Blue Team Level 1 Certification (Standard)

Introduction to BTL1

- ~~Welcome to Blue Team Level 1!~~ — 4 Topics
- ~~Lab and Forum Access~~

SECURITY FUNDAMENTALS DOMAIN

- ~~Introduction to Security Fundamentals~~ — 1 Topic
- ~~Soft Skills~~ — 7 Topics
- ~~Security Controls~~ — 5 Topics | 1 Quiz
- ~~Networking 101~~ — 6 Topics | 1 Quiz
- ~~Management Principles~~ — 4 Topics | 1 Quiz

PHISHING ANALYSIS DOMAIN

- ~~PA1) Introduction to Emails and Phishing~~ — 7 Topics | 1 Quiz
- ~~PA2) Types of Phishing Emails~~ — 10 Topics | 2 Quizzes
- ~~PA3) Tactics and Techniques Used~~ — 12 Topics | 2 Quizzes
- ~~PA4) Investigating a Phishing Email~~ — 8 Topics | 2 Quizzes
- ~~PA5) Analysing URLs, Attachments, and Artifacts~~ — 8 Topics | 1 Quiz
- PA6) Taking Defensive Actions — 12 Topics | 1 Quiz
- PA7) Report Writing — 7 Topics | 1 Quiz
- PA8) Phishing Response Challenge — 3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

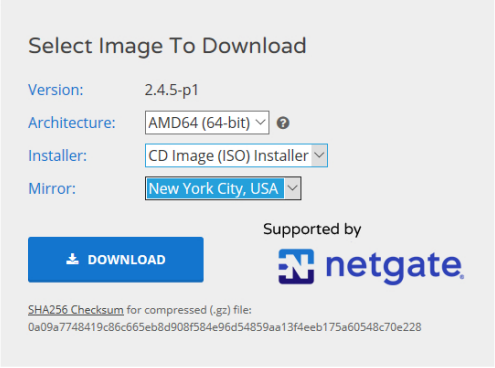
- TI1) Introduction to Threat Intelligence — 7 Topics
- TI2) Threat Actors & APTs — 6 Topics | 2 Quizzes
- TI3) Operational Threat Intelligence — 7 Topics | 1 Quiz
- TI4) Tactical Threat Intelligence — 7 Topics | 1 Quiz
- TI5) Strategic Threat Intelligence — 5 Topics | 1 Quiz
- TI6) Malware and Global Campaigns — 6 Topics | 1 Quiz

DIGITAL FORENSICS DOMAIN

- DF1) Introduction to Digital Forensics — 5 Topics
- DF2) Forensics Fundamentals — 10 Topics | 5 Quizzes

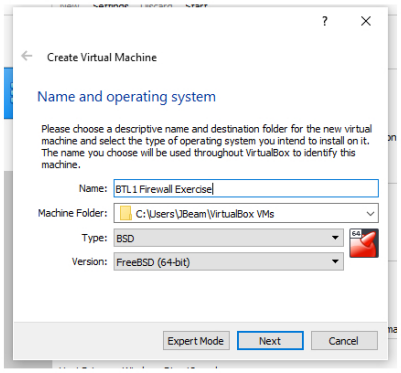
Legacy Activity) Setting up a Firewall

For this activity, we'll be creating a brand new virtual machine that will act as a firewall. Firstly, head over to the pfSense website and download the ISO install file shown in the below screenshot. If you're unsure what version to download for your host system, read the information at the bottom of this page.



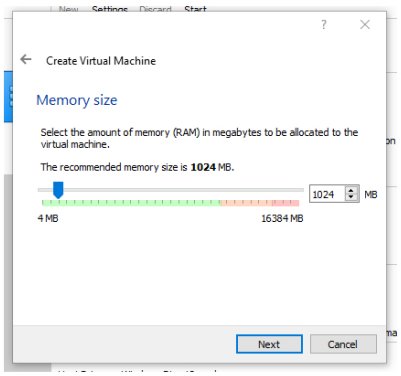
Now that we have the .iso.gz file we need to unzip it, so we can access the .iso file. If you don't already have 7Zip installed, you'll need to download it, install it, and use it to extract the files. You should now have the .iso file!

Next, open VirtualBox and click on New in the top middle of the VirtualBox Manager windows. Name the virtual machine anything, we've gone with "BTL1 Firewall Exercise", set the type as BSD, and the version as FreeBSD. If your host system is 64-bit, then download FreeBSD (64-bit).

