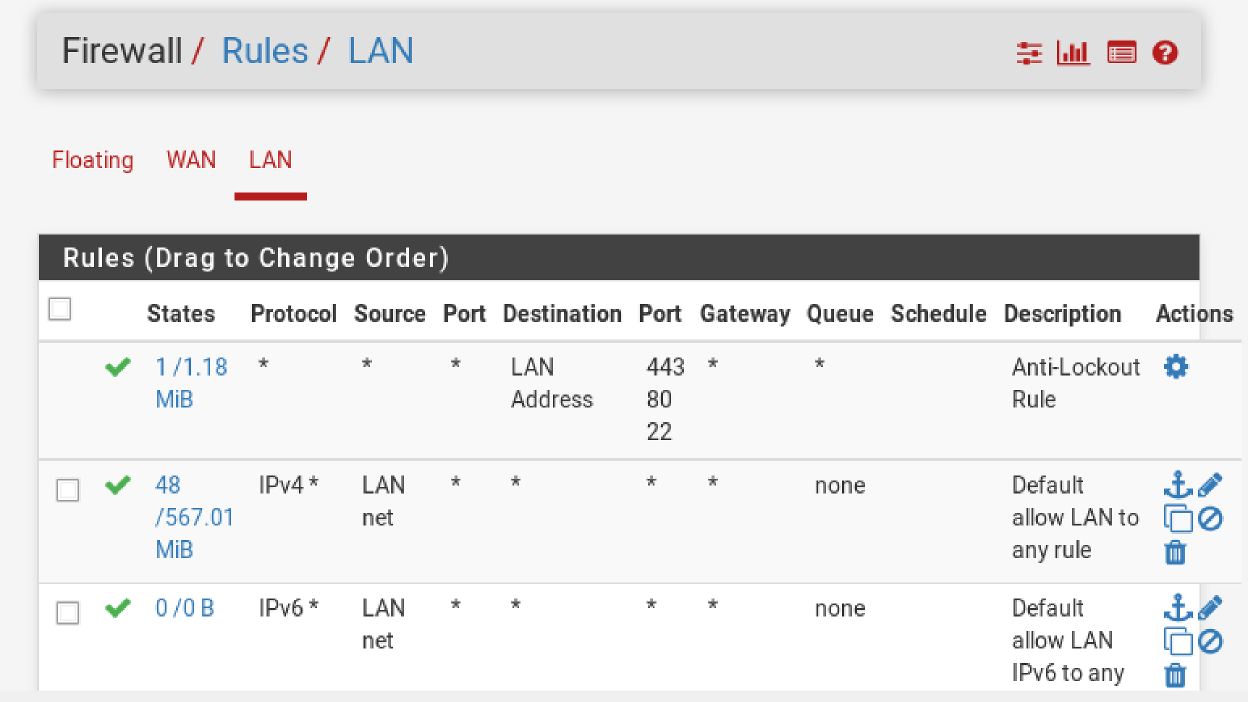
Section 1. Blocking HTTP

1. Mark down your ip addresses

Ubuntu1: __________________ (run ifconfig and look at eth0 inet)

Pfsense LAN ip: ______________________

1. On your ubuntu machine type in the pfsense LAN ip
2. Go to Firewall - Rules - LAN



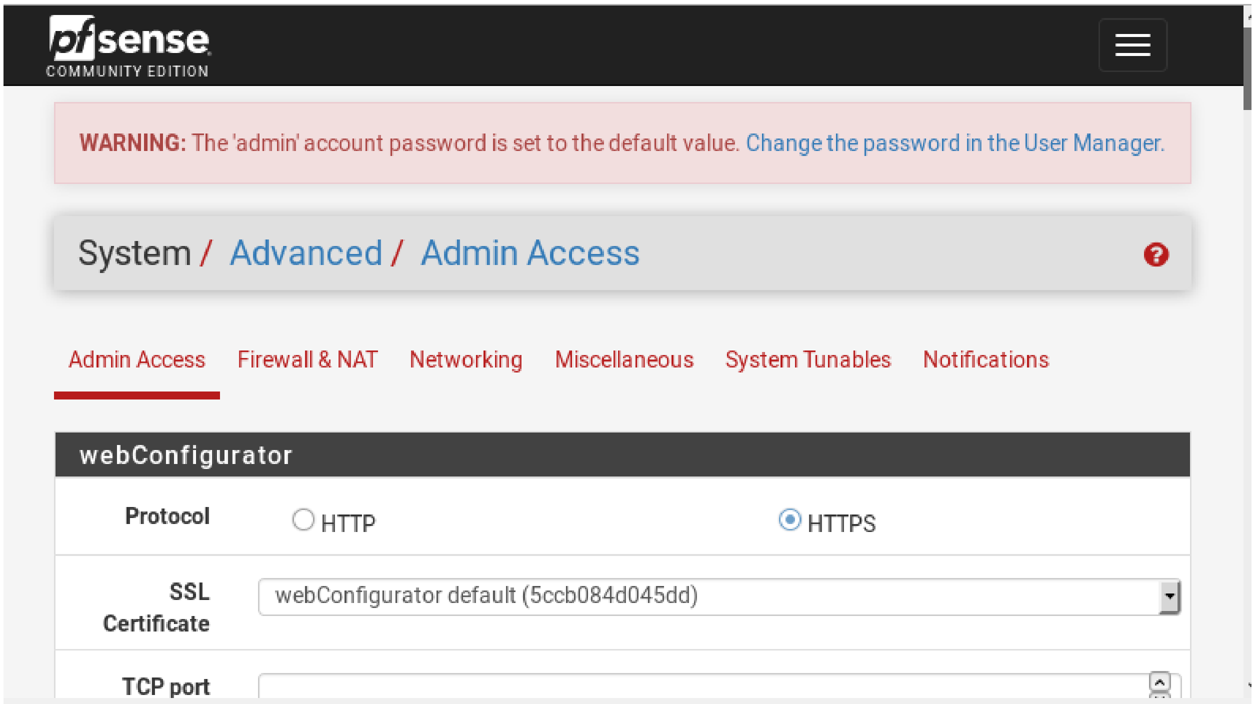
Firewall / Rules / LAN

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1 /1.18 MiB	*	*	*	LAN Address	443 80 22	*	*		Anti-Lockout Rule	
□	✓	48 /567.01 MiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any	

