Updated Aug 26, 2023

Lab 1.1 - Routing and DMZ

Pre-Lab: Start Tech Journal

Many of the commands and configurations used in this lab will be repeated throughout the course. Therefore, creating a well organized and thorough Tech Journal is critical to success. Deliverables 9 and 10 of the lab require submission of your Tech Journal. Instead of completing at the end, it is ideal to collect your notes as you go through the lab.

1. Open a Google Doc (or if you prefer - go directly into your Tech Journal)
2. **Take notes on commands and configurations that you complete**
3. Use heading or other labels to help keep the notes organized

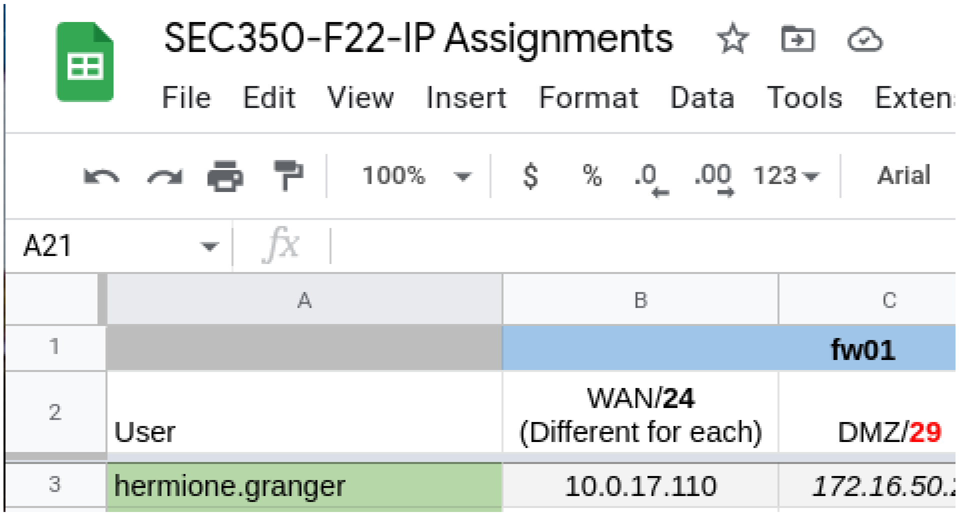
Student IP assignments

IP Assignment Spreadsheet
Default Passwords

Lab 1.1 - Steps

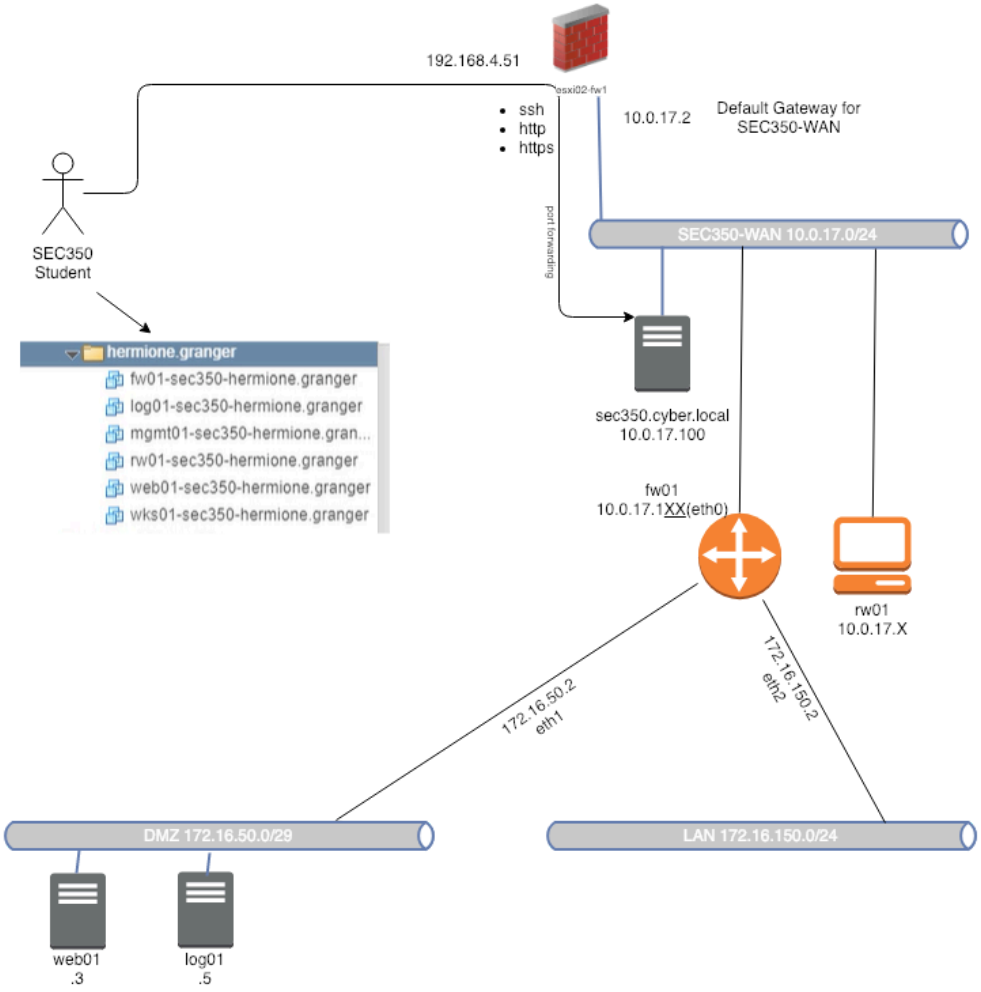
> The figure below can appear daunting, but we are going to build this architecture one step at a time. Our tasks will include establishing a host on the WAN called rw01 (road warrior 1), configuring a firewall and adding two hosts to our DMZ network.

Take a look at your network and IP assignments. These can be found on the course CANVAS Home Page Under Resources. The illustration below shows an example of a student's IP assignments. An important thing to note is that any WAN IP address such as the first interface on fw01 and rw01 are different for each student. The italicized IP addresses are the same for all.



	A	B	C
1			fw01
2	User	WAN/**24** (Different for each)	DMZ/**29**
3	hermione.granger	10.0.17.110	*172.16.50.*

Routing and DMZ Architecture



Lab 1 - Overview and checklist

In this lab, you will be completing the following configurations. This is just to give you a picture of where you are headed with the lab - and following the steps below the list will get you there!

Rw01: This is the “road warrior” linux laptop. A computer that sits outside your organization's network

- Add sudo user
- Configure IP configuration (ip, mask, gateway etc.)
- Configure IP route to direct certain traffic to the organization’s DMZ

Fw01: This is a vyos router/firewall that connects the SEC-350 (ISP), DMZ, and LAN networks

- Add and set adapters in VSphere
- Configure hostname
- Configure ip address configuration per the 3 interfaces
- Set default routing rules
- Set DNS forwarding and forwarding rules
- Set NAT rules

Web01: This is the organization's CENTOS web server in the DMZ

- Add user, set password, add to sudo (wheel) group
- Set hostname
- Set ip configuration (static) including Gateway and DNS
- Set firewall rules
- Configure as a web server
- Configure as rsyslog client

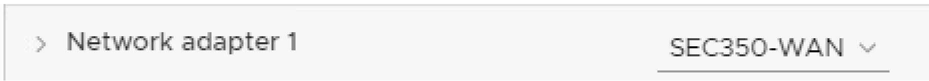
Log01: This is the organization’s CentOS log server (in DMZ for now)

- Add user, set password, add to sudo (wheel) group
- Set hostname
- Set ip configuration (static) including Gateway and DNS
- Set firewall rules
- Configure as rsyslog server