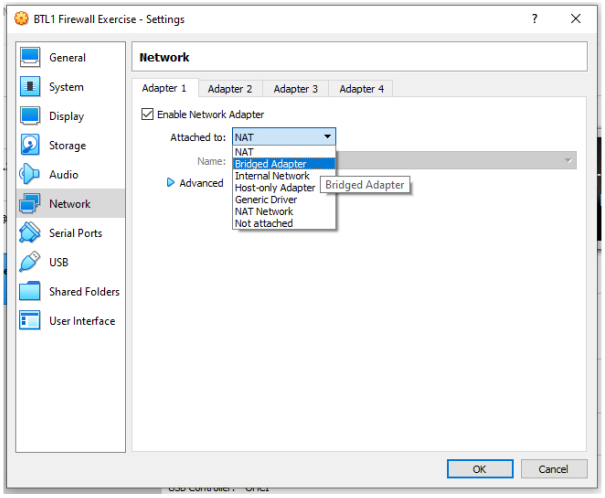


The RAM minimum is 512 MB, but as we are just experimenting with pfSense it doesn't need to have high resources to deal with traffic and operations. We suggest you set the memory size to 1024 MB. When creating a new virtual hard drive, select the VirtualBox Disk Image (VDI) file type.

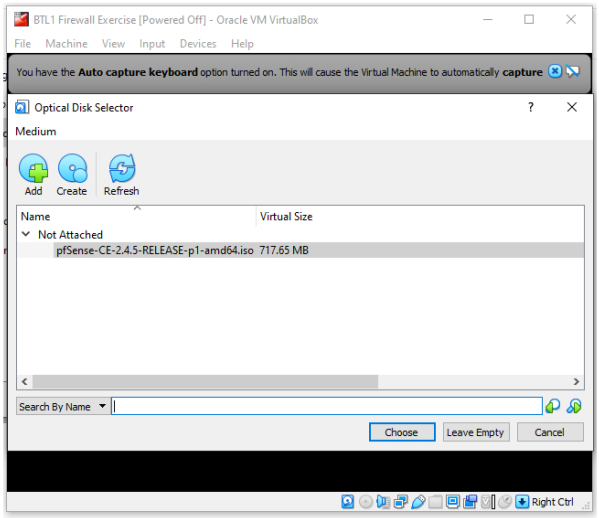
DF3) Digital Evidence Collection
8 Topics | 1 Quiz
DF4) Windows Investigations
3 Topics | 3 Quizzes
DF5) Linux Investigations
4 Topics | 2 Quizzes
DF6) Volatility
3 Topics | 1 Quiz
DF7) Autopsy
4 Topics | 1 Quiz
SECURITY INFORMATION AND EVENT MANAGEMENT DOMAIN
SI1) Introduction to SIEM
7 Topics | 1 Quiz
SI2) Logging
6 Topics | 2 Quizzes
SI3) Aggregation
2 Topics | 1 Quiz
SI4) Correlation
6 Topics | 1 Quiz
SI5) Using Splunk
5 Topics | 2 Quizzes
INCIDENT RESPONSE DOMAIN
IR1) Introduction to Incident Response
8 Topics | 1 Quiz
IR2) Preparation Phase
10 Topics | 2 Quizzes
Section Introduction, Preparation
Preparation: Incident Response Plan
Preparation: Incident Response Teams
Preparation: Assest Inventory and Risk Assessments
Prevention: DMZ
Prevention: Host Defenses
Prevention: Network Defenses
Legacy Activity) Setting up a Firewall
Prevention: Email Defenses
Prevention: Physical Defenses
Prevention: Human Defenses
Activity) End of Section Review, Preparation
IR3) Detection and Analysis Phase
7 Topics | 4 Quizzes
IR4) Containment, Eradication, and Recovery Phase
5 Topics | 1 Quiz
IR5) Lessons Learned and Reporting
7 Topics
IR6) MITRE ATT&CK
13 Topics | 2 Quizzes
BTL1 EXAM
Exam Preparation
Using RDP and SSH
How to Start Your Exam



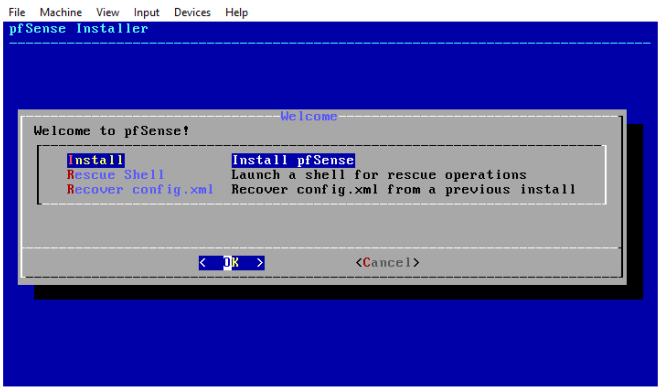
Next we need to ensure that the virtual machine is in Bridged networking mode, so that the system has it's own IP address instead of sharing the IP of our host system. Select your new virtual machine by left-clicking on it once in the VirtualBox Manager, then click the Settings cog at the top of the window. Go to the Network tab and change from NAT to Bridged Adapter.