3. Notice the Anti-Lockout Rule that is allowing all web traffic, due to order of precedence we have to remove this rule

4. Go to system – advanced – admin access and scroll down until you see anti-lockout. Check the box. Scroll all the way down and hit save



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

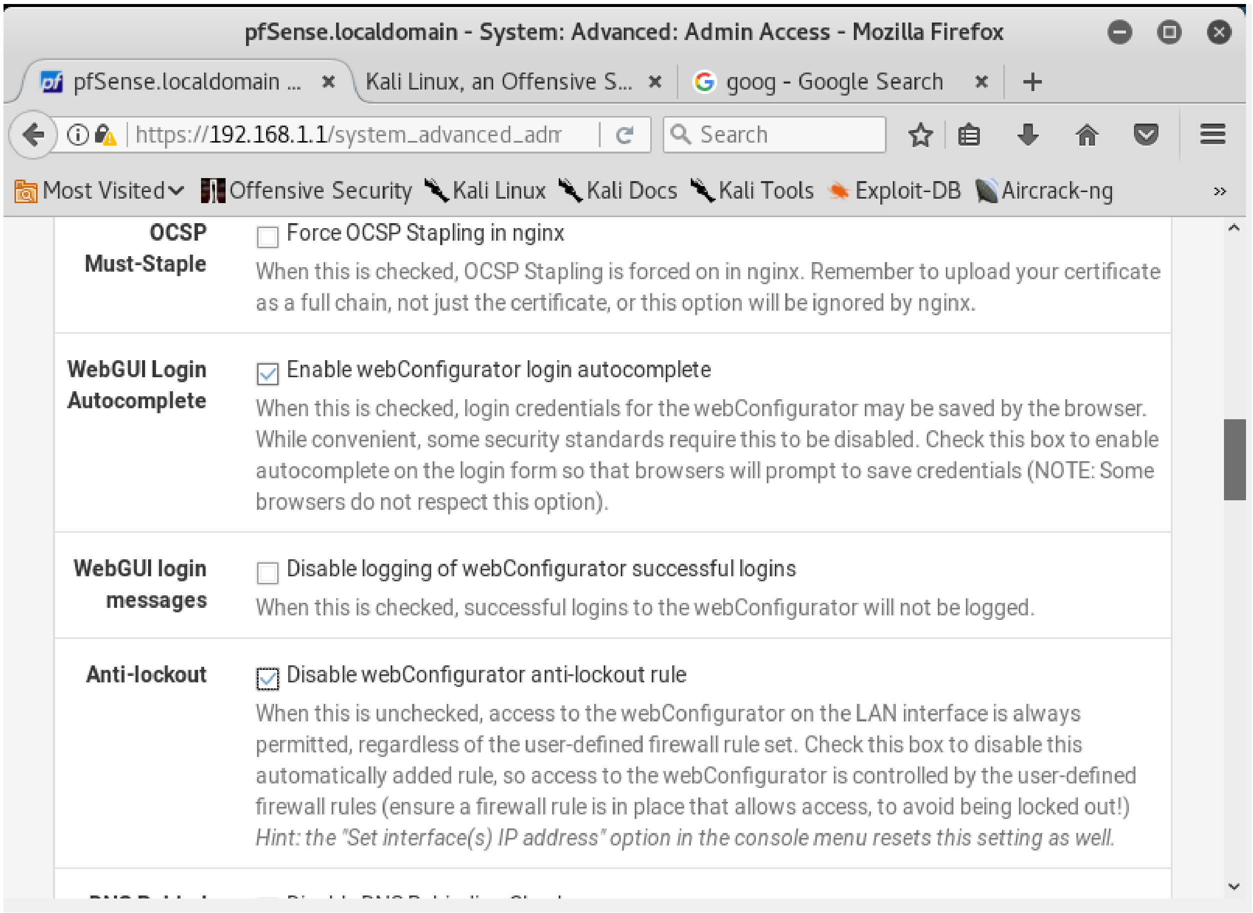
System / Advanced / Admin Access

webConfigurator

Protocol ○ HTTP ● HTTPS

SSL Certificate: webConfigurator default (5ccb084d045dd)

TCP port


pfSense.localdomain - System: Advanced: Admin Access - Mozilla Firefox
pfSense.localdomain ...
Kali Linux, an Offensive S...
goog - Google Search
https://192.168.1.1/system_advanced_adm
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng

OCSP Must-Staple: □ Force OCSP Stapling in nginx
When this is checked, OCSP Stapling is forced on in nginx. Remember to upload your certificate as a full chain, not just the certificate, or this option will be ignored by nginx.

WebGUI Login Autocomplete: ☑ Enable webConfigurator login autocomplete
When this is checked, login credentials for the webConfigurator may be saved by the browser. While convenient, some security standards require this to be disabled. Check this box to enable autocomplete on the login form so that browsers will prompt to save credentials (NOTE: Some browsers do not respect this option).

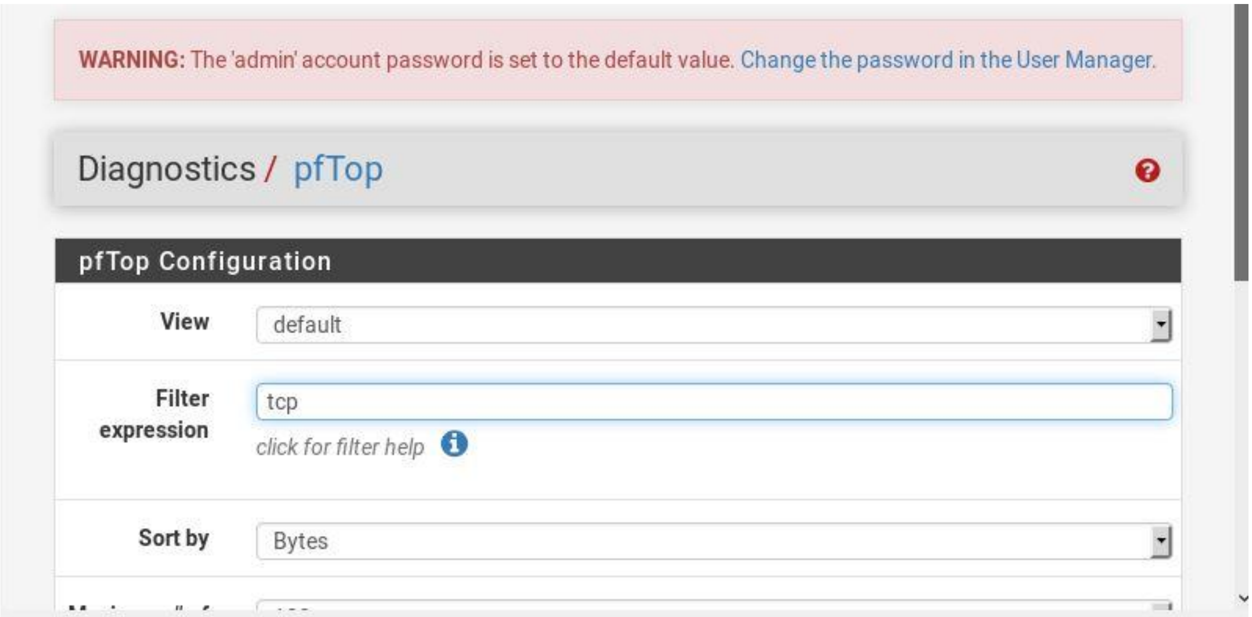
WebGUI login messages: □ Disable logging of webConfigurator successful logins
When this is checked, successful logins to the webConfigurator will not be logged.