Configuring rw01

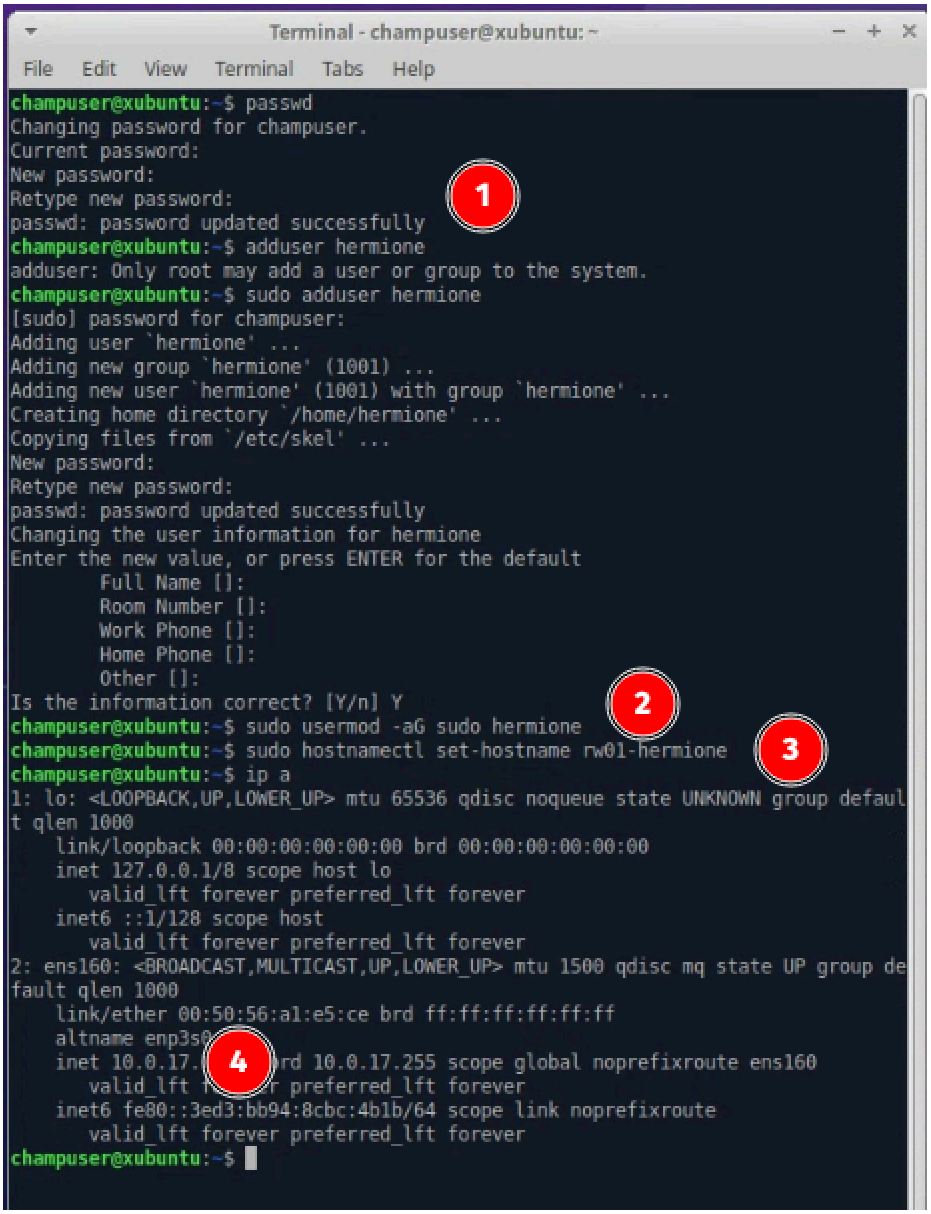
Login to https://vcenter02.cyber.local from a champlain networked computer. Use the HTML5 client.

rw01 is a Linux system based upon Ubuntu (xubuntu) that will be used to test your firewall defenses. Find the Virtual machine's settings and ensure that your system is on the correct network.



> Network adapter 1 SEC350-WAN

1. Secure your champuser default account by changing the password
2. Add a new sudo user called yourname
3. Set your hostname
4. Make sure you have a static ip that matches the one in the IP assignments spreadsheet.

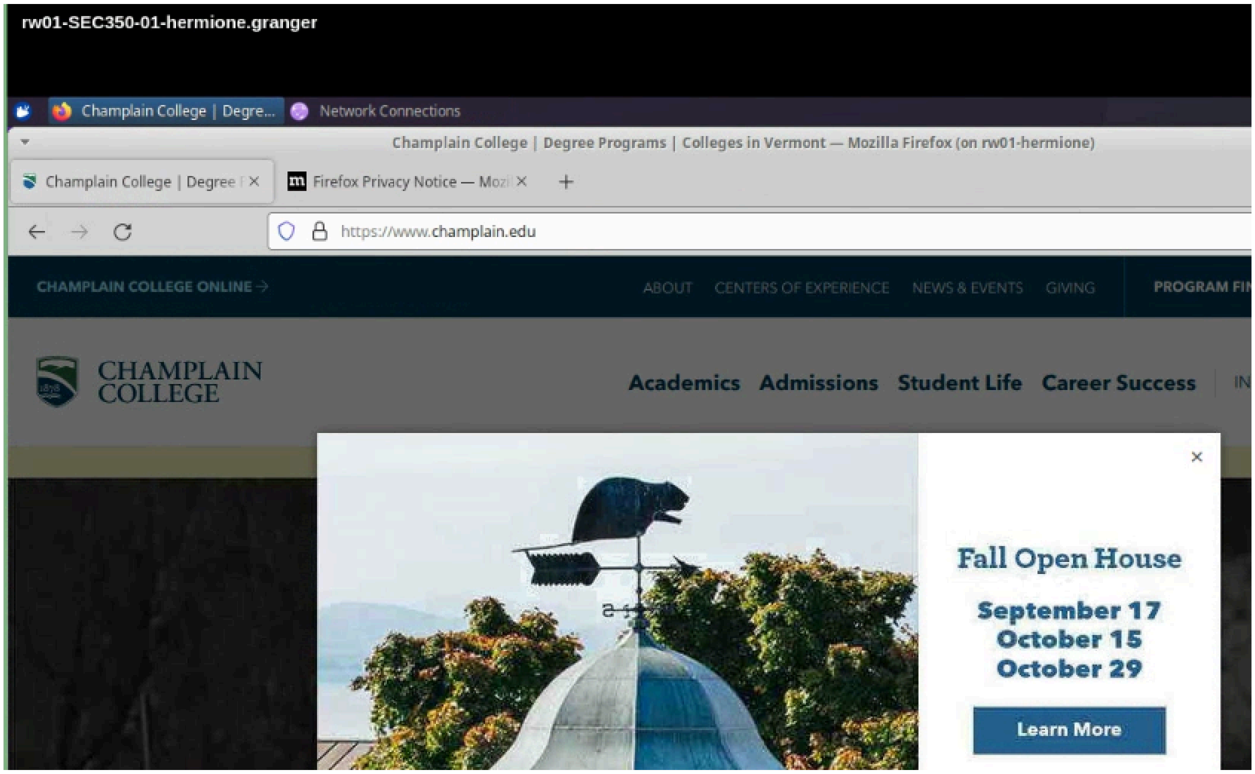


Terminal - champuser@xubuntu: ~
File Edit View Terminal Tabs Help
1
2
3
4

```
champuser@xubuntu:~$ passwd
Changing password for champuser.
Current password:
New password:
Retype new password:
passwd: password updated successfully
champuser@xubuntu:~$ adduser hermione
adduser: Only root may add a user or group to the system.
champuser@xubuntu:~$ sudo adduser hermione
[sudo] password for champuser:
Adding user `hermione' ...
Adding new group `hermione' (1001) ...
Adding new user `hermione' (1001) with group `hermione' ...
Creating home directory `/home/hermione' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for hermione
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
champuser@xubuntu:~$ sudo usermod -aG sudo hermione
champuser@xubuntu:~$ sudo hostnamectl set-hostname rw01-hermione
champuser@xubuntu:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group de
fault qlen 1000
    link/ether 00:50:56:a1:e5:ce brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 10.0.17.     rd 10.0.17.255 scope global noprefixroute ens160
       valid_lft f     r preferred_lft forever
    inet6 fe80::3ed3:bb94:8cbc:4b1b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
champuser@xubuntu:~$ 
```

Configure your network based upon your Network and IP Address Assignment. DO NOT USE THE EXAMPLE IP ADDRESS. Your Default Gateway and DNS will be 10.0.17.2. Find this IP address on the diagram.

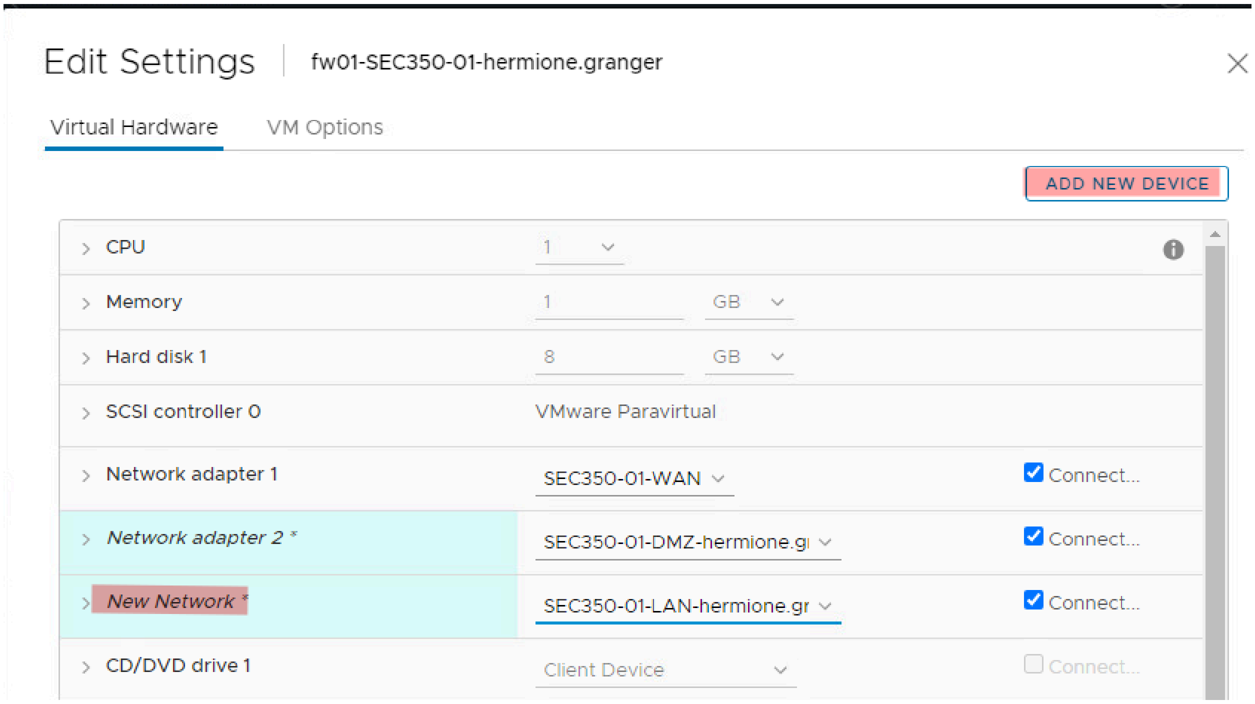
```
Deliverable 1:  Using rw01's web browser, go to champlain.edu.  Take
a screenshot that shows your vsphere console name and your browser
window similar to the following screenshot.
```


rw01-SEC350-01-hermione.granger
Champlain College | Degre...
Network Connections
Champlain College | Degree Programs | Colleges in Vermont — Mozilla Firefox (on rw01-hermione)
Champlain College | Degree
Firefox Privacy Notice — Mozi
https://www.champlain.edu
CHAMPLAIN COLLEGE ONLINE →
ABOUT
CENTERS OF EXPERIENCE
NEWS & EVENTS
GIVING
PROGRAM FI
CHAMPLAIN COLLEGE
Academics
Admissions
Student Life
Career Success
Fall Open House
September 17
October 15
October 29
Learn More

Configuring basic routing on fw01

vyOS is a fully functional but console based network appliance and it is a favorite among networking and security professionals. Today we are going to deal with it as a router, saving firewall functionality for another class. Your job will be to join fw01's three network interfaces to the appropriate networks and provide routing and NAT service to clients residing on those networks.