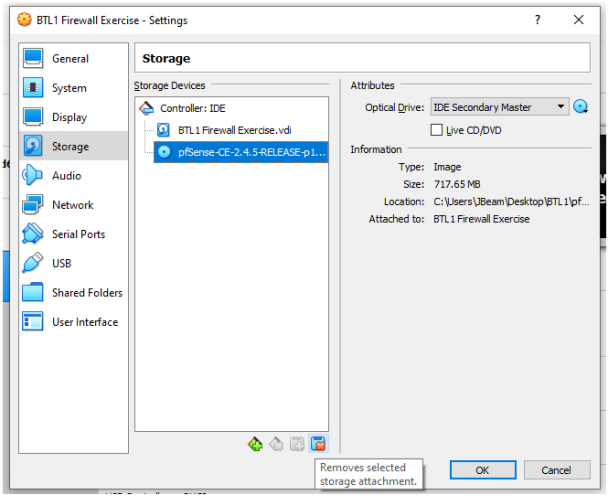
Go back to the VirtualBox Manager window, and double click your firewall virtual machine to run it. You will be prompted with the below window, asking you to import an optical disk – this is our .iso file for pfSense! Select it, and click Choose.



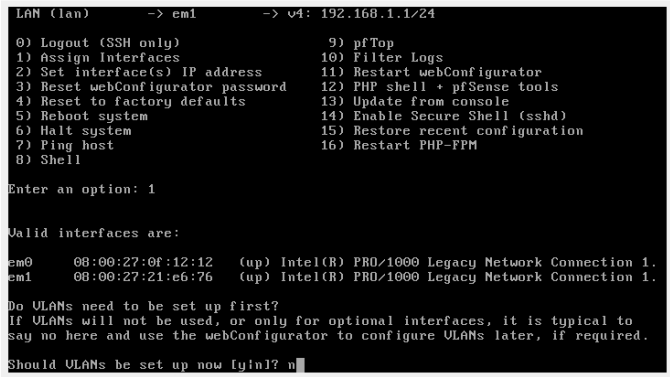
Follow the pfSense installer to get pfSense initialized correctly.



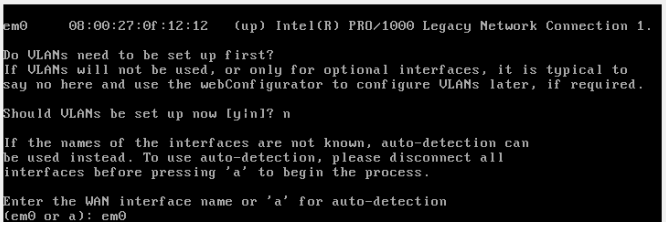
Once the installation is complete, manually shut down the virtual machine. If you don't it will attempt to run the installer again. To stop this, we need to open the virtual machine settings from the VirtualBox Manager and remove the .iso file we used for installation.



Now that you can boot into your pfSense virtual machine properly, select option 1 and when asked "Should VLANs be set up now?" type "n".



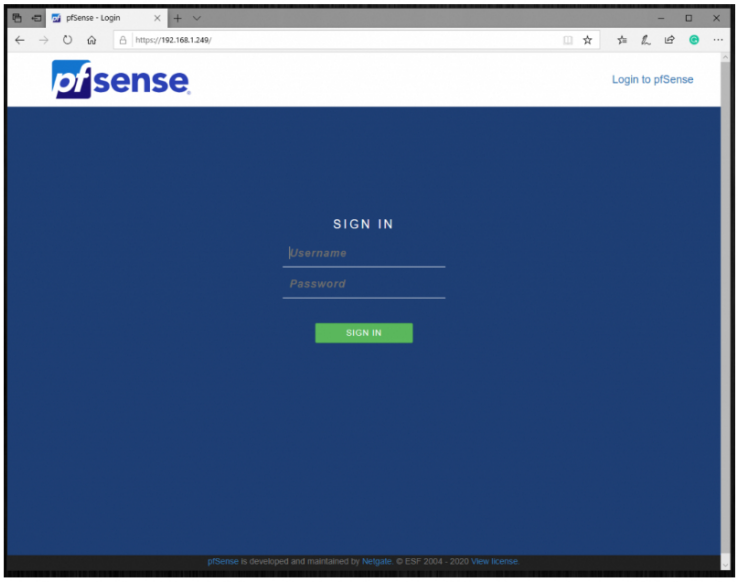
When asked to enter a WAN interface name, enter "em0", and when asked to enter the LAN interface name, don't enter anything and press Enter. When asked to remove the LAN IP address, type "y".