Anti-lockout: ☑ Disable webConfigurator anti-lockout rule
When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!) *Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.*

7. Double check to ensure that the anti lockout rule is gone (firewall – rules – lan)

8. On a separate tab go to Tyler’s website

9. Go to diagnostics -pftop



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

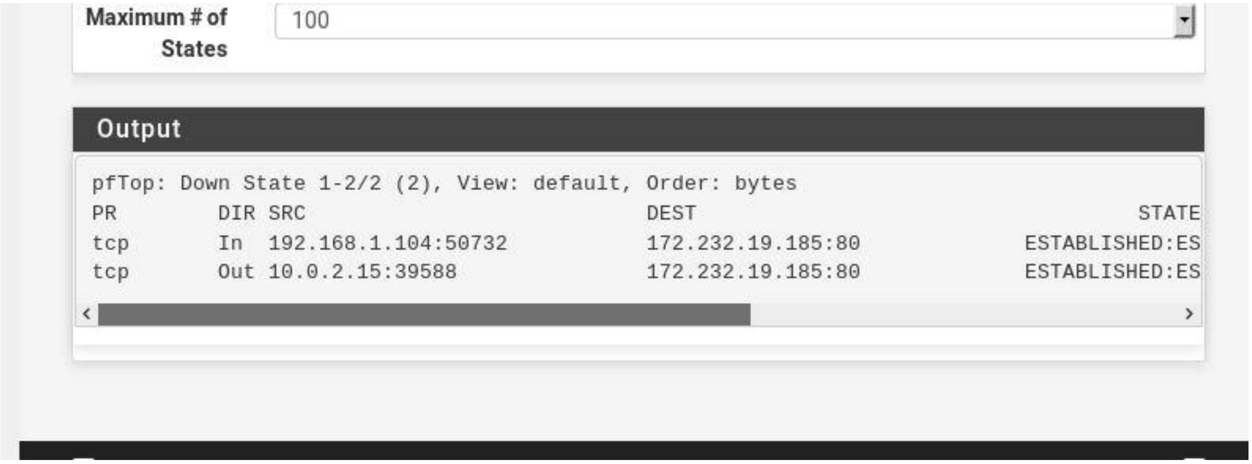
Diagnostics / pfTop

pfTop Configuration

View: default

Filter expression: tcp

Sort by: Bytes



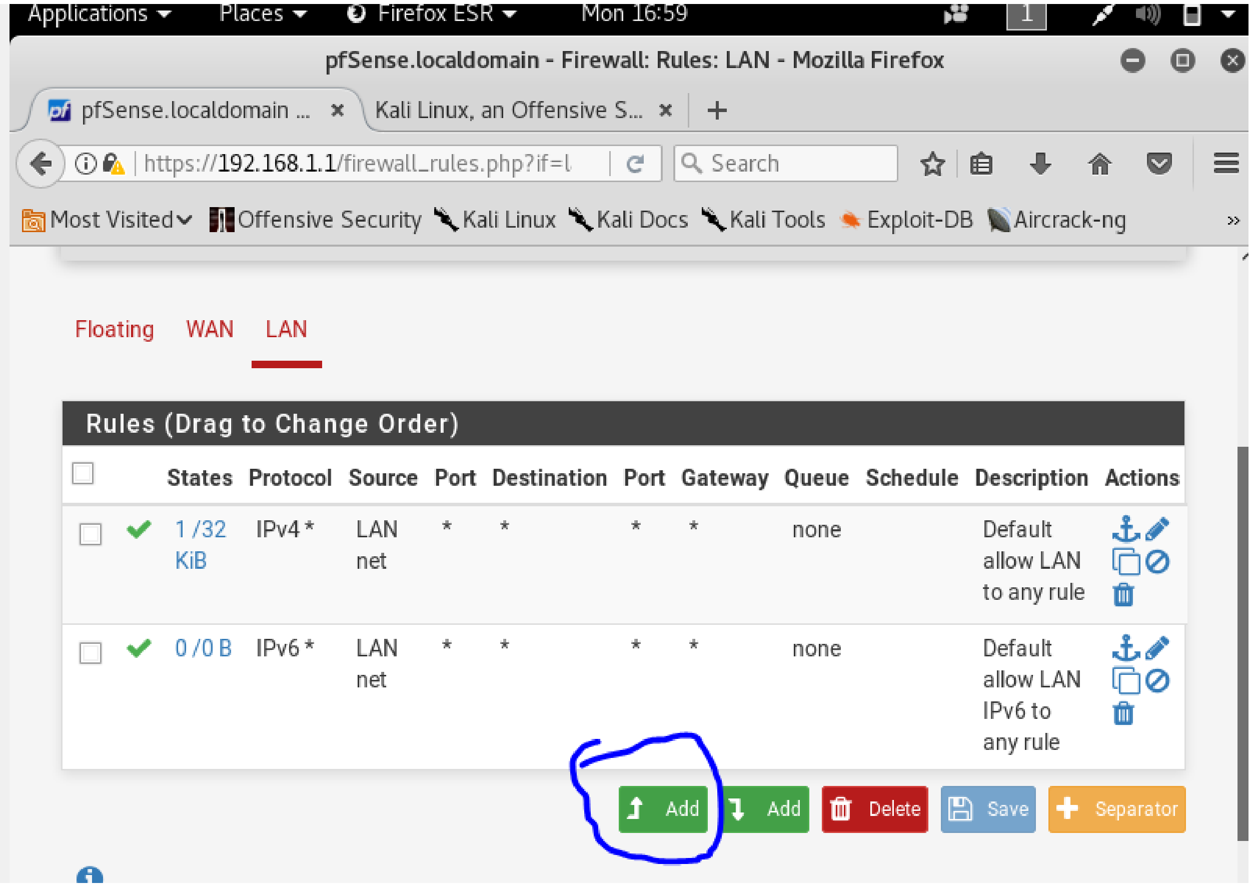
Maximum # of States: 100

Output

```
pfTop: Down State 1-2/2 (2), View: default, Order: bytes
PR        DIR SRC                         DEST                         STATE
tcp       In  192.168.1.104:50732         172.232.19.185:80         ESTABLISHED:ES
