# Update #11 - Syncthing UFW DDNS Cron Recovery & Long-Term Rule Persistence

**Date:** May 11, 2025
**Category:** Security / Automation

**Backlink:** Update #10 – Fail2Ban IP Geolocation Lookup Script with Auto-Filtering

## Overview

This update builds upon our existing Syncthing and UFW/DDNS configuration and addresses the issue of persistent firewall rules disappearing after system events such as upgrades or restarts. It introduces mechanisms to automatically recover and persist UFW rules linked to DDNS-resolved IPs, as well as implement log rotation for our custom scripts.

## Problem Summary

- UFW rules allowing DDNS-bound access to Syncthing ports (8384, 22000, 21027) were occasionally disappearing.
- There was no persistent re-application of these rules on reboot or after package upgrades.
- A need existed to reduce log file size growth from regular UFW rule updates.

## Key Changes Implemented

### 1. **Syncthing DDNS-based UFW Script Improvements**

- Script Path: `/usr/local/bin/update-syncthing-ufw.sh`
- Now includes:

- Cleanup of old rules
- Re-application of DDNS-resolved IP
- IPv6 exception handling
- Console output when run manually
- Logged output when run via cron

```
#!/bin/bash

DDNS_HOST="your-ddns.example.com"
PORTS=(8384/tcp 22000/tcp 21027/udp)
LOG_TAG="Syncthing DDNS Access"

# Resolve IP
IP=$(dig +short "$DDNS_HOST" | grep -E '^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$' | head -n1)

if [[ -z "$IP" ]]; then
    echo "□ Failed to resolve IP for $DDNS_HOST"
    exit 1
fi

# Clean up existing rules for this tag
for port in "${PORTS[@]}"; do
    ufw status numbered | grep "$LOG_TAG" | grep "$port" | awk -F'[][]' '{print $2}' | tac | while read -r num; do
        ufw --force delete "$num"
    done
done

# Add new rules
for port in "${PORTS[@]}"; do
    ufw allow from "$IP" to any port "${port%/*}" proto "${port##*/}" comment "$LOG_TAG"
done

echo "□ Cleaned and updated UFW rules for Syncthing from $IP"
```

# 2. **Cron Automation for Rule Recovery**

- **Location:** `sudo crontab -e`
- **Jobs Added:**

```
# Run daily at 3:00 AM
0 3 * * * /usr/local/bin/update-syncthing-ufw.sh
```

```
# Run every 10 minutes, prevents overlapping runs
*/10 * * * * flock -n /tmp/ufw-ddns.lock /usr/local/bin/update-syncthing-ufw.sh >> /var/log/update-syncthing-ufw.log 2>&1

# Run on reboot
@reboot /usr/local/bin/update-syncthing-ufw.sh >> /var/log/update-syncthing-ufw.log 2>&1
```

---

## 3. **Logrotate Setup for UFW Update Logs**

- **File:** `/etc/logrotate.d/update-syncthing-ufw`
- **Content:**

```
/var/log/update-syncthing-ufw.log {
    su root root
    daily
    rotate 7
    compress
    missingok
    notifempty
    create 644 root root
}
```

# Additional Files and Paths

| Script | Path |
|---|---|
| Syncthing DDNS UFW Script | `/usr/local/bin/update-syncthing-ufw.sh` |
| Cron Log File | `/var/log/update-syncthing-ufw.log` |
| Logrotate Config | `/etc/logrotate.d/update-syncthing-ufw` |

# Testing

- Verified successful rule refresh via `sudo ufw status`
- Confirmed script logs rotation using `logrotate --debug`
- Confirmed cron execution via `grep update-syncthing-ufw /var/log/syslog`
- Script executes correctly manually and via cron.

# Conclusion

This update ensures that DDNS-based access to Syncthing is consistently maintained with automatic recovery and no risk of bloat from excessive log growth. The solution is now reliable through reboots, daily updates, and in the event of system changes like package upgrades

---

Revision #2
Created 11 May 2025 15:39:08 by Nate Nash
Updated 7 June 2025 00:14:24 by Nate Nash