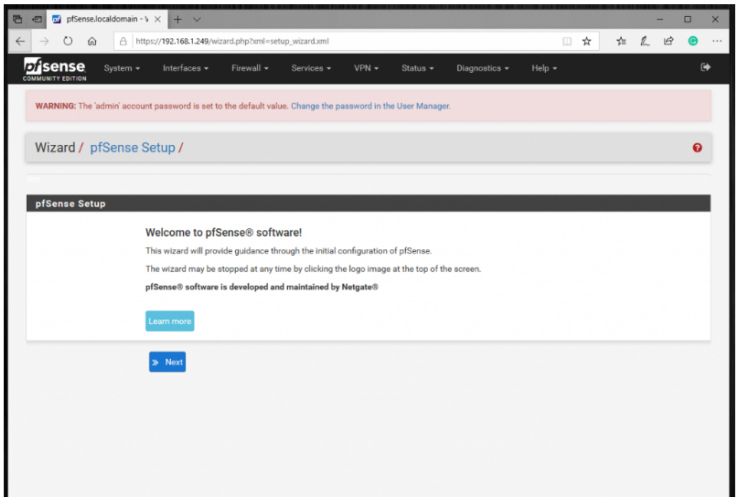
```
Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
( a or nothing if finished):

The interfaces will be assigned as follows:

WAN  -> em0

Do you want to proceed [y|n]? y
```

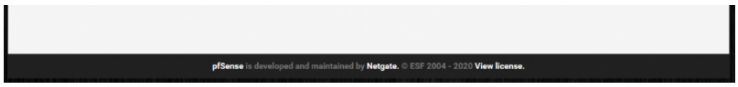
In the below screenshot we can see that the em0 interface is enabled, and in our case we see the IP address 192.168.1.249. If you enter this IP into your browser on your host system, you will see the pfSense login portal.

```
unload the interface now [y|n]? y

Writing configuration...done.
One moment while the settings are reloading... done!
route: writing to routing socket: Network is unreachable
route: route has not been found
VirtualBox Virtual Machine - Netgate Device ID: 397603f30813fed78b60

*** Welcome to pfSense 2.4.5-RELEASE-p1 (amd64) on pfSense ***

WAN (wan)       -> em0        -> v4/DHCP4: 192.168.1.249/24
                                          a00:27ff:fe0f:1212/
64

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
```

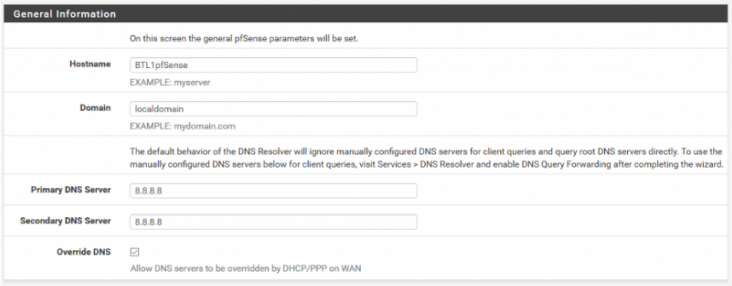


Use the username:admin and the password:pfsense to log into the management console. On the first page we are presented with the configuration wizard, which we will be following to get everything set up correctly. Click Next to begin.

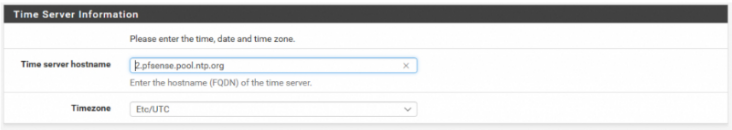




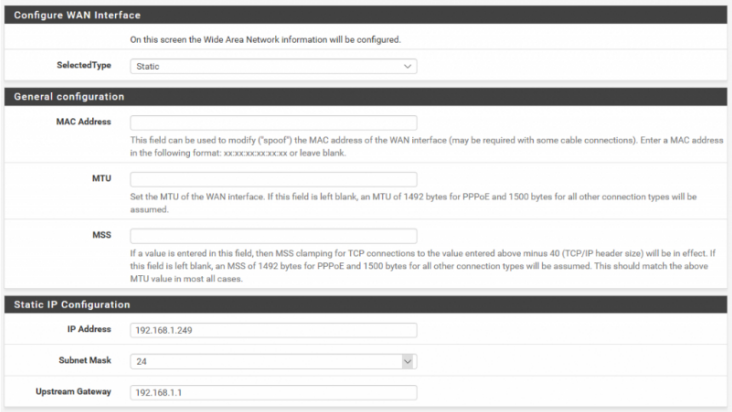
Configure the setting as shown below.



