Building a Home Lab

\*This lab was adapted from

***Building Virtual Machine Labs, A Hand-On Guide Second Edition Volumes I and II***

by Tony Robinson

<https://www.amazon.com/Building-Virtual-Machine-Labs-Hands/dp/B09GXD7QL8/ref=sr_1_1?keywords=building+virtual+machine+labs&qid=1657166863&sprefix=building+vertua%2Caps%2C114&sr=8-1>

<https://www.amazon.com/Building-Virtual-Machine-Labs-Hands/dp/B09GZJPYFX/ref=sr_1_14?qid=1657166908&refinements=p_27%3ATony+Robinson&s=books&sr=1-14&text=Tony+Robinson>

&

Professor Ian Burres (University of Texas at San Antonio)

Recommended setting of each VM…

* **PfSense**: 512MB RAM, 5GB Disk, 1 CPU/core
* **SIEM**: 4GB RAM, 80GB Disk, 1 CPU/core
* **IPS**: 4GB RAM, 80GB Disk, 1 CPU/core
* **Kali**: 4GB RAM, 80GB Disk, 1 CPU/core
* **Ubuntu**: 4GB RAM, 80GB Disk, 1 CPU/core
* **Metasploitable 2**: 512MB RAM, 10GB Disk, 1 CPU/core

# Download List

Download the following prior to starting lab…

* Virtual Box - https://www.virtualbox.org/wiki/Downloads
* PFSense - https://www.pfsense.org/download/
* Ubuntu Server (select latest LTS version) - <https://releases.ubuntu.com/>
* Ubuntu https://ubuntu.com/download/desktop
* Kali Linux - https://www.kali.org/get-kali/#kali-virtual-machines
* Metasploitable 2 - <https://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

# Virtual Box Setup

1. Download and install VirtualBox (<https://www.virtualbox.org/wiki/Downloads>)
2. Ensure your default machine is set to where you would like your VMs to be saved.
   1. Navigate to “File” then Click “Preferences”
   2. Select the dropdown menu for “Default Machine Folder”
   3. Select your preferred area of storage.
      1. \***Suggestion**\* If possible, try and store your VMs outside of your hosts disk I/O
3. Disable DHCP
   1. Click “**File**”
   2. Click “**Host Network Manager**”
   3. Click on DHCP tab
   4. Unselect “**DHCP**”
   5. Graphical user interface, text, application, email

      Description automatically generated

# pfSense VM Setup

VM Settings

* Name: **“Pfsense”**
* Type: **“BSD”**
* Version: **“FreeBSD (64-bit)”**
* Memory Size: **512MB**
* Hard Disk: **“Create a virtual hard disk now”**
* Hard disk file type: **“VDI (VirtualBox Disk Image)”**
* Storage of physical hard disk: **“Fixed size”**
* File location and size: **5.00 GB8**
* Network Settings:
  + Adapter 1: **Bridged Adapter**
  + Adapter 2: **Host-Only Adapter**
  + Adapter 3: **Internal Network**

Setup

1. Download Pfesnse (<https://www.pfsense.org/download/>)
2. Configure VM (*Complete step prior to starting VM*)
   1. Click “**Settings**”
   2. On “**System**” tab uncheck “**Floppy**”
   3. On “**Storage**” tab select “**Empty**” then select the blue disc next to “**Optical Drive**”
      1. Graphical user interface

         Description automatically generated
   4. Select “**Choose/Create a Virtual Optical Disk…**”
      1. Graphical user interface, application

         Description automatically generated
   5. Select “Add” and navigate to your pfSense iso
   6. Once iso is selected, select “**Choose**”
   7. Click on “**Audio**” tab and uncheck “**Enable Audio**”
   8. Click on “**USB**” tab and uncheck “**Enable USB Controller**”
   9. Click on “**Network**” tab and enable adapters 1, 2, and 3. (*Record the MAC address for each adapter*)
      1. Adapter 1: **Bridged Adapter**
      2. Adapter 2: **Host-Only Adapter**
      3. Adapter 3: **Internal Network**
   10. Select “**OK**” at the bottom of the settings box and start the VM

**\*\*\* If you receive an error when trying to start the VM, you will have to restart your PC/laptop. This is a known bug, and there are other workarounds, but the easiest is to just restart the computer. You won’t have the problem again once you restart; it has do to with Windows 10 and the Host-only network you created in VirtualBox. \*\*\***

* 1. Once VM is started select “**Accept**”
  2. Select “**Install pfSense**”
  3. Select “**Continue with default keymap**”
  4. Select “**Auto (UFS) BIOS**”
  5. Select “**No**” for Manual Configuration
  6. **DO NOT** reboot, select “**Machine**” > “**ACPI Shutdown**” at top of VM Application
  7. Select “**Settings**” again and navigate to “**Storage**” tab
  8. Select “**pfSence-CE-…”**
  9. At the bottom of the box select disk with red “**X**” on it and remove the storage device
  10. Select “**System**” tab and reorder the “**Boot Order**”
      1. Graphical user interface, application

         Description automatically generated
  11. Select “**OK**” and start VM again

Configuration of pfSense

Once it has finished booting, you will see a prompt and 16 different options to choose from.

1. Type the number **8** into the prompt and hit enter.
2. Type the following command in the shell:
   1. **ifconfig -a | egrep “em|ether”**
      1. Text

         Description automatically generated
   2. Notate that “**em0**”, “**em1**”, and “**em2**” correlate to network adapters 1, 2, and 3 in the VM settings.
3. Type “**exit**” in the terminal
4. Type “**1**” in the terminal to start assigning the interfaces
   1. Type “**n**” for the first question
   2. Type “**em0**” for the WAN
   3. Type “**em1**” for the LAN
   4. Type “**em2**” for the OPT1rt
   5. Text

      Description automatically generated
   6. Type “**y**” to proceed forward
5. Enter “**2**” and “**2**” again to start assigning static IP addresses to the LAN.
   1. Use the following configurations
      1. IP: “**172.16.1.1**”
      2. Bit count: “**24**”
      3. Hit the ENTER key
      4. Hit the ENTER key
      5. Enable DHCP? “**y**”
      6. LAN DHCP Start Address: “**172.16.1.10**”
      7. LAN DHCP Ending Address: “**172.16.1.254**”
      8. Do you want to revert to HTTP? “**n**”
6. Hit the ENTER key to go back to prompt where you will enter “**2**” then “**3**” to assign static IP addresses to the OPT1
   1. Use the following configurations
      1. IP: “**172.16.2.1**”
      2. Bit count: “**24**”
      3. Hit the ENTER key
      4. Hit the ENTER key
      5. Enable DHCP? “**y**”
      6. LAN DHCP Start Address: “**172.16.2.10**”
      7. LAN DHCP Ending Address: “**172.16.2.254**”
      8. Do you want to revert to HTTP? “**n**”

Host Machine Network Configuration

1. Without shutting down the VM, outside the VM on your host machine, navigate to your “**Control Panel**” and select “**Network and Internet**”
2. Select “**Network and Sharing Center**”
3. Select “**Change adapter setting**”
4. Right click “**VituralBox Host-Only Network**”
5. Select “**Properties**”
6. Check the following box only
   1. *VirtualBox NDIS6 Bridged Networking Driver*
   2. *QoS Package Scheduler*
   3. *Internet Protocol Version 4 (TCP/IPv4)*
7. Select “**Internet Protocol Version 4 (TCP/IPv4)**”
8. Select “**Properties**”
9. Select “**Use the following IP address:**”
   1. IP address: **172.16.1.2**
   2. Subnet mask: **255.255.255.0**
   3. Default gateway: BLANK
10. Leave the bottom DNS server addresses blank
11. Select “**Advanced…**”
12. Select “**WINS**”
13. Select “**Disable NetBIOS over TCP/IP**”
14. Select “**OK**”
15. Select “**OK**”
16. Select “**Close**”

