

Jason Hodge

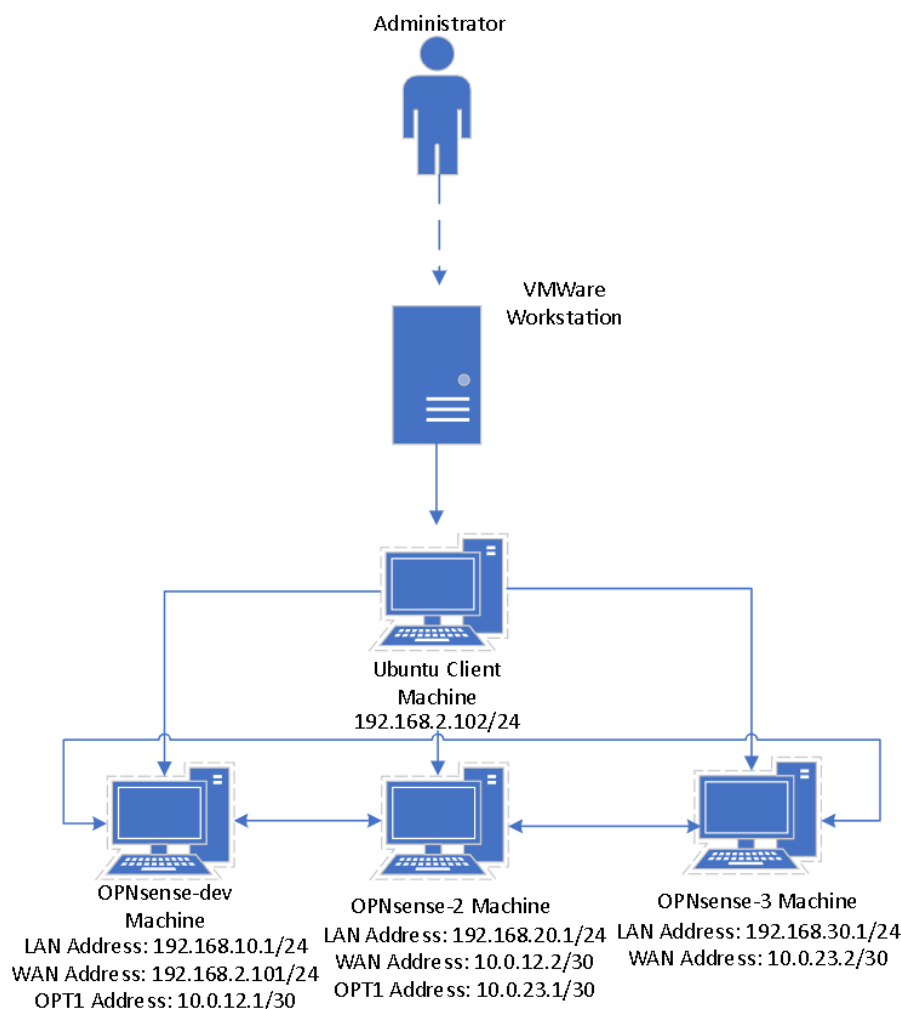
Lab 03 – Establishing BGP Peers with Opensource Router VNFs

April 1, 2024

Description:

The primary objective of this lab was to set up three OPNsense virtual machines (VMs) and configure them all as virtual router instances. Next, I updated the software on the machines and downloaded the FRR package. Then I set up virtual adapters and properly configured the networks with the appropriate static addresses. I then set up the BGP section of routing to establish communication as BGP Peers so two hosts would be able to communicate with one another.

Topology:



opnsense-dev

NA1: WAN, em0, vmnet12, 00:0C:29:A2:90:CA, 192.168.2.101/24
NA2: LAN, em1, vmnet9, 00:0C:29:A2:90:D4, 192.168.10.1/24
NA3: OPT1, em2, vmnet13, 00:0C:29:A2:90:DE, 10.0.12.1/30

opnsense-2

NA1: WAN, em0, vmnet13, 00:0C:29:06:2F:2F, 10.0.12.2/30
NA2: OPT1, em2, vmnet14, 00:0C:29:06:2F:39, 10.0.23.1/30
NA3: LAN, em1, vmnet10, 00:0C:29:06:2F:43, 192.168.20.1/24

opnsense-3

NA1: WAN, em0, vmnet14, 00:0C:29:DF:3D:3E:CA, 10.0.23.2/30
NA2: LAN, em1, vmnet11, 00:0C:29:DF:3D:48:D4, 192.168.30.1/24

This is an overview of the virtual machines built in this lab.

Key Syntax:

OPNsense:

Username: root or installer

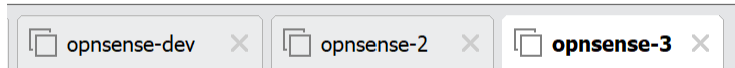
Password: opnsense

Note: Newer versions of OPNsense require more memory allocated when updating to the latest firmware. In this lab each machine had 2GB of memory.

Verification:

TASK ONE: OPNsense Installation

My OPNsense Appliance VM is up and running.



Here we can see the three machines are created.



