

# Foolish Firewall Configurations

Author: Mike Korcha

**Framework Category:** Protect and Defend

**Specialty Area:** Cybersecurity Defense Infrastructure Support

**Work Role:** Cyber Defense Infrastructure Support Specialist

**Task Description:** Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems). (T0438)

## Scenario

An intern of ours installed a new core firewall about a month ago. A recent network security audit has shown that, while being installed, the new firewall was not properly configured. Additionally, three of our server's host firewalls have not been configured to filter inbound traffic properly. You are tasked with configuring the firewalls on each ill-configured host as well as the core firewall to reject all but necessary traffic.

## Additional Information

More details and objectives about this challenge will be introduced during the challenge meeting, which will start once you begin deploying the challenge.

You will be able to check your progress during this challenge using the check panel within the workspace once the challenge is deployed. The checks within the check panel report on the state of some or all of the required tasks within the challenge.

Once you have completed the requested tasks, you will need to document the methodology you used with as much detail and professionalism as necessary. This should be done on the documentation tab within the workspace once the challenge is deployed. Below the main documentation section be sure to include a tagged list of applications you used to complete the challenge.

Your username/password to access all virtual machines and services within the workspace will be the following...

Username: playerone

Password: password123

The username/password used to access the Firewall's web interface within the workspace will be the following...

Username: admin

Password: password123

Virtual Machines				Checks				
Machine Name	Status	Actions	Open Console ?	Status	Check Description	Check Type	Check State	Last Changed
Asteroids-PoS	Powered On	Action ▾	HTML5 VMRC	✓	Network firewall only allows external HTTP and HTTPS traffic to Prod-Joomla [Approx. 2m Refresh]	Challenge Check ?	Desired State	01:25 PM PDT
Asteroids-Router	Powered On	Action ▾	HTML5 VMRC	✓	Prod-Joomla has HTTP HTTPS and SSH available via host firewall [Should Stay Green]	Availability Check ?	Desired State	09:39 AM PDT
Centipede-PoS	Powered On	Action ▾	HTML5 VMRC	✓	Prod-Joomla only has HTTP HTTPS and SSH available via host firewall	Challenge Check ?	Desired State	11:32 AM PDT
Centipede-Router	Powered On	Action ▾	HTML5 VMRC	✓	Database has MySQL available via host firewall [Should Stay Green]	Availability Check ?	Desired State	09:45 AM PDT
Database	Powered On	Action ▾	HTML5 VMRC	✓	Database only has MySQL available via host firewall	Challenge Check ?	Desired State	09:46 AM PDT
Domain-Controller	Powered On	Action ▾	HTML5 VMRC	✓	Fileshare has SFTP and Samba available via host firewall [Should Stay Green]	Availability Check ?	Desired State	09:39 AM PDT
Fileshare	Powered On	Action ▾	HTML5 VMRC	✓	Fileshare only has SFTP and Samba available via host firewall	Challenge Check ?	Desired State	11:36 AM PDT
Firewall	Powered On	Action ▾	HTML5 VMRC					
Prod-Joomla	Powered On	Action ▾	HTML5 VMRC					
Security-Desk	Powered On	Action ▾	HTML5 VMRC					
Workstation-Desk	Powered On	Action ▾	HTML5 VMRC					

## Meetings Notes

**Ashley Steele** Our managed service provider just sent us their findings from the security audit they conducted for us. Apparently, we aren't really doing anything to limit the traffic coming into our network...

**Ricardo Cortes** We paid a pretty hefty amount of money for that fancy new firewall. Are you telling me that it's just sitting there not being used?

**Jacques Raffin** Wasn't Rob, the intern, put in charge of setting it up? Whose idea was that?

**Ricardo Cortes** I may have had a bit too much confidence in that boy. I'll admit, that was pretty foolish of me.

**Ashley Steele** Regardless, based on what I am seeing, we have issues beyond the main Firewall. Important servers on our internal networks have no host-level firewalls active or configured. This can, and eventually will, cause us issues if anything malicious ever got into our internal network. Defense-in-depth, anyone?

**Jacques Raffin** Someone should try fixing these issues. @playerone, you're our security person. Time to show us what you've got!

**Ricardo Cortes** Yeah, that's a great idea! @playerone, you're pretty new around here. This sounds like just the task to help you get your feet wet.

