FR

CrowdSec et fail2ban

avec OPNsense

IDS/IPS collaboratif et protection SSH

SERIE STACK OPNSENSE — BILLET 5

Mars 2026

Sommaire

1. Pourquoi CrowdSec + fail2ban ?

Le firewall OPNsense bloque les attaques au perimetre. Mais les serveurs derriere — SSH ouvert, Nginx en reverse proxy — restent des cibles permanentes. La combinaison :

• **CrowdSec** : IDS/IPS collaboratif. Analyse logs, detecte comportements malveillants, bloque les IPs au niveau firewall OPNsense via le bouncer.

• **fail2ban** : protection locale par analyse de logs. Ban les IPs qui echouent trop souvent (SSH, Nginx...) via iptables/nftables.

• **Integration** : fail2ban signale les IPs a CrowdSec, qui les propage au bouncer OPNsense et a la communaute mondiale.

2. Prerequis

• OPNsense operationnel — voir Billet 1 : blog.botum.ca/installer-opnsense-proxmox/

• OPNsense expose sur internet (WAN avec IP publique ou DDNS)

• Serveurs Linux derriere OPNsense (Ubuntu/Debian) avec SSH active

• Acces SSH admin sur les serveurs backend

• Compte gratuit sur app.crowdsec.net

3. Installer le plugin CrowdSec sur OPNsense

OPNsense propose le plugin officiel os-crowdsec via son gestionnaire de plugins :

```
# OPNsense GUI :
# System -> Firmware -> Plugins
# Rechercher : crowdsec
# Trouver : os-crowdsec
# Cliquer le "+" pour installer
# Apres installation : recharger la page
# Nouveau menu : Services -> CrowdSec

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

Services -> CrowdSec -> Overview : verifier que le daemon et le bouncer sont Running.

4. Configurer le bouncer firewall

Le bouncer traduit les decisions CrowdSec en regles firewall OPNsense (mode pf) :

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

# Fichier de config bouncer :
# /usr/local/etc/crowdsec/bouncers/crowdsec-firewall-bouncer.yaml
api_url: http://127.0.0.1:8080/
api_key: <genere automatiquement>
mode: pf
blacklists_ipv4: crowdsec_blacklists
blacklists_ipv6: crowdsec6_blacklists

# Verifier les decisions actives :
cscli bouncers list
cscli decisions list
# IP              Raison               Duree   Source
# 185.220.x.x    crowdsecurity/ssh-bf  4h      CrowdSec CTI
```

5. Enroller dans la console CrowdSec

La console app.crowdsec.net centralise les alertes et donne acces aux blocklists premium :

```
# 1. Creer un compte sur app.crowdsec.net (gratuit)
# 2. Security Engines -> Add -> Copier la commande d'enrollment

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

# 3. Dans la console : Security Engines -> Pending -> Accept

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

6. Installer fail2ban sur les serveurs backend

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

sudo systemctl status fail2ban
# Active: active (running)

# Ne PAS modifier jail.conf directement :
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

7. Creer des jails custom (SSH + Nginx)

Jail SSH

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

[DEFAULT]
bantime  = 3600     # 1 heure de ban
findtime = 600      # fenetre de 10 minutes
maxretry = 5        # 5 tentatives max
backend  = systemd

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

Jail Nginx

```
[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

# Recharger fail2ban :
sudo systemctl reload fail2ban

# Verifier les jails actifs :
sudo fail2ban-client status
sudo fail2ban-client status sshd
# Currently banned: 3 | Total banned: 47
```

8. Integration fail2ban -> CrowdSec

fail2ban signale les IPs malveillantes a CrowdSec, qui les bloque au niveau OPNsense :

```
# Installer CrowdSec sur le serveur backend :
curl -s https://packagecloud.io/install/repositories/crowdsec/crowdsec/script.deb.sh \
  | sudo bash
sudo apt install crowdsec -y

# Enroller ce serveur :
sudo cscli console enroll <votre-enroll-key>

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

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

Flux de protection :

- 1. Bot tente brute-force SSH sur le serveur
- 2. fail2ban detecte apres 3 tentatives, ban IP localement
- 3. fail2ban envoie la decision a CrowdSec via cscli
- 4. CrowdSec propage au bouncer OPNsense
- 5. OPNsense bloque l'IP au niveau firewall pour tous les services
- 6. IP contribuee a la communaute CrowdSec mondiale

9. Monitoring

```
# Sur OPNsense (SSH) :
cscli alerts list     # alertes en temps reel
cscli decisions list  # decisions actives
cscli metrics         # metriques de l'agent

# Sur le serveur backend :
sudo tail -f /var/log/fail2ban.log
sudo fail2ban-client status sshd

# Dé-bannir une IP (faux positif) :
sudo fail2ban-client set sshd unbanip 192.168.10.50
```

Console CrowdSec (app.crowdsec.net) : carte mondiale des attaques, timeline alertes, CTI, blocklists premium, notifications Telegram/Slack/Email.

10. Tests de validation

```
# 1. Verifier CrowdSec sur OPNsense :
cscli version && cscli machines list

# 2. Simuler attaque SSH depuis IP externe :
for i in {1..5}; do ssh invalid_user@<IP-serveur> 2>/dev/null; done
# -> fail2ban doit bannir l'IP

# 3. Verifier le bannissement :
sudo fail2ban-client status sshd

# 4. Verifier propagation vers OPNsense :
# SSH OPNsense -> cscli decisions list

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

Prochaines etapes

Ce billet conclut la serie Stack OPNsense Enterprise. Recap complet :

- **Billet 1 :** Installer OPNsense dans Proxmox — base du routeur/firewall
- **Billet 2 :** VLANs & Zero Trust — segmentation reseau
- **Billet 3 :** WireGuard VPN & SD-WAN LTE — acces distant + failover
- **Billet 4 :** WiFi & APs avec UniFi/Omada — segmentation WiFi par VLAN
- **Billet 5 :** CrowdSec + fail2ban — IDS/IPS collaboratif (ce guide)

Article complet : blog.botum.ca/opnsense-crowdsec-fail2ban-protection

Hub de la serie : blog.botum.ca/opnsense-stack-securite-enterprise-proxmox

Site web : www.botum.ca • contact@botum.ca