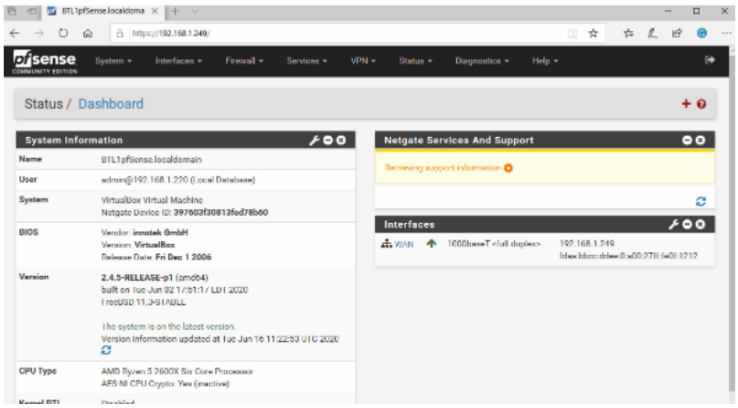
Leave the following settings as they are by default.



Below, we have changed the SelectedType from DHCP to Static. Under the Static IP Configuration section we have set the IP address to match the IP we're currently using to access this web console (look at your address bar!). Make sure to change the subnet mask to 24, and the gateway as 192.168.1.1.

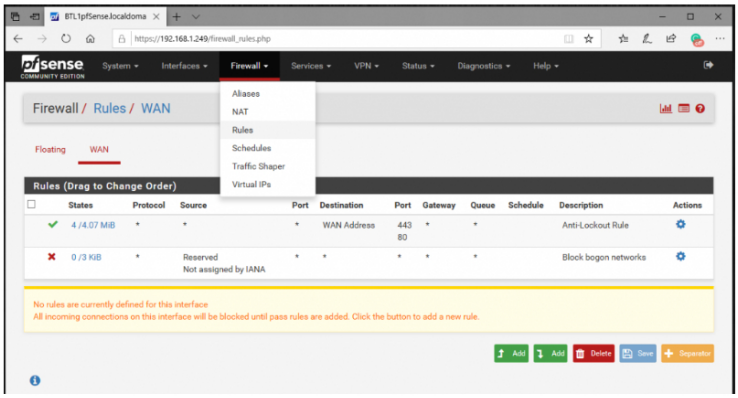


Next, you'll be asked to enter an admin password. We have chosen "password" for now. Then you'll be asked to Reload pfSense with the new changes. Once this is done, we're ready to get onto the fun stuff! 🙂 Click on the pfSense logo in the top left-hand corner to view the Dashboard. This provides valuable information about our firewall, such as; interfaces, system, uptime, and resource usage as shown in the below GIF.



WRITING FIREWALL RULES

From your pfSense web console, hover over Firewall on the top menu and click on Rules.



As we don't currently have any firewall rules in place, all incoming connections are blocked by default as a safety measure. We're going to quickly cover how to write some basic firewall rules. To get started click on the left Add button at the bottom of the page. Before we actually create our own rules, we're going to explain the properties that we can set when creating a rule.

Action

There are three actions we can take with our firewall rules:

- **Pass:** Allow the traffic to pass through the firewall.
- **Block:** Prevents the traffic from passing through the firewall by dropping the connection, and not notifying the source IP (known as silent dropping).
- **Reject:** Prevents the traffic from passing through the firewall by dropping the connection, and informing the source IP.

Disabled

Ticking this box will disable the rule, meaning that it is not actively used by the firewall, but the rule is not deleted so it can be enabled in the future.

Interface

Choose the interface from which packets must come to match this rule. For this walkthrough, we only have a WAN interface configured.

Address Family

Choose whether the rule applies to IPv4 traffic, IPv6 traffic, or both.

Protocol

Which protocol this rule applies to. For example, we could block TCP traffic but allow UDP traffic. We can also choose to use Any protocol, instead of a specific one.

Source

The source of the network connection the rule will apply to. For example, if we wanted to block connections to Facebook from this network, the source value would be 192.168.1.0/24, with a destination value of Facebook's IP range.

Destination

The destination of the network connection the rule will apply to. See the example under the Source heading to understand what this means.

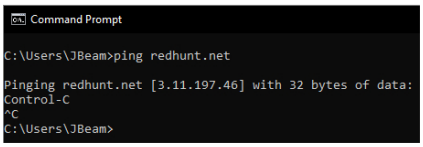
Log

We can optionally log traffic that matches this rule. If we were blocking connection to Facebook, we could log when this rule is enforced, allowing us to identify which hosts are attempting to connect to Facebook. In an enterprise, we would push these logs to a SIEM platform for centralized management and alerting.