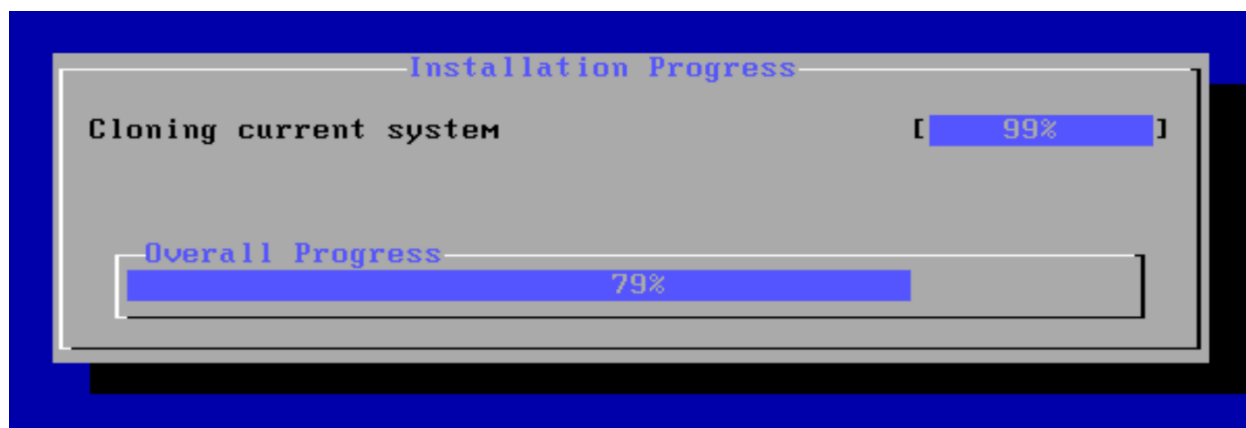
Here I clicked the first install option.



After, I clicked "OK" for the "da0" option as to where the VM should be stored on the disk.



Then, a safety page comes up asking if you are sure you want to destroy any contents on the disk. We click "YES".



This is the installation of the machine in progress.

