

pfSense - Local System Config Backup and send to S3 Buckets

To automate backing up your pfSense configuration to Amazon S3, you can use pfSense's built-in **rclone** package. This eliminates the need for complex custom shell scripts because **rclone** can natively authenticate with AWS S3 and encrypt your files.

Here is the step-by-step guide to setting it up.

Step 1: Install the Required Packages

pfSense does not include backup utilities or cron management by default. You need to install them from the Package Manager. [\[1\]](#)

1. Log into your pfSense WebGUI.
2. Navigate to **System > Package Manager > Available Packages**.
3. Search for and install **rclone**.
4. Search for and install **cron** (this gives you a visual interface to schedule the backup).

Step 2: Configure Rclone for Amazon S3

Next, create a connection profile (called a "remote") between your pfSense box and your S3 bucket.

1. Connect to your pfSense firewall via **SSH** (or use the WebGUI via **Diagnostics > Command Prompt**).
2. Run the rclone configuration tool:

```
rclone config
```

■

3. Type **n** for "New remote" and name it **s3-backup**.
4. When prompted for the storage type, type **s3** (or look for the number corresponding to Amazon S3).
5. Choose your S3 provider by typing **Amazon** (or press enter for the default AWS S3).
6. Select **false** for entering AWS credentials from the env_auth.
7. Enter your AWS account details when prompted:
 - **access_key_id**: Your AWS Access Key
 - **secret_access_key**: Your AWS Secret Key
8. Select your AWS Region (e.g., **us-east-1**).

9. For all other advanced settings (endpoint, ACLs, encryption), you can press **Enter** to accept the defaults.
10. Type **y** to confirm and save the configuration, then **q** to quit.

Optional if `rclone` is not available and install `rclone` Manually

1. Download and Extract the Binary

SSH into your pfSense box (or use **Diagnostics > Command Prompt**) and execute these commands to download the FreeBSD version of Rclone:

```
# 1. Navigate to a temporary folder
cd /tmp

# 2. Download the official FreeBSD 64-bit binary zip archive
fetch https://downloads.rclone.org/v1.75.0/rclone-v1.75.0-freebsd-amd64.zip

# 3. Unzip the downloaded archive
tar -xf rclone-current-freebsd-amd64.zip
```

2. Move `rclone` to the System Path

Move the extracted binary file into the folder where pfSense looks for standard utilities:

```
# 1. Move the executable binary into your local execution path
mv /tmp/rclone-*-freebsd-amd64/rclone /usr/local/bin/

# 2. Grant execution permissions to the binary file
chmod +x /usr/local/bin/rclone

# 3. Clean up the leftover installation files from /tmp
rm -rf /tmp/rclone-*
```

3. Verify the Installation

Run the version check command to verify it executes perfectly:

bash

```
rclone version
```

Step 3: Create the Backup Script on pfSense

pfSense stores its active configuration file at `/conf/config.xml`. We will write a simple 3-line script to copy this file, timestamp it, and upload it.

1. In the WebGUI, go to **Diagnostics > Command Prompt**.
2. In the **Execute Shell Command** box, run this command to create a backup directory:

bash

```
mkdir -p /root/backups
```

■

3. Go to **Diagnostics > Edit File**.
4. In the **Path to file to edit** box, type: `/root/backup_pfsense.sh` and click **Load**.
5. Paste the following script into the text area:

bash

```
#!/bin/sh
DATE=$(date +%Y%m%d-%H%M%S)
BACKUP_FILE="/root/backups/pfsense-config-`${DATE}`.xml"

# 1. Copy the live config to the local backup folder
cp /conf/config.xml "${BACKUP_FILE}"

# 2. Push the file to your S3 bucket (replace "your-bucket-name" with your actual bucket)
/usr/local/bin/rclone copy "${BACKUP_FILE}" s3-backup:your-bucket-name/pfsense/

# 3. Clean up local files older than 7 days to save space on pfSense
find /root/backups/ -name "pfsense-config-*.xml" -type f -mtime +7 -delete
```

6. Click **Save**.
7. Go back to **Diagnostics > Command Prompt** and make the script executable by running:

bash

```
chmod +x /root/backup_pfsense.sh
```

■

(Optional Testing: You can test if it works right now by running `/root/backup_pfsense.sh` in the Command Prompt box and checking your S3 bucket).

Step 4: Schedule the Automation with Cron

Now, use the Cron package you installed in Step 1 to make this run automatically every day.

1. Navigate to **Services > Cron** in the WebGUI. [\[1\]](#)

2. Click **+ Add** to create a new cron job.
3. Configure the schedule (e.g., to run daily at 3:00 AM):
 - **Minute:**
 - **Hour:**
 - **Day of the Month:**
 - **Month:**
 - **Day of the Week:**
 - **User:**
 - **Command:**
4. Click **Save**.

☐ Security Warning for pfSense Backups

Your `config.xml` file contains your firewall's root password hashes, VPN private keys, and network topology.

- **Encrypt the Remote Bucket:** Ensure your S3 bucket has Server-Side Encryption (SSE) turned on.
- **Alternative (Rclone Encryption):** If you want absolute zero-knowledge security, you can run `rclone config` again, add a new remote of type `crypt`, and point it at `s3-backup:your-bucket-name`. This will encrypt the file locally on pfSense *before* it touches AWS infrastructure.

Revision #1

Created 9 August 2026 20:55:35 by Steve Ling

Updated 9 August 2026 21:36:14 by Steve Ling