tcp       Out 10.0.2.15:39588             172.232.19.185:80         ESTABLISHED:ES
```

10. Find your connection to Tyler’s website, this is what we will be blocking

Click on the add on top button



Rules (Drag to Change Order)

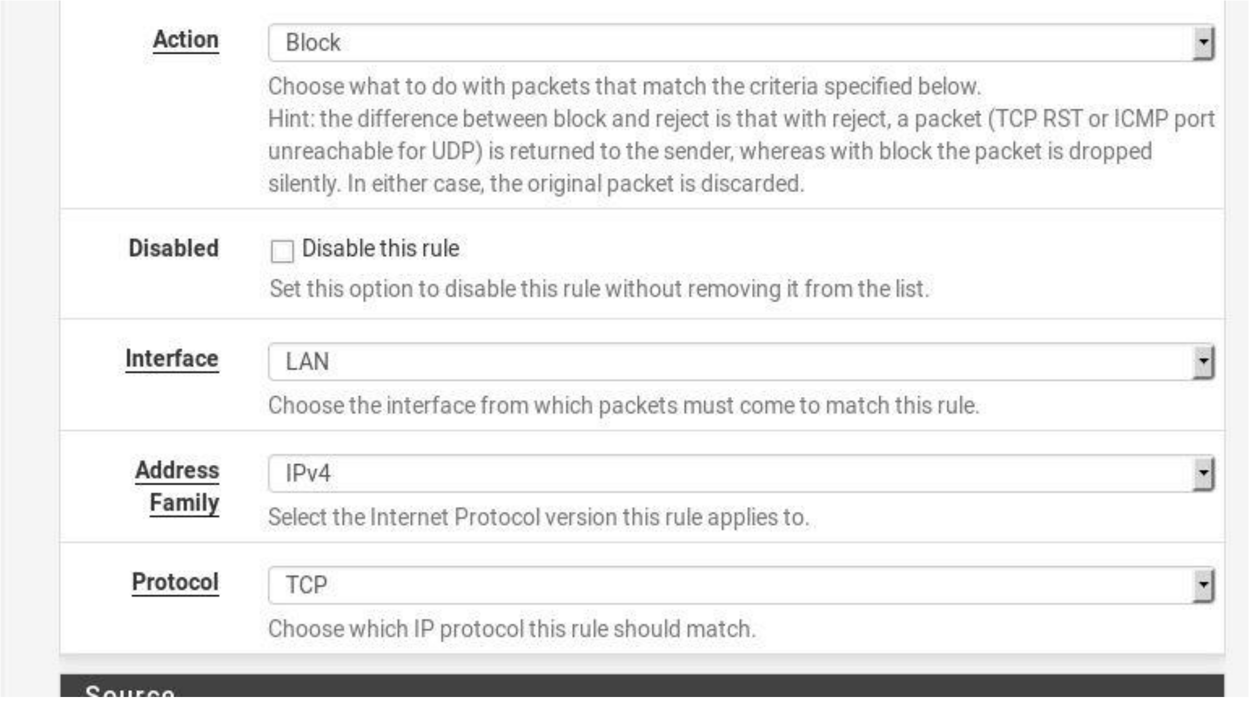
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	1 /32 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

9. Change source to Lan Net

10. Change destination to the ip address of the web server

12. For destination port block 80 for Http

Your rule should look like this:



Action: Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface: LAN

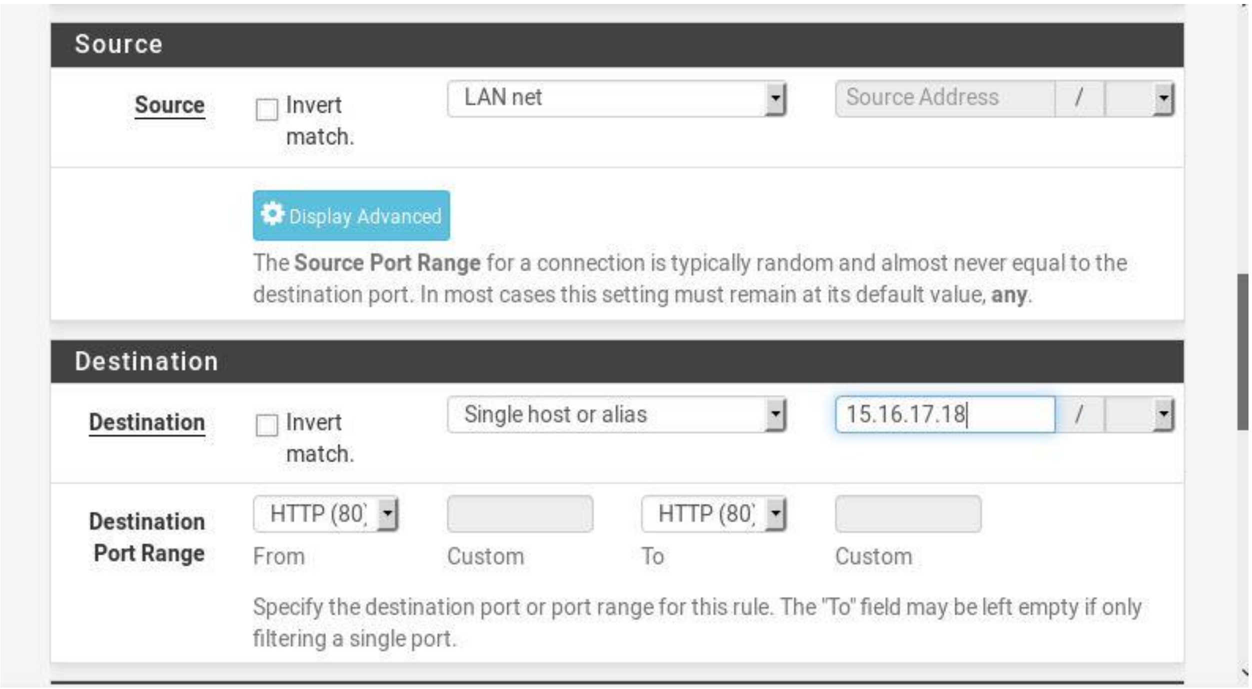
Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: TCP

Choose which IP protocol this rule should match.