Configuration of Host Machine Firewall

1. Navigate to your host machine’s firewall settings
2. Select “**Start Menu**”
3. Type “**Windows Firewall with Advanced Security**” in the Windows search bar
4. Select “**Inbound Rules**”
5. Select “**New Rule…**”
6. Select “**Custom**”
7. Select “**Next**”
8. Select “**All programs**”
9. Select “**Next**”
10. Select “**Next**”
11. Select “**These IP addresses:**” under the question “**Which local IP addresses does this rule apply to?**”
12. Select “**Add**”
13. Type IP address: **172.16.1.2**
14. Select “**OK**”
15. Select “**Next**”
16. Select “**Block the connection**”
17. Select “**Next**”
18. Select “**Next**”
19. Name the rule and give it a description
20. Select “**Finish**”

*\*Navigate to “Kali Setup”. Create the machine and come back here to finish setting up pfSense\**

pfSense Web Configuration Settings

1. Open web browser on host machine
2. Enter IP address: **172.16.1.1**
   1. If you get a non-secure warning, select advance and continue
3. Sign into pfSense with default username and password
   1. Username: **admin**
   2. Password: **pfsense**
4. Complete the Wizard setup
   1. Select “**Next**”
   2. Select “**Next**”
   3. Type “**8.8.8.8**” for the Primary DNS Server
   4. Type “**4.2.2.2**” for the Secondary DNS Server
   5. Select “**Next**”
   6. Select “**Nex**t”
   7. Scroll down to the bottom of the page and uncheck “**Block RFC1918 Private Networks**” and “**Block bogon networks**”
   8. Select “**Next**”
   9. Select “**Next**”
   10. Change password
   11. Select “**Next**”
   12. Select “**Reload**”
   13. Select “**Finish**”
5. Navigate to “**Firewall**”
6. Select “**Rules**”
7. Select “**LAN**”
8. Select the green “**Add**” button with the arrow facing up
9. Configure the settings according to the following screenshot
   1. Graphical user interface, text, application, email

      Description automatically generated
10. Select “**Save**”
11. Select “**Apply Changes**”
12. Navigate to “**Firewall**”
13. Select “**Aliases**”
14. Go to “**IP**” tab
15. Select “**Add**”
16. Configure settings to look like the following screenshot
    1. Graphical user interface, text, application, email

       Description automatically generated
17. Select “**Save**”
18. Select “**Apply Changes**”
19. Navigate to “**System**”
20. Select “**Advanced**”
21. Place a checkmark in the “**Disable webConfigurator anti-lockout rule**”
22. Select “**Save**”

Take a snapshot of VM

1. Navigate to pfSense VM
2. Select “**Machine**” at the top of the VM application
3. Select “**Take Snapsot**”
4. Give it a name and description
   1. Graphical user interface, text, application

      Description automatically generated
5. Select “**OK**”

Back to Firewall Setup

1. Re-enter IP address to pfSense in browser to ensure pfSense is still running
2. Navigate to “**Firewall**”
3. Select “**Rules**”
4. Select “**WAN**”
   1. Create a rule that blocks ALL traffic.
   2. Graphical user interface, text, application, email

      Description automatically generated
   3. Graphical user interface, text, application

      Description automatically generated
   4. Select “**Save**”
   5. Select “**Apply Changes**”
5. Select “**LAN**”
6. On the LAN settings page, you will create several rules that resemble the screenshots below.

**After completing LAN rules, continue to OPT1 Firewall settings**

* 1. If you see Allow, then choose the **PASS** option in the first drop-down
  2. If you see Deny, then choose the **Block** option in the first drop-down.
  3. If you see a network address with a CIDR, use Network in the drop-down box.
  4. Save the order at the bottom of the page BEFORE clicking Apply Changes.

**Make sure you have the EXACT ORDER as me in the firewall rules. If you put a Deny rule out of order you may prevent access to the firewall webConfigurator. If that happens, read below.**

**IF you make a mistake and get locked out of the webConfigurator, go into the pfsense VM and choose option 15. You can restore a previous state that was saved before you made the mistake. Reboot the machine afterward (option 5), and you should be able to access the webConfigurator again.**

* 1. LAN Settings (ORDER IS IMPORTANT)
     1. Graphical user interface, table

        Description automatically generated
  2. OPT1 Firewall Settings (ORDER IS IMPORTANT)
     1. Graphical user interface, application, table

        Description automatically generated

1. Once settings are complete, navigate back to the pfSense VM and type “8” to get to shell.
2. Type in the following commands to test your network connection
   1. **ping -c 5 google.com**
   2. **nslookup google.com**
   3. **curl -l** [**https://www.google.com**](https://www.google.com)
3. So long as all three commands return successfully, you can move forward. If not, troubleshooting maybe required. Please refer to the book in the “References” section for help, use Google, or ask for help.
4. Return to the webConfigurator in your browser
5. Select “**Services**”
6. Select “**DHCP** **Server**”
7. Select “**OPT1**”
8. Select “**ADD**” at the bottom of the page
9. Fill in the following
   1. MAC Address: Use the MAC address of the Kali VM Network adapter
      1. this can be located by navigating to VirtualBox Manager
      2. select “**Kali VM**”
      3. select “**Settings**”
      4. select “**Network**” tab
      5. expand the “**Advanced**” tab
   2. Client Identifier: “**Kali VM**”
   3. IP Address: **172.16.2.2**
   4. Description: Whatever you would like to put
10. Select “**Save**”
11. Select “**Apply Changes**”

Continue to “**Kali VM Setup**”

# Kali VM Setup

VM Settings

* Name: **“Kali VM”**
* Type: **“Linux”**
* Version: **“Debian (64-bit)”**
* Memory Size: **4096 MB**
* Hard Disk: **“Create a virtual hard disk now”**
* Hard disk file type: **“VDI (VirtualBox Disk Image)”**
* Storage of physical hard disk: **“Fixed size”**
* File location and size: **80.00 GB**
* Network Settings: Adapter 1: **Internal Network**

Setup

1. Download Kali Linux (https://cdimage.kali.org/kali-2022.3/kali-linux-2022.3-installer-amd64.iso)
2. Configure VM (*Complete step prior to starting VM*)
   1. Click “**Settings**”
   2. On “**System**” tab uncheck “**Floppy**”
   3. Select “**PS/2 Mouse**” for the Pointing Device
   4. On “**Storage**” tab select “**Empty**” then select the blue disc next to “**Optical Drive**”
   5. Select “**Choose/Create a Virtual Optical Disk…**”
   6. Select “Add” and navigate to your Kali Linux iso
   7. Once iso is selected, select “**Choose**”
   8. Click on “**Audio**” tab and uncheck “**Enable Audio**”
   9. Click on “**USB**” tab and uncheck “**Enable USB Controller**”
   10. Click on “**Network**” tab and enable adapter 1 and select “**Internal Network**”. (*Record the MAC address for each adapter*)

DHCP Mapping

1. Select “**Services**”
2. Select “**DHCP Server**”
3. Select “**OPT1**”
4. Select “**ADD**” at the bottom of the page
5. Fill in the following
   1. MAC Address: Use the MAC address of the Kali VM Network adapter
      1. this can be located by navigating to VirtualBox Manager
      2. select “**Kali VM**”
      3. select “**Settings**”
      4. select “**Network**” tab
      5. expand the “**Advanced**” tab under “**Adapter 3**”
   2. Client Identifier: “**Kali VM**”
   3. IP Address: **172.16.2.2**
   4. Description: Whatever you would like to put
6. Select “**Save**”
7. Select “**Apply** **Changes**”

Start VM and Update VM Settings

1. Follow the standard steps to fully install Kali Linux
2. Once completed shutdown VM and return the VirtualBox Manager Settings
3. Navigate to Ubuntu VM Settings
4. Select “**Storage**” tab
5. Select the Ubuntu ISO optical drive
6. Select the disk at the bottom of the box with the red “**X**” to remove the optical drive
7. Select “**System**”
8. Uncheck “**Optical**”
9. Highlight “**Hard** **Disk**”
10. Move “**Hard** **Disk**” to the top if the list