Adjust the network adapter settings so that they look like this. Pay particular attention to the mapping of the Network Adapter to the named interface. You will need to add the third interface.



Edit Settings | fw01-SEC350-01-hermione.granger

CPU	1		
Memory	1	GB	
Hard disk 1	8	GB	
SCSI controller 0	VMware Paravirtual		
Network adapter 1	SEC350-01-WAN		☑ Connect...
*Network adapter 2 **	SEC350-01-DMZ-hermione.gı		☑ Connect...
*New Network **	SEC350-01-LAN-hermione.gr		☑ Connect...
CD/DVD drive 1	Client Device		□ Connect...

💣 Pay very close attention to your IP and Network assignments, as a mistake here may cause problems for not just you but other students as well.

Configure, Commit, Save and Exit … Learn this!

VyOS configuration is very similar to Cisco. Changes are made to the running configuration by entering "configure" mode. These changes are applied to the running configuration via "commit". The changes persist after reload only if you "save" them. You leave configuration mode via the "exit" command.

The default username/passwords can be found here

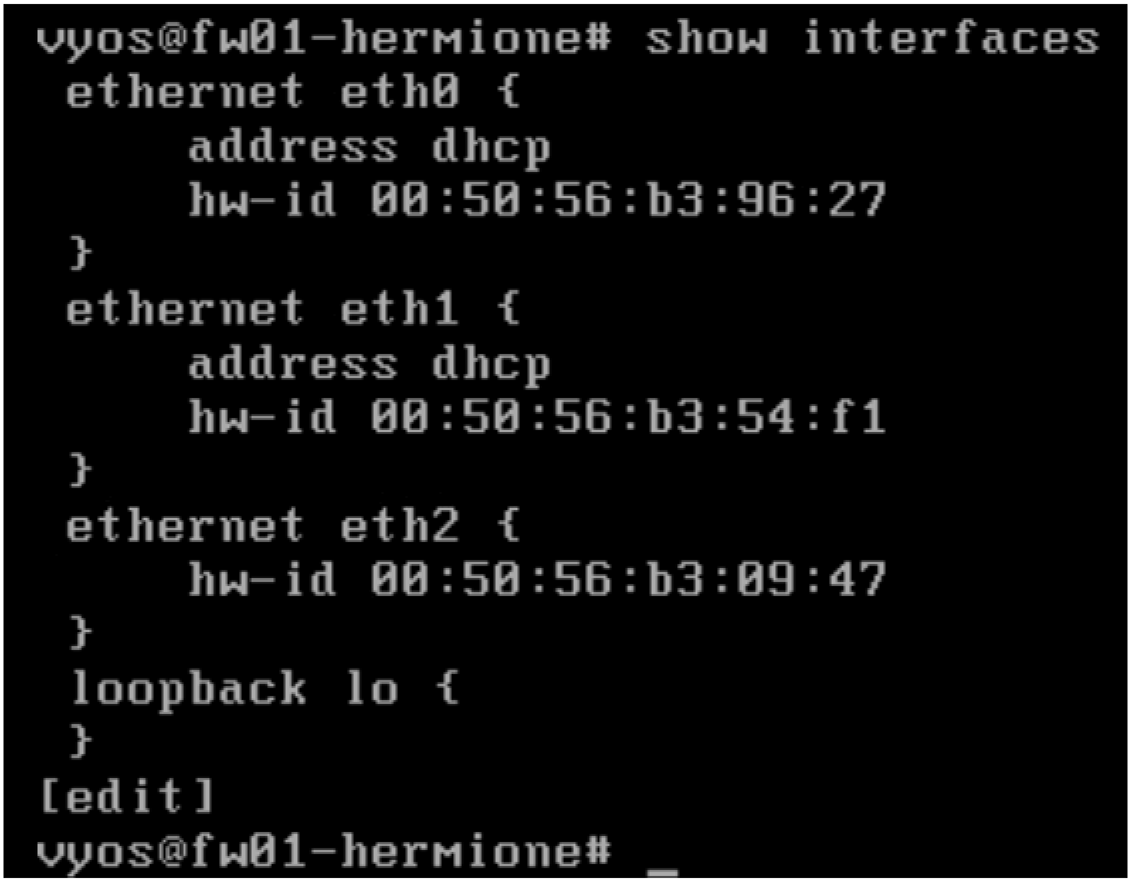
Setting the Hostname

```
configure
set system host-name fw1-yourname
commit
save
exit
```

Repeat exit until you get to a login prompt. Then you should see your new hostname, so go ahead and log in back to configure.

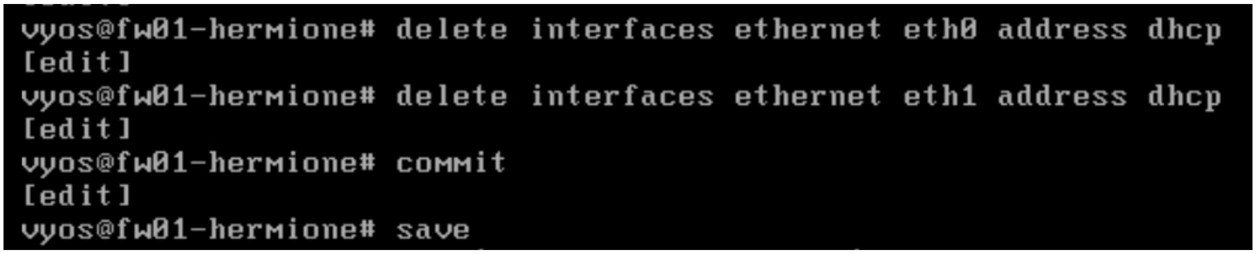
> 💡 Accurate hostnames are very important in security logging and monitoring scenarios. Make sure you do this or the default name (localhost) will be displayed in the logs, thus making it very difficult for you to determine which system produced a given log entry.

Interface Assignment



```
vyos@fw01-hermione# show interfaces
 ethernet eth0 {
     address dhcp
     hw-id 00:50:56:b3:96:27
 }
 ethernet eth1 {
     address dhcp
     hw-id 00:50:56:b3:54:f1
 }
 ethernet eth2 {
     hw-id 00:50:56:b3:09:47
 }
 loopback lo {
 }
[edit]
vyos@fw01-hermione# _
```

Note: First, check if any interfaces are configured with a dhcp. If it is, then you will need to run the delete command as seen below to delete the DHCP configuration. If there is no dhcp configuration, then you do not & can skip it.

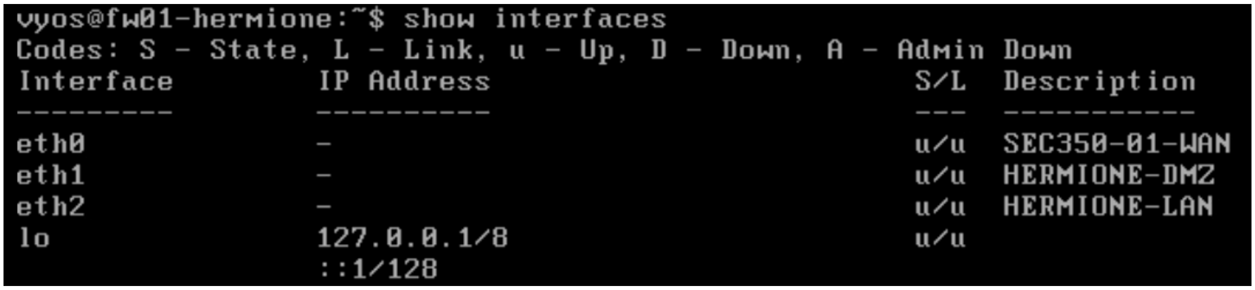


```
vyos@fw01-hermione# delete interfaces ethernet eth0 address dhcp
[edit]
vyos@fw01-hermione# delete interfaces ethernet eth1 address dhcp
[edit]
vyos@fw01-hermione# commit
[edit]
vyos@fw01-hermione# save
```

You should always set a description on each interface.

```
configure
set interfaces ethernet eth0 description SEC350-WAN
commit
save
exit
```