**Ashley Steele** Alright, @playerone. It looks like it is all up to you. Set up rules on the main Firewall that allow external access to our website which uses http and https via NAT but block everything else. Basically, all external traffic going to the Joomla Website that is not over the VPN tunnels should be directed to the main Firewall's external interface and then be routed internally to Prod-Joomla. Also, make sure you don't do anything to block VPN access, don't want to block out our MSP or take down our storefront locations. Once you're done with that, set up the host firewalls on Prod-Joomla, Fileshare, and Database.

**Jacques Raffin** Just to be clear, Prod-Joomla should allow only HTTP, HTTPS, and SSH traffic through on their standard ports. Let's see... Fileshare should have the SSH port open for SFTP access. It should also have ports 137, 138, 139, and 445 open for anything samba needs. Database, however, should only have the MySQL port, 3306, open.

**Ricardo Cortes** Get to it, @playerone! I know you won't disappoint me like Rob did.

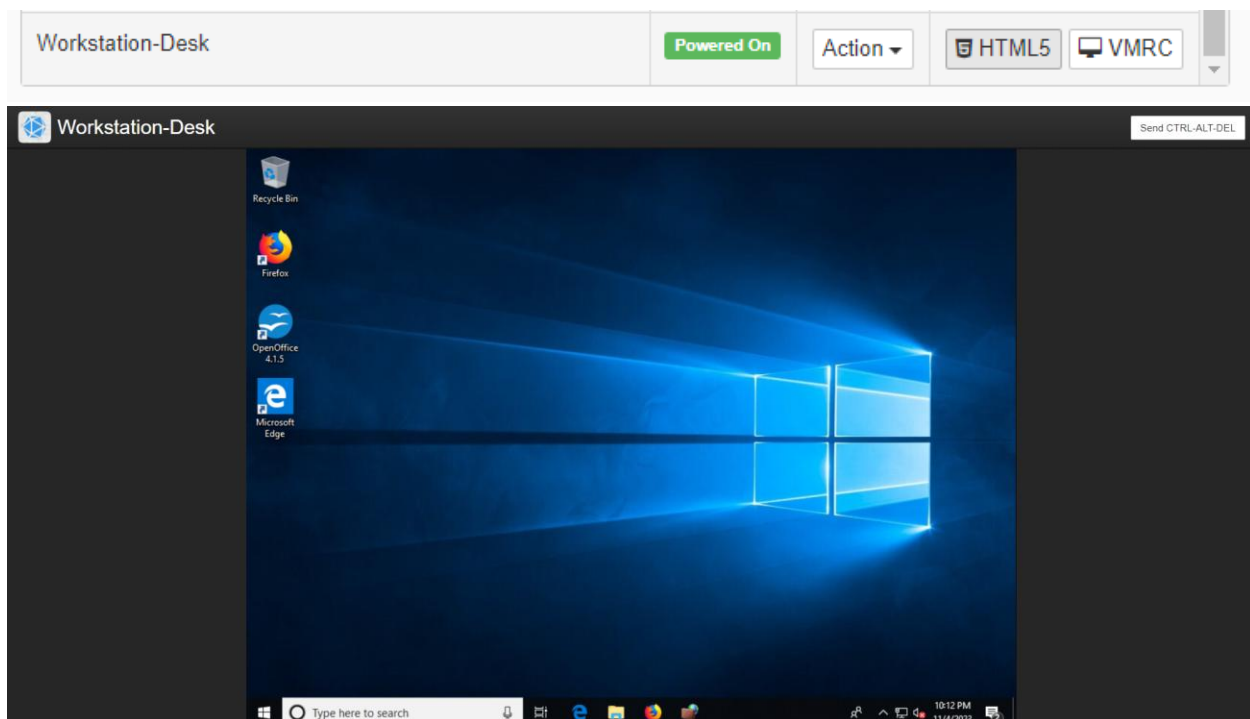
## Network Map



## Setting up a Network Firewall

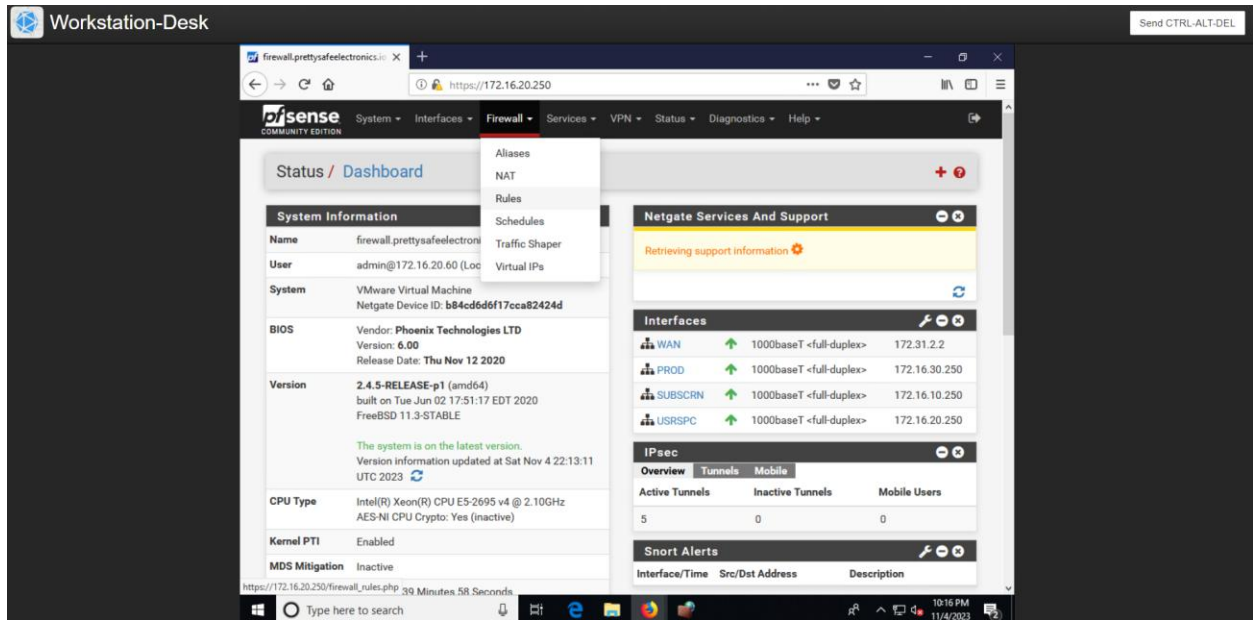
We configured the network firewall to selectively allow external HTTP and HTTPS traffic to the web server using Network Address Translation (NAT). This was achieved by setting up three specific rules in the firewall's interface: two to permit traffic through standard web ports 80 (HTTP) and 443 (HTTPS), and a third to deny all other non-web traffic. This configuration ensures that only web traffic can reach the Joomla website while maintaining the integrity of VPN access and not disrupting Managed Service Provider (MSP) connections or the operations of retail locations. Additionally, firewall, NAT, and port forwarding settings can be managed remotely by logging into the firewall using the IP address 10.16.172.100 with the username "playerone" and password "password123."