Update and Upgrade Machine

1. Open terminal
2. Execute the following commands
   1. **sudo apt update**
   2. **sudo apt upgrade -y**

# Ubuntu VM Setup

VM Settings

* Name: **“Ubuntu VM”**
* Type: **“Linux”**
* Version: **“Ubuntu (64-bit)”**
* Memory Size: **4096 MB**
* Hard Disk: **“Create a virtual hard disk now”**
* Hard disk file type: **“VDI (VirtualBox Disk Image)”**
* Storage of physical hard disk: **“Fixed size”**
* File location and size: **80.00 GB**
* Network Settings: Adapter 1: **Internal Network**

Setup

1. Download Ubuntu (https://ubuntu.com/download/desktop)
2. Configure VM (*Complete step prior to starting VM*)
   1. Click “**Settings**”
   2. On “**System**” tab uncheck “**Floppy**”
   3. Select “**PS/2 Mouse**” for the Pointing Device
   4. On “**Storage**” tab select “**Empty**” then select the blue disc next to “**Optical Drive**”
   5. Select “**Choose/Create a Virtual Optical Disk…**”
   6. Select “**Add**” and navigate to your **Ubuntu** iso
   7. Once iso is selected, select “**Choose**”
   8. Click on “**Audio**” tab and uncheck “**Enable Audio**”
   9. Click on “**USB**” tab and uncheck “**Enable USB Controller**”
   10. Click on “**Network**” tab and enable adapter 1 and select “**Internal Network**”. (*Record the MAC address for each adapter*)

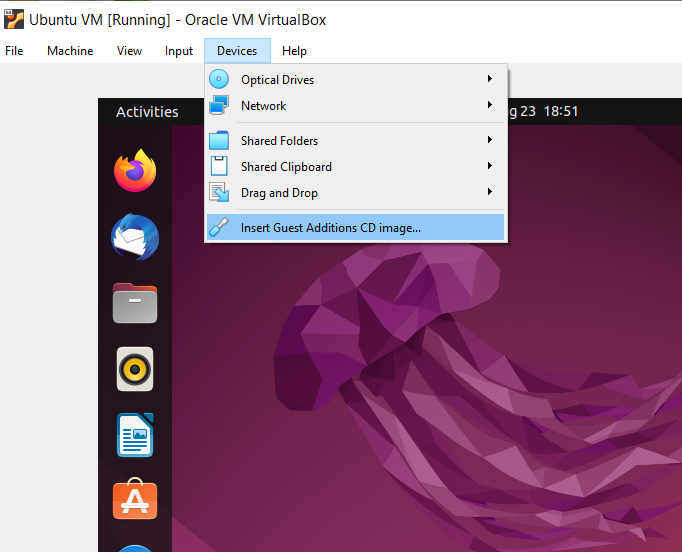
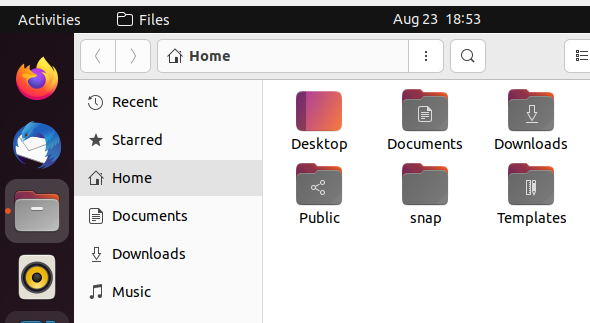
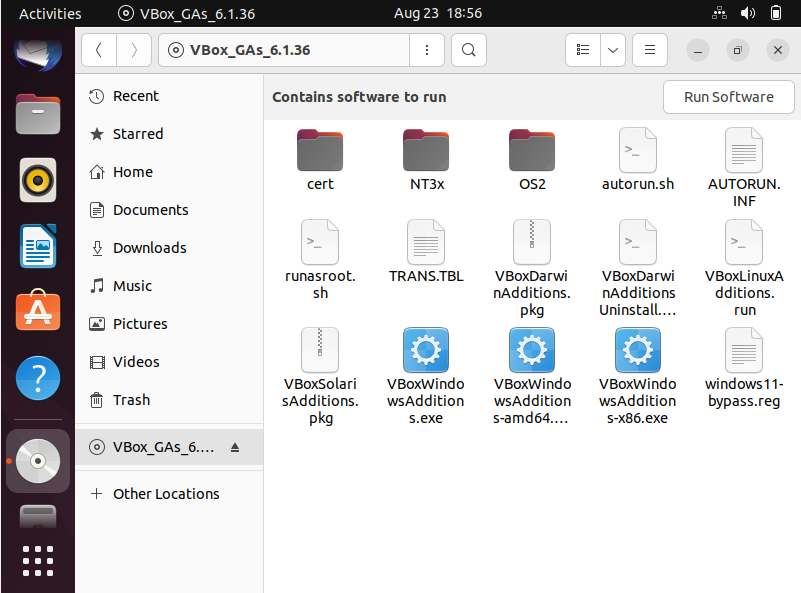
DHCP Mapping

1. Select “**Services**”
2. Select “**DHCP Server**”
3. Select “**OPT1**”
4. Select “**ADD**” at the bottom of the page
5. Fill in the following
   1. MAC Address: Use the MAC address of the Ubuntu VM Network adapter
      1. this can be located by navigating to VirtualBox Manager
      2. select “**Ubuntu VM**”
      3. select “**Settings**”
      4. select “**Network**” tab
      5. expand the “**Advanced**” tab under “**Adapter 1**”
   2. Client Identifier: “**Ubuntu VM**”
   3. IP Address: **172.16.2.5**
   4. Description: Whatever you would like to put
6. Select “**Save**”
7. Select “**Apply** **Changes**”

Start VM and Update VM Settings

1. Follow the standard steps to fully install Ubuntu
2. Once completed shutdown VM and return the VirtualBox Manager Settings
3. Navigate to Ubuntu VM Settings
4. Select “**Storage**” tab
5. Select the Ubuntu ISO optical drive
6. Select the disk at the bottom of the box with the red “**X**” to remove the optical drive
7. Select “**System**”
8. Uncheck “**Optical**”
9. Highlight “**Hard** **Disk**”
10. Move “**Hard** **Disk**” to the top if the list

Restart VM

1. Once restarted, at the top of the VM application, select “**Device**”
2. Select “**Insert Guest Additions CD Image**”
   1. 
3. Select “**Files**”
   1. 
4. Select “**VBox\_Gas\_6…”**
5. Select “**Run Software**”
   1. 
6. Allow to run and restart the VM
7. Restart the VM from the terminal or the desktop
8. After VM has restarted, you should be able to adjust the application window size

Update and Upgrade Machine

1. Open terminal
2. Execute the following commands
   1. **sudo apt update**
   2. **sudo apt upgrade -y**

Install CALDERA

1. **$ git clone https://github.com/mitre/caldera.git --recursive --branch**
2. **$ cd /caldera**
3. **$ pip install -r requirements.txt**
4. **$ python3 server.py --insecure**

# SIEM VM Setup

VM Settings

* Name: **“SIEM”**
* Type: **“Linux”**
* Version: **“Ubuntu (64-bit)”**
* Memory Size: **4096 MB**
* Hard Disk: **“Create a virtual hard disk now”**
* Hard disk file type: **“VDI (VirtualBox Disk Image)”**
* Storage of physical hard disk: **“Fixed size”**
* File location and size: **80.00 GB**
* Network Settings: Adapter 1: **Host-Only Adapter**

Setup

1. Download Ubuntu Server (<https://ubuntu.com/download/server>)
2. Configure VM (*Complete step prior to starting VM*)
   1. Click “**Settings**”
   2. On “**System**” tab uncheck “**Floppy**”
   3. Select “**PS/2 Mouse**” for the Pointing Device
   4. On “**Storage**” tab select “**Empty**” then select the blue disc next to “**Optical Drive**”
   5. Select “**Choose/Create a Virtual Optical Disk…**”
   6. Select “Add” and navigate to your Kali Linux iso
   7. Once iso is selected, select “**Choose**”
   8. Click on “**Audio**” tab and uncheck “**Enable Audio**”
   9. Click on “**USB**” tab and uncheck “**Enable USB Controller**”
   10. Click on “**Network**” tab and enable adapter 1 and select “**Host-Only Adapter**”. (*Record the MAC address for each adapter*)