← ↻ ⚠ Not secure | https://192.168.68.128/ui/core/firmware#updates

OPNsense <

Lobby

Reporting

System

Access

Configuration

Firmware

Status

Settings

Changelog

Updates

Plugins

Packages

Reporter

Log File

Gateways

High Availability

Routes

Settings

Trust

Wizard

Log Files

Diagnostics

Interfaces

Firewall

VPN

Services

Power

Help

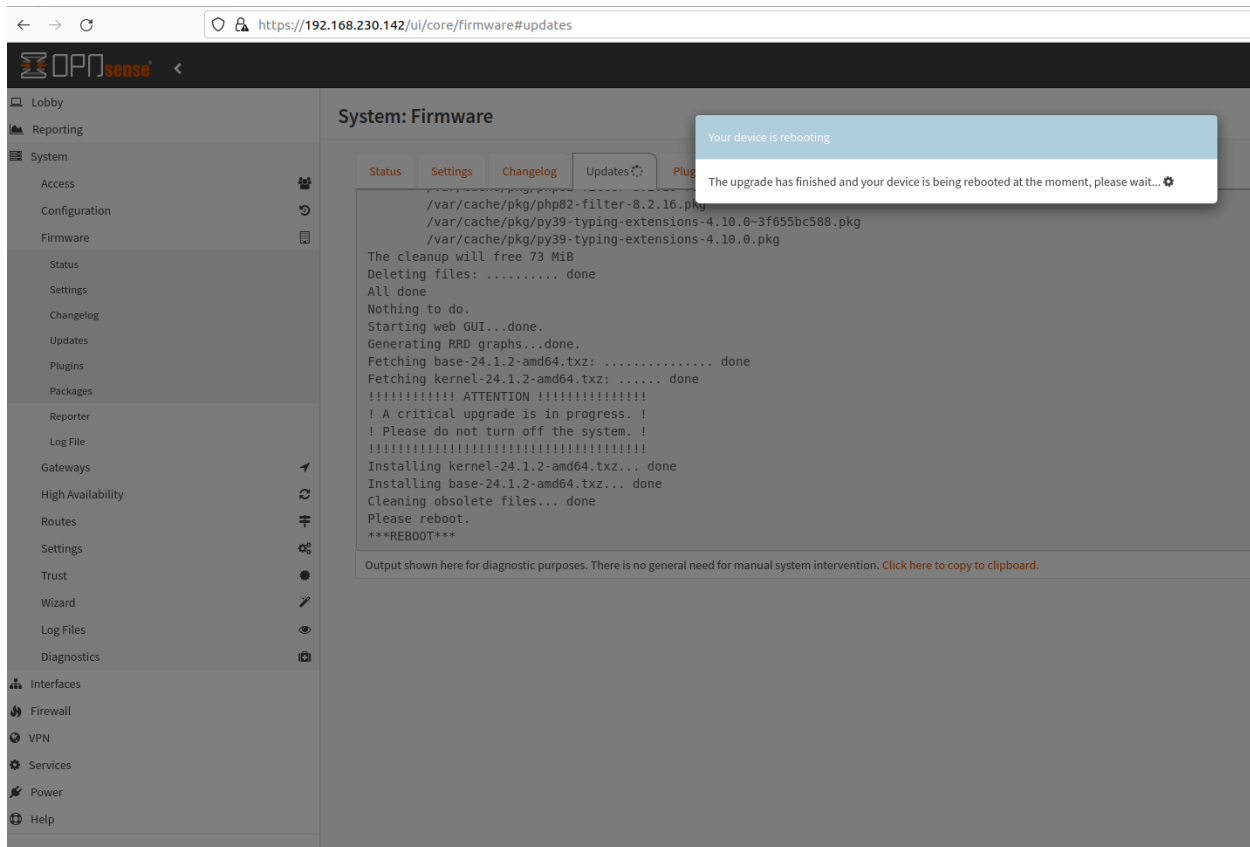
System: Firmware

StatusSettingsChangelogUpdates*PluginsPackages

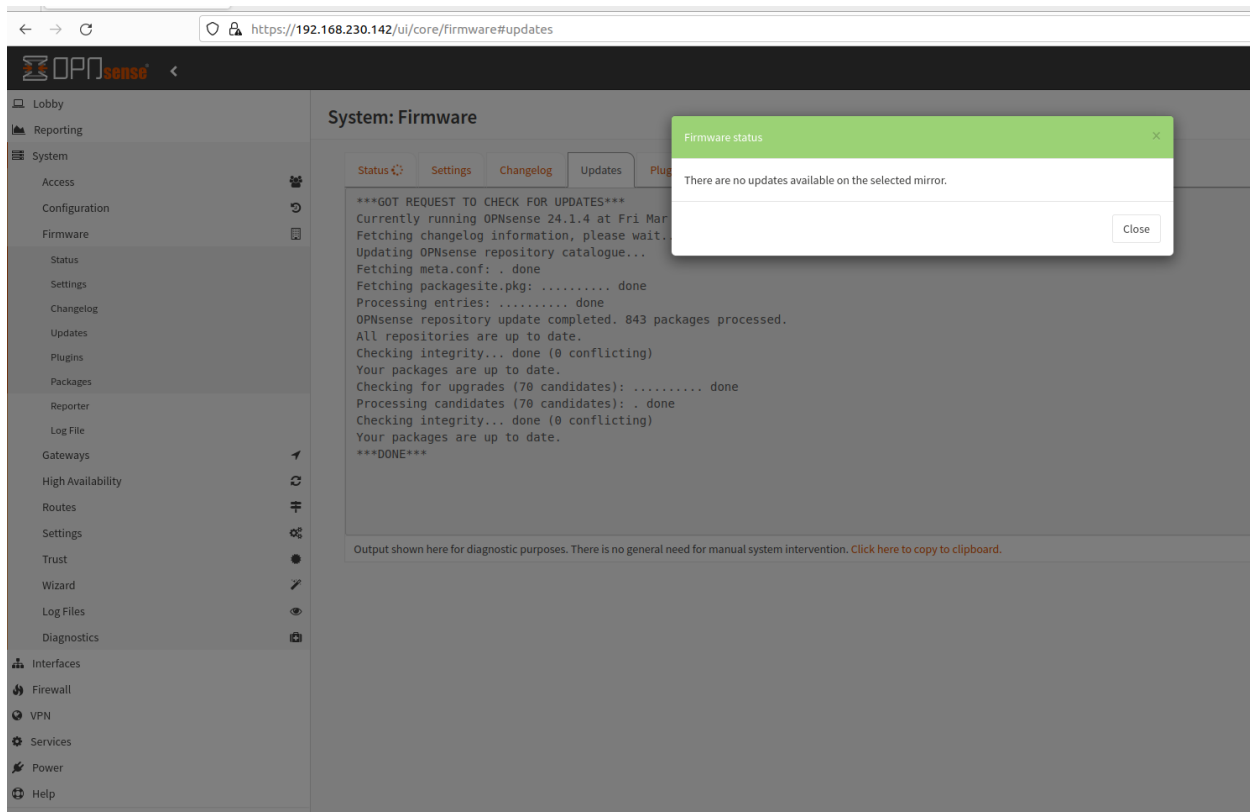
[23/64] Fetching libnghttp2-1.59.0.pkg: done
[24/64] Fetching libxml2-2.11.7.pkg: done
[25/64] Fetching krb5-1.21.2_3.pkg: done
[26/64] Fetching py39-dnspython-2.6.1,1.pkg: done
[27/64] Fetching php82-curl-8.2.16.pkg: done
[28/64] Fetching dnsmasq-2.90,1.pkg: done
[29/64] Fetching rrdtool-1.8.0_4.pkg: done
[30/64] Fetching py39-aioquic-0.9.25.pkg: done
[31/64] Fetching php82-phalcon-5.6.1.pkg: done
[32/64] Fetching radvd-2.19_3.pkg: done
[33/64] Fetching php82-mbstring-8.2.16.pkg: done
[34/64] Fetching ntp-4.2.8p17_2.pkg: done
[35/64] Fetching syslog-ng-4.6.0.pkg: done
[36/64] Fetching libpsl-0.21.5.pkg: done
[37/64] Fetching py39-numexpr-2.9.0.pkg: done
[38/64] Fetching py39-tzdata-2024.1.pkg: done
[39/64] Fetching php82-ldap-8.2.16.pkg: done
[40/64] Fetching libcjson-1.7.17.pkg: done
[41/64] Fetching ivykis-0.43.pkg: done
[42/64] Fetching kea-2.4.1_2.pkg: done

Output shown here for diagnostic purposes. There is no general need for manual system intervention. [Click here to copy to clipboard.](#)

Then after logging into one of the machines I started by updating to the latest firmware.



Here we can see the update was successful and the machine will reboot now.



Here we see, after checking for updates again, that the machine is up to date with the latest version and other updates.

