Kevin Varghese 09/5/25

Project: Linux Firewall VM Overview

_____

Objective:

Set up an Ubuntu virtual machine as a working firewall, using UFW, iptables, and DNS overrides to block access to specific websites and IP ranges. Verified functionality via both command-line and browser testing.

Environment & Tools:

• Ubuntu Linux (UTM VM on macOS)

• UFW (Uncomplicated Firewall) and iptables

• DNS overrides via /etc/hosts

• subnet masking (/16 CIDR), ping (ICMP), and Firefox browser for validation

Implementation Steps:

1. Activated firewall:

   sudo ufw enable

2. Blocked site IP range:

   sudo ufw deny out to 157.240.0.0/16

3. Redirected domain locally:

   facebook.com → 127.0.0.1 in /etc/hosts

4. Verified blocking:

   • ping facebook.com → 100% packet loss

   • Browser attempt → connection error

Results:

• Successfully blocked access to Facebook and WWE.

• Confirmed rule effectiveness through both terminal and browser.

• Demonstrated understanding of firewall rules, subnet blocking, and DNS behavior.
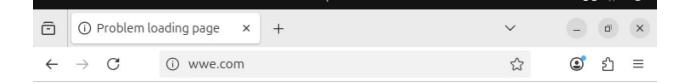
Lessons Learned:

• Subnet masks (/16) enable effective blocking of large IP ranges.

• DNS overrides test hostname-level control.

• Well-documented proof (screenshots, tests) enhances clarity and credibility.

Visual Evidence:

```
darkdev@domes:~$ sudo ufw status
Status: active

To                          Action      From
--                          ------      ----
80/tcp                      ALLOW       Anywhere
443/tcp                     ALLOW       Anywhere
80/tcp (v6)                 ALLOW       Anywhere (v6)
443/tcp (v6)                ALLOW       Anywhere (v6)

52.4.235.80 80/tcp          REJECT OUT  Anywhere
52.4.235.80 443/tcp         REJECT OUT  Anywhere
54.236.192.188 80/tcp       REJECT OUT  Anywhere
54.236.192.188 443/tcp      REJECT OUT  Anywhere
157.240.241.35 80/tcp       REJECT OUT  Anywhere
157.240.241.35 443/tcp      REJECT OUT  Anywhere
157.240.0.0/16              DENY OUT    Anywhere

darkdev@domes:~$
```

```
darkdev@domes:~$ ping -c 4 wwe.com
PING wwe.com (54.236.192.188) 56(84) bytes of data.

--- wwe.com ping statistics ---
4 packets transmitted, 0 received, 100% packet loss, time 3062ms

darkdev@domes:~$
```

wwe.com

Unable to connect

Firefox can't establish a connection to the server at wwe.com.

- The site could be temporarily unavailable or too busy. Try again in a few moments.
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the web.

Try Again

Further Resources:

Complete project write-up: Linux-Firewall-Showcase.pdf

Project repository: https://github.com/Darktheo-dev/linux-firewall-project