DHCP Mapping

1. Select “**Services**”
2. Select “**DHCP Server**”
3. Select “**LAN**”
4. Select “**ADD**” at the bottom of the page
5. Fill in the following
   1. MAC Address: Use the MAC address of the SIEMVM Network adapter
      1. this can be located by navigating to VirtualBox Manager
      2. select “**SIEM VM**”
      3. select “**Settings**”
      4. select “**Network**” tab
      5. expand the “**Advanced**” tab under “**Adapter 1**”
   2. Client Identifier: “**SIEM VM**”
   3. IP Address: **172.16.1.3**
   4. Description: Whatever you would like to put
6. Select “**Save**”
7. Select “**Apply** **Changes**”

Start SIEM VM

1. Select installer
2. Select “**English**”
3. Select “**Update to the new installer**”
4. Select “**Done**”
5. Select “**Done**”
6. Select “**Done**”
7. Use UP arrow to “**Proxy** **Address**” and add [**http://172.16.1.1:3128**](http://172.16.1.1:3128)
8. Select “**Done**”
9. Select “**Done**”
10. Select “**Continue**”
11. Fill out “**Profile** **Setup**”
12. Select “**Done**”
13. Use SPACE bar to select “**Install OpenSSH server**”
14. Select “**Done**”
15. Use DOWN arrow until bottom and select “**Done**”
16. Once update and setup is complete, **DO NOT** reboot the VM. Shutdown the VM by pressing the “**X**” at the top of the application and selecting “**Power off the machine**”

Update SIEM VM Settings

1. Navigate to SIEM VM Settings
2. Select “**Storage**” tab
3. Select the Ubuntu ISO optical drive
4. Select the disk at the bottom of the box with the red “**X**” to remove the optical drive
5. Select “**System**”
6. Uncheck “**Optical**”
7. Highlight “**Hard** **Disk**”
8. Move “**Hard** **Disk**” to the top if the list

More pfSense Configuration

1. Navigate back to the pfSense webConfigurator in your browser
2. Select “**Services**”
3. Select “**NTP**”
4. Select both “**LAN**” and “**OPT1**”
5. Under “**Time** **Servers**”
   1. Delete the default one and add the following
      1. **0.north-america.pool.ntp.org**
      2. **1.north-america.pool.ntp.org**
      3. **2.north-america.pool.ntp.org**
      4. **3.north-america.pool.ntp.org**
6. Select “**Save**”
7. Select “**System**”
8. Select “**Package** **Manager**”
9. Select “**Available** **Packages**”
10. Search for “**squid**”
11. Select “**Install**” for squid
12. Select “**Services**”
13. Select “**Squid Proxy Server**”
14. Select “**Local Cache**”
15. Select “**Clear Cache**”
16. Ensure that “**Hard Disk Cache**” is **100**
17. Select “**Save**”
18. Select “**General**”
19. Place checkmark in box to “**Enable Squid Proxy**”
20. Select both “**LAN**” and “**OPT1**”
21. On “**Outgoing Network Interface**” select “**LAN**”
22. Ensure your settings resemble following screenshot
    1. Graphical user interface, text, application

       Description automatically generated
23. Select “Save”

Restart SIEM VM

1. Start SIEM VM
2. Sign in
3. Run the following commands
   1. **ip -br a**
   2. **nslookup** [**www.google.com**](http://www.google.com)
   3. **curl -I** [**https://www.google.com**](https://www.google.com)
4. Update VM (Use the following commands)
   1. **sud su –**
   2. **apt-get update**
   3. **apt-get -y dist-upgrade**
   4. **init 6** (this will reboot the VM)

***Refer to “Setting up the SIEM VM using Splunk” and “Setting up the Universal Forwarder” document to complete the SIEM Setup***

# IPS VM Setup

VM Settings

* Name: **“SIEM”**
* Type: **“Linux”**
* Version: **“Ubuntu (64-bit)”**
* Memory Size: **4096 MB**
* Hard Disk: **“Create a virtual hard disk now”**
* Hard disk file type: **“VDI (VirtualBox Disk Image)”**
* Storage of physical hard disk: **“Fixed size”**
* File location and size: **80.00 GB**
* Network Settings: Adapter 1: **Host-Only Adapter**

Setup

1. Download Ubuntu Server (<https://ubuntu.com/download/server>) *(use the same ISO from the SIEM VM)*
2. Configure VM (*Complete step prior to starting VM*)
   1. Click “**Settings**”
   2. On “**System**” tab uncheck “**Floppy**”
   3. Select “**PS/2 Mouse**” for the Pointing Device
   4. On “**Storage**” tab select “**Empty**” then select the blue disc next to “**Optical Drive**”
   5. Select “**Choose/Create a Virtual Optical Disk…**”
   6. Select “Add” and navigate to your Kali Linux iso
   7. Once iso is selected, select “**Choose**”
   8. Click on “**Audio**” tab and uncheck “**Enable Audio**”
   9. Click on “**USB**” tab and uncheck “**Enable USB Controller**”
   10. Click on “**Network**” tab and enable adapters 1, 2, and 3. ONLY change adapter 1 to “**Host-Only Adapter**” leave adapters 2 and 3 as “**Not Attached**” (*Record the MAC address for each adapter*)

DHCP Mapping in pfSense WebConfigurator in browser

1. Select “**Services**”
2. Select “**DHCP Server**”
3. Select “**LAN**”
4. Select “**ADD**” at the bottom of the page
5. Fill in the following
   1. MAC Address: Use the MAC address of the IPS VM Network adapter
      1. this can be located by navigating to VirtualBox Manager
      2. select “**IPS VM**”
      3. select “**Settings**”
      4. select “**Network**” tab
      5. expand the “**Advanced**” tab under “**Adapter 1**”
   2. Client Identifier: “**IPS VM**”
   3. IP Address: **172.16.1.4**
6. Description: Whatever you would like to put
7. Select “**Save**”
8. Select “**Apply Changes**”