OPNsense

Lobby

Reporting

System

Access

Configuration

Firmware

Status

Settings

Changelog

Updates

Plugins

Packages

Reporter

Log File

Gateways

High Availability

Routes

Settings

Trust

Wizard

Log Files

Diagnostics

Interfaces

Firewall

VPN

Services

Power

Help

System: Firmware

Status

Settings

Changelog

Updates

Plugins

Packages

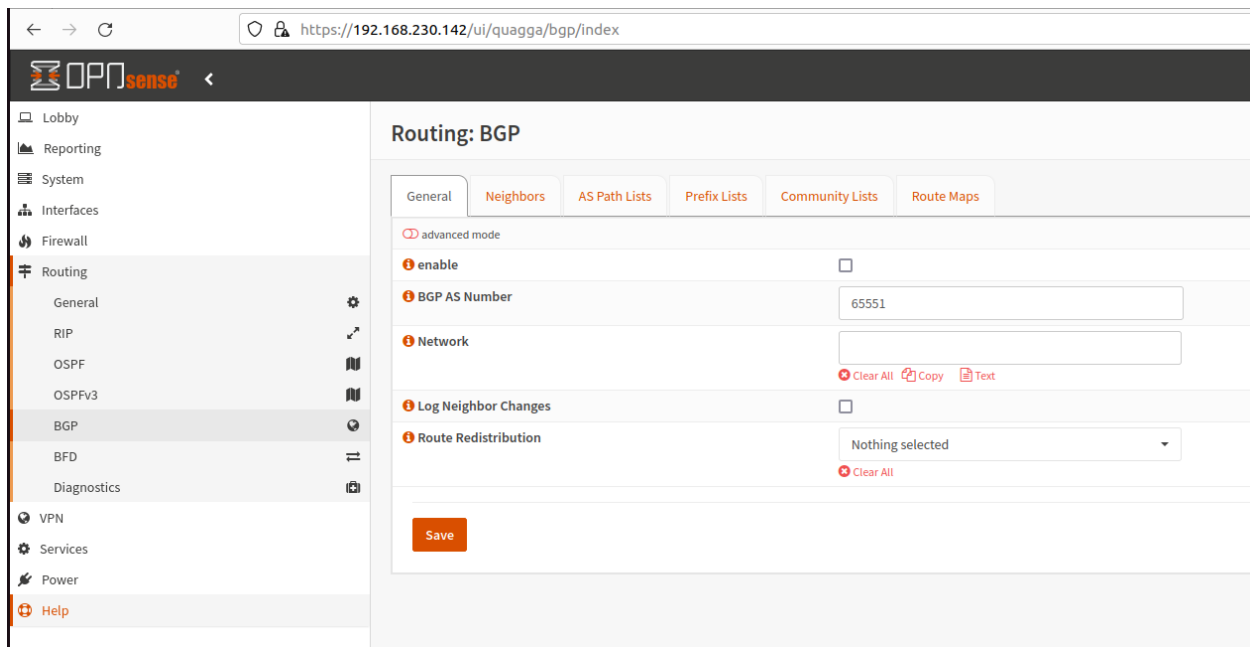
```
BATCH="yes"
=====
Message from frr8-8.5.4:

--
Beware that remote control of frr8 daemons over TCP sockets is enabled by
default.
Use daemon flags in /etc/rc.conf to disable it if unneeded, for example:
zebra_flags="-P0"
ospfd_flags="-P0"

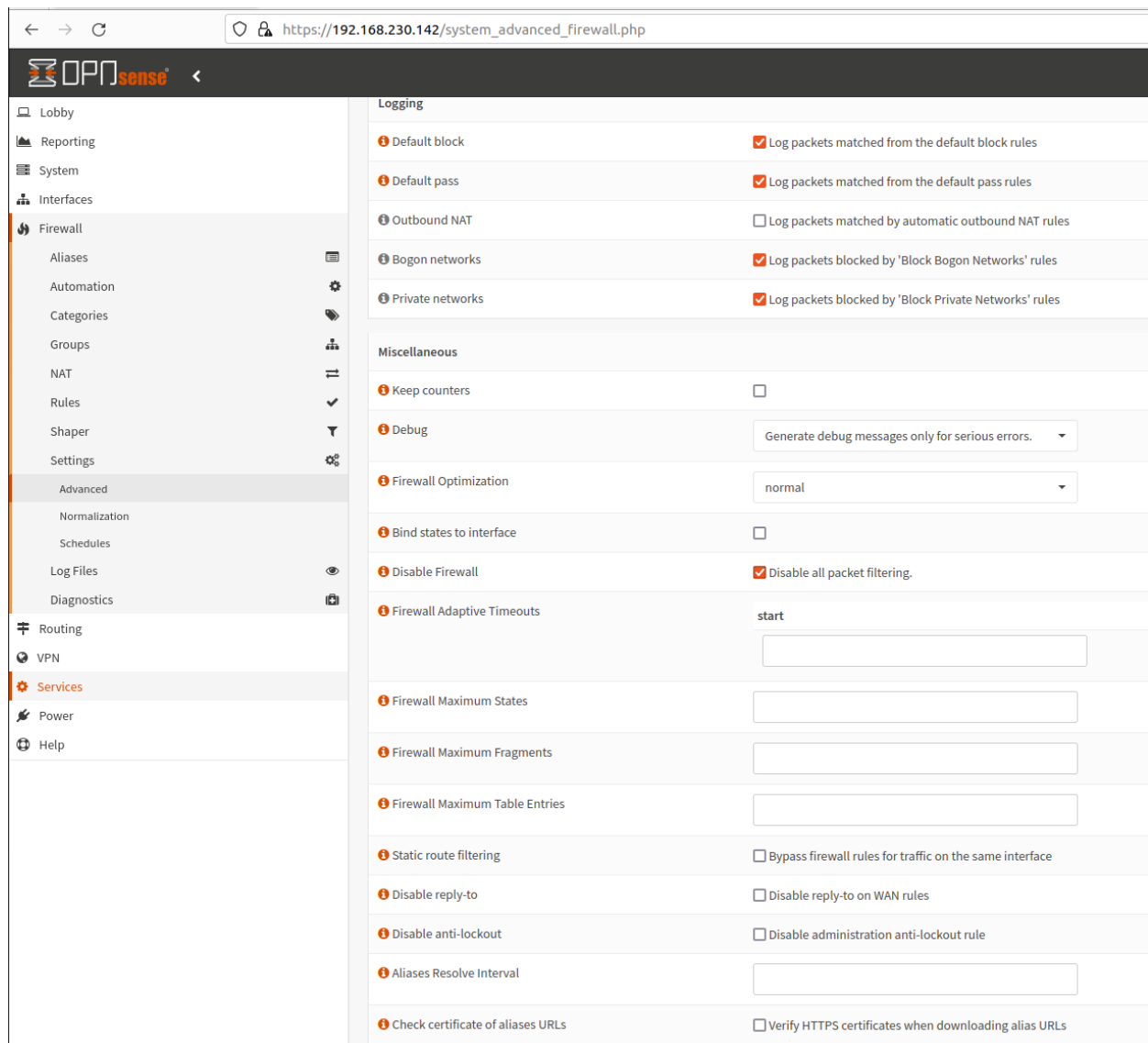
FRR's OSPF daemons tries to allocate big socket buffer, so generate warning
messages like:
"setsockopt_so_sendbuf: fd 6: SO_SNDBUF set to 1048576 (requested 8388608)"
To prevent such message kern.ipc.maxsockbuf can be increased:
sysctl kern.ipc.maxsockbuf=16777216
Checking integrity... done (0 conflicting)
Nothing to do.
***DONE***
```