## Launching the Workstation-Desk Machine [ HTML 5 ]

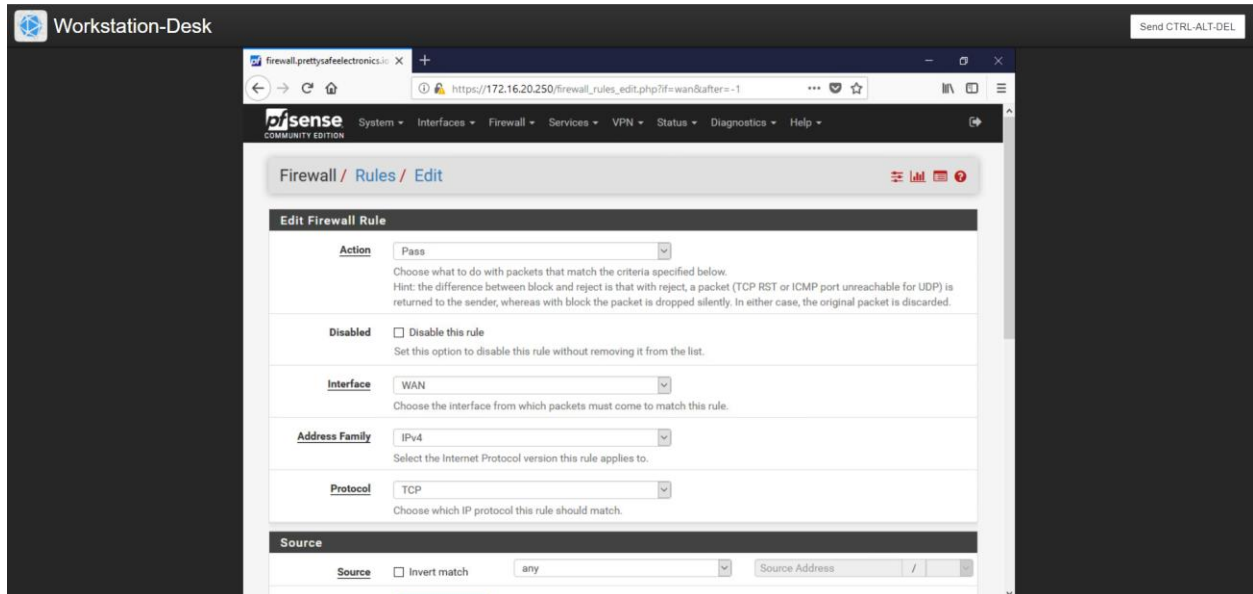


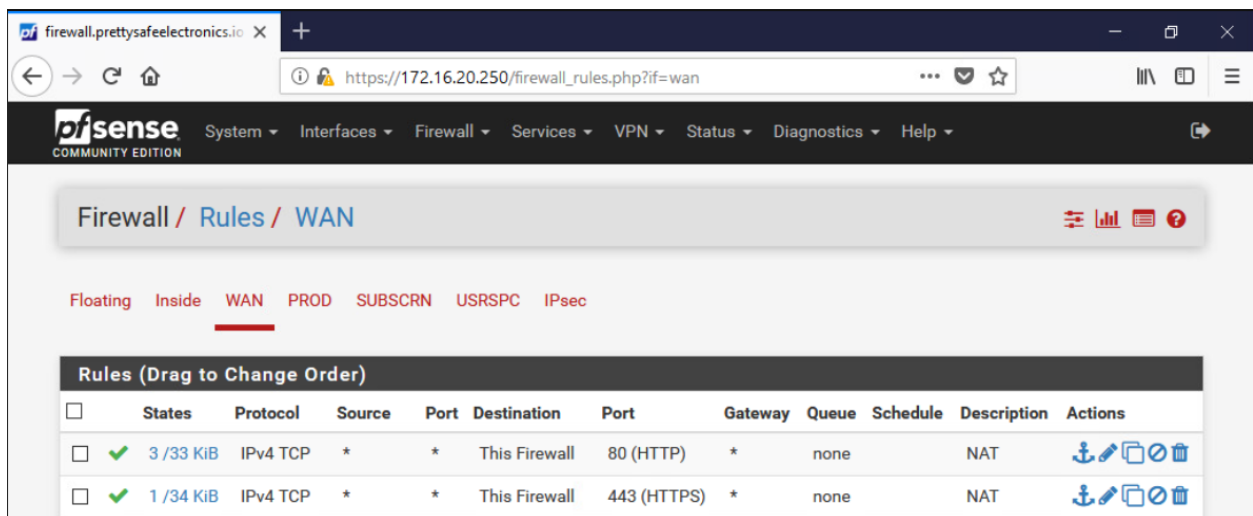