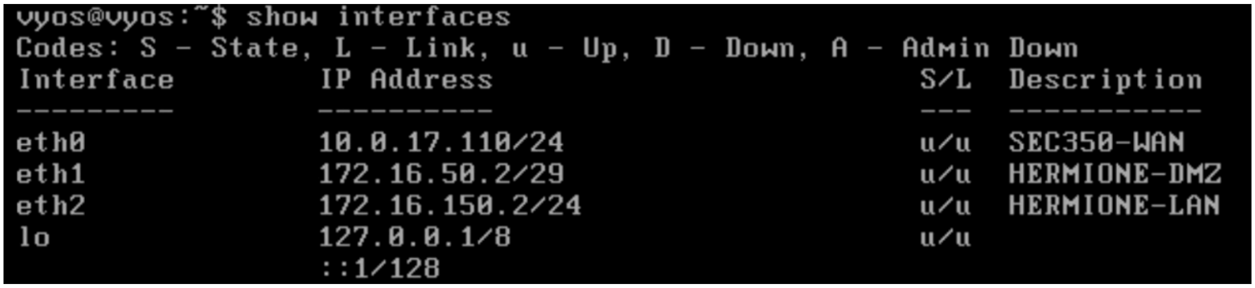
In a similar manner, set the descriptions for eth1 (DMZ) and eth2 (LAN). Make sure you commit and save and exit such that show interfaces now looks like this:



```
vyos@fw01-hermione:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             -                                 u/u  SEC350-01-WAN
eth1             -                                 u/u  HERMIONE-DMZ
eth2             -                                 u/u  HERMIONE-LAN
lo               127.0.0.1/8                       u/u
                 ::1/128
```

Set your DMZ and LAN interfaces to the common IP addresses shown in the spreadsheet. The following example shows Hermione's interface configuration when complete. Your IPs for DMZ and LAN should be identical to those shown below. Your WAN IP Address will be individual Again, you are <u>not</u> 10.0.17.110.

```
set interfaces ethernet ethX address IPADDRESS/MASK
```

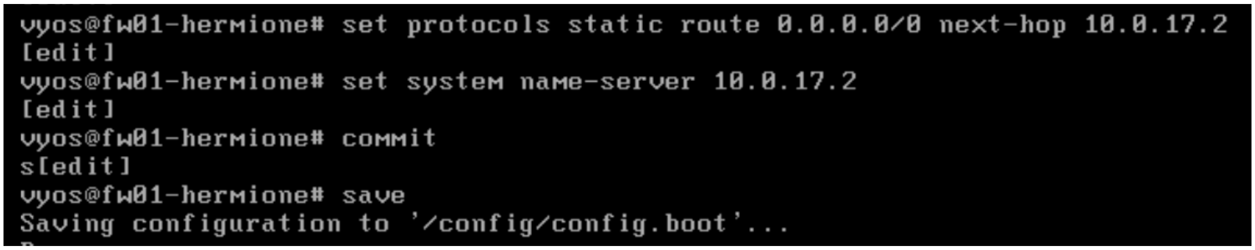


```
vyos@vyos:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             10.0.17.110/24                    u/u  SEC350-WAN
eth1             172.16.50.2/29                    u/u  HERMIONE-DMZ
eth2             172.16.150.2/24                   u/u  HERMIONE-LAN
lo               127.0.0.1/8                       u/u
                 ::1/128
```

Gateway and DNS

The SEC350-WAN interface on fw01 needs to be informed on how to get out to the internet. We will set both the default gateway and DNS server to the SEC350-Gateway Firewall at 10.0.17.2.

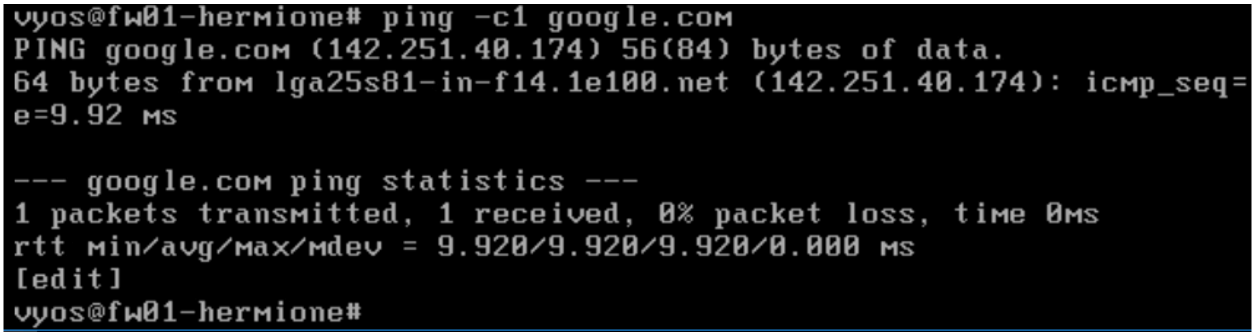
> **Note**: Notice the “set system name” entry below … Vyos allows for Tab Completion, as well as displaying available commands.



```
vyos@fw01-hermione# set protocols static route 0.0.0.0/0 next-hop 10.0.17.2
[edit]
vyos@fw01-hermione# set system name-server 10.0.17.2
[edit]
vyos@fw01-hermione# commit
s[edit]
vyos@fw01-hermione# save
Saving configuration to '/config/config.boot'...
```

Don’t forget to commit and save.

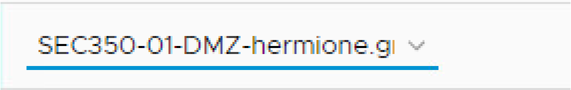
Deliverable 2. Successfully ping google.com and provide a screenshot similar to the one below.



```
vyos@fw01-hermione# ping -c1 google.com
PING google.com (142.251.40.174) 56(84) bytes of data.
64 bytes from lga25s81-in-f14.1e100.net (142.251.40.174): icmp_seq=
e=9.92 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 9.920/9.920/9.920/0.000 ms
[edit]
vyos@fw01-hermione#
```

Configuring web01

Web01 is a Rocky Web Server that should be placed on the DMZ Network with the IP Address of 172.16.50.3/29. Ensure web01’s network adapter is on the SEC350-DMZ Network.



You should recall how to set an IP address and hostname in CentOS Linux (SYS 255), so this process should be rather familiar. Remember: the DMZ is a /29, and not a /24.

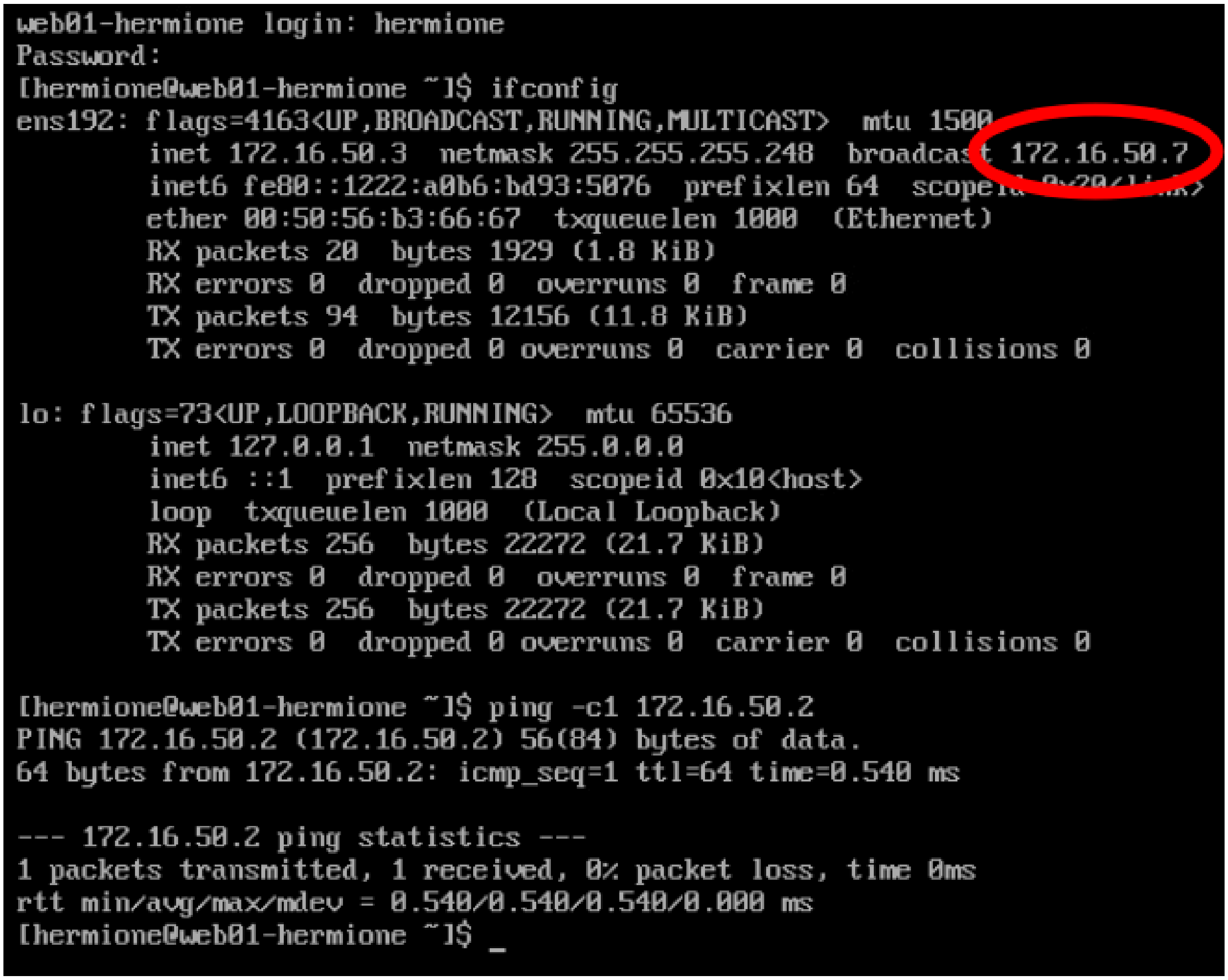
Add a sudo user called "yourname" **(remember - the sudo group in CentOS is called ‘wheel’)**

Change the hostname to be "web01-yourname".