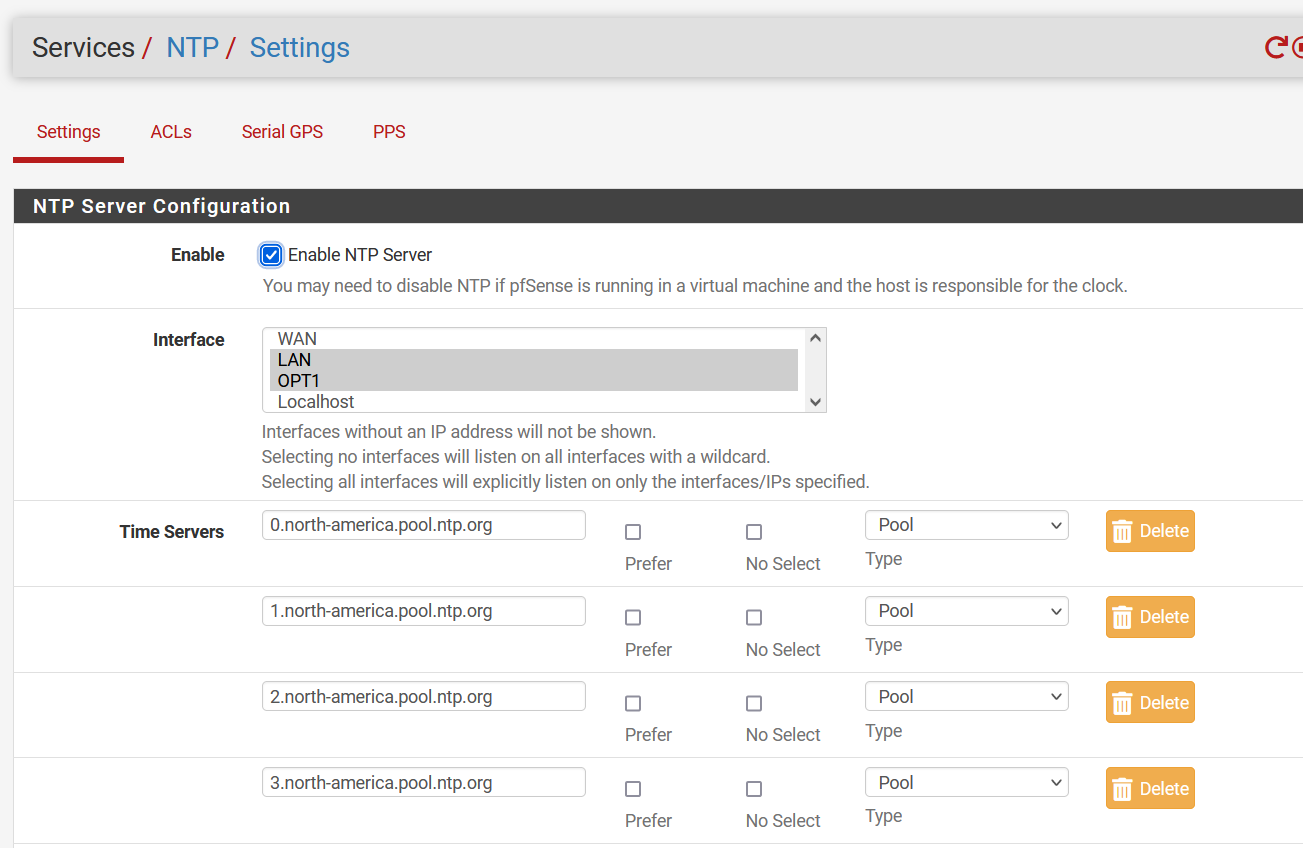
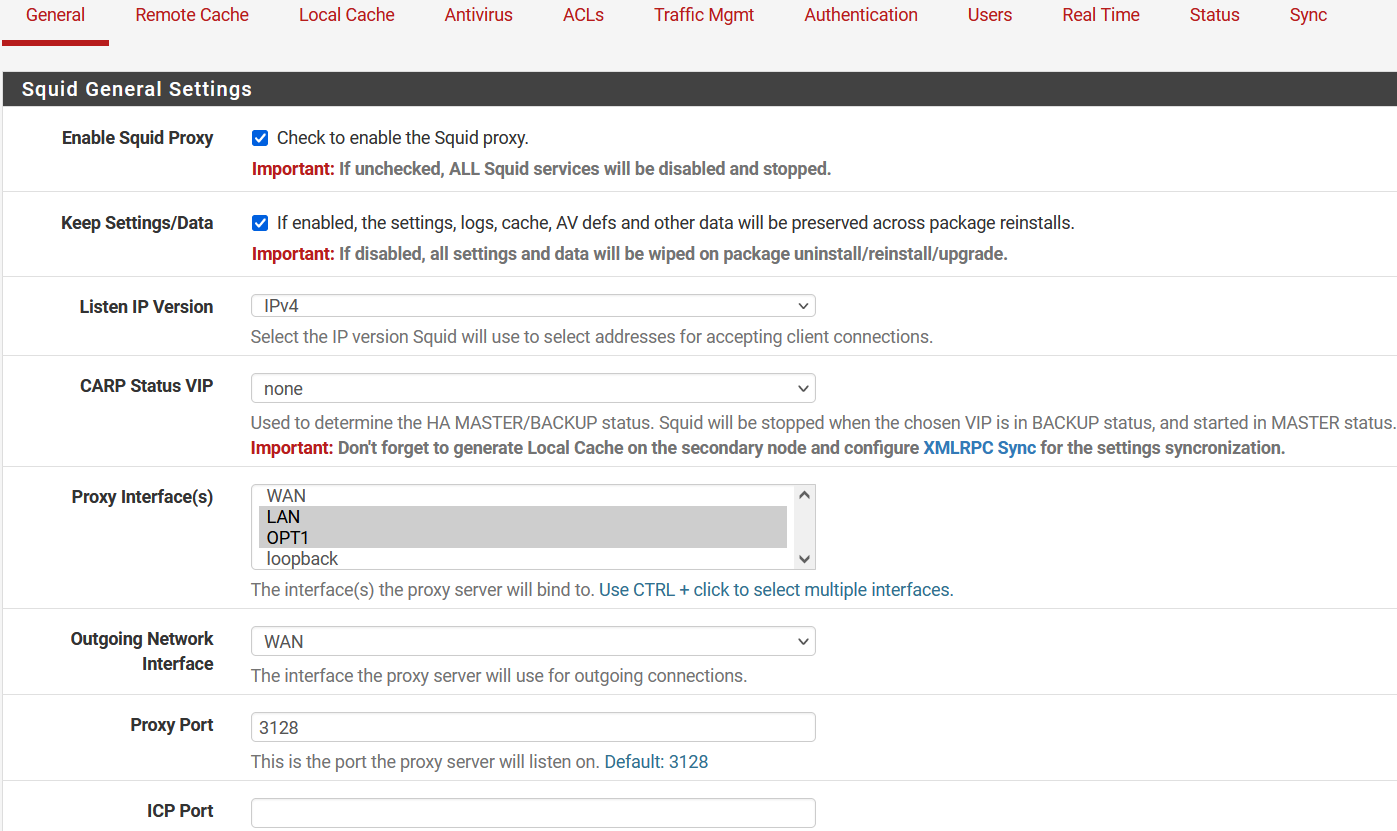
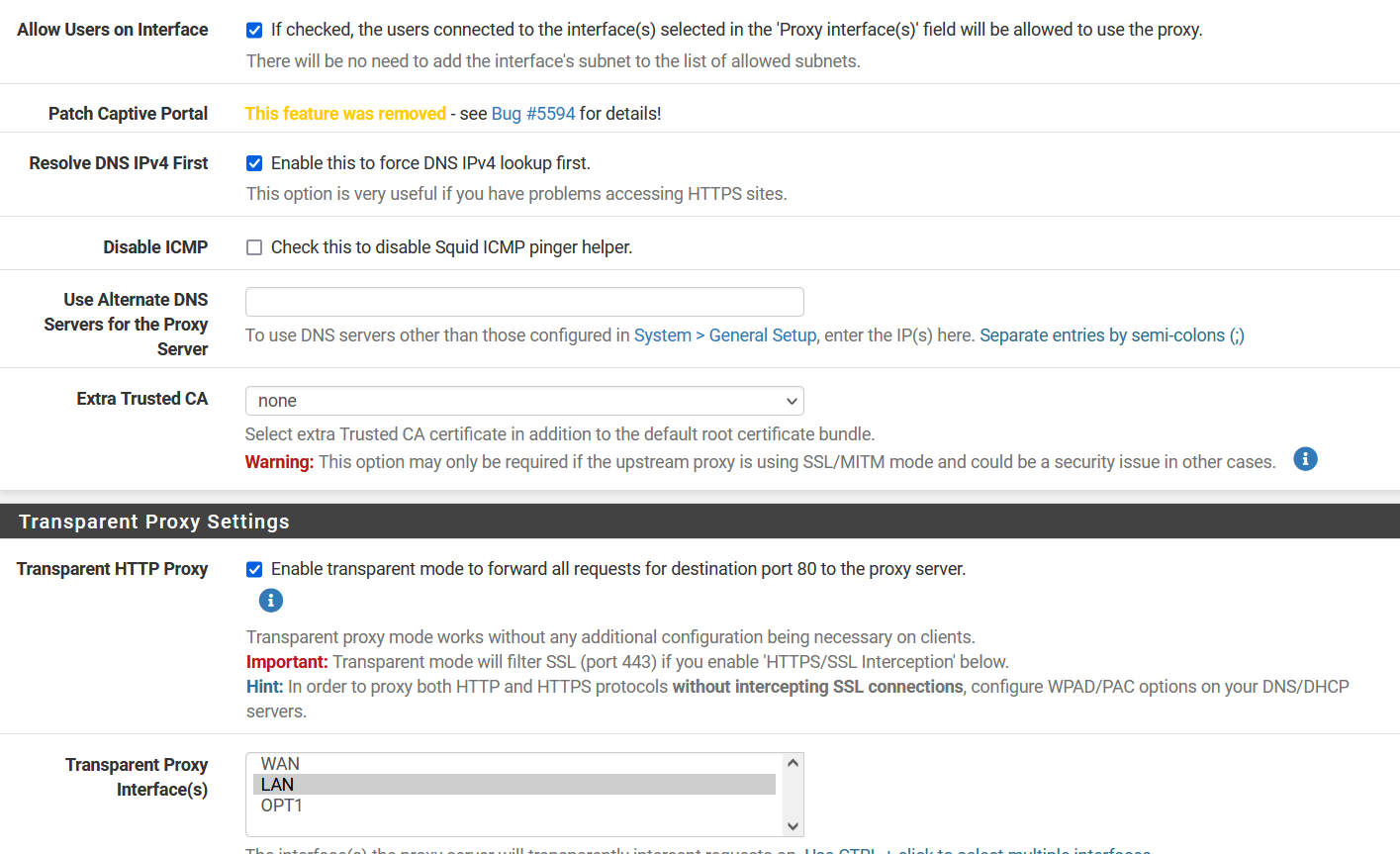
