Introduction to Cybersecurity
CS/IS 193

LAB13 REPORT

5/22/2022

DAVID ARCHER

Table of Contents

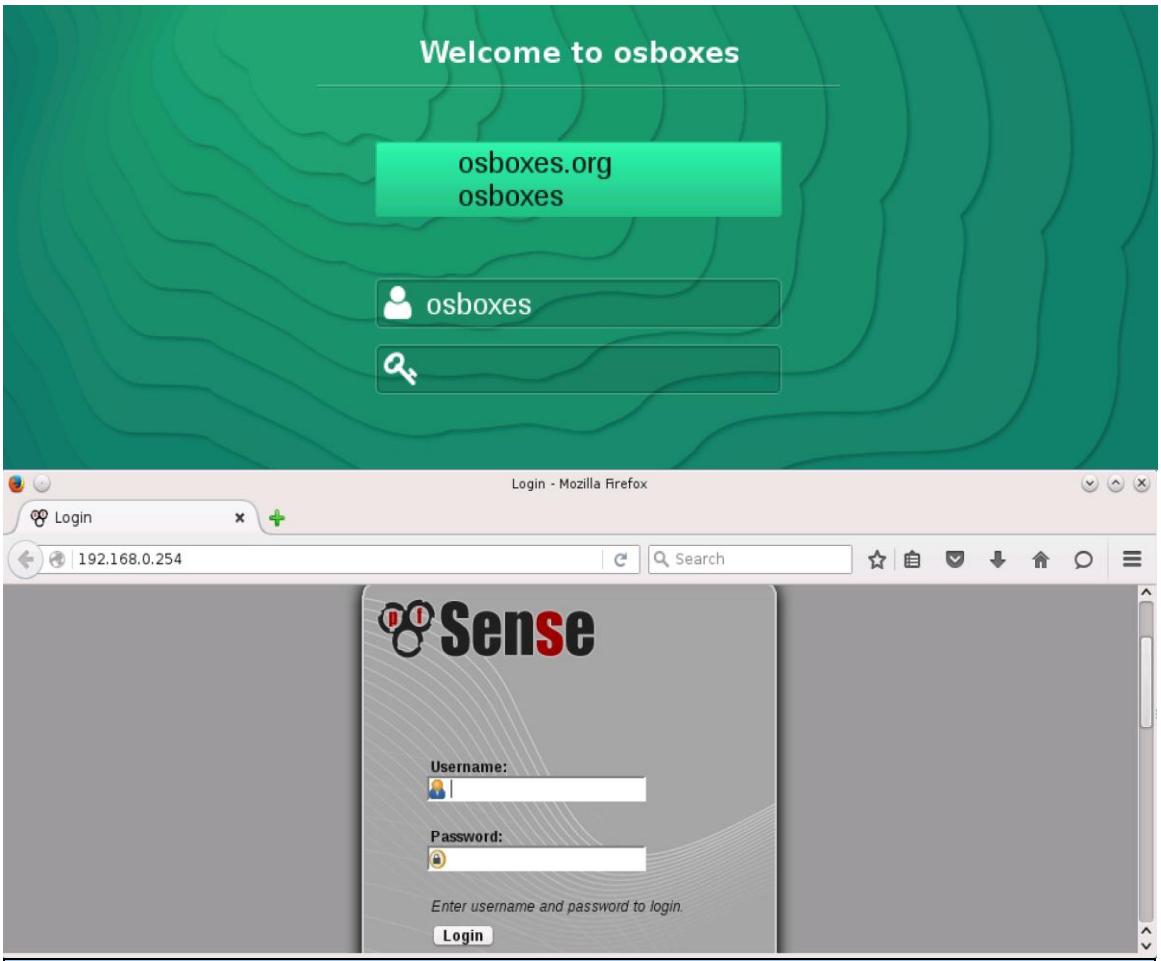
1. Introduction

Firewall rules are important in controlling inbound and outbound traffic in a network. I will be performing the following tasks: Navigating to the pfSense Dashboard, Scanning for Firewall Rules with Firewalk, Configuring ACL Rules, and Testing Configured Firewall Rules with Firewalk.