Make sure to change the password for root and the default password for champuser to something you know and that others do not.

You will need to set the IP/Netmask, Gateway, DNS Servers and Automatically connect. The following shows hermione's IP address. Note that the DMZ interface of fw01 is pingable from web01.

For systems in the DMZ, your gateway and DNS server will be the DMZ interface on fw01 or 172.16.50.2

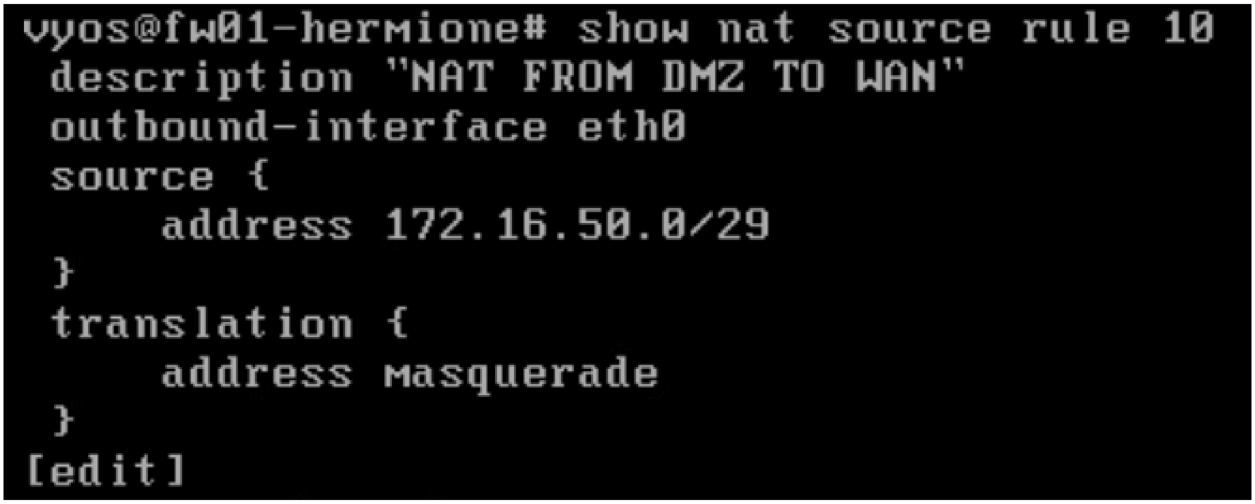


```
web01-hermione login: hermione
Password:
[hermione@web01-hermione ~]$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.50.3  netmask 255.255.255.248  broadcast 172.16.50.7
        inet6 fe80::1222:a0b6:bd93:5076  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b3:66:67  txqueuelen 1000  (Ethernet)
        RX packets 20  bytes 1929 (1.8 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 94  bytes 12156 (11.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 256  bytes 22272 (21.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 256  bytes 22272 (21.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[hermione@web01-hermione ~]$ ping -c1 172.16.50.2
PING 172.16.50.2 (172.16.50.2) 56(84) bytes of data.
64 bytes from 172.16.50.2: icmp_seq=1 ttl=64 time=0.540 ms

--- 172.16.50.2 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.540/0.540/0.540/0.000 ms
[hermione@web01-hermione ~]$ _
```

Note: in order to see your new hostname at the bash prompt, logout (exit) and log back in again. Try to ping google.com or 8.8.8.8 from web01. **It will fail because fw01 is not configured to translate IP addresses from the DMZ yet, nor is it configured to forward DNS from the DMZ Subnet. Take special note of the broadcast address. A /29 is a lot smaller than a /24 isn't it?**

Configuring fw01 for NAT and DNS Forwarding on fw01.

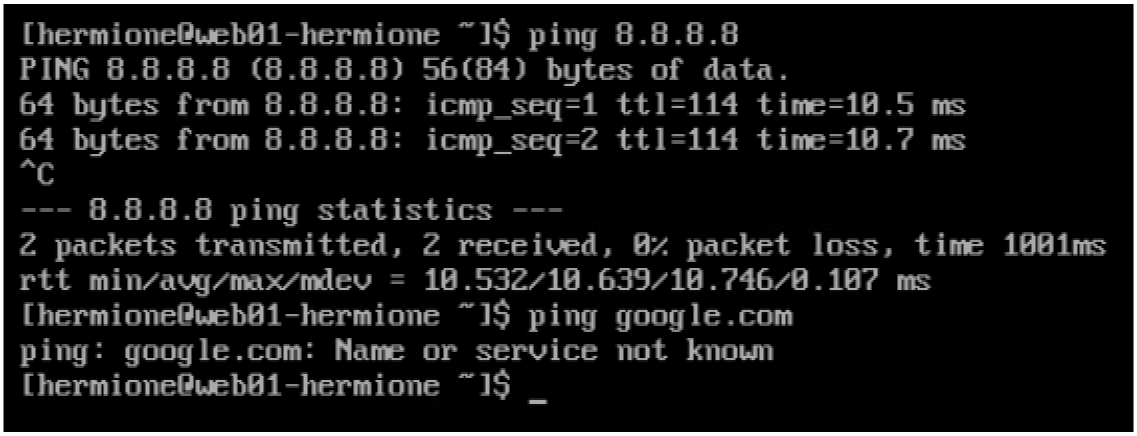
```
configure
set nat source rule 10 description "NAT FROM DMZ to WAN"
set nat source rule 10 outbound-interface eth0
set nat source rule 10 source address 172.16.50.0/29
set nat source rule 10 translation address masquerade
commit
save
```



```
vyos@fw01-hermione# show nat source rule 10
 description "NAT FROM DMZ TO WAN"
 outbound-interface eth0
 source {
     address 172.16.50.0/29
 }
 translation {
     address masquerade
 }
[edit]
```

On web01, you should now be able to ping by IP address, but not hostname yet:

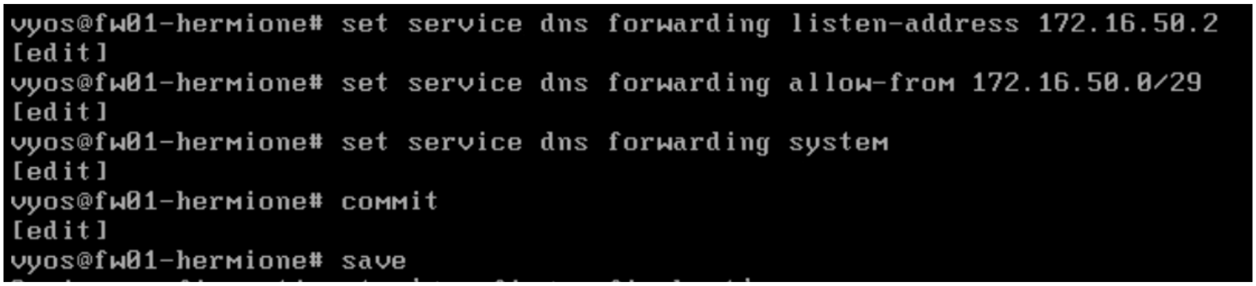
Deliverable 3: Provide a screenshot of a successful ping from web01 to 8.8.8.8 followed by a failed DNS lookup for google.com



```
[hermione@web01-hermione ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=10.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=10.7 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 10.532/10.639/10.746/0.107 ms
[hermione@web01-hermione ~]$ ping google.com
ping: google.com: Name or service not known
[hermione@web01-hermione ~]$ _
```

Configuring fw01 for DNS forwarding

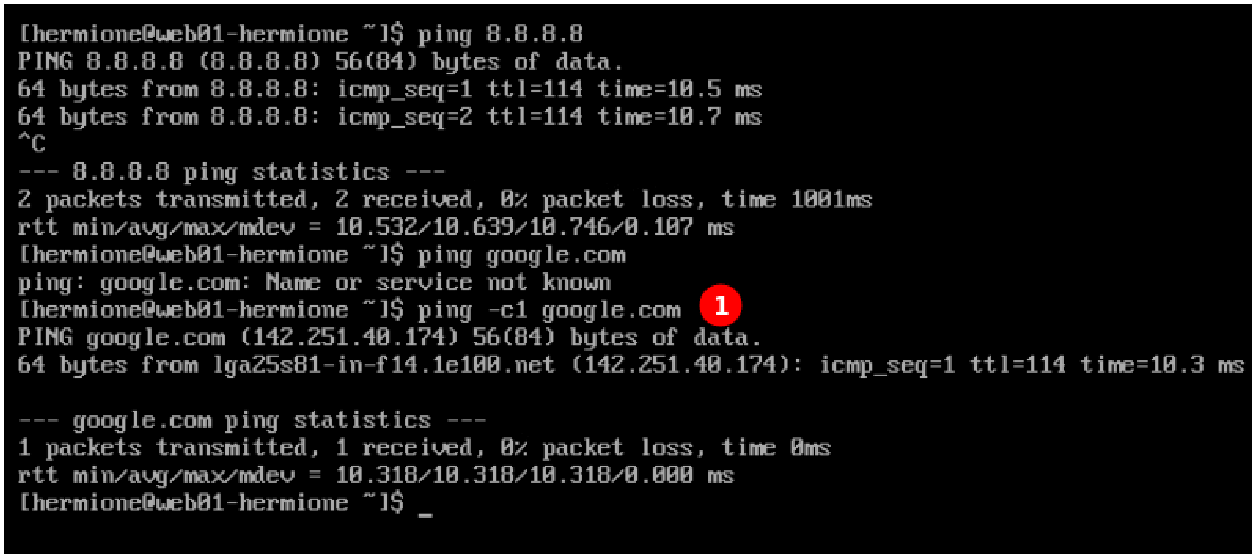
Tell fw1 to forward DNS requests from the DMZ interface.



```
vyos@fw01-hermione# set service dns forwarding listen-address 172.16.50.2
[edit]
vyos@fw01-hermione# set service dns forwarding allow-from 172.16.50.0/29
[edit]
vyos@fw01-hermione# set service dns forwarding system
[edit]
vyos@fw01-hermione# commit
[edit]
vyos@fw01-hermione# save
```