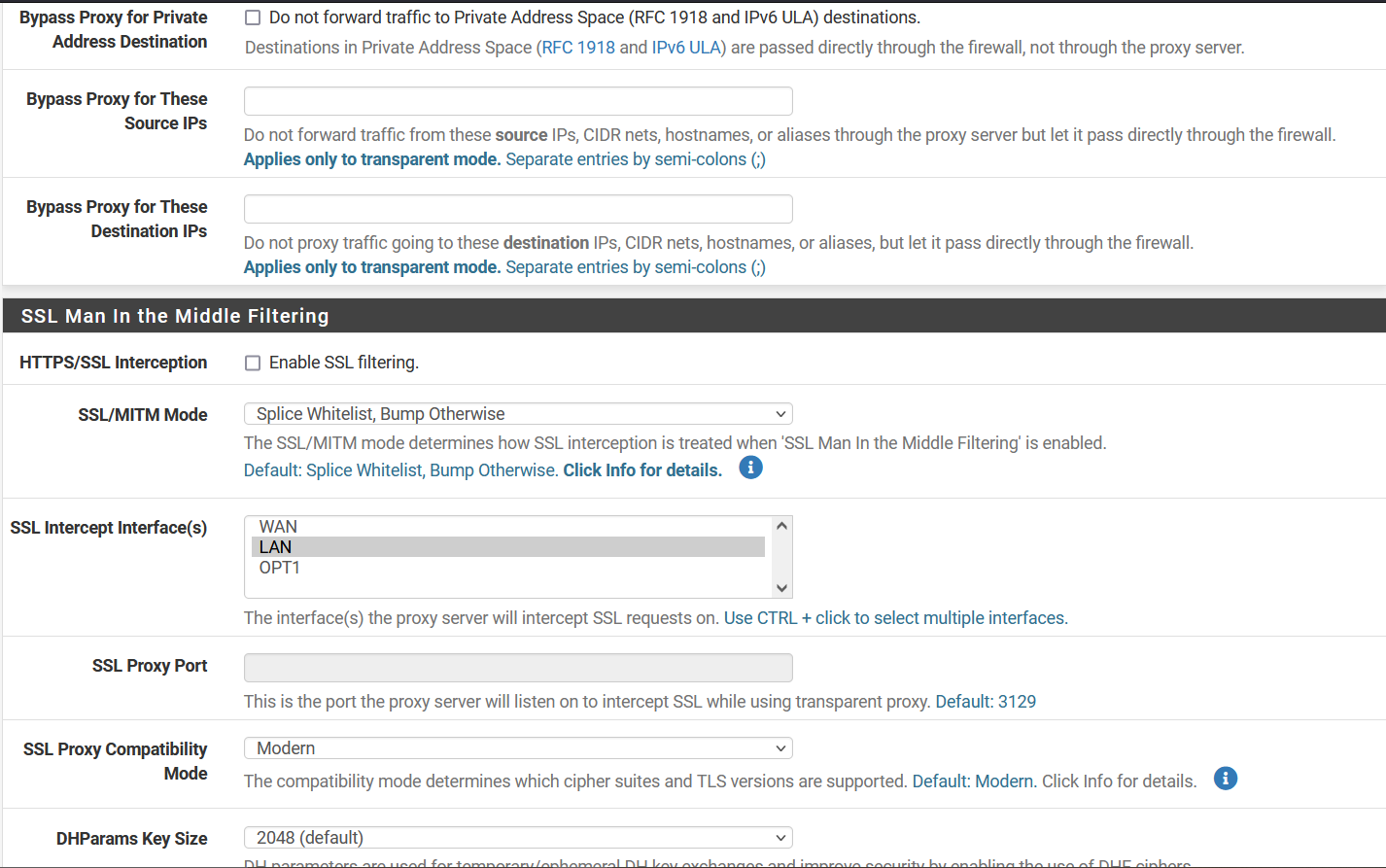
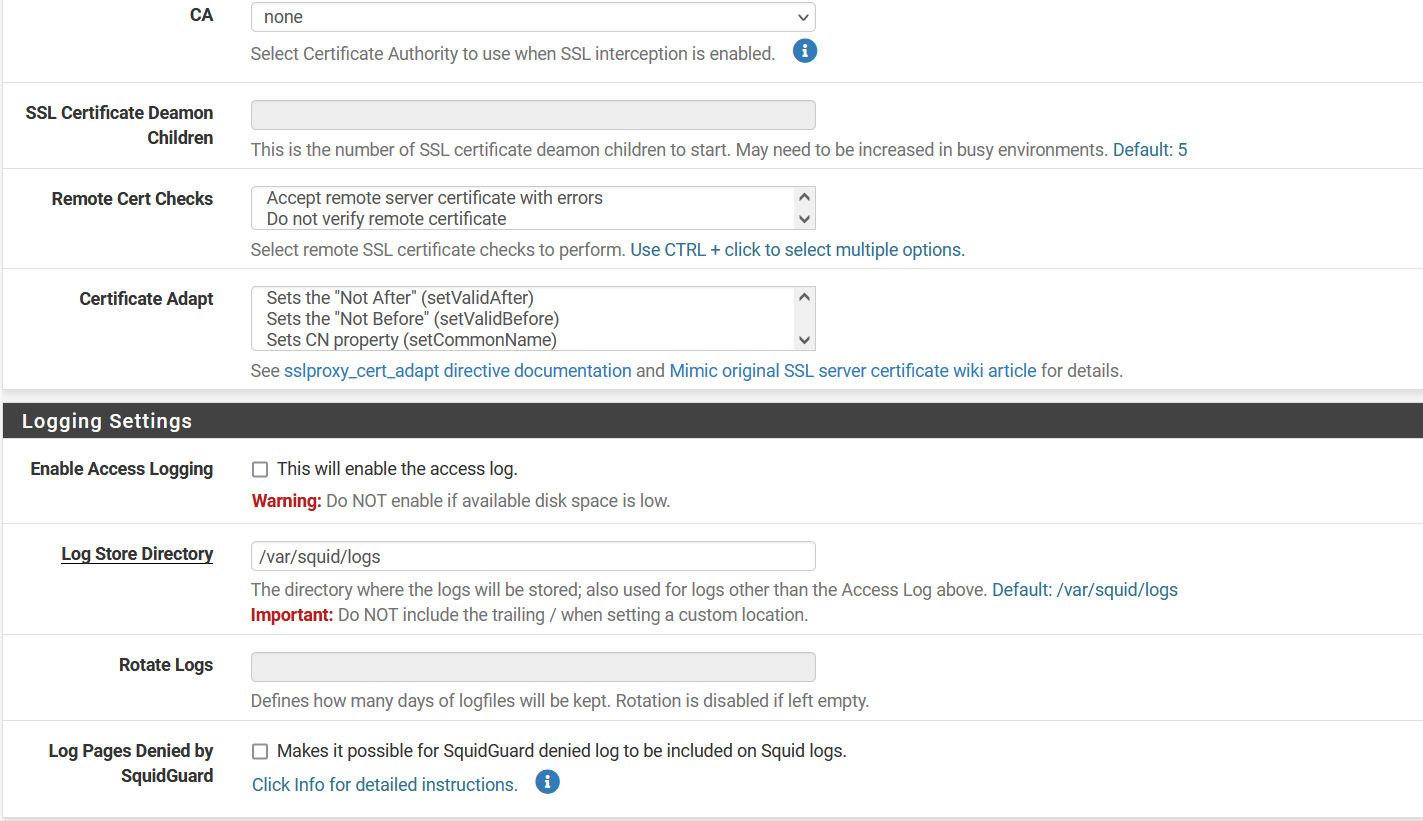
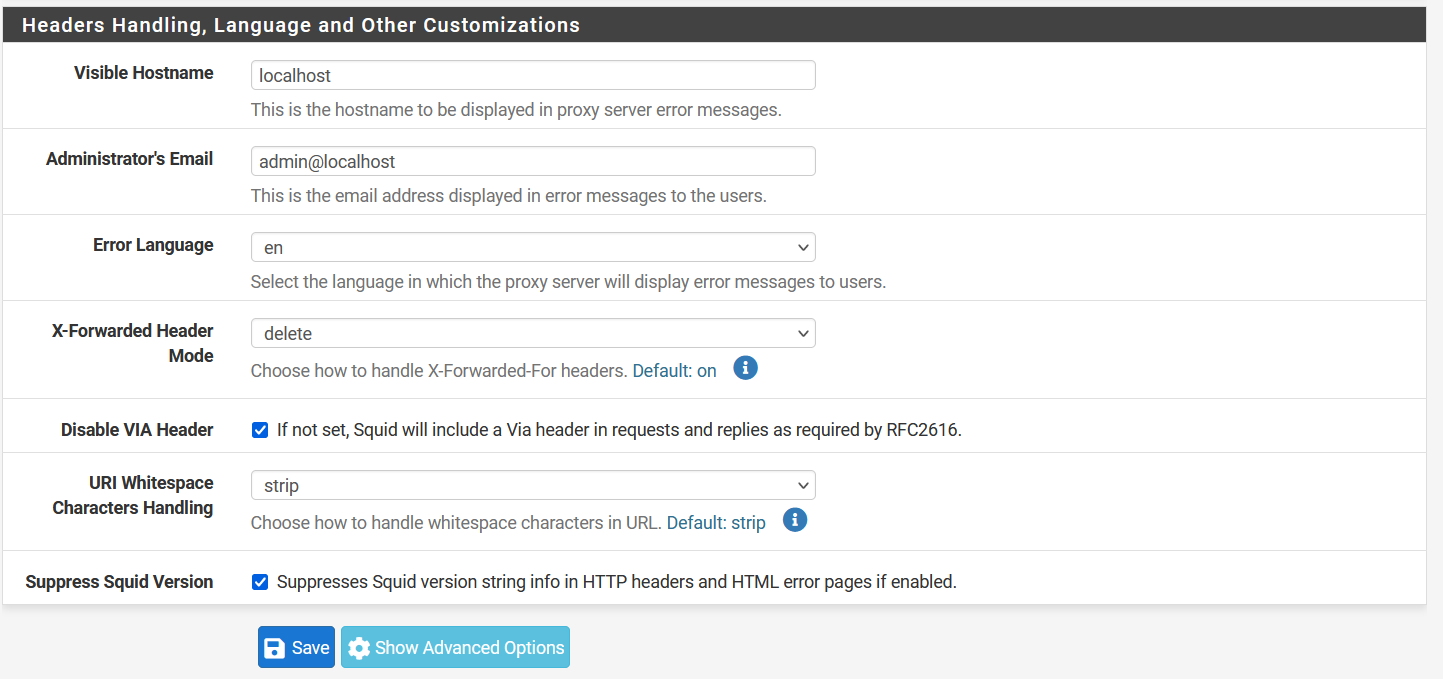