2. Lab Results

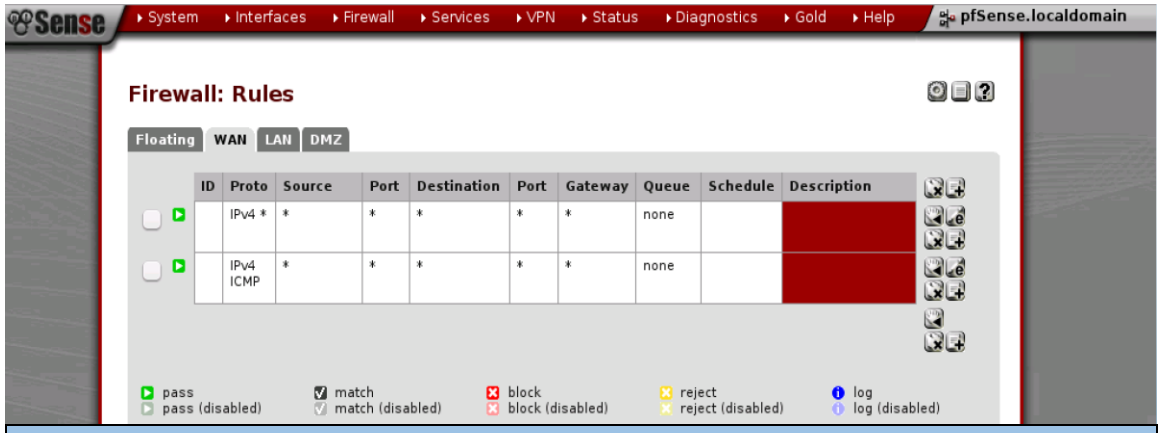
1. Navigating to the pfSense Dashboard

1. OpenSUSE Virtual Machine
2. pfSense login



Opened OpenSUSE's Firefox web browser, inputted and searched **192.168.0.254.** I inputted the appropriate login credentials after being redirected to the pfSense login page then clicked **Login**.

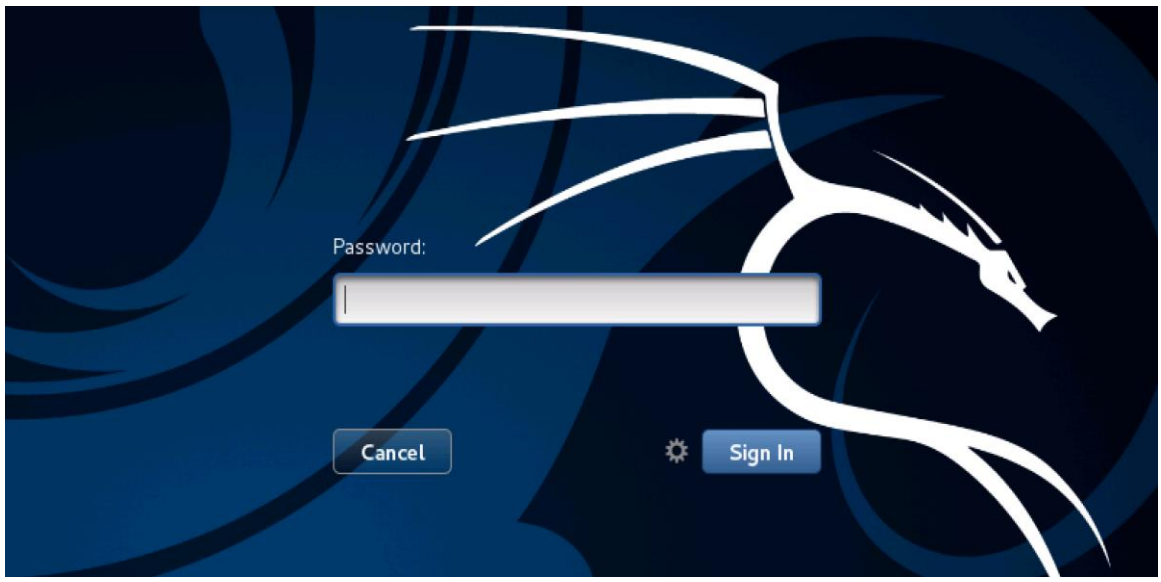
3. Firewall Rules



Navigated to **Firewall** > Rules. When observing the WAN rules, I noticed that all protocols are allowed to pass through.

