Update #7 - Syncthing UFW Rule Automation with DDNS Integration

Date: May 10, 2025
Category: Security / Automation

Backlink: Update #6 – Fail2Ban Security Hardening

□□ Overview

This update focused on hardening access to Syncthing on the VPS. Instead of allowing unrestricted access to the Syncthing web UI and sync ports, I created a secure and automated solution that dynamically resolves a DDNS hostname (masked here for privacy) and updates UFW rules accordingly. This ensures only the current home IP can connect to the Syncthing interface and sync services.

□□ Tools & Technologies Used

- **Syncthing** – Installed and configured on a headless Ubuntu VPS
- **UFW (Uncomplicated Firewall)** – Manages allowed IP access
- **DDNS (Dynamic DNS)** – Tracks home IP address
- **Bash Script** – Automates the rule refresh process
- **Systemd Cron Job** – Scheduled execution of the automation

□□ The Process

1. **Validated Syncthing Setup**
   - Confirmed Syncthing was installed and running.
   - Located its config and ensured `127.0.0.1:8384` was listening.
2. **Allowed Necessary Ports**

- Syncthing uses:
  - `8384/tcp` – Web GUI
  - `22000/tcp` – Sync traffic
  - `21027/udp` – Local discovery
- Initially opened ports to `Anywhere` to confirm functionality.

3. **Wrote an Automation Script**
   I created `/usr/local/bin/update-syncthing-ufw.sh` to:
   - Resolve the DDNS hostname to a public IP.
   - Delete any existing UFW rules for `8384`, `22000`, and `21027`.
   - Add new rules allowing traffic only from the current IP.

   Sample success message:

   ```
   UFW rules updated for Syncthing services from [masked DDNS IP]
   ```

4. **Confirmed It Works**
   - Ran the script manually.
   - Verified UFW rules with `sudo ufw status numbered`.
   - Accessed the Syncthing Web UI remotely from home IP to confirm access.
5. **Cleaned Up UFW Rules**
   - Removed `Anywhere` rules for Syncthing ports.
   - Only the resolved DDNS IP is now allowed per service port.
6. **Created a Daily Cron Job**
   - Added the following to root's crontab:

     ```
     0 */6 * * * /usr/local/bin/update-syncthing-ufw.sh
     ```

   - This updates the rule every 6 hours in case the home IP changes.

The Result

- Syncthing Web UI and sync features are only accessible from home IP.
- All UFW rules now reflect the current public IP automatically.
- No more manual UFW updates or security exposure.
- This complements previous hardening efforts made in Update #6.

What I Learned

- UFW’s rule numbers change dynamically; scripting is essential for removal before re-addition.
- You can safely update firewall rules on a schedule without needing manual login.
- Protecting even the Web GUI of Syncthing is important in public VPS setups.
- DDNS + automation = powerful security combo.

Revision #4
Created 10 May 2025 01:52:46 by Nate Nash
Updated 7 June 2025 00:14:24 by Nate Nash