Source

Source: □ Invert match. | LAN net | Source Address /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match. | Single host or alias | 15.16.17.18 /

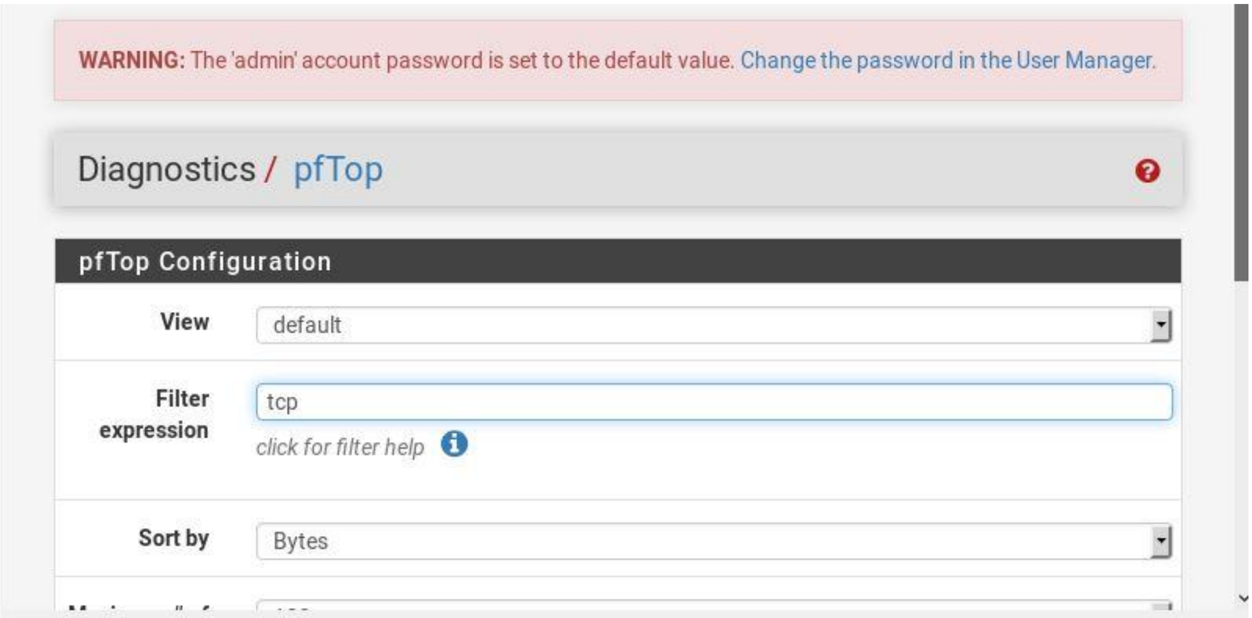
Destination Port Range: From: HTTP (80) | Custom: | To: HTTP (80) | Custom:

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

13. Click apply changes

Part 2: SSH

1. ssh into the pfsense box using ssh -p 22 root@192.168.1.1
2. With the connection established, go into diagnostics - pftop to see network states



WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Diagnostics / pfTop

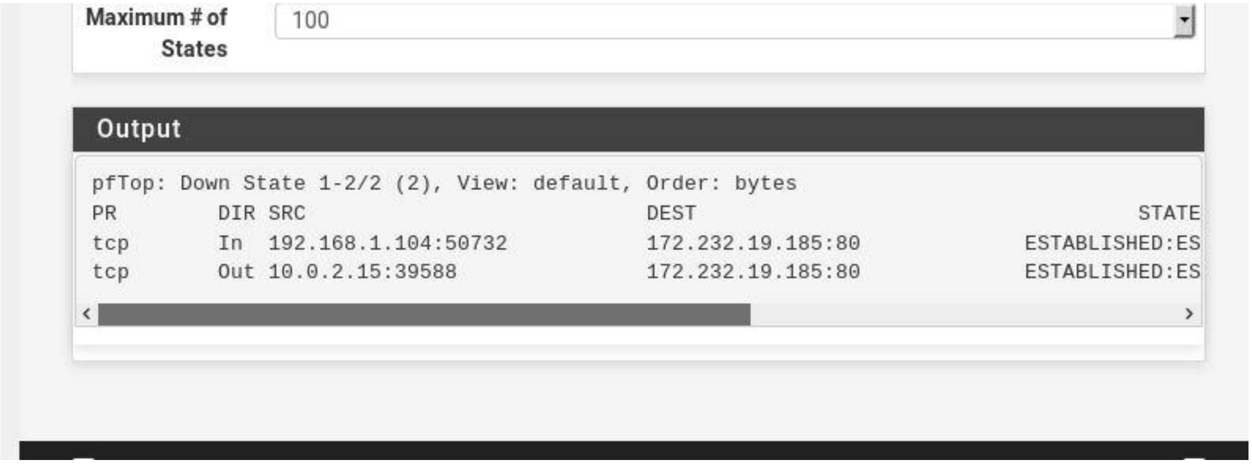
pfTop Configuration

View: default

Filter expression: tcp

click for filter help

Sort by: Bytes

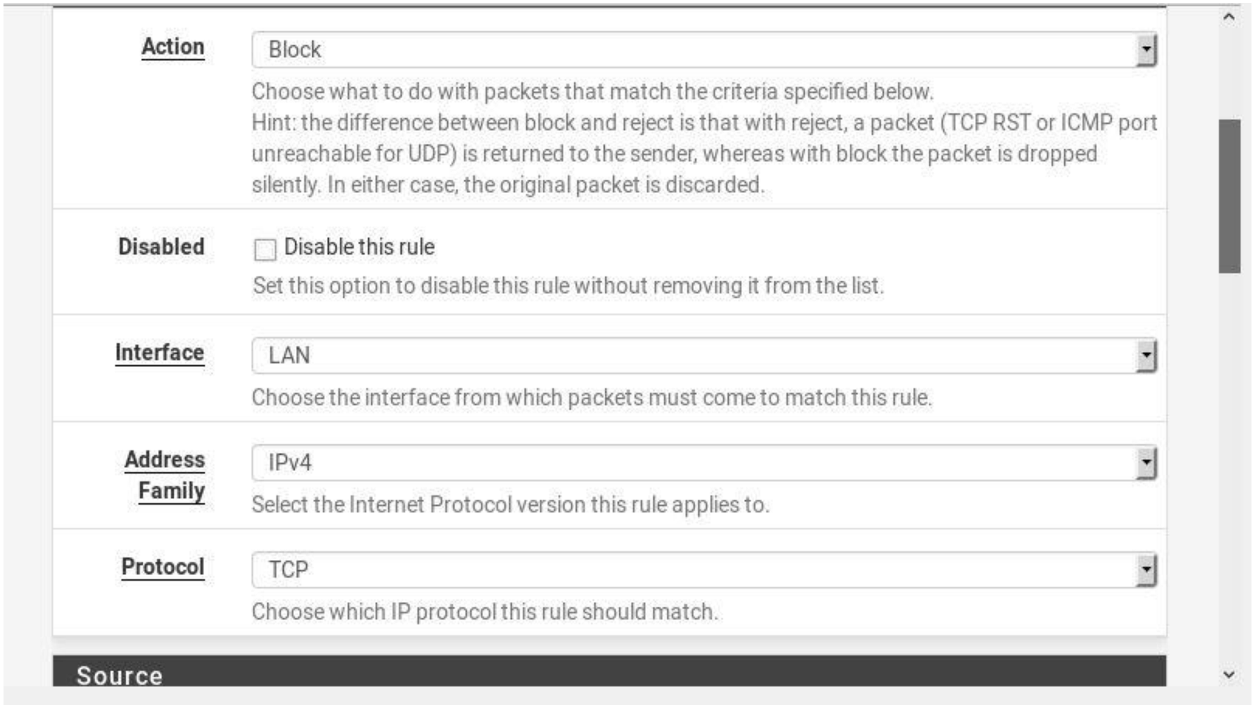


Maximum # of States: 100

Output

```
pfTop: Down State 1-2/2 (2), View: default, Order: bytes
PR       DIR SRC                         DEST                           STATE
tcp      In  192.168.1.104:50732         172.232.19.185:80        ESTABLISHED:ES
tcp      Out 10.0.2.15:39588             172.232.19.185:80        ESTABLISHED:ES
```

3. Look for your ssh connection. This is the connection we will block
4. Go back to the firewall LAN rule page (rules - LAN)
5. Change source to your ubuntu ip, change destination to this firewall, change destination port to 22. Should look like this:



Action Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled □ Disable this rule

Set this option to disable this rule without removing it from the list.

Interface LAN

Choose the interface from which packets must come to match this rule.

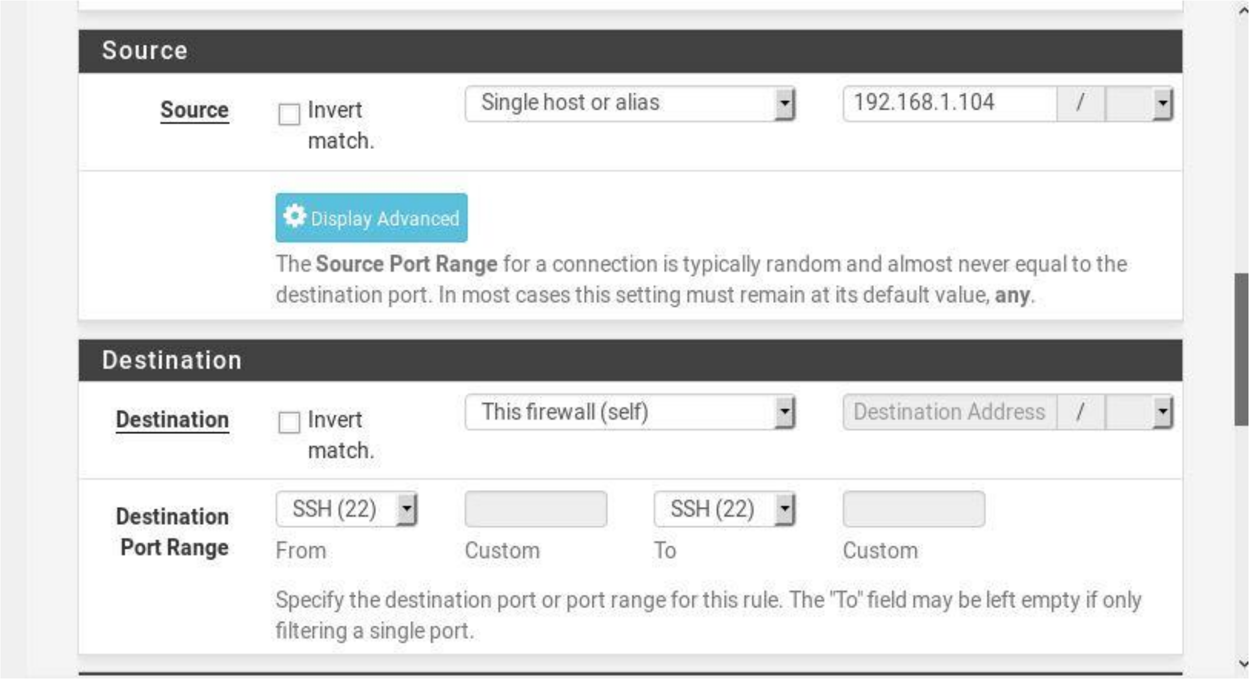
Address Family IPv4

Select the Internet Protocol version this rule applies to.

Protocol TCP

Choose which IP protocol this rule should match.