2. Scan for Firewall Rules with Firewalk

1. Launch Kali Linux VM



2. Terminal

```
root@Kali2: ~
File  Edit  View  Search  Terminal  Help
root@Kali2:~# firewalk
Firewalk 5.0 [gateway ACL scanner]
Usage : firewalk [options] target_gateway metric
                   [-d 0 - 65535] destination port to use (ramping phase)
                   [-h] program help
                   [-i device] interface
                   [-n] do not resolve IP addresses into hostnames
                   [-p TCP | UDP] firewalk protocol
                   [-r] strict RFC adherence
                   [-S x - y, z] port range to scan
                   [-s 0 - 65535] source port
                   [-T 1 - 1000] packet read timeout in ms
                   [-t 1 - 25] IP time to live
                   [-v] program version
                   [-x 1 - 8] expire vector

root@Kali2:~#
```

To familiarize myself with the available firewalk command options, I inputted the command **firewalk**

3. Nmap scan

```
root@Kali2:~# nmap 192.168.9.1

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2022-05-22 07:10 CDT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.9.1
Host is up (0.00013s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 00:50:56:9A:63:AC (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.20 seconds
root@Kali2:~#
```

Attempted an Nmap scan against the firewall with **nmap 192.168.9.1** command. I noticed that there are two open ports reported by Nmap: ports **53** and **80**.

4. ACL rules

```
root@Kali2:~# firewalk -n -p TCP -S 23 -d 23 192.168.9.1 192.168.68.12
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 23
Hotfoot through 192.168.9.1 using 192.168.68.12 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.9.1]
Binding host reached.
Scan bound at 2 hops.
Scanning Phase:
port  23: A! open (port not listen) [192.168.68.12]

Scan completed successfully.

Total packets sent:                2
Total packet errors:               0
Total packets caught               2
Total packets caught of interest   2
Total ports scanned                1
Total ports open:                  1
Total ports unknown:               0
root@Kali2:~#
```

Command **firewalk -n –p TCP -S 23 –d 23 192.168.9.1 192.168.68.12** was used to test if there is an ACL rule for port 23

5. ACL rules

```
root@Kali2:~# firewalk -n -p TCP -S 25 -d 25 192.168.9.1 192.168.68.12
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 25
Hotfoot through 192.168.9.1 using 192.168.68.12 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.9.1]
Binding host reached.
Scan bound at 2 hops.
Scanning Phase:
port  25: A! open (port not listen) [192.168.68.12]

Scan completed successfully.

Total packets sent:                2
Total packet errors:               0
Total packets caught               2
Total packets caught of interest   2
Total ports scanned                1
Total ports open:                  1
Total ports unknown:               0
root@Kali2:~#
```

Command **firewalk -n –p TCP -S 25 –d 25 192.168.9.1 192.168.68.12** was used to test if there is an ACL rule for port 25.