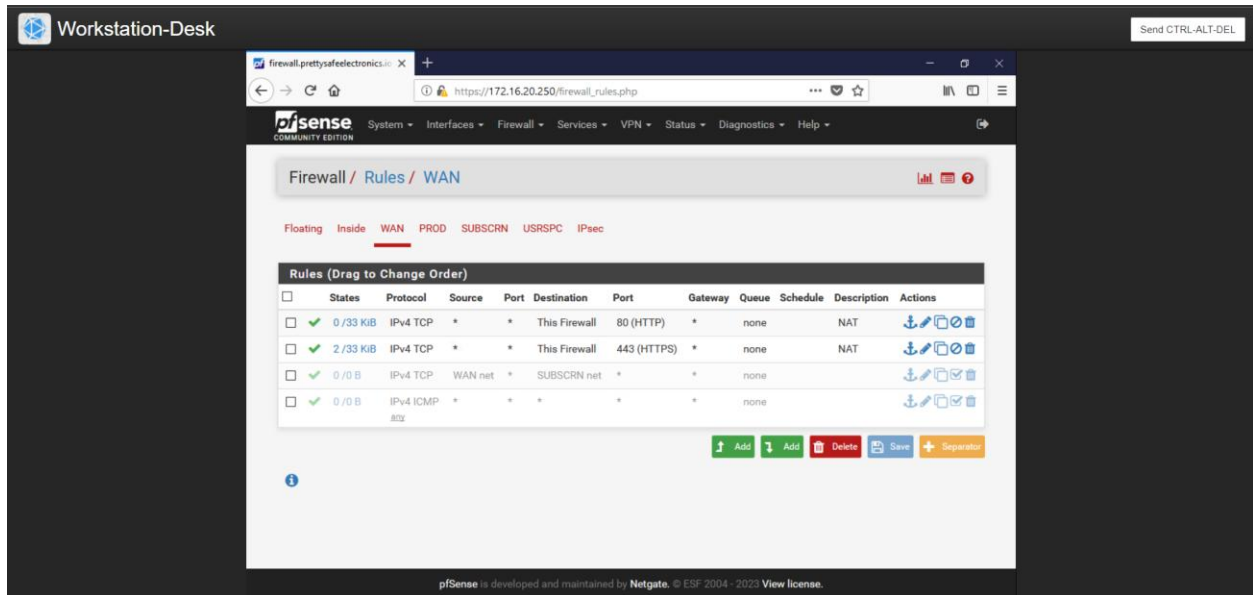
We're going to launch the search engine and go to 172.16.20.250.