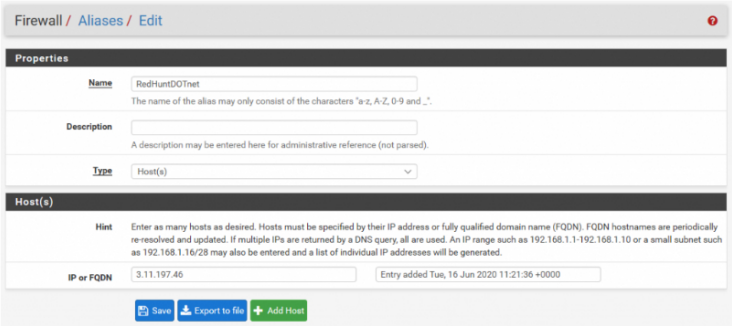
Description

We can assign a description for this rule. This is a good idea when working in teams, so that other team members can understand what this rule does, and what it's being used for.

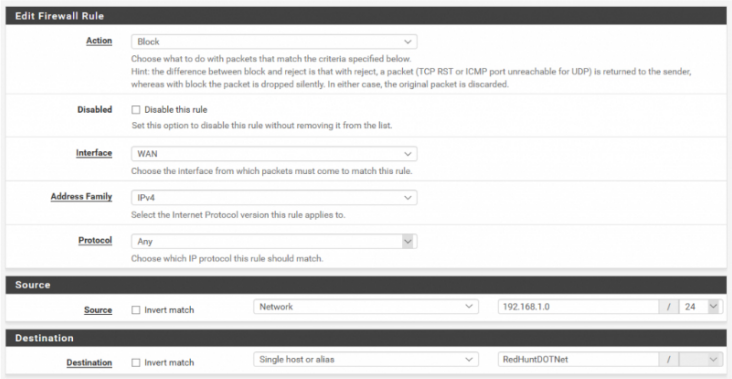
Now that you understand the properties we can set within a rule, let's create a rule to block a Security Blue Team-owned domain, Redhunt.net. Open a command prompt on your Windows system, or a terminal on a Kali Linux virtual machine, and type **`ping redhunt.net`**. You can instantly press CTRL+C to stop pinging. You now have the IP address of Redhunt.net!



Hover over Firewall on the top menu, and click Aliases. Aliases act as placeholders for real hosts, networks or ports. They can be used to minimize the number of changes that have to be made if a host, network or port changes. For example, if we create an Alias for a site we want to block, we can use that as the source or destination within firewall rules. If the IP of the site changes, we only need to change the Alias instead of every single rule. In the below screenshot we have set a name and the IP address of redhunt.net.



Now let's create a firewall rule to block any host in our network connecting to the redhunt.net! Copy the below settings – we will explain them below



- **Action:** Block – we want to block traffic to Redhunt.net
- **Protocol:** Any – we want to block all traffic (alternatively, we could choose to just block http (TCP 80) and https (TCP 443)).
- **Source:** Network, 192.168.1.0/24 – we want to enforce this rule for any system on our private home network.
- **Destination:** Single host or alias, RedHuntDOTNet (the alias we created earlier for the IP address of the website).

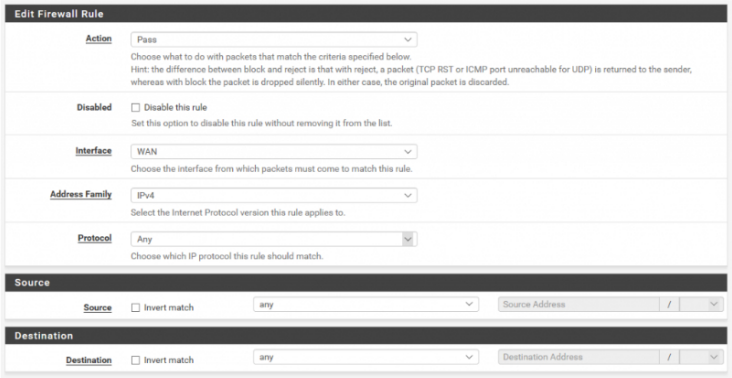
Before we change our host system's default gateway, pushing all of our traffic through pfSense, we need to think about how the firewall is currently constructed. All traffic is blocked by default with pfSense, so technically, we have two rules at the moment:

- **Block ANY traffic to Redhunt.net (3.11.197.46)**
- **Block ANY traffic**

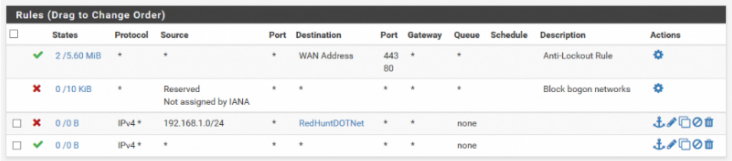
So if we change the default gateway on our host system, we will have absolutely no internet connection, because pfSense is blocking everything. We need to create something known as an ALLOW ALL rule. This might sound scary, but remember that your host is (or should be) running a local web application firewall, which will still work to block malicious traffic. This rule means that pfSense allows communications to come in and out from the internet, giving us a connection.