Output shown here for diagnostic purposes. There is no general need for manual system intervention. [Click here to copy to clipboard.](#)

Next, I downloaded the plugin package for “The FRRouting Protocol Suite”, os-frr.



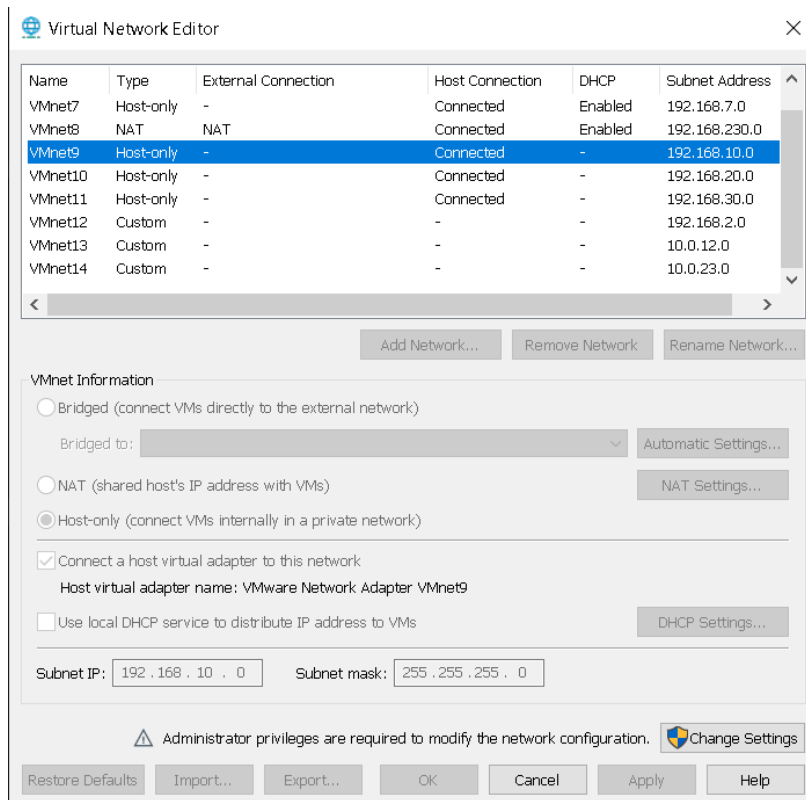
Here we can see the “Routing” tab is now available and BGP can now be configured.



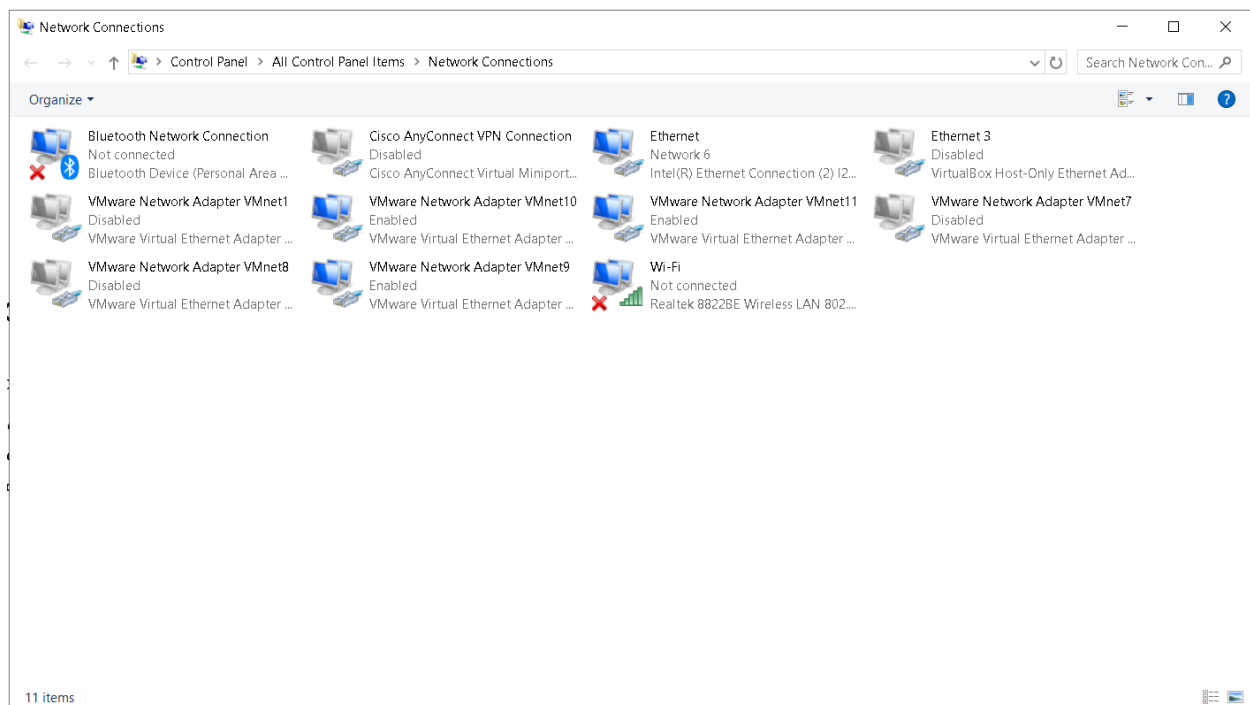
Then, under Firewall-settings I went to advanced and checked the box to disable all packet filtering from disable firewall.