Firewall > Rules



We can add the desired configuration after clicking "Add."





These two directives were to pass port 80 and port 443 to the web server via the firewall.

We have successfully completed Task 1

Checks				
Status	Check Description	Check Type	Check State	Last Changed
✓	Network firewall only allows external HTTP and HTTPS traffic to Prod-Joomla [Approx. 2m Refresh]	Challenge Check ?	Desired State	01:25 PM PDT

## Web Server Host Firewall Configuration

### Prod-Joomla

We have updated the iptables ruleset for Prod-Joomla to permit only HTTP, HTTPS, and SSH traffic. This involved adding specific rules to accept connections on their respective default ports: 80 for HTTP, 443 for HTTPS, and 22 for SSH. We used the command format ``sudo iptables -A INPUT -p tcp --dport [port number] -j ACCEPT`` to allow incoming connections on these ports. Additionally, we set a default policy to drop all other traffic using ``sudo iptables -A INPUT -j DROP``. The command ``sudo iptables -L -v`` was used to list the current iptables ruleset with verbose output.

Making sure this Ubuntu webserver's iptables firewall was up to date was my first step.

```
playerone@Prod-Joomla:~$ sudo apt-get install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
iptables is already the newest version (1.6.0+snapshot20161117-6).
0 upgraded, 0 newly installed, 0 to remove and 136 not upgraded.
playerone@Prod-Joomla:~$ _
```

I then reviewed the previously established rules. It didn't seem like any were in place.

```
playerone@Prod-Joomla:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                                   destination

Chain FORWARD (policy ACCEPT)
target     prot opt source                                   destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                                   destination
playerone@Prod-Joomla:~$ _
```

I then updated the web server with the accepted rules.

```
playerone@Prod-Joomla:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
playerone@Prod-Joomla:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
playerone@Prod-Joomla:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
playerone@Prod-Joomla:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                                   destination
ACCEPT     tcp  --  anywhere                                 anywhere    tcp dpt:http
ACCEPT     tcp  --  anywhere                                 anywhere    tcp dpt:https
ACCEPT     tcp  --  anywhere                                 anywhere    tcp dpt:ssh

Chain FORWARD (policy ACCEPT)
target     prot opt source                                   destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                                   destination
```