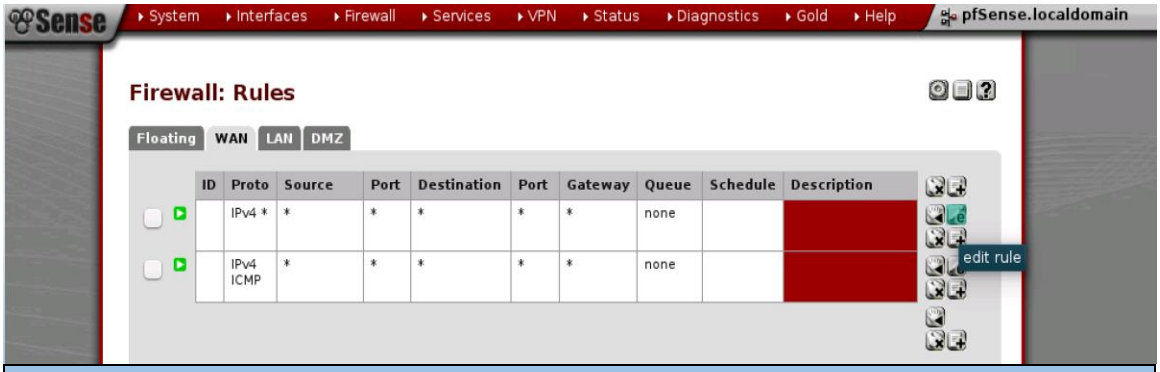
6. Ports 53 to port 80

```
root@Kali2:~# firewalk -S 53-80 -n -p TCP 192.168.9.1 192.168.68.12
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 33434
Hotfoot through 192.168.9.1 using 192.168.68.12 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.9.1]
Binding host reached.
Scan bound at 2 hops.
Scanning Phase:
port  53: A! open (port not listen) [192.168.68.12]
port  54: A! open (port not listen) [192.168.68.12]
port  55: A! open (port not listen) [192.168.68.12]
port  56: A! open (port not listen) [192.168.68.12]
port  57: A! open (port not listen) [192.168.68.12]
port  58: A! open (port not listen) [192.168.68.12]
port  59: A! open (port not listen) [192.168.68.12]
port  60: A! open (port not listen) [192.168.68.12]
port  61: A! open (port not listen) [192.168.68.12]
port  62: A! open (port not listen) [192.168.68.12]
port  63: A! open (port not listen) [192.168.68.12]
port  64: A! open (port not listen) [192.168.68.12]
port  65: A! open (port not listen) [192.168.68.12]
port  66: A! open (port not listen) [192.168.68.12]
port  67: A! open (port not listen) [192.168.68.12]
port  68: A! open (port not listen) [192.168.68.12]
port  69: A! open (port not listen) [192.168.68.12]
port  70: A! open (port not listen) [192.168.68.12]
port  71: A! open (port not listen) [192.168.68.12]
port  72: A! open (port not listen) [192.168.68.12]
port  73: A! open (port not listen) [192.168.68.12]
port  74: A! open (port not listen) [192.168.68.12]
port  75: A! open (port not listen) [192.168.68.12]
port  76: A! open (port not listen) [192.168.68.12]
port  77: A! open (port not listen) [192.168.68.12]
port  78: A! open (port not listen) [192.168.68.12]
port  79: A! open (port not listen) [192.168.68.12]
port  80: A! open (port listen) [192.168.68.12]

Scan completed successfully.

Total packets sent:                29
Total packet errors:               0
Total packets caught               29
Total packets caught of interest   29
Total ports scanned                28
Total ports open:                  28
Total ports unknown:               0
root@Kali2:~#
```

To use firewalk against a range of ports between 53-80, I input command **firewalk -S 53-80 –n –p TCP 192.168.9.1 192.168.68.12**

