St. Louis Unix Users Group

Main Presentation

9 April 2025

How to Rescue Your Firewall When the SHTF

A Production Firewall Fails...

- A Cisco RVN042, in service for over 20 years, died during a power failure
  - **Symptoms:** No lights, power supply OK
  - **Backups:** Do they exist?
  - **Hardware Check:**
    - Is there a current backup device?
    - Is compatible spare hardware on hand?
    - If not, what *is* available?
- Action Plan
  - New HW
  - Choose OS SW
  - Install SW
  - Initial Configuration
  - Final Setup
  - Put into production
  - Update & Improve

Outline

The process:

1. **Source Replacement Hardware**

2. **Choose Replacement Software**
3. **Install SW**
4. **Initial Configuration**
5. **Final Setup**
6. **Improve Configuration**

Steps to Recovery - #1

1. **Source Replacement Hardware**

- HW: look for fanless, firewall, or routers:
  - Amazon
  - NewEgg
  - eBay
  - Vendors (a la Advantech)
- What specs are needed?
- One IS available, .. https://www.ebay.com/itm/355365058072?_skw=Fanless%2Bmini%2Bcompute%2BJ4125%2B8GB%2BRAM%2B32GB%2BSSD%2Brouter%2BpFsense%2Bopnsense%2Bopenwrt&itmmeta=01JR928GMAD22PAJ1XD92BSVVH&hash=item52bd687618:g:mu4AAOSwCWFlSvE4&itmprp=enc%3AAQAKAAABEFkggFvd1GGDu0w3yXCmi1c%2BlcsJcvnzq%2FovL1s6NX%2FpCr8UmBSt8qDbc3CwiQvaYXPXn90T8jkEmEk%2Fy6tXLpRulm1EC0%2FcpkQF%2Ft56btxbsY%2FxtqDLO2mPiZlQ35lkwAiyPhxxYoq3E6oP0yQHSeG8Ejnok87nVEH2wt7FPajB7CVKBiSCxlRdDmrLhCjv7z8FjMBVWvxTBCjnY%2F9ZI1fAXGnj8v1Ul4uJnkoxFju5OlVhaFU7ox%2Bq89Ms1p5hHnSuuk%2BZAdoVcVtwxrQbkT0x10Ri7dI%2BBdDWIMwVy90IT%2FYP2GsS%2FZ5JVPw5Kk6C2%2BLlhyuPQKqA1G65LIi%2F5BSk3ZOAnpjMwvne%2B8WFM8eA%7Ctkp%3ABk9SR6KKoqLCZQ

Steps to Recover - #2

- **Choose Replacement Software**
  - Evaluate options (OPNsense, pfSense, ipFire, etc.)
  - Tried pfSense, do **not** like registration requirement to download!
  - So, .. let's use OPNSense!

Steps to Recovery - #3

- **Install the SW**
  - Download image
  - Burn thumb drive
  - Install base system

Steps to Recovery - #4

- **Initial Configuration**
  - Use WAN for temporary access
  - Connect to GUI via browser
  - Setup base configuration

Steps to Recovery - #5

- **Intial Setup**
  - Bridge internal interfaces
  - Setup base firewall rules
  - Test GUI on LAN side
  - Put into prod

Steps to Recovery - #6

- **Improve Configuratu**
  - Secure GUI - ensureavailable on INTERNAL network only
  - Setup CERT
  - Expand firewall rules
  - Improve over time

Demo - Step #1

- **Setup Hardware**
  - Power
  - Display
  - Keyboard

Demo - Step - #2

- **Choose Replacement Software**
  - Evaluate options (OPNsense, pfSense, ipFire, etc.)
  - Tried pfSense, do not like new registration requirement!
  - So, .. let's go with OPNSense!

Demo - Step - #3

- **Install the SW**
  - Download image
  - Burn image to thumb drive
  - Install base system

Demo - Step - #4

- **Base Configuration**
  - Use local WAN IP or DHCP
  - Connect GUI via browser
  - Login with default creds: root & opnsense
  - Setup base configuration

Demo - Step - #5

- **Initial Setup**
  - Bridge internal interfaces to use all available ports

    - Setup base firewall rules
    - Test GUI on LAN side
    - Put into production

Improve configuration

- Once in prod, continue to:
    - Improve security [firewall rules]
    - Add security tools [addins]
    - Monitor traffic
    - Add monitoring [e.g. Nagios]

But WAIT, .. there's MORE!!!

- What if you **HAVE** a backup, but it's from **different** HW?
  ESPECIALLY if the port IDs have changed?

- It **is** possible to migrate the backup!

    - Best for OS projects (pfSense, OPNSense)
    - Parse the backup into components
    - Use that to build the new configuration

- OS SW Backups are normally in JSON

    - Export to plain text
    - View with a text editor

- Commercial Backups may be **proprietary**!

    - Capture the backup ON the device
    - Export locally
    - View with a text editor

Lee Lammert

Thank you for your time!