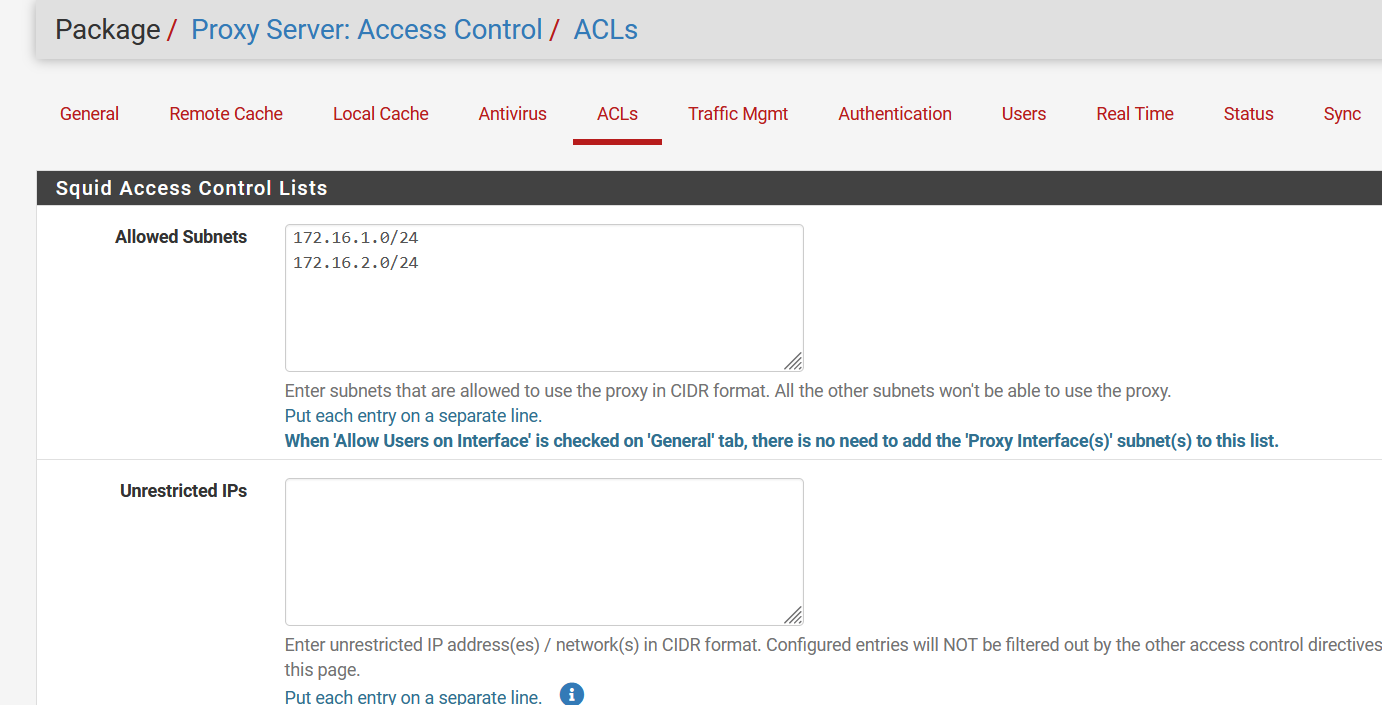
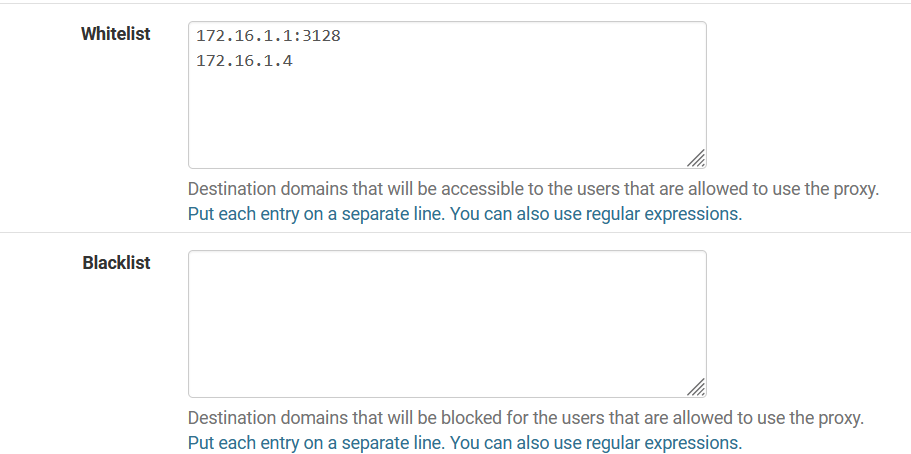
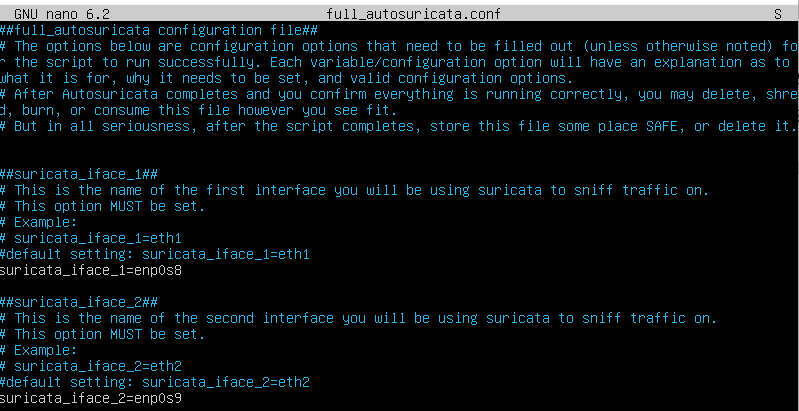
Start IPS VM

