Update #9 - Syncthing UFW Log Monitoring with Active Fail2Ban Enforcement

Date: May 10, 2025
Category: Security / Monitoring

Backlink: Update #8 – Syncthing Systemd Recovery After Upgrade

Overview

This update strengthens the security posture of Syncthing on the VPS by combining **UFW logging** with **active Fail2Ban enforcement**. In addition to passively monitoring IPs attempting to access Syncthing ports (8384, 22000, 21027), we now **automatically ban repeat offenders**, reducing risk and exposure from persistent probing.

A custom Fail2Ban filter and jail were added to detect and block malicious IPs based on UFW blocks. Link-local IPv6 traffic (fe80::/10) is ignored to avoid false positives.

Goals

- Detect blocked access attempts on Syncthing ports via UFW.
- Ban repeated offenders automatically using Fail2Ban.
- Maintain a summarized view of access attempts for visibility.

Files and Configuration

UFW Log Summary Script

Stored at: `~/syncthing-log-summary.sh`

```
#!/bin/bash

# Syncthing ports of interest
PORTS="8384|22000|21027"

# Log file
LOGFILE="/var/log/ufw.log"

# Output summary
echo "Top IPs attempting to access Syncthing ports (8384, 22000, 21027):"
echo "------------------------------------------------------------------"

# Extract and count IPs, excluding fe80::/10 (IPv6 link-local)
sudo grep "UFW BLOCK" "$LOGFILE" | \
grep -E "DPT=($PORTS)" | \
grep -v "SRC=fe80:" | \
grep -oP 'SRC=\K\S+' | \
sort | uniq -c | sort -rn | head -20
```

Fail2Ban Filter: `/etc/fail2ban/filter.d/ufw-block.conf`

```
[Definition]
failregex = \[UFW BLOCK\].*SRC=<HOST>.*DPT=(8384|22000|21027)
ignoreregex = SRC=fe80::
```

Fail2Ban Jail Configuration: `/etc/fail2ban/jail.local`

```
[ufw-block]
enabled = true
filter = ufw-block
action = iptables[name=UFW-Blocked, port=all, protocol=all]
logpath = /var/log/ufw.log
maxretry = 3
findtime = 600
bantime = 43200
```

> This jail looks for repeated blocks on Syncthing ports and bans IPs for **12 hours** after **3 failed attempts within 10 minutes**.

Monitoring

Run this command at any time to review the top offending IPs:

```
bash ~/syncthing-log-summary.sh
```

To review currently banned IPs by this jail:

```
sudo fail2ban-client status ufw-block
```

To unban an IP (example):

```
sudo fail2ban-client set ufw-block unbanip 192.0.2.1
```

Status

- UFW logging confirmed active.
- Syncthing ports protected behind dynamic DDNS-controlled rules.
- Fail2Ban jail banning repeat offenders.
- Link-local IPv6 traffic excluded to reduce noise.

Revision #3
Created 10 May 2025 20:32:36 by Nate Nash
Updated 7 June 2025 00:14:24 by Nate Nash