Update #12 - Step-by-Step Breakdown of UFW DDNS Update Script

Date: May 11, 2025
Category: Automation / Firewall

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

Overview

This update documents the full working version of the `update-syncthing-ufw.sh` script, designed to automatically update UFW rules for Syncthing ports based on the current IP address of a DDNS hostname.

Script Location

```
/usr/local/bin/update-syncthing-ufw.sh
```

Log File

```
/var/log/update-syncthing-ufw.log
```

Full Script Breakdown

```
#!/bin/bash
```

Starts a bash shell script.

```
DDNS_HOST="<your-ddns-name"
```

Specifies your DDNS hostname to resolve dynamically.

```
LOGFILE="/var/log/update-syncthing-ufw.log"
```

Sets the path where all log entries will be stored.

```
PORTS=(
    "8384/tcp"
    "22000/tcp"
    "21027/udp"
)
```

Defines an array of Syncthing-related ports (Web UI, sync port, and discovery port).

```
timestamp() {
    date "+%Y-%m-%d %H:%M:%S"
}
```

Defines a helper function for timestamp formatting.

```
RESOLVED_IP=$(dig +short "$DDNS_HOST" | grep -E '^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$' | head -n 1)
```

Uses `dig` to resolve the IP for your DDNS and filter for valid IPv4 results.

```
if [[ -z "$RESOLVED_IP" ]]; then
    echo "$(timestamp) □ Failed to resolve IP for $DDNS_HOST" | tee -a "$LOGFILE"
    exit 1
else
    echo "$(timestamp) □□ Resolved IP for $DDNS_HOST: $RESOLVED_IP" | tee -a "$LOGFILE"
fi
```

Logs resolution status and aborts if the IP can't be resolved.

```
for PORT in "${PORTS[@]}"; do
    sudo ufw delete allow from any to any port "$PORT" comment 'Syncthing DDNS Access' > /dev/null 2>&1 ||
true
done
```

Deletes any prior rules with the comment 'Syncthing DDNS Access' silently. `|| true` ensures the script continues even if a rule doesn't exist.

```
ALL_ADDED=true
```

Tracks success status across all rule additions.

```
for PORT in "${PORTS[@]}"; do
```

Loops over each port.

```
    if sudo ufw status | grep -q "$PORT.*$RESOLVED_IP"; then
        echo "$(timestamp) ✳ Rule already exists: $PORT from $RESOLVED_IP" | tee -a "$LOGFILE"
```

If the rule already exists, log it as a no-op.

```
    elif sudo ufw allow from "$RESOLVED_IP" to any port "$PORT" comment 'Syncthing DDNS Access' > /dev/null
2>&1; then
        echo "$(timestamp) □ Rule added: $PORT from $RESOLVED_IP" | tee -a "$LOGFILE"
```

If the rule doesn’t exist, add it and log success.

```
    else
        echo "$(timestamp) □ Failed to add rule: $PORT from $RESOLVED_IP" | tee -a "$LOGFILE"
        ALL_ADDED=false
    fi
done
```

If adding fails, log an error and flag the batch as partially failed.

```
if $ALL_ADDED; then
    echo "$(timestamp) □ All UFW rules successfully updated for Syncthing from $RESOLVED_IP" | tee -a
"$LOGFILE"
else
    echo "$(timestamp) ⚠ Partial failure updating UFW rules for Syncthing from $RESOLVED_IP" | tee -a
"$LOGFILE"
fi
```

Provides a final summary log depending on success/failure of all rule additions.

Fixes & Adjustments Made

- Fixed `Permission denied` errors by ensuring the script runs with `sudo` when needed and logs are only written by root.
- Replaced silent failures with emoji-marked status outputs (, , ⚠, ✳) for readability.
- Confirmed logs rotate daily via `/etc/logrotate.d/update-syncthing-ufw`.

Testing & Verification

- Manual execution verified with:

```
sudo /usr/local/bin/update-syncthing-ufw.sh
```

- UFW rules confirmed using:

```
sudo ufw status verbose
```

- Log output tail:

```
sudo tail -n 20 /var/log/update-syncthing-ufw.log
```

Revision #2
Created 11 May 2025 22:51:46 by Nate Nash
Updated 7 June 2025 00:14:24 by Nate Nash