I then included a rule that drops all other traffic to unlisted ports.

```
playerone@Prod-Joomla:~$ sudo iptables -A INPUT -j DROP
playerone@Prod-Joomla:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:http
ACCEPT     tcp  --  anywhere              anywhere               tcp dpt:https
ACCEPT     tcp  --  anywhere              anywhere               tcp dpt:ssh
DROP       all  --  anywhere              anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

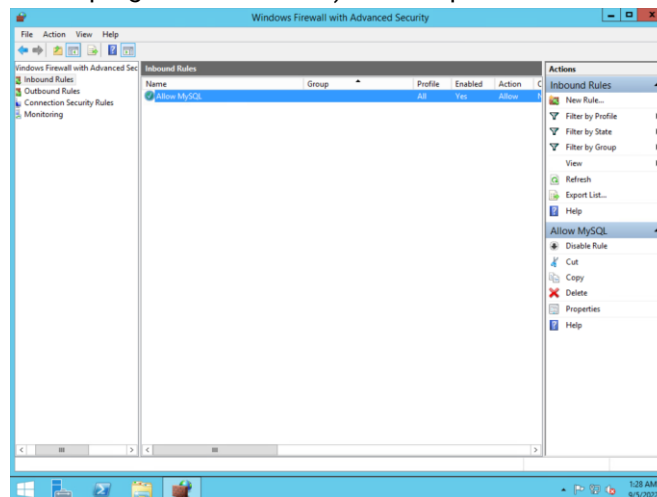
Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

✓	Prod-Joomla has HTTP HTTPS and SSH available via host firewall [Should Stay Green]	Availability Check ?	Desired State	09:39 AM PDT
✓	Prod-Joomla only has HTTP HTTPS and SSH available via host firewall	Challenge Check ?	Desired State	11:32 AM PDT



## Database Server

For this round of the assignment, I had to visit a Windows-based server and set up the host-based firewall to only allow MySQL on port 3306. As soon as I went on the system, the firewall was off, so I made sure to turn it on first. Next, I added a rule to the incoming rules allowing traffic to flow over port 3306. I then checked to see if implicit deny was activated for incoming traffic.

However, the database should only have port 3306 (for MySQL) available. We Navigated it to Windows Firewall, we can locate it by clicking on the bottom left of the screen and using the magnifying glass to type the word "firewall" into the program search field). Include pertinent InBound rules.





	Database has MySQL available via host firewall [Should Stay Green]	Availability Check ?	Desired State	09:45 AM PDT
	Database only has MySQL available via host firewall	Challenge Check ?	Desired State	09:46 AM PDT

## Fileshare Firewall Configuration

Since this was a Linux machine, I started by looking at the existing firewall rules. It didn't take me long to understand that the system was missing its firewall. Installing iptables was my first step.

We Shared the files For SFTP access, Fileshare's SSH port has to be open. Additionally, ports 137, 138, 139, and 445 ought to be available for everything that Samba requires. Iptables installation is required. apt-get update sudo Install iptables with sudo apt-get Then, we proceeded as we chose, akin to prod-joomla



```
playerone@fileshare:~$ sudo iptables -L
sudo: iptables: command not found
playerone@fileshare:~$ sudo apt install iptables
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libnftnl0
The following NEW packages will be installed:
  iptables libnftnl0
0 upgraded, 2 newly installed, 0 to remove and 97 not upgraded.
Need to get 279 kB of archives.
After this operation, 1,724 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 libnftnl0 amd64 1.0.1-3 [13.3 kB]
Get:2 http://us.archive.ubuntu.com/ubuntu xenial/main amd64 iptables amd64 1.6.0-2ubuntu3 [266 kB]
Fetched 279 kB in 0s (468 kB/s)
Selecting previously unselected package libnftnl0:amd64.
(Reading database ... 55191 files and directories currently installed.)
Preparing to unpack .../libnftnl0_1.0.1-3_amd64.deb ...
Unpacking libnftnl0:amd64 (1.0.1-3) ...
Selecting previously unselected package iptables.
Preparing to unpack .../iptables_1.6.0-2ubuntu3_amd64.deb ...
Unpacking iptables (1.6.0-2ubuntu3) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
Processing triggers for man-db (2.7.5-1) ...
Setting up libnftnl0:amd64 (1.0.1-3) ...
Setting up iptables (1.6.0-2ubuntu3) ...
Processing triggers for libc-bin (2.23-0ubuntu9) ...
playerone@fileshare:~$ _
```

I then added all of my rules to the iptables to configure the firewall.