Note: These same steps outlined above were repeated in the setup of the three virtual router instances.

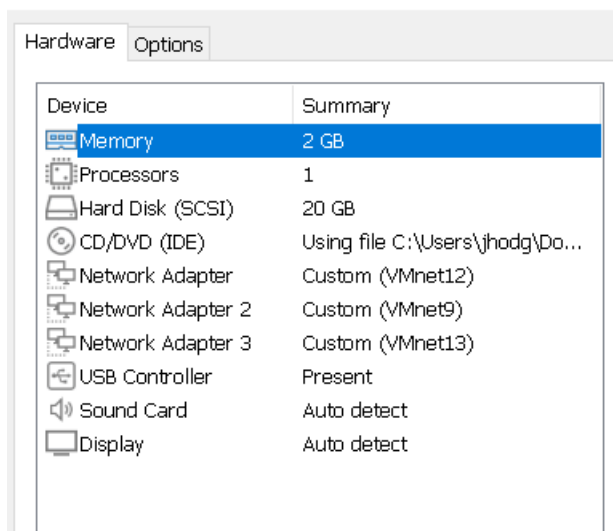
TASK TWO: Lab Environment VNF and VM Configuration



Here we can see the virtual network editor on VMware found under the edit tab. Here I added the appropriate subnet IP addresses and masks and created 6 VMnet adapters.



Here we see the Windows Network Connections on our physical host machine showing the proper network adapters. I configured the appropriate LAN bound network adapters with the proper static IP addresses valid on the appropriate networks.



Here we can see the network adapters configured to the OPNsense-dev machine.

```
https://192.168.10.1

*** opnsense-dev.localdomain: OPNsense 24.1.4 ***

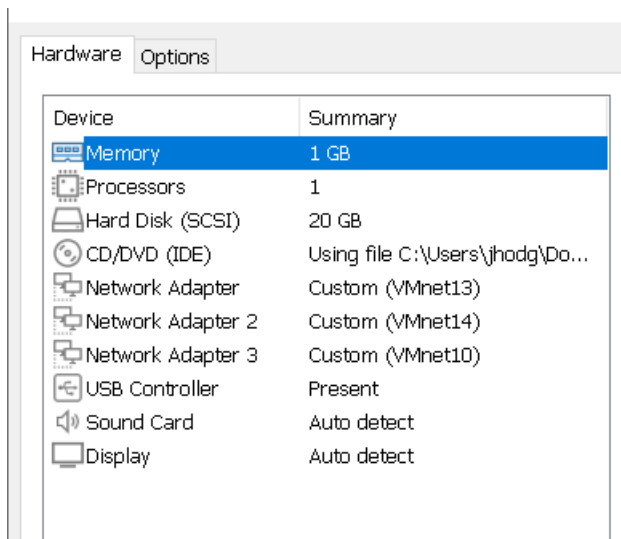
LAN (em1)      -> v4: 192.168.10.1/24
OPT1 (em2)     -> v4: 10.0.12.1/30
WAN (em0)      -> v4: 192.168.2.101/24

HTTPS: SHA256 8D 3E 56 26 25 43 89 8A C5 53 1C E2 74 EA DE AD
               14 03 11 20 7B 8A D3 F3 3D AF 2D 47 FA 81 4C 17

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system               13) Restore a backup

Enter an option: █
```

Here we see the configured OPNsense-dev machine with the proper interfaces and static addresses assigned to them.



Here we can see the network adapters configured to the OPNsense-2 machine.

```

*** OPNsense.localdomain: OPNsense 24.1.4 ***

LAN (em1)      -> v4: 192.168.20.1/24
OPT1 (em2)     -> v4: 10.0.23.1/30
WAN (em0)      -> v4: 10.0.12.2/30

HTTPS: SHA256 00 5F 90 71 CA 8B D8 C9 34 ED A3 79 5D 5C 73 3A
               F2 E4 4D B2 A9 1D 19 C5 AF 92 2B E1 51 46 3A 76

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system               13) Restore a backup

Enter an option: █

```

Here we see the configured OPNsense-2 machine with the proper interfaces and static addresses assigned to them.