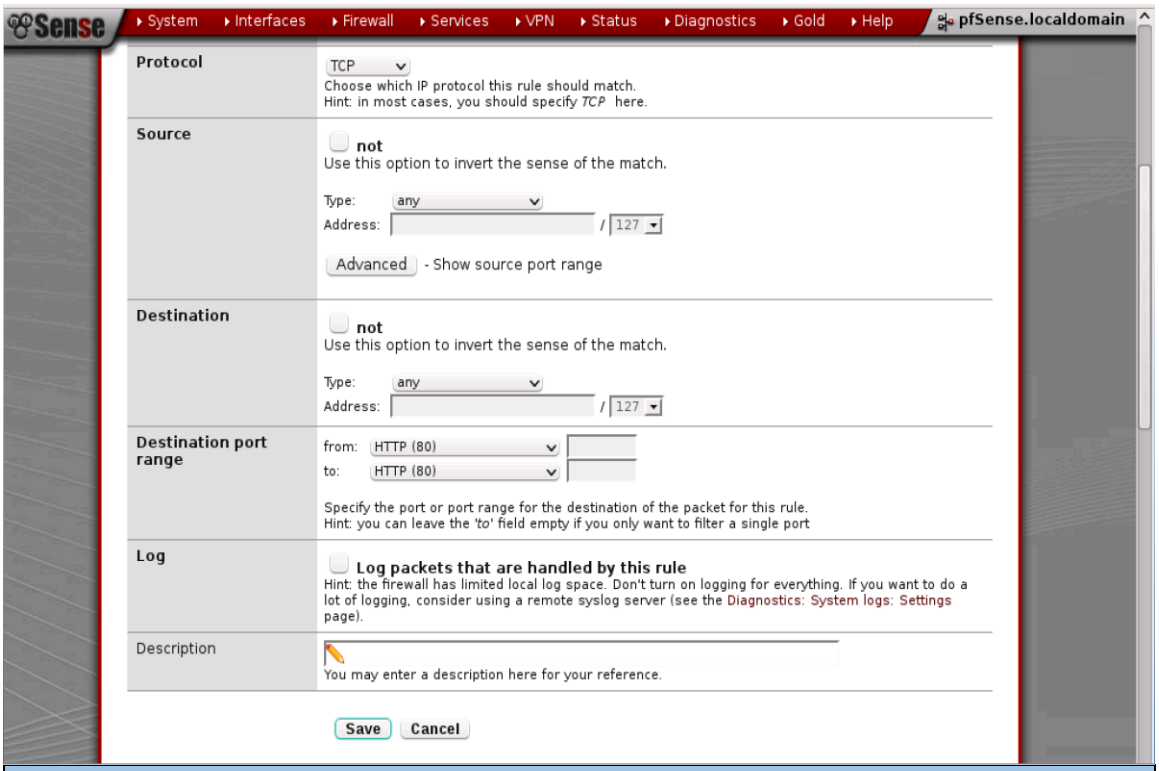
3. Configuring ACL Rules

1. OpenSUSE VM



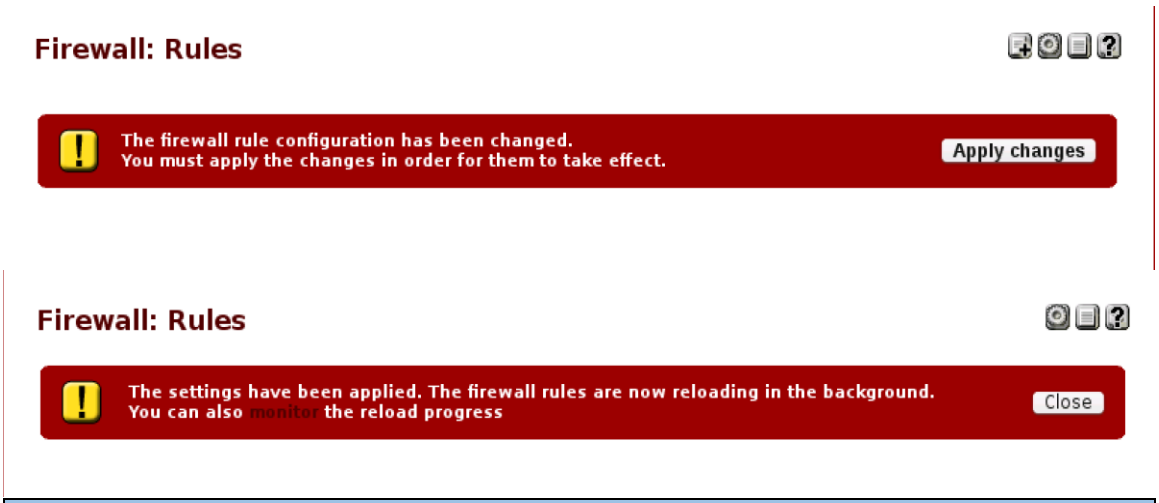
Navigated back to the OpenSUSE Virtual Machine and from the **Firewall: Rules** page, clicked the first Edit Rule icon to edit the first WAN rule.

2. Edit page



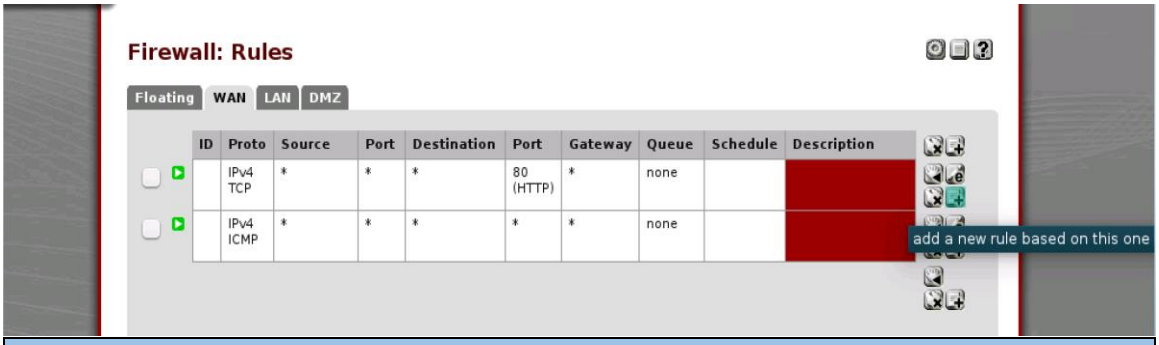
I configured the edit page to reflect the below information:
Protocol: **TCP**
Destination port range:
from: **HTTP (80)**
to: **HTTP (80)**
I left everything else in default and I clicked **Save** after I was done inputting the necessary information