> *Firewalls follow a hierarchy when it comes to rules, working from the top down. This means pfSense will inspect the traffic and apply the rules in the following order:*
>
> ***1. Firewall sees that Redhunt.net is blocked. If the packet is attempting to reach out to 3.11.197.46, drop the packet to prevent the connection.***
> ***2. Firewall sees that all traffic is allowed.***

Let's create our allow all rule. Copy the settings we have used below.



Once this rule has been created, make sure it is placed **below** the redhunt.net blocking rule, otherwise when we change our default gateway, you're going to lose internet connection until you restore it.



> ***IMPORTANT NOTE:***
>
> *Due to human error, during this walkthrough we encountered an issue with our pfSense virtual machine, so we had to do a fresh install. Prior to this message, our pfSense IP address was 192.168.1.249. Our new instance has the IP address 192.168.1.251.*

Make sure you've clicked on the Save Changes button that appears at the top of the page whenever a change is made, so pfSense can update itself. Now it's time to see if everything has worked! First, we need to understand how

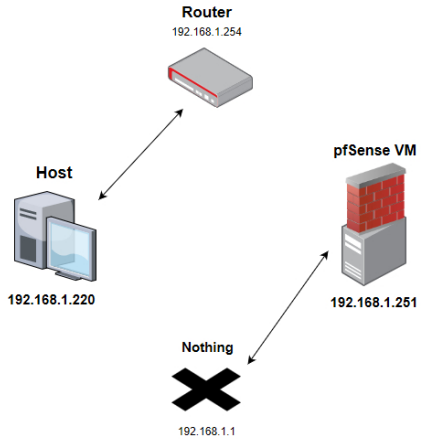
our home network is set up, considering both our pfSense virtual machine and our host system. In my case, I am on a wired ethernet connection, with a network named "GardenNET". We already know the following details:

- pfSense virtual machine IP (the IP you log into the pfSense web console with): **192.168.1.251**
- pfSense upstream gateway IP address (we set this when we first logged into pfSense web console): **192.168.1.1**
- pfSense DNS server IP (we set this when we first logged into pfSense web console): **8.8.8.8**

What we need to know next is our host system's IP address, our host system's DNS server IP, and our current default gateway. We can open a command prompt and use the command **`ipconfig /all`** to gather the information we need.

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : home
   Description . . . . . . . . . . . : Intel(R) I211 Gigabit Network Connection
   Physical Address. . . . . . . . . : 04-D9-F5-20-72-97
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2a00:23c6:4e03:200:6587:3ba5:3542:756d(Preferred)
   IPv6 Address. . . . . . . . . . . : fdaa:bbcc:ddee:0:6587:3ba5:3542:756d(Preferred)
   Temporary IPv6 Address. . . . . . : 2a00:23c6:4e03:200:b5e8:4e5b:c092:1af(Preferred)
   Temporary IPv6 Address. . . . . . : fdaa:bbcc:ddee:0:b5e8:4e5b:c092:1af(Preferred)
   Link-local IPv6 Address . . . . . : fe80::6587:3ba5:3542:756d%2(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.220(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 17 June 2020 16:07:23
   Lease Expires . . . . . . . . . . : 18 June 2020 16:07:23
   Default Gateway . . . . . . . . . : fe80::a608:f5ff:fe89:ff57%2
                                       192.168.1.254

