log/nginx/error.log
maxretry = 5

[nginx-botsearch]
enabled  = true
port     = http,https
filter   = nginx-botsearch
logpath  = /var/log/nginx/access.log
maxretry = 2
bantime  = 86400

# Reload fail2ban:
sudo systemctl reload fail2ban

# Check active jails:
sudo fail2ban-client status
sudo fail2ban-client status sshd
# Currently banned: 3 | Total banned: 47
```

8. fail2ban -> CrowdSec Integration

fail2ban reports malicious IPs to CrowdSec, which blocks them at the OPNsense level:

```
# Install CrowdSec on backend server:
curl -s https://packagecloud.io/install/repositories/crowdsec/crowdsec/script.deb.sh \
  | sudo bash
sudo apt install crowdsec -y

# Enroll this server:
sudo cscli console enroll <your-enroll-key>

# fail2ban -> CrowdSec action:
# /etc/fail2ban/action.d/crowdsec.conf
[Definition]
actionban   = cscli decisions add --ip <ip> --duration 4h \
              --reason "fail2ban-<name>"
actionunban = cscli decisions delete --ip <ip>

# Enable in jail.local:
[DEFAULT]
action = %(action_)s
         crowdsec
```

Protection flow:

- 1. Bot attempts SSH brute-force on backend server
- 2. fail2ban detects after 3 attempts, bans IP locally
- 3. fail2ban sends decision to CrowdSec via cscli
- 4. CrowdSec propagates to OPNsense bouncer
- 5. OPNsense blocks IP at firewall level for all services
- 6. IP contributed to global CrowdSec community

9. Monitoring

```
# On OPNsense (SSH):
cscli alerts list     # real-time alerts
cscli decisions list  # active decisions
cscli metrics         # agent metrics

# On backend server:
sudo tail -f /var/log/fail2ban.log
sudo fail2ban-client status sshd

# Unban an IP (false positive):
sudo fail2ban-client set sshd unbanip 192.168.10.50
```

CrowdSec console (app.crowdsec.net): world attack map, alert timeline, CTI, premium blocklists, Telegram/Slack/Email notifications.

10. Validation Tests

```
# 1. Verify CrowdSec on OPNsense:
cscli version && cscli machines list

# 2. Simulate SSH attack from external IP:
for i in {1..5}; do ssh invalid_user@<server-IP> 2>/dev/null; done
# -> fail2ban should ban the IP

# 3. Verify the ban:
sudo fail2ban-client status sshd

# 4. Verify propagation to OPNsense:
# SSH OPNsense -> cscli decisions list

# 5. Cleanup (unban):
sudo fail2ban-client set sshd unbanip <test-IP>
cscli decisions delete --ip <test-IP>
```

Next Steps

This post concludes the OPNsense Enterprise Stack series. Complete recap:

- **Post 1:** Install OPNsense in Proxmox — router/firewall base
- **Post 2:** VLANs & Zero Trust — network segmentation
- **Post 3:** WireGuard VPN & SD-WAN LTE — remote access + failover
- **Post 4:** WiFi & APs with UniFi/Omada — WiFi segmentation by VLAN
- **Post 5:** CrowdSec + fail2ban — collaborative IDS/IPS (this guide)

Full article: blog.botum.ca/opnsense-crowdsec-fail2ban-guide

Series hub: blog.botum.ca/opnsense-stack-securite-enterprise-proxmox

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