You should now be able to ping resolve DNS

Deliverable 4: Submit a successful ping to google.com from web01, and make sure your hostname is correct as well.



```
[hermione@web01-hermione ~]$ ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=114 time=10.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=10.7 ms
^C
--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 10.532/10.639/10.746/0.107 ms
[hermione@web01-hermione ~]$ ping google.com
ping: google.com: Name or service not known
[hermione@web01-hermione ~]$ ping -c1 google.com
PING google.com (142.251.40.174) 56(84) bytes of data.
64 bytes from lga25s81-in-f14.1e100.net (142.251.40.174): icmp_seq=1 ttl=114 time=10.3 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.318/10.318/10.318/0.000 ms
[hermione@web01-hermione ~]$ _
```

Configuring log01

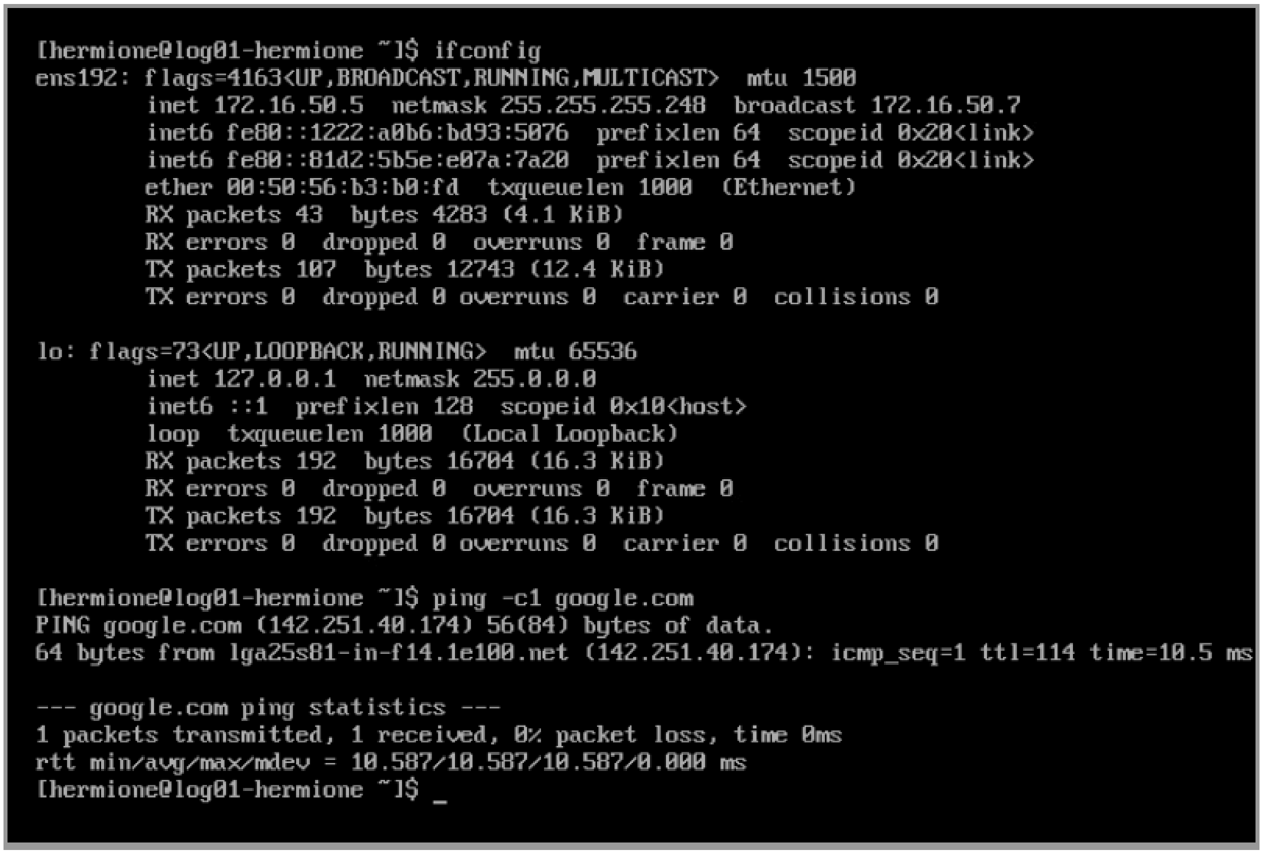
💡We are going to initially put our log server on the DMZ network, & later we will place this server in a segmented area of our network.

Configure log01 with an IP address ending in .5. **Make sure log01 is on the DMZ network**.

Ensure you have set the hostname of web01 and log01 to web01-yourname and log01-yourname respectively, & create a sudo user on both.

💣Screenshots showing trivial commands run as root, rather than by a sudo user or non-privileged user will be penalized. Remember … least privilege!

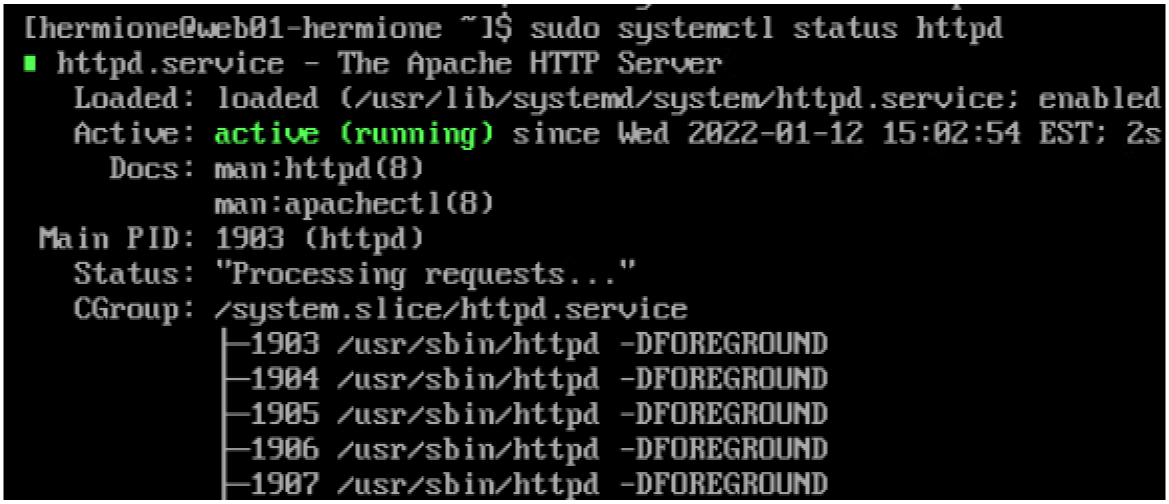
`Deliverable 5:  Submit a screenshot of your ifconfig followed by a successful ping to google.com from log01`



```
[hermione@log01-hermione ~]$ ifconfig
ens192: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.50.5  netmask 255.255.255.248  broadcast 172.16.50.7
        inet6 fe80::1222:a0b6:bd93:5076  prefixlen 64  scopeid 0x20<link>
        inet6 fe80::81d2:5b5e:e07a:7a20  prefixlen 64  scopeid 0x20<link>
        ether 00:50:56:b3:b0:fd  txqueuelen 1000  (Ethernet)
        RX packets 43  bytes 4283 (4.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 107  bytes 12743 (12.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 192  bytes 16704 (16.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 192  bytes 16704 (16.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

[hermione@log01-hermione ~]$ ping -c1 google.com
PING google.com (142.251.40.174) 56(84) bytes of data.
64 bytes from lga25s81-in-f14.1e100.net (142.251.40.174): icmp_seq=1 ttl=114 time=10.5 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 10.587/10.587/10.587/0.000 ms
[hermione@log01-hermione ~]$ _
```

Configuring httpd on web01

Figure out how to Install (*if not already installed for you*), enable and start httpd.