Hardware Options	
Device	Summary
Memory	1 GB
Processors	1
Hard Disk (SCSI)	20 GB
CD/DVD (IDE)	Using file C:\Users\jhodg\Do...
Network Adapter	Custom (VMnet14)
Network Adapter 2	Custom (VMnet11)
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Here we can see the network adapters configured to the OPNsense-3 machine.

```
*** OPNsense.localdomain: OPNsense 24.1.4 ***

LAN (em1)      -> v4: 192.168.30.1/24
WAN (em0)      -> v4: 10.0.23.2/30

HTTPS: SHA256 CC 5A 8A 4C 0E F9 3D 4F 98 F6 92 34 BA D2 A6 8F
              0D B2 66 09 94 4D 38 E3 89 EF 36 55 A9 69 EC 2D

0) Logout                      7) Ping host
1) Assign interfaces           8) Shell
2) Set interface IP address    9) pfTop
3) Reset the root password     10) Firewall log
4) Reset to factory defaults   11) Reload all services
5) Power off system            12) Update from console
6) Reboot system               13) Restore a backup

Enter an option: █
```

Here we see the configured OPNsense-3 machine with the proper interfaces and static addresses assigned to them.

TASK THREE: OPNsense FRR BGP Installation and Configuration

Under the Routing-BGP tab I then set up my BGP for the neighbor configurations on each of the OPNsense virtual router machines.

https://192.168.10.1/ui/quagga/bgp/index

Routing: BGP

General Neighbors AS Path Lists Prefix Lists Community Lists Route Maps

advanced mode

enable ☒

BGP AS Number

Network [Clear All](#) [Copy](#) [Text](#)

Log Neighbor Changes ☐

Route Redistribution [Clear All](#)

[Save](#)

Here I set the proper configurations on the general tab. The Autonomous System Number: 1000, the proper network subnet, and the route distribution to the proper option.

Routing: BGP

General

Neighbors

AS Path List

Enabled

Description

dev to 2

dev to 2

dev to 2

1

2

3

4

advanced mode

full help

Enabled

Description

Peer-IP

Remote AS

Update-Source Interface

Next-Hop-Self

Next-Hop-Self All

Multi-Hop

Route Reflector Client

Soft reconfiguration inbound

BFD

Send Defaultroute

Enable AS-Override

Disable Connected Check

Prefix-List In

Prefix-List Out

Route-Map In

Route-Map Out

dev to 2

192.168.20.1

2000

LAN

Cancel

Save

Here I configured the first neighbor, dev to 2, and filled out the proper fields.

Routing: BGP

General Neighbors AS Path Lists

Advanced mode full help

Edit Neighbor

Enabled ☒

Description dev to 3

Peer-IP 192.168.30.1

Remote AS 3000

Update-Source Interface LAN

Next-Hop-Self ☒

Next-Hop-Self All ☐

Multi-Hop ☒

Route Reflector Client ☐

Soft reconfiguration inbound ☐

BFD ☒

Send Defaultroute ☐

Enable AS-Override ☐

Disable Connected Check ☐

Prefix-List In None

Prefix-List Out None

Route-Map In None

Route-Map Out None







Cancel Save


Here I configured the second neighbor, dev to 3, and filled out the proper fields.

Routing: BGP

General Neighbors AS Path Lists Prefix Lists Community Lists Route Maps

Search 7

Enabled	Description	Neighbor Address	Remote AS	Prefix List inbound	Prefix List outbound	Route Map inbound	Route Map outbound	Commands
<input checked="" type="checkbox"/>	dev to 2	192.168.20.1	2000	None	None	None	None	  
<input checked="" type="checkbox"/>	dev to 3	192.168.30.1	3000	None	None	None	None	  

+ 

Showing 1 to 2 of 2 entries

Here we can see both neighbors have been added to the neighbors list.

Routing: Diagnostics: BGP
routerid: 192.168.10.1, localAS: 1000

IPv4 Routing Table IPv6 Routing Table Neighbors Summary

Search

Valid	Best	Internal	Network	Next Hop	Metric	LocPrf	Weight	Path	Origin
✓	✓	✗	10.0.12.0/30	0.0.0.0	1		32768	Internal	?
✓	✓	✗	192.168.2.0/24	0.0.0.0	1		32768	Internal	?
✓	✗	✗	192.168.10.0/24	0.0.0.0	1		32768	Internal	?
✓	✓	✗	192.168.10.0/24	0.0.0.0	0		32768	Internal	IGP

Showing 1 to 4 of 4 entries

Here we can see the neighbors BGP connections on the OPNsense-dev machine.

https://192.168.20.1/ui/quagga/bgp/index

Routing: BGP

General Neighbors AS Path Lists Prefix Lists Community Lists Route Maps

advanced mode

enable ☒

BGP AS Number 2000

Network 192.168.20.0
 Clear All Copy Text

Log Neighbor Changes ☐

Route Redistribution Connected routes (directly attached subnet or host)
 Clear All

Save

Here I set the proper configurations on the general tab. The Autonomous System Number: 2000, the proper network subnet, and the route distribution to the proper option.

Routing: BGP

General Neighbors AS

Enabled

2

2

« < 1 > »

advanced mode full help

Edit Neighbor

Enabled	<input checked="" type="checkbox"/>
Description	2 to dev
Peer-IP	192.168.10.1
Remote AS	1000
Update-Source Interface	LAN
Next-Hop-Self	<input checked="" type="checkbox"/>
Next-Hop-Self All	<input type="checkbox"/>
Multi-Hop	<input checked="" type="checkbox"/>
Route Reflector Client	<input type="checkbox"/>
Soft reconfiguration inbound	<input type="checkbox"/>
BFD	<input checked="" type="checkbox"/>
Send Defaultroute	<input type="checkbox"/>
Enable AS-Override	<input type="checkbox"/>
Disable Connected Check	<input type="checkbox"/>
Prefix-List In	None
Prefix-List Out	None
Route-Map In	None
Route-Map Out	None

Cancel Save

Here I configured the first neighbor, 2 to dev, and filled out the proper fields.