1. Select installer
2. Select “**English**”
3. Select “**Update to the new installer**”
4. Select “**Done**”
5. Select “**Done**”
6. Select “**Done**”
7. Use UP arrow to “**Proxy Address**” and add [**http://172.16.1.1:3128**](http://172.16.1.1:3128)
8. Select “**Done**”
9. Select “**Done**”
10. Select “**Continue**”
11. Fill out “**Profile Setup**”
12. Select “**Done**”
13. Use SPACE bar to select “**Install OpenSSH server**”
14. Select “**Done**”
15. Use DOWN arrow until bottom and select “**Done**”
16. Once update and setup is complete, DO NOT reboot the VM. Shutdown the VM by pressing the “**X**” at the top of the application and selecting “**Power off the machine**”

Update IPS VM Settings

1. Navigate to IPS VM Settings
2. Select “**Storage**” tab
3. Select the Ubuntu ISO optical drive
4. Select the disk at the bottom of the box with the red “**X**” to remove the optical drive
5. Select “**System**”
6. Uncheck “**Optical**”
7. Highlight “**Hard Disk**”
8. Move “**Hard Disk**” to the top if the list
9. Select “**Network**” tab
10. On “**Adapter 2**” change to “**Internal Network**” and Name to “**intent**”
11. Select “Advanced”
12. Change Promiscuous Mode to “**Allow VMs**”
13. On “**Adapter 3**” change to “**Internal Network**” and Name to “**intent1**”
14. Select “**Advanced**”
15. Change Promiscuous Mode to “**Allow VMs**”

Installing

1. Navigate back to pfSense WebConfigurator
   1. Select “**Services**”
   2. Select “**NTP**”
   3. Apply the following settings and save
      1. 
   4. Select “**System**”
   5. Select “**Package** **Manager**”
   6. Select “**Available** **Packages**”
   7. In the search bar type in “**squid**”
   8. Select the green button labeled “**Install**”
   9. Once installed select “**Services**”
   10. Select “**Squid Proxy Server**”
   11. Ensure that your setting match the following screenshots
       1. 
       2. 
       3. 
       4. 
       5. 
       6. Select “**Save**” once complete
   12. Scroll up to the top of the page and select “**ACLs**”
   13. Ensure your settings resemble screenshots below
       1. 
       2. 
   14. Return to IPS VM and execute the following commands (You will have to do the same on your Kali VM)
       1. **export HTTP\_PROXY=http://172.16.1.1:3128**
       2. **export http\_proxy=http://172.16.1.1:3128**
       3. **export HTTPS\_PROXY=**
       4. **export https\_proxy=**
2. In your IPS VM Install Suricata.
   1. Open terminal
   2. Use command **ip addr** and notate the two ethernet adapters
      1. Adapters should be **eth1** and **eth2** or **enp0s8** and **enp0s9**
   3. Run the following commands
      1. **git clone https://github.com/da667/Autosuricata**
      2. **cd Autosuricata/Autosuricata-Deb/AVATAR**
      3. **nano full\_autosuricata.conf**
         1. In the .conf file, edit the suricata\_iface names as shown in screenshot below
         2. 
      4. Save .conf file
      5. Use the following command to finish installing suricata
         1. **sudo bash autosuricata-deb-AVATAR.sh**
      6. After installation, the VM will reboot. Once rebooted, use the following command to ensure Suricata is up and running.

# Metasploitable 2 VM Setup

VM Settings

* Name: **“Metasploitable 2 VM”**
* Type: **“Linux”**
* Version: **“Ubuntu (64-bit)”**
* Memory Size: **512 MB**
* Hard Disk: **“Use and existing virtual hard disk file”**
* Hard disk file type: **“VDI (VirtualBox Disk Image)”**
* Storage of physical hard disk: **“Fixed size”**
* Network Settings: Adapter 1: “**Internal Network”**

Setup

1. Download Metasploitable2 (<https://www.vulnhub.com/entry/metasploitable-2,29/>)
2. Configure VM (*Complete step prior to starting VM*)
   1. Click “**Settings**”
   2. On “**System**” tab uncheck “**Floppy**”
   3. Select “**PS/2 Mouse**” for the Pointing Device
   4. On “**Storage**” tab select “**Empty**” then select the blue disc next to “**Optical Drive**”
   5. Select “**Choose/Create a Virtual Optical Disk…**”
   6. Select “Add” and navigate to your Kali Linux iso
   7. Once iso is selected, select “**Choose**”
   8. Click on “**Audio**” tab and uncheck “**Enable Audio**”
   9. Click on “**USB**” tab and uncheck “**Enable USB Controller**”
   10. Click on “**Network**” tab and enable adapter 1 and select “**Internal Network**” Use “**intnet1**” (*Record the MAC address for each adapter*)

DHCP Mapping in pfSense WebConfigurator in browser

1. Select “**Services**”
2. Select “**DHCP Server**”
3. Select “**OPT1**”
4. Select “**ADD**” at the bottom of the page
5. Fill in the following
   1. MAC Address: Use the MAC address of the Metasploitable 2 VM Network adapter
      1. this can be located by navigating to VirtualBox Manager
      2. select “**Metasploitable 2 VM**”
      3. select “**Settings**”
      4. select “**Network**” tab
      5. expand the “**Advanced**” tab under “**Adapter 1**”
   2. Client Identifier: “**Metasploitable 2 VM**”
   3. IP Address: **172.16.2.3**
6. Description: Whatever you would like to put
7. Select “**Save**”
8. Select “**Apply Changes**”

Start Metasploitable 2 VM

1. Allow VM to start and **DO NOT** sign in just yet.

# References

Burres, Ian. (2021). Personal Communication

Robinson, Tony. *Building Virtual Machine Labs: A Hands-On Guide*. 2017