Source



Source

Source □ Invert match. Single host or alias 192.168.1.104 /

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination □ Invert match. This firewall (self) Destination Address /

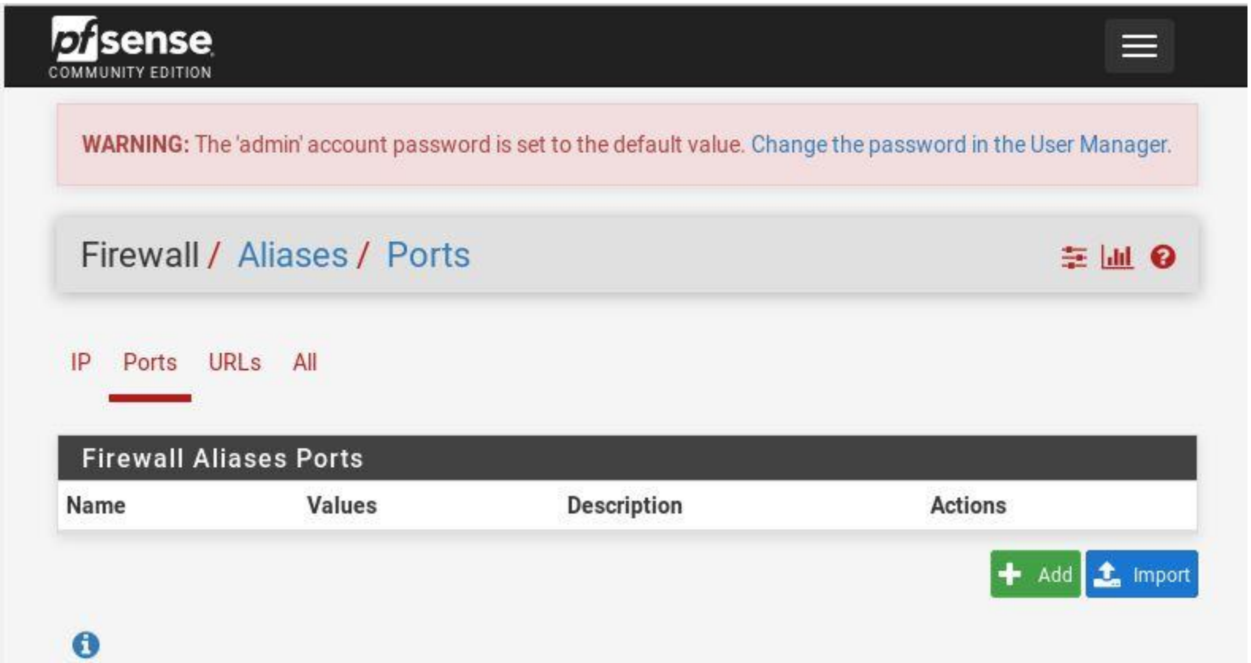
Destination Port Range SSH (22) From, Custom, SSH (22) To, Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

4. Try ssh now

Part 3: If we have time, Aliases!

1. Go to Firewall - Alias - ports



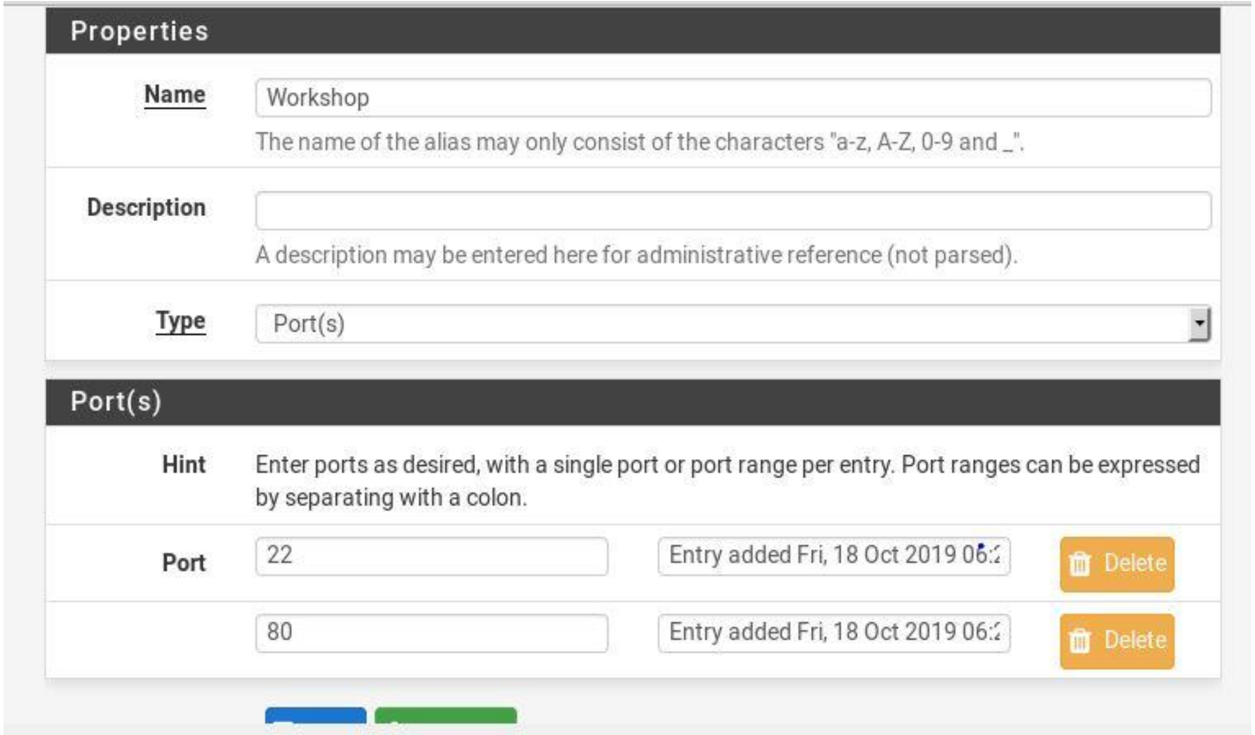
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Firewall / Aliases / Ports

Firewall Aliases Ports

Name	Values	Description	Actions

2. Click the Add button
3. Name it whatever you want (no spaces)
4. Add in port 22 and then click add port and add in port 80



Properties

Name: Workshop

The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and _".

Description:

A description may be entered here for administrative reference (not parsed).

