Install CrowdSec on pfSense

Step?by?Step Guide: Install CrowdSec on pfSense & Enroll in Console

1. **Access pfSense via SSH or Console**

- Connect to your pfSense firewall via SSH or the physical console.
- Gain shell access to run commands.

2. **Install CrowdSec Package**

- **Preferred method (using install script):**

```
fetch https://raw.githubusercontent.com/crowdsecurity/pfSense-pkg-crowdsec/refs/heads/main/install-crowdsec.sh
sh install-crowdsec.sh
```

  This script handles dependencies and installation automatically(docs.crowdsec.net).
- **Manual method (if script not available):**

```
setenv IGNORE_OSVERSION yes
pkg add -f <link to abseil>
pkg add -f <link to re2>
pkg add -f <link to crowdsec-firewall-bouncer>
pkg add -f <link to crowdsec>
pkg add -f <link to pfSense-pkg-crowdsec>
```

  Use the appropriate links from the Release "Assets" matching your FreeBSD version(docs.crowdsec.net, forum.pfsense.com).

3. **Configure CrowdSec via GUI**

- In pfSense Web UI, go to **Services → CrowdSec**.
- Enable these components depending on the desired setup size:
  - **Large** (Full setup): Remediation Component, Log Processor, **Local API** – default.

- **Medium**: Disable Local API; connect to remote LAPI.
- **Small**: Only Remediation enabled(docs.crowdsec.net).

- Click **Save** to activate your configuration.

4. Verify Service Status

- Navigate to **Status → Services** to start/stop CrowdSec or firewall-bouncer services(docs.crowdsec.net).
- Alternatively, use shell commands:

```
service crowdsec.sh start|stop|restart
service crowdsec_firewall.sh start|stop|restart
```

5. Viewing Alerts & Blocked IPs

- In pfSense UI, open **Status → CrowdSec** to see:
  - Registered log processors and remediations.
  - Installed hub items (scenarios, parsers).
  - Alerts and local decisions (you can manually revoke/unban)(docs.crowdsec.net).
- From **Diagnostics → Tables**, view blocked IPs lists. Or via shell:

```
pfctl -T show -t crowdsec_blacklists
pfctl -T show -t crowdsec6_blacklists
cscli decisions list -a
```

6. Test the Setup

- To safely test blocking:

```
cscli decisions add -t ban -d 2m -i <your_ip_address>
```

- Be aware: your SSH session will drop briefly; use a secondary IP or disable the anti-lockout rule(docs.crowdsec.net).

7. Optional: Whitelist Local Networks

- If you want to allow local subnet ranges (10.0.0.0/8, 192.168.x.x, etc.), install the whitelist parsers:

```
cscli parsers install crowdsecurity/whitelists
```

- As of version 1.6.3, private networks are whitelisted by default(doc.crowdsec.net, docs.crowdsec.net).

Enroll Your pfSense Instance in CrowdSec Console

A. **Setup Integration in the CrowdSec Console**

1. Log in to your [CrowdSec Console] account.
2. Go to **Blocklist → Integrations**.
3. Click **Connect** under pfSense.
4. Provide a meaningful name (e.g., "My Firewall").
5. Copy the credentials and integration ID — **this will only display once**(docs.crowdsec.net).

B. **Configure pfSense to Fetch Blocklists**

1. In pfSense Web UI, go to **Firewall → Aliases → URLs → Add**.
2. Create a new URL alias:
   - Name: `crowdsec_blocklist` (or similar)
   - Type: `URL Table (IPs)`
   - URL:

     ```
     https://<username>:<password>@admin.api.crowdsec.net/v1/integrations/<integration_id>/content
     ```

   - Set update frequency (e.g., daily)(docs.crowdsec.net).
3. **Save** and **Apply**.

C. **Create Firewall Rule to Block Malicious IPs**

1. Navigate to **Firewall → Rules → WAN (or desired interface)**.
2. Add a rule:
   - Action: **Block**
   - Interface: **WAN**

- Source: use the alias created (`crowdsec_blocklist`)
- Destination: Any
- Description: e.g., “Block CrowdSec IPs”

3. Save and apply changes(docs.crowdsec.net).

Summary Table of Steps

Step	Action
1️	SSH into pfSense
2️	Install CrowdSec package (script or manual)
3️	Enable components in **Services → CrowdSec**
4️	Verify and manage services in GUI or shell
5️	Monitor alerts, decisions, and blocked IPs
6️	Test blocking with a temporary ban rule
7️	Optionally whitelist local networks
8️	Enroll instance in CrowdSec Console (Integrations)
9️	Set up URL alias to fetch CrowdSec blocklist
1️ 0️	Create firewall rule to block malicious IPs

Tips & Caveats

- **Backup** your CrowdSec config separately — it does not migrate with pfSense backups(docs.crowdsec.net).
- After major pfSense updates, **reinstall** the CrowdSec package if necessary — UI items may be removed even though configs remain(Netgate Forum).
- Ensure compatibility between your pfSense/FreeBSD version and the package architecture (e.g. amd64 vs ARM)(CrowdSec).

By following these steps, you'll achieve a well-integrated CrowdSec deployment on pfSense — complete with automated blocking, visibility into attacks, and centralized management via the CrowdSec Console.

Ins0mniA

Revision #2
Created 2025-08-25 18:52:46 EEST by Green

Updated 2025-09-04 02:12:01 EEST by Green