   DHCPv6 IAID . . . . . . . . . . . : 100981237
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-25-22-9E-B2-04-D9-F5-20-72-97
   DNS Servers . . . . . . . . . . . : 192.168.1.254
   NetBIOS over Tcp/Ip . . . . . . . : Enabled
   Connection-specific DNS Suffix Search List :
                                       home
```

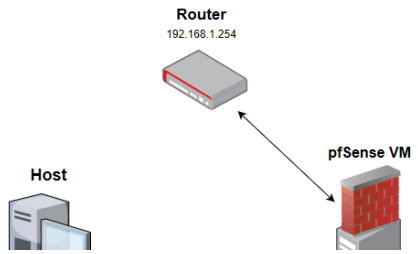
In our case (yours may be different), our **host IP is 192.168.1.220**, our **default gateway to the internet is 192.168.1.254**, and our **DNS server is 192.168.1.254** (same as the gateway). At the moment, our host is sending traffic from 192.168.1.220 to 192.168.1.254, then out to the internet. Below is a network diagram showing how we need to configure our host to push traffic through pfSense out to the internet. We'll explain it more below.



So at the moment, our host communicates with the router at 192.168.1.254 and that's how we have internet connectivity. Our pfSense has the default gateway we assigned earlier, which is 192.168.1.1. Sometimes your router will sit at .1 in home networks, but in our case, it is at .254. What we need to do is:

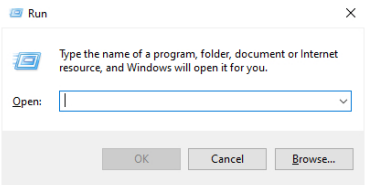
- Tell our host system to use the pfSense virtual machine (192.168.1.251) as its default gateway. Traffic outbound for the internet will now go to pfSense.
- Tell our pfSense VM to use the router (192.168.1.254) as its default gateway, giving it internet connectivity.

The new network should look like the below diagram.

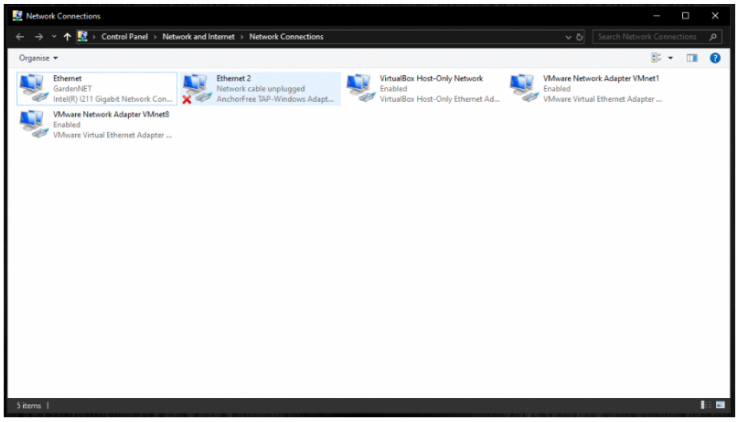


First things first, let's change the default gateway in pfSense from 192.168.1.1 to the correct value, 192.168.1.254, giving us access to the internet. You can see the change we have made in the below screenshot by clicking on "Add a new gateway" and entering our router's IP.

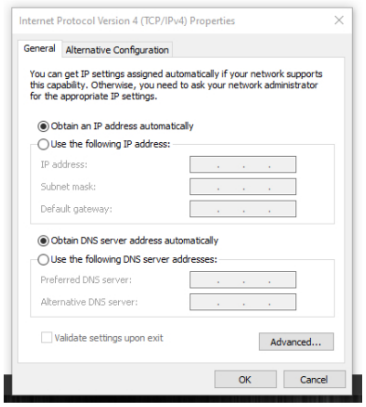
Next it's time to update the settings for our host. In the Windows search bar, type "run" and press enter. The following popup will display.

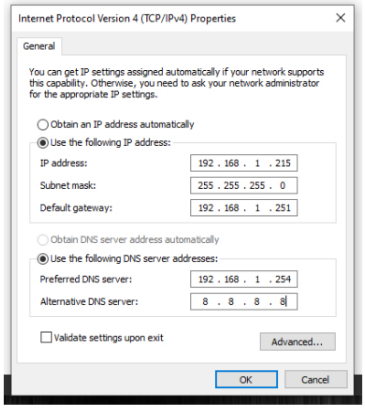


Enter in "ncpa.cpl" and press enter. You should see something similar to the below screenshot. Our ethernet network connection is shown in the top right, as GardenNET.

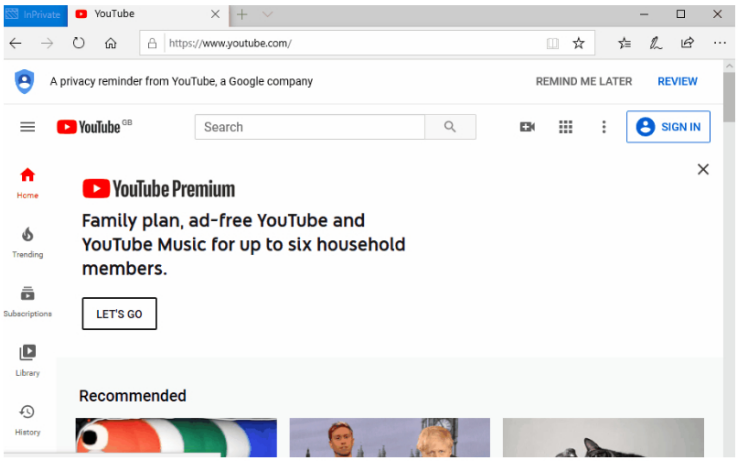


Right-click on your primary connection, and select "Properties". Find the line that reads "Internet Protocol Version 4", and double left-click to open a new window, shown below. Here we can change from "obtain an IP address automatically" and "obtain DNS server address automatically" to set the values we need from our pfSense system. We have shown the before and after screenshots below. We will also explain what we've done underneath these images.





So now, our traffic is going through pfSense to the router, then to the internet. Please note your connection speed may be slower, depending on the resources you assigned to the pfSense virtual machine, as it is having to scan all traffic coming through to match it against the two rules we have created. We can now see that we can browse any other internet site except Redhunt.net! Our blocking rule has worked!



Privacy & Cookies Policy
Privacy - Terms