3. Apply changes



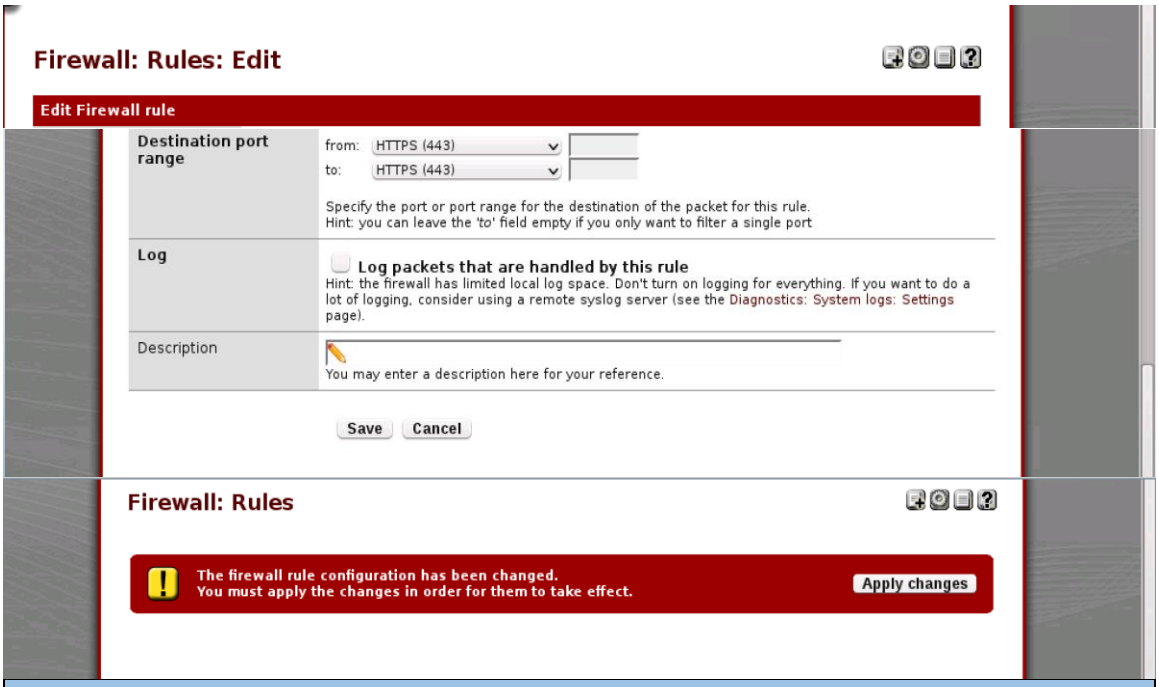
Once the page redirects, I click on the **Apply changes** button that appears at the top of the page.

4. New rule



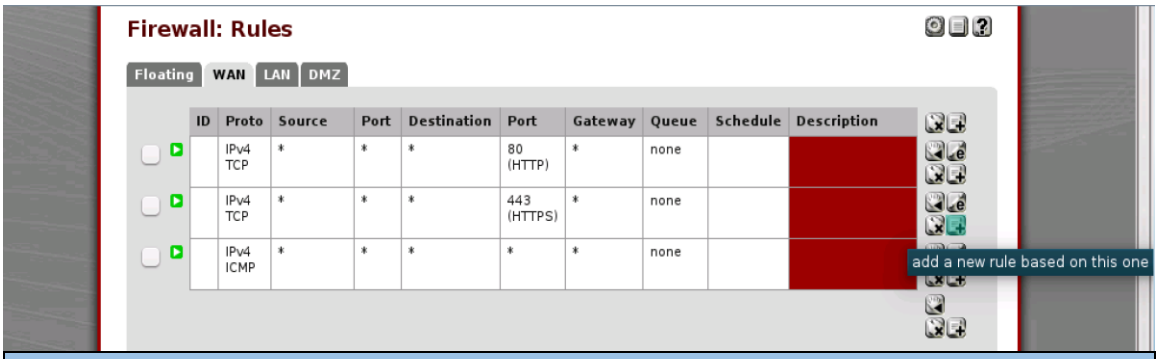
Once the edited changes have been applied, I click the **add a new rule based on this one (+)** icon next to the first rule.

