pfSense

Guides, Tweaks and Tips for pfSense.

- Install CrowdSec on pfSense
- pfSense Auto Update OS + Packages

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

pfSense Auto Update OS + Packages

pfSense Auto Update OS + Packages

For administrators who prefer managing their pfSense firewall from the command line, knowing the right tools for updating is essential. Two key utilities are `pkg-static` for managing add-on packages and `pfSense-upgrade` for handling major OS releases.

? One-Line Download & Execute:

```
clear && curl -fsSL https://docs.greenhome.stream/attachments/46 -o auto_upgrade.sh && chmod +x auto_upgrade.sh && clear && ./auto_upgrade.sh
```

This guide breaks down two powerful one-liner commands for automating these updates.

Part 1: Updating Installed Packages (`pkg-static`)

This command updates all installed add-on packages (like pfBlockerNG, Suricata, or other packages from the System > Package Manager menu) to their latest versions, without changing the core pfSense OS.

The Command:

```
/usr/local/sbin/pkg-static update -f && /usr/local/sbin/pkg-static upgrade -y
```

What It Does:

This is a two-part command joined by `&&`, which means the second part only runs if the first part succeeds.

1. `/usr/local/sbin/pkg-static update -f`
   - This command contacts the pfSense package repositories and forces a refresh of the package catalog. The `-f` (force) flag ensures you have the absolute latest list of available package versions, bypassing any local cache.[^1][^2]
2. `/usr/local/sbin/pkg-static upgrade -y`
   - This command compares the versions of your installed packages to the newly updated catalog. It then proceeds to download and install the latest versions for all packages that have an update available. The `-y` flag automatically answers "yes" to any confirmation prompts, making the process non-interactive.[^1]

Use Case:

Run this command when you want to update your add-on packages but are not ready to upgrade the entire pfSense operating system.

Part 2: Upgrading the pfSense OS (`pfSense-upgrade`)

This command initiates a full pfSense software upgrade, moving the system to the next major or minor release (e.g., from version 2.7.0 to 2.7.2).

The Command:

```
pfSense-upgrade -d -u -y
```

What It Does:

This command uses the official pfSense upgrade script with several flags to automate the process.

- `pfSense-upgrade`: This is the core script responsible for managing the entire OS upgrade, including fetching the new base system, applying it, and reinstalling compatible packages post-upgrade.[^11]
- `-d`: Enables **debug** mode, which provides verbose, detailed output of the entire upgrade process. This is extremely useful for troubleshooting if something goes wrong.[^5]
- `-u`: Tells the script to first **update** the repository metadata. This ensures the upgrader is checking against the latest available firmware release information.[^6]
- `-y`: Automatically answers "**yes**" to all confirmation prompts, allowing the upgrade to run from start to finish without user intervention.

Use Case:

This is the command to use for a complete, non-interactive system OS upgrade. Be aware that this process will download several hundred megabytes of data and will **automatically reboot** the firewall upon completion.

Important Considerations & Best Practices

- **Backup First:** Before running any upgrade, always create a backup of your pfSense configuration from **Diagnostics > Backup & Restore**.
- **The Recommended Upgrade Path:** For a major OS upgrade, it is best practice to run **only the `pfSense-upgrade` command**. The upgrade script is designed to handle the reinstallation of your packages correctly for the new OS version. Running `pkg-static upgrade -y` right before a major OS upgrade is generally unnecessary and can occasionally lead to dependency issues.
- **Schedule Downtime:** A full OS upgrade using `pfSense-upgrade` will result in a reboot and a brief period of network downtime. Plan accordingly.

Ins0mniA