```
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 137 -j ACCEPT
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 138 -j ACCEPT
iptables v1.6.0: unknown protocol "tcp" specified
Try 'iptables -h' or 'iptables --help' for more information.
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 138 -j ACCEPT
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 139 -j ACCEPT
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 445 -j ACCEPT
playerone@fileshare:~$ sudo iptables -A INPUT -j DROP
playerone@fileshare:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination            tcp dpt:ssh
ACCEPT    tcp  --  anywhere               anywhere               tcp dpt:netbios-ns
ACCEPT    tcp  --  anywhere               anywhere               tcp dpt:netbios-dgm
ACCEPT    tcp  --  anywhere               anywhere               tcp dpt:netbios-ssn
ACCEPT    tcp  --  anywhere               anywhere               tcp dpt:microsoft-ds
DROP      all  --  anywhere               anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
```

	Fileshare has SFTP and Samba available via host firewall [Should Stay Green]	Availability Check <sup>?</sup>	Desired State	09:39 AM PDT
	Fileshare only has SFTP and Samba available via host firewall	Challenge Check <sup>?</sup>	Desired State	11:36 AM PDT

## Commands Used

```
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 137 -j ACCEPT
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 138 -j ACCEPT
iptables v1.6.0: unknown protocol "tcp" specified
```

Try `iptables -h` or `iptables --help` for more information.

```
playerone@fileshare:~$ sudo iptables -A INPUT -p udp --dport 138 -j ACCEPT
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 139 -j ACCEPT
playerone@fileshare:~$ sudo iptables -A INPUT -p tcp --dport 445 -j ACCEPT
playerone@fileshare:~$ sudo iptables -L
playerone@fileshare:~$ sudo iptables -L
playerone@fileshare:~$ sudo apt install iptables
playerone@Prod-Joomla:~$ sudo iptables -A INPUT -j DROP
playerone@Prod-Joomla:~$ sudo iptables -L
playerone@Prod-Joomla:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
playerone@Prod-Joomla:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
playerone@Prod-Joomla:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
playerone@Prod-Joomla:~$ sudo iptables -L
playerone@Prod-Joomla:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
playerone@Prod-Joomla:~$ _
playerone@Prod-Joomla:~$ sudo apt-get install iptables
playerone@Prod-Joomla:~$ _
sudo apt-get install iptables
```

## Summary

As this was my first NICE challenge, I'm quite pleased with the result. Firewall setting is one of the best ways to practice defense in depth. If your network or system does not have a properly configured firewall, it is open to many malicious actors.

Virtual Machines			
Machine Name	Status	Actions	Open Console ?
Asteroids-PoS	Powered On	Action ▾	HTML5 VMRC
Asteroids-Router	Powered On	Action ▾	HTML5 VMRC
Centipede-PoS	Powered On	Action ▾	HTML5 VMRC
Centipede-Router	Powered On	Action ▾	HTML5 VMRC
Database	Powered On	Action ▾	HTML5 VMRC
Domain-Controller	Powered On	Action ▾	HTML5 VMRC
Fileshare	Powered On	Action ▾	HTML5 VMRC
Firewall	Powered On	Action ▾	HTML5 VMRC
Prod-Joomla	Powered On	Action ▾	HTML5 VMRC
Security-Desk	Powered On	Action ▾	HTML5 VMRC
Workstation-Desk	Powered On	Action ▾	HTML5 VMRC

Checks				
Status	Check Description	Check Type	Check State	Last Changed
✓	Network firewall only allows external HTTP and HTTPS traffic to Prod-Joomla [Approx. 2m Refresh]	Challenge Check ?	Desired State	01:25 PM PDT
✓	Prod-Joomla has HTTP HTTPS and SSH available via host firewall [Should Stay Green]	Availability Check ?	Desired State	09:39 AM PDT
✓	Prod-Joomla only has HTTP HTTPS and SSH available via host firewall	Challenge Check ?	Desired State	11:32 AM PDT
✓	Database has MySQL available via host firewall [Should Stay Green]	Availability Check ?	Desired State	09:45 AM PDT
✓	Database only has MySQL available via host firewall	Challenge Check ?	Desired State	09:46 AM PDT
✓	Fileshare has SFTP and Samba available via host firewall [Should Stay Green]	Availability Check ?	Desired State	09:39 AM PDT
✓	Fileshare only has SFTP and Samba available via host firewall	Challenge Check ?	Desired State	11:36 AM PDT