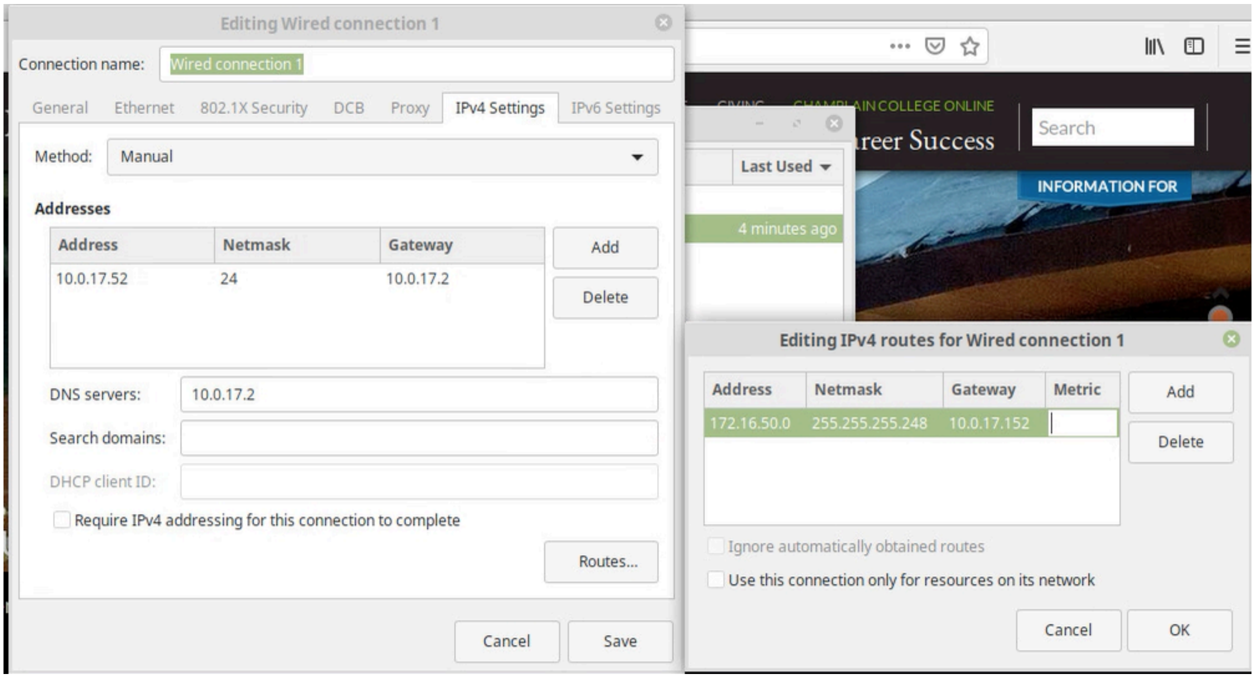
```
[hermione@web01-hermione ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled
   Active: active (running) since Wed 2022-01-12 15:02:54 EST; 2s
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 1903 (httpd)
   Status: "Processing requests..."
   CGroup: /system.slice/httpd.service
           ├─1903 /usr/sbin/httpd -DFOREGROUND
           ├─1904 /usr/sbin/httpd -DFOREGROUND
           ├─1905 /usr/sbin/httpd -DFOREGROUND
           ├─1906 /usr/sbin/httpd -DFOREGROUND
           ├─1907 /usr/sbin/httpd -DFOREGROUND
```

Configuring firewall on web01

Figure out how to add either the ports (80,443 TCP) or services (http, https) required for your http server.

Testing httpd on web01 from rw01

rw01's default gateway is 10.0.17.2, we need to tell it that any address in your DMZ should route via your firewall’s WAN interface. We do this with a static route on rw01. **Remember, your IP address will not be the same as the following illustration, so refer to your WAN assignment.** In this case, we are saying that anything addressed to the 172.16.50.0/29 network will go through the 10.0.17.1XX router.



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
10.0.17.52	24	10.0.17.2

DNS servers: 10.0.17.2

Search domains:

DHCP client ID:

□ Require IPv4 addressing for this connection to complete

Editing IPv4 routes for Wired connection 1

Address	Netmask	Gateway	Metric
172.16.50.0	255.255.255.248	10.0.17.152	

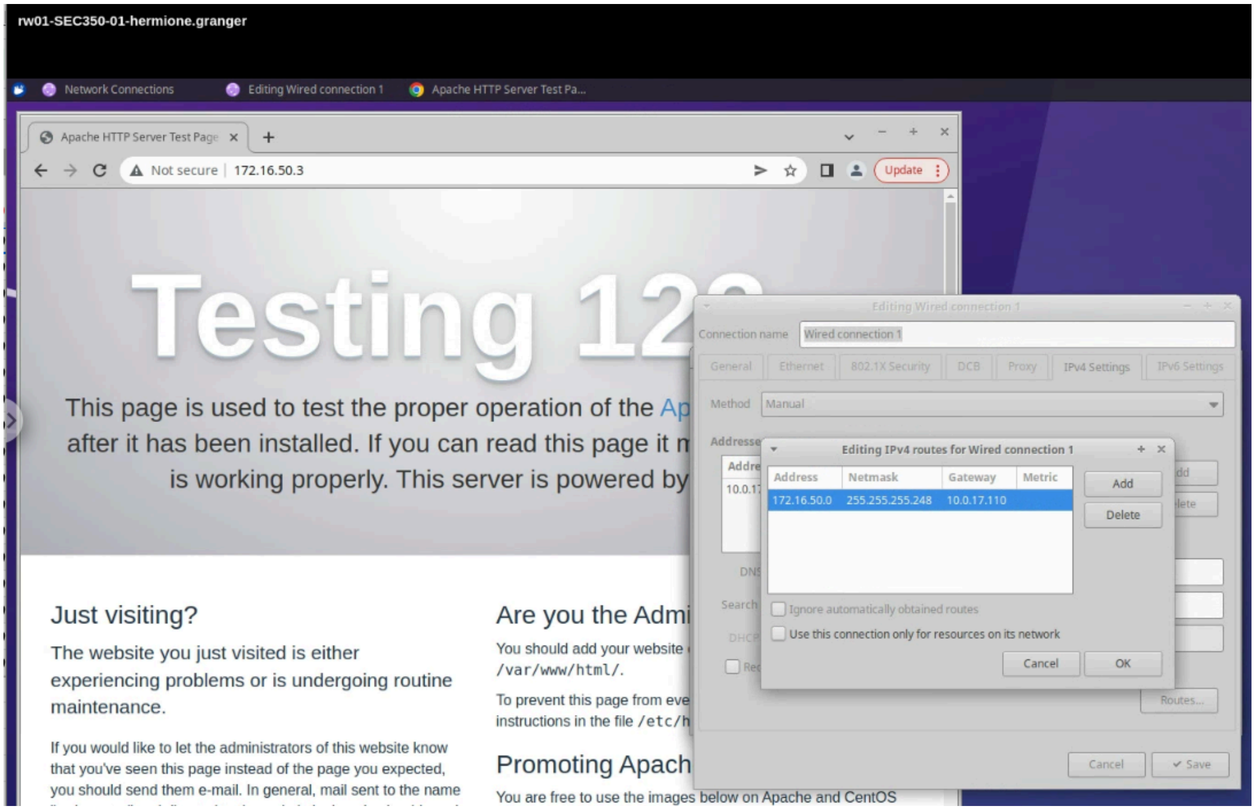
□ Ignore automatically obtained routes

□ Use this connection only for resources on its network

Make sure to restart your network through the gui or from a privileged terminal command.

Deliverable 6: Submit a screenshot showing rw01 successfully browsing the test page on your httpd server.

NOTE:make sure to type http://172.16.50.3 as the browser may default to https



rw01-SEC350-01-hermione.granger

Not secure | 172.16.50.3

Testing 123..

This page is used to test the proper operation of the Ap after it has been installed. If you can read this page it m is working properly. This server is powered by

Just visiting?

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name

Editing Wired connection 1

Connection name: Wired connection 1

Tab: IPv4 Settings

Method: Manual

Editing IPv4 routes for Wired connection 1

Address	Netmask	Gateway	Metric
172.16.50.0	255.255.255.248	10.0.17.110	

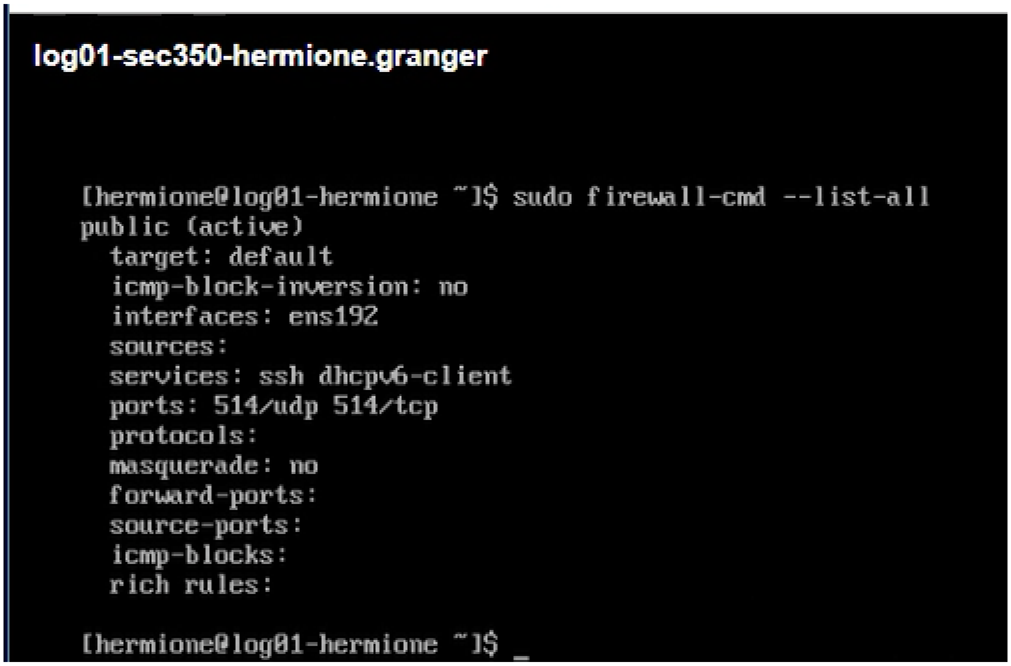
□ Ignore automatically obtained routes

□ Use this connection only for resources on its network

Configuring rsyslog services on log01

log01 will be receiving syslog traffic from fw01 and web01. Figure out how to allow UDP and TCP 514 for syslog traffic permanently.