Routing: BGP

General Neighbors AS

advanced mode full help

Enabled ☒

Description 2 to 3

Peer-IP 192.168.30.1

Remote AS 3000

Update-Source Interface LAN

Next-Hop-Self ☒

Next-Hop-Self All ☐

Multi-Hop ☒

Route Reflector Client ☐

Soft reconfiguration inbound ☐

BFD ☒

Send Defaultroute ☐

Enable AS-Override ☐

Disable Connected Check ☐

Prefix-List In None

Prefix-List Out None

Route-Map In None

Route-Map Out None

Cancel Save

Here I configured the second neighbor, 2 to 3, and filled out the proper fields.

Routing: BGP

General Neighbors AS Path Lists Prefix Lists Community Lists Route Maps

Search

Enabled	Description	Neighbor Address	Remote AS	Prefix List inbound	Prefix List outbound	Route Map inbound	Route Map outbound	Commands
<input checked="" type="checkbox"/>	2 to dev	192.168.10.1	1000	None	None	None	None	
<input checked="" type="checkbox"/>	2 to 3	192.168.30.1	3000	None	None	None	None	

Showing 1 to 2 of 2 entries

Here we can see both neighbors have been added to the neighbors list.

Routing: Diagnostics: BGP
 routerId: 192.168.20.1, localAS: 2000

IPv4 Routing Table IPv4 Routing Table Neighbors Summary

Valid	Best	Internal	Network	Next Hop	Metric	LocPrf	Weight	Path	Origin
✓	✓	✗	10.0.32.0/30	0.0.0.0	1		32768	Internal	?
✓	✓	✗	10.0.23.0/30	0.0.0.0	1		32768	Internal	?
✓	✗	✗	192.168.20.0/24	0.0.0.0	1		32768	Internal	?
✓	✓	✗	192.168.20.0/24	0.0.0.0	0		32768	Internal	IGP

Showing 1 to 4 of 4 entries

Here we can see the neighbors BGP connections on the OPNsense-2 machine.

https://192.168.30.1/ui/quagga/bgp/index

Routing: BGP

General Neighbors AS Path Lists Prefix Lists Community Lists Route Maps

advanced mode

enable ☒

BGP AS Number 3000

Network 192.168.30.0
 Clear All Copy Text

Log Neighbor Changes ☐

Route Redistribution Connected routes (directly attached subnet or host)
 Clear All

Save

Here I set the proper configurations on the general tab. The Autonomous System Number: 3000, the proper network subnet, and the route distribution to the proper option.

Routing: BGP

General

Neighbors

AS

Enabled

3

3

«

<

1

>

»

Edit Neighbor

advanced mode

full help

Enabled

Description

Peer-IP

Remote AS

Update-Source Interface

Next-Hop-Self

Next-Hop-Self All

Multi-Hop

Route Reflector Client

Soft reconfiguration inbound

BFD

Send Defaultroute

Enable AS-Override

Disable Connected Check

Prefix-List In

Prefix-List Out

Route-Map In

Route-Map Out

3 to dev

192.168.10.1

1000

LAN

None

None

None

None

Cancel

Save

Here I configured the first neighbor, 3 to dev, and filled out the proper fields.

Here I configured the second neighbor, 3 to 2, and filled out the proper fields.

Here we can see both neighbors have been added to the neighbors list.

Routing: Diagnostics: BGP
routerId : 192.168.30.1, localAS : 3000

IPv4 Routing Table IPv6 Routing Table Neighbors Summary

Search

Valid	Best	Internal	Network	Next Hop	Metric	LocPrf	Weight	Path	Origin
✓	✓	✗	10.0.23.0/30	0.0.0.0	1		32768	Internal	?
✓	✗	✗	192.168.30.0/24	0.0.0.0	1		32768	Internal	?
✓	✓	✗	192.168.30.0/24	0.0.0.0	0		32768	Internal	IGP

Showing 1 to 3 of 3 entries

Here we can see the neighbors BGP connections on the OPNsense-3 machine.

OPNsense

Lobby Reporting System Interfaces Firewall Routing

Routing: General

advanced mode

Enable ☒

Enable CARP Failover ☐

Enable SNMP AgentX Support ☐

Enable logging ☒

Log Level Notifications

Firewall rules ☒

Save

For all three machines I checked off the “Enable” box to activate the routing service.

The “Announce All” setting was not apparent, and it seems I was not the only one who could not find it. It could potentially be possible this setting was changed or called something different in the latest update of OPNsense. This setting being turned on/configured would have allowed me to announce all of the network routes to its peers. Without this setting being activated the routers could not learn about their peers.

Conclusion:

This lab was challenging as OPNsense is a relatively new software and there are not many resources to help with all of its features. I had some trouble along the way with updating the firmware, which the solution was to increase the memory allocated to the OPNsense machine to greater than previously anticipated. It seems the software feature updates are getting bigger as the software progresses. Then I hit a roadblock with properly setting up the interfaces, which thanks to your help I got through! I hit a stopping point with not finding the

“Announce All” setting, which as stated above was not apparent. Other than that, I enjoyed the lab and gained further experience with using OPNsense.

References:

https://docs.securedrop.org/en/stable/admin/installation/firewall_opnsense.html

<https://polarclouds.co.uk/opnsense-bgp-bfd-config/>