Type: Port(s)

Port(s)

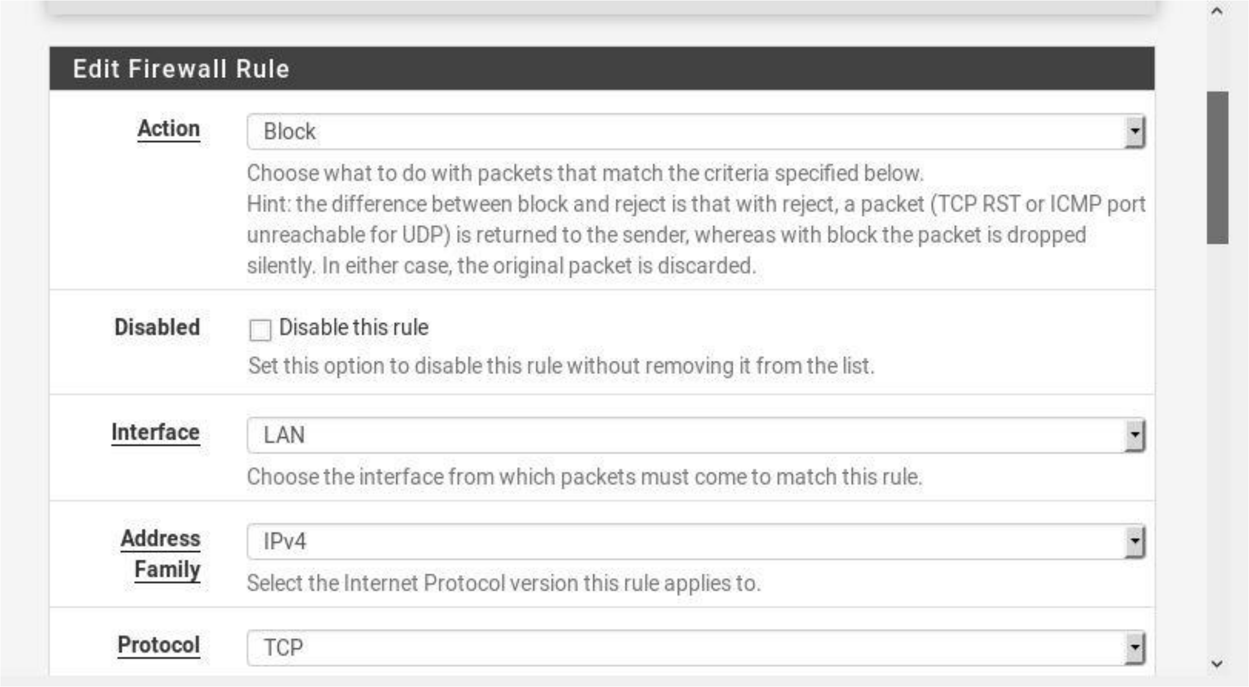
Hint: Enter ports as desired, with a single port or port range per entry. Port ranges can be expressed by separating with a colon.

Port: 22 — Entry added Fri, 18 Oct 2019 06:2

80 — Entry added Fri, 18 Oct 2019 06:2

5. Click apply changes
6. Go to firewall - rules - LAN
7. Click green add to the top button

8. Change action to block
9. Change source to Lan net
10. Change Destination to any
11. Type in your alias name under the custom field of destination port range
12. Click apply changes



Edit Firewall Rule

Action: Block

Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule

Set this option to disable this rule without removing it from the list.

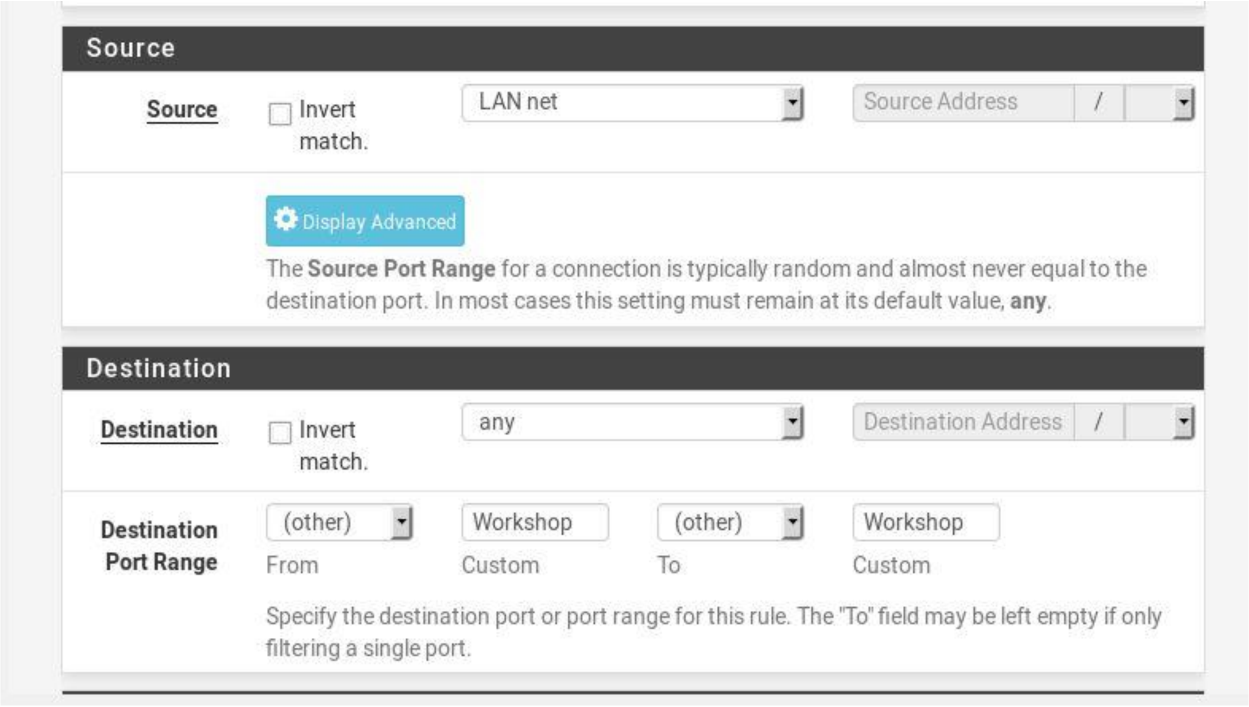
Interface: LAN

Choose the interface from which packets must come to match this rule.

Address Family: IPv4

Select the Internet Protocol version this rule applies to.

Protocol: TCP



Source

Source: □ Invert match. LAN net Source Address /

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination: □ Invert match. any Destination Address /

Destination Port Range: (other) From, Workshop Custom, (other) To, Workshop Custom

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

13. Now click on the disable icon on the two individual rules you created previously
14. Try sshing and connecting to tyler’s website now