5. Firewall: Rules: Edit page



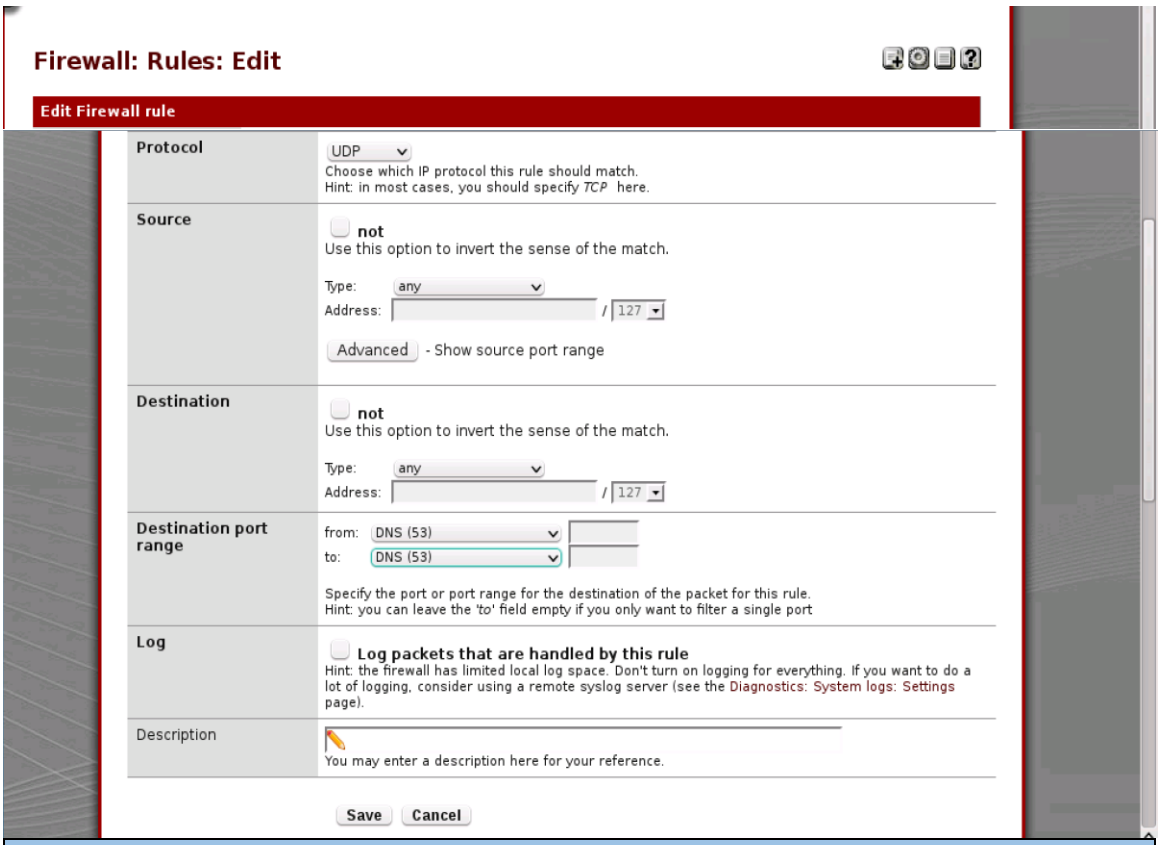
On the Firewall: Rules: Edit page, I chose **HTTP (443)** as the from: and to: for Destination port range and I left the rest at their default settings. Clicked the **Save** button to have my choices saved. Once the page redirected, I clicked the **Apply changes** button.

6. Firewall: Rules: Edit page



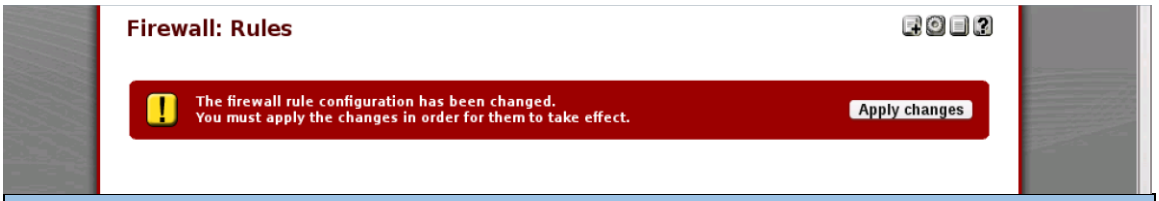
Clicked the **add a new rule based on this one (+)** icon next to the last rule.

