CrowdSec

Overview

CrowdSec is a collaborative intrusion detection and prevention system integrated directly into Traefik. It analyses Traefik access logs in real time, detects attack patterns (brute force, CVE exploitation, bad bots, etc.), and instructs Traefik to block flagged IPs before they reach any backend service.

The stack consists of two containers:

- `crowdsec` — the Security Engine (LAPI + agent). Ingests logs, applies detection scenarios, maintains a decision list, and shares signals with the CrowdSec community.
- `crowdsec-bouncer-traefik` — the Traefik bouncer. Traefik forwards every incoming request to it via ForwardAuth; the bouncer checks the IP against CrowdSec's local decision database and returns allow/deny.

Access

Neither CrowdSec container has a web UI. Management is via the `cscli` CLI inside the `crowdsec` container:

```
docker exec -it crowdsec cscli decisions list
docker exec -it crowdsec cscli alerts list
docker exec -it crowdsec cscli metrics
```

Configuration

Compose project: `crowdsec` (managed via Portainer)

Containers

`crowdsec` — Security Engine

Image: `crowdsecurity/crowdsec:latest`

Property	Value
Network	`traefik-net`
Restart policy	`unless-stopped`

Key environment variables:

Variable	Value / Notes
`GID`	`1000`
`COLLECTIONS`	`crowdsecurity/traefik crowdsecurity/http-cve crowdsecurity/whitelist-good-actors`
`BOUNCER_KEY_TRAEFIK`	**REDACTED** — shared secret used by the bouncer to authenticate with LAPI

Collections installed:

Collection	Purpose
`crowdsecurity/traefik`	Detects attack patterns in Traefik access logs
`crowdsecurity/http-cve`	Detects exploitation of known HTTP CVEs
`crowdsecurity/whitelist-good-actors`	Whitelists known-good crawlers and services

`crowdsec-bouncer-traefik` — Traefik Bouncer

Image: `fbonalair/traefik-crowdsec-bouncer:latest`

Property	Value
Network	`traefik-net`
Internal port	`8080` (ForwardAuth endpoint)

Key environment variables:

Variable	Value / Notes
`GIN_MODE`	`release`
`CROWDSEC_AGENT_HOST`	`crowdsec:8080` — CrowdSec LAPI endpoint
`CROWDSEC_BOUNCER_API_KEY`	**REDACTED** — must match `BOUNCER_KEY_TRAEFIK`

How the Bouncer Integrates with Traefik

The middleware is defined in `/home/jeeves/docker/traefik/config/crowdsec.yml`:

```
http:
  middlewares:
    crowdsec-bouncer:
      forwardAuth:
        address: http://crowdsec-bouncer-traefik:8080/api/v1/forwardAuth
        trustForwardHeader: true
```

This middleware is referenced on external Traefik routes as `crowdsec-bouncer@file`.

Log Ingestion

CrowdSec reads Traefik access logs from two bind-mounted paths:

Host Path	Container Path	Notes
`/var/log/traefik`	`/var/log/traefik:ro`	Primary log location
`/home/jeeves/docker/traefik/logs`	`/logs/traefik:ro`	Secondary / rotated logs

The `acquis.yaml` config file at `/home/jeeves/docker/crowdsec/config/acquis.yaml` defines which log files to tail and in what format.

Volumes / Bind Mounts

Host Path	Container Path	Purpose
`/home/jeeves/docker/crowdsec/data`	`/var/lib/crowdsec/data`	Decision database and GeoIP data
`/home/jeeves/docker/crowdsec/config`	`/etc/crowdsec`	Scenarios, parsers, config
`/var/log/traefik`	`/var/log/traefik:ro`	Traefik access log (read-only)
`/home/jeeves/docker/traefik/logs`	`/logs/traefik:ro`	Traefik rotated logs (read-only)

Dependencies

- Traefik (must be running and writing access logs for CrowdSec to process)
- `crowdsec` LAPI must be healthy before `crowdsec-bouncer-traefik` starts
- Internet access required for CrowdSec community hub sync (pulling updated block lists)

Notes / Gotchas

- The `BOUNCER_KEY_TRAEFIK` / `CROWDSEC_BOUNCER_API_KEY` pair must match exactly. If mismatched, the bouncer will fail to authenticate with LAPI and Traefik will receive a 200 (passthrough) response from ForwardAuth — **effectively disabling the bouncer silently**.
- CrowdSec community sharing (`online_api_credentials.yaml`) requires an account at `app.crowdsec.net`. The credentials file is stored at `/home/jeeves/docker/crowdsec/config/online_api_credentials.yaml`.
- `crowdsec-bouncer@file` middleware must be applied to external routes only. Applying it to internal (`*.home.local`) routes will check LAN IPs against the community block list, which may block legitimate traffic unexpectedly.
- Manually ban an IP with:

  ```
  docker exec -it crowdsec cscli decisions add --ip <IP> --duration 24h --reason "manual"
  ```

- Remove a ban:

  ```
  docker exec -it crowdsec cscli decisions delete --ip <IP>
  ```

Last Updated: 2026-06-16

Revision #1
Created 2026-06-17 00:30:15 UTC by Admin
Updated 2026-06-17 00:31:19 UTC by Admin