Implementing Firewalls with UFW

Andrew Mallett

Linux Author and Trainer

@theurbanpenguin   www.theurbanpenguin.com
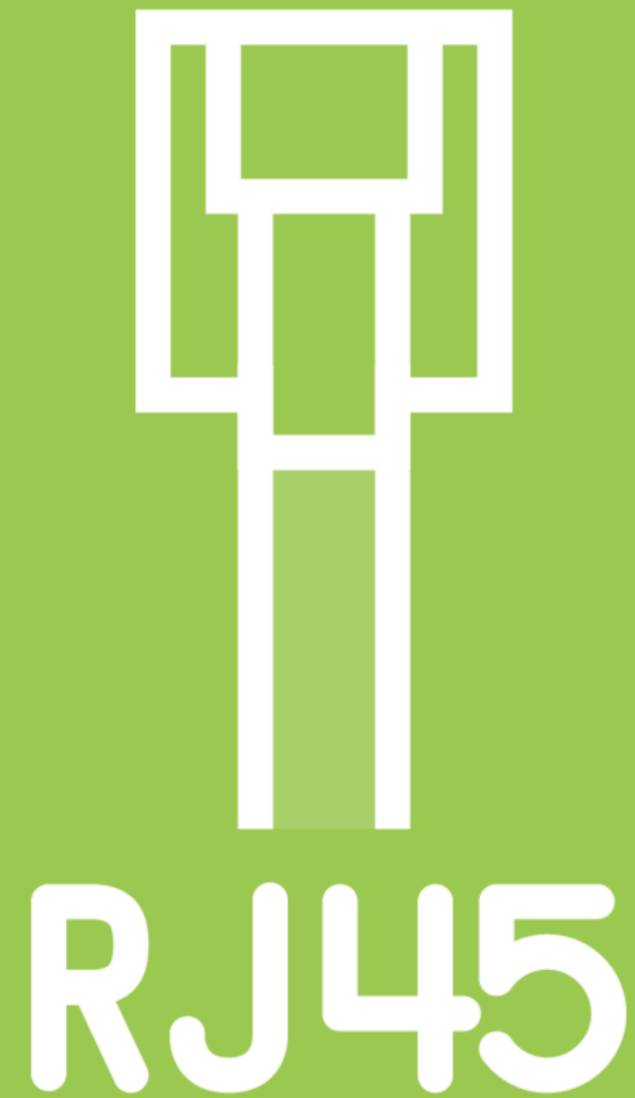
Overview

Securing your System via Host Based Firewall

- ufw

  - defaults

  - configure basic rules before enabling

  - enable, disable and reset

UFW

Uncomplicated **F**ire**w**all:
Now there's an oxymoron if
ever I heard one!

RJ45

Lab Systems

AlmaLinux 8
  - client

Ubuntu 20.04
  - ufw

Host-Based Firewalls

As before, with firewalld, host-based firewalls add security protecting against internal attacks and failures in the border gateway. UFW is the default firewall manager on Ubuntu but firewalld could be installed

```
$ sudo -i

# ufw status

# ufw status verbose

# ufw status numbered
...
```

Managing UFW

The main command is ufw, status will show the current settings, we can add the numbered option which can be useful when deleting rules or the verbose option to print more details

```
# cat /etc/default/ufw
# ufw allow ssh
# ufw enable
```

The Default Incoming Rule is to Block

Default inbound rules block all new traffic. Be careful when enabling UFW to check your access is not denied

Demo

Let's begin by examining the basic UFW setup

- View defaults

- Allow inbound SSH

- Enable UFW

```
# ufw allow from 10.0.2.0/24 to any port 22

# ufw status numbered

# ufw --dry-run delete 3

# ufw delete 3

# ufw status
```

Tuning Allow Rules

We may only want to allow inbound IPv4 to SSH, and only from the 10.0.2.0/24 network, the NAT network we are using

Demo

We can now tune the SSH rule to our needs

- add rule from address range
- use dry-run to test effects
- remove IPv6 allow rule
- remove allow from anywhere rule
- test access from different networks

```
# apt install -y apache2

# ufw enable from 192.168.33.11 to any port http
```

Enable HTTP Access

We can enable HTTP access from the AlmaLinux system

Demo

Enable HTTP Access

- Install Apache2

- Allow access from the AlmaLinux system only

```
# ufw show raw

# ufw show added

# ufw reset
```

Firewall Details

UFW is a firewall manager, the backend uses IPTables. We can also reset to the originally settings

Demo

We now investigate:

- Reports
- Reset

Summary

In this module we have introduced host-based firewalls and ufw:

- ufw command
- Adding and deleting rules
- Reporting
- Resetting to defaults

Congratulations