7. Firewall: Rules: Edit page



On the Firewall: Rules: Edit page, I configured the information to reflect:
Protocol: **UDP**
Destination port range:
from: **DNS (53)**
to: **DNS (53)**
I left everything else on default and **clicked** Save.

8. Apply changes



Clicked **Apply** changes

4. Test Configured Firewall Rules with Firewalk

1. Kali Linux VM

```
root@Kali2:~# firewalk -n -p TCP -S 23 -d 23 192.168.9.1 192.168.68.12
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 23
Hotfoot through 192.168.9.1 using 192.168.68.12 as a metric.
Ramping Phase:
 1 (TTL  1): *no response*
 2 (TTL  2): *no response*
 3 (TTL  3): *no response*
 4 (TTL  4): *no response*
 5 (TTL  5): *no response*
 6 (TTL  6): *no response*
 7 (TTL  7): *no response*
 8 (TTL  8): *no response*
 9 (TTL  9): *no response*
10 (TTL 10): *no response*
11 (TTL 11): *no response*
```

Navigated back to the terminal and inputted the command **firewalk -n –p TCP -S 23 –d 23 192.168.9.1 192.168.68.12** to try port 23 with firewalk.

3. Port 53

```
root@Kali2:~# firewalk -n -p TCP -S 53 -d 53 192.168.9.1 192.168.68.12
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
TCP-based scan.
Ramping phase source port: 53, destination port: 53
Hotfoot through 192.168.9.1 using 192.168.68.12 as a metric.
Ramping Phase:
 1 (TTL  1): *no response*
 2 (TTL  2): *no response*
 3 (TTL  3): *no response*
 4 (TTL  4): *no response*
 5 (TTL  5): *no response*
 6 (TTL  6): *no response*
 7 (TTL  7): *no response*
 8 (TTL  8): *no response*
 9 (TTL  9): *no response*
10 (TTL 10): *no response*
11 (TTL 11): *no response*
```

inputted the command **firewalk -n –p TCP -S 53 –d 53 192.168.9.1 192.168.68.12** to try port 53 with firewalk.

4. Port 53 with UDP

```
root@Kali2:~# firewalk -n -p UDP -S 53 -d 53 192.168.9.1 192.168.68.12
Firewalk 5.0 [gateway ACL scanner]
Firewalk state initialization completed successfully.
UDP-based scan.
Ramping phase source port: 53, destination port: 53
Hotfoot through 192.168.9.1 using 192.168.68.12 as a metric.
Ramping Phase:
 1 (TTL  1): expired [192.168.9.1]
Binding host reached.
Scan bound at 2 hops.
Scanning Phase:
port  53: A! unknown (unreach ICMP_UNREACH_PORT) [192.168.68.12]

Scan completed successfully.

Total packets sent:                2
Total packet errors:               0
Total packets caught               4
Total packets caught of interest   2
Total ports scanned                1
Total ports open:                  0
Total ports unknown:               1
root@Kali2:~#
```

Attempted port 53 again but this time with UDP selected **firewalk -n –p UDP -S 53 –d 53 192.168.9.1 192.168.68.12**. I noticed that a response is now given, this response, ICMP_UNREACH_PORT indicates that a rule may be in place.

Reflections

1. **What is the difference between Cisco Extended ACL vs Standard ACL?**

   With Standard ACL, source addresses are checked, and protocols are either permitted or denied. Extended ACL examines the source and destination addresses, allowing or disallowing particular protocols as well as an application's source and destination TCP and UDP ports.

2. **Why is it important for an ethical hacker to learn about open ports on the firewall?**

   It is important for an ethical hacker to learn about open ports on the firewall because doing so helps with familiarizing themselves in determining which hacking software or program is best suited for utilizing the port that is open on the firewall.

3. **Research, what is the difference between Routed Firewall vs Transparent Firewall mode?**

   Routed Firewall is when each firewall interface is linked to a distinct IP subnet and allocated an IP address on that subnet.
   A transparent firewall mode has no IP addresses, and it cannot be detected or manipulated.