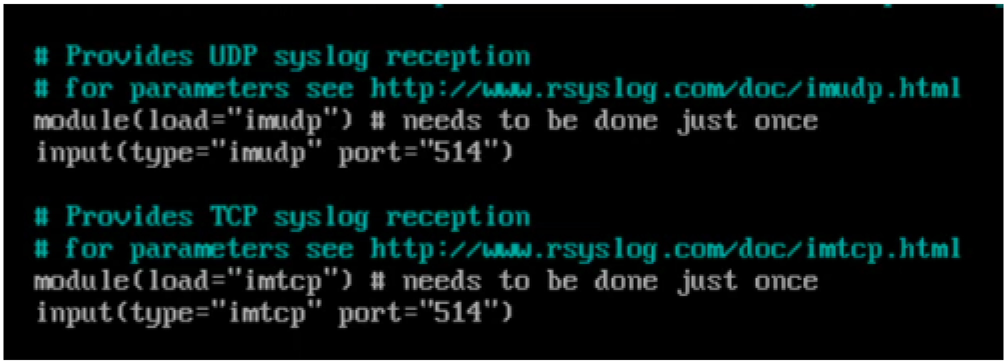
NOTE: rsyslog should be installed and running on log01 (systemctl status rsyslog) If rsyslog is not present, figure out how to install it.



```
log01-sec350-hermione.granger

[hermione@log01-hermione ~]$ sudo firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens192
  sources:
  services: ssh dhcpv6-client
  ports: 514/udp 514/tcp
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[hermione@log01-hermione ~]$ _
```

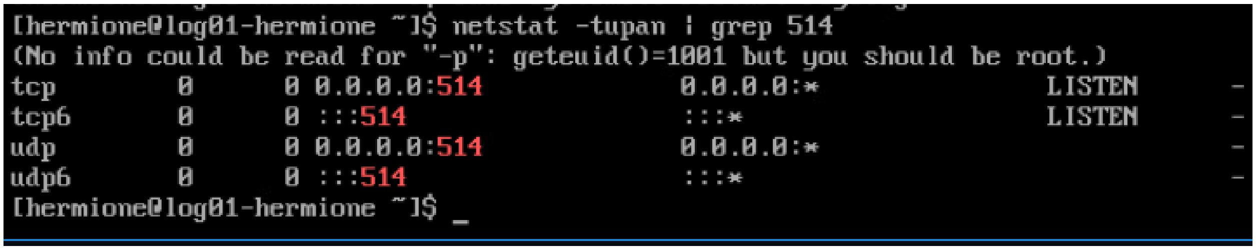
On log01, the /etc/rsyslog.conf file needs to be modified to receive syslog messages over ports 514 tcp and udp. Uncomment the appropriate lines (see below) and restart the rsyslog service. **NOTE: the text in the config file is simplified in newer versions than the screenshot. Should see similar lines under Provide UDP syslog reception" and "Provides TCP syslog reception"**

Just uncomment the lines in the newer config file - you do not need to change any text



```
# Provides UDP syslog reception
# for parameters see http://www.rsyslog.com/doc/imudp.html
module(load="imudp") # needs to be done just once
input(type="imudp" port="514")

# Provides TCP syslog reception
# for parameters see http://www.rsyslog.com/doc/imtcp.html
module(load="imtcp") # needs to be done just once
input(type="imtcp" port="514")
```

You can check to see if rsyslog is listening appropriately to these ports

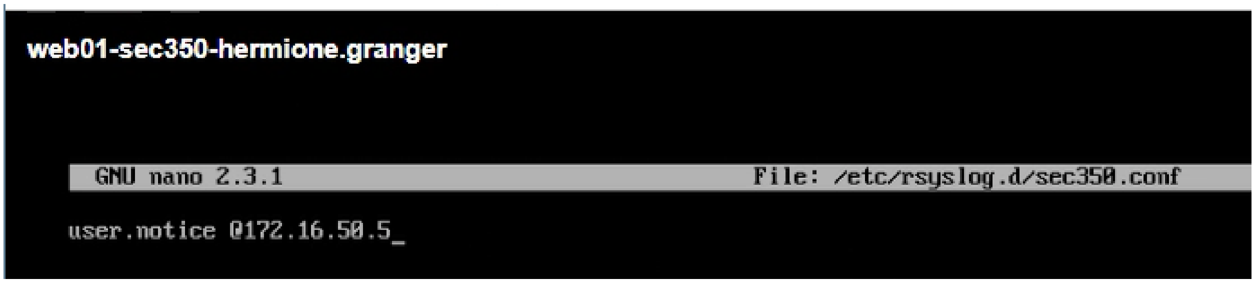


```
[hermione@log01-hermione ~]$ netstat -tupan | grep 514
(No info could be read for "-p": geteuid()=1001 but you should be root.)
tcp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      -
tcp6       0      0 :::514                  :::*                    LISTEN      -
udp        0      0 0.0.0.0:514             0.0.0.0:*                           -
udp6       0      0 :::514                  :::*                                -
[hermione@log01-hermione ~]$ _
```

Configuring rsyslog client on web01

NOTE: rsyslog may not be installed and running on web01. Use systemctl status to test. If it is not, easy to install with “yum install rsyslog”

Create the following file: /etc/rsyslog.d/sec350.conf and restart rsyslog on web01



web01-sec350-hermione.granger

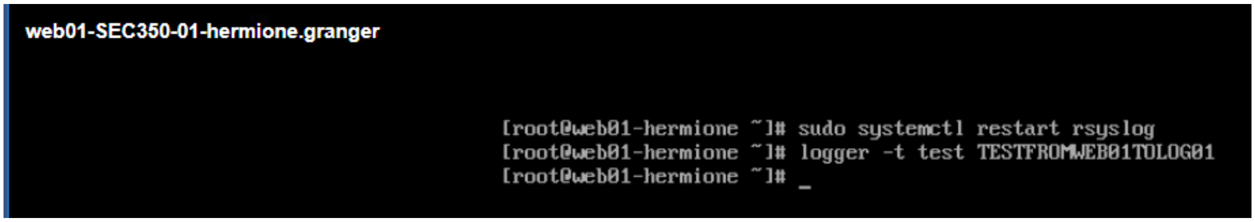
```
  GNU nano 2.3.1                              File: /etc/rsyslog.d/sec350.conf

user.notice @172.16.50.5_
```

💡 the line in sec350.conf means:
user=syslog facility
notice=syslog priority
@=UDP, @@ means TCP, so we are only going to send UDP
172.16.50.5=Remote Syslog Server

Test rsyslog messaging from web01 to log01

On log01, tail -f the /var/log/messages file

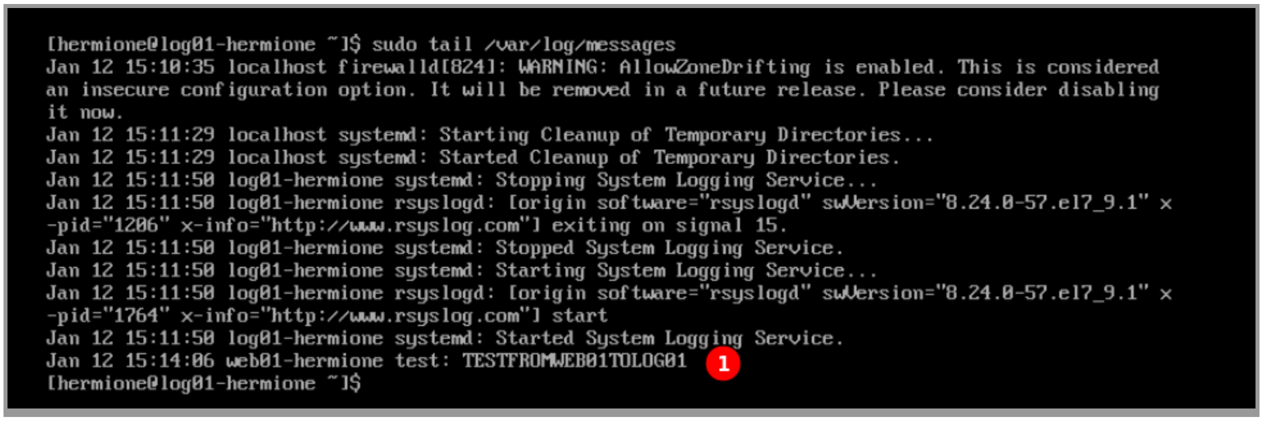
On web01, use the local logger utility to send a syslog message



web01-SEC350-01-hermione.granger

```
[root@web01-hermione ~]# sudo systemctl restart rsyslog
[root@web01-hermione ~]# logger -t test TESTFROMWEB01TOLOG01
[root@web01-hermione ~]# _
```

Deliverable 7: Take a screenshot that shows the test message arriving in log01's /var/log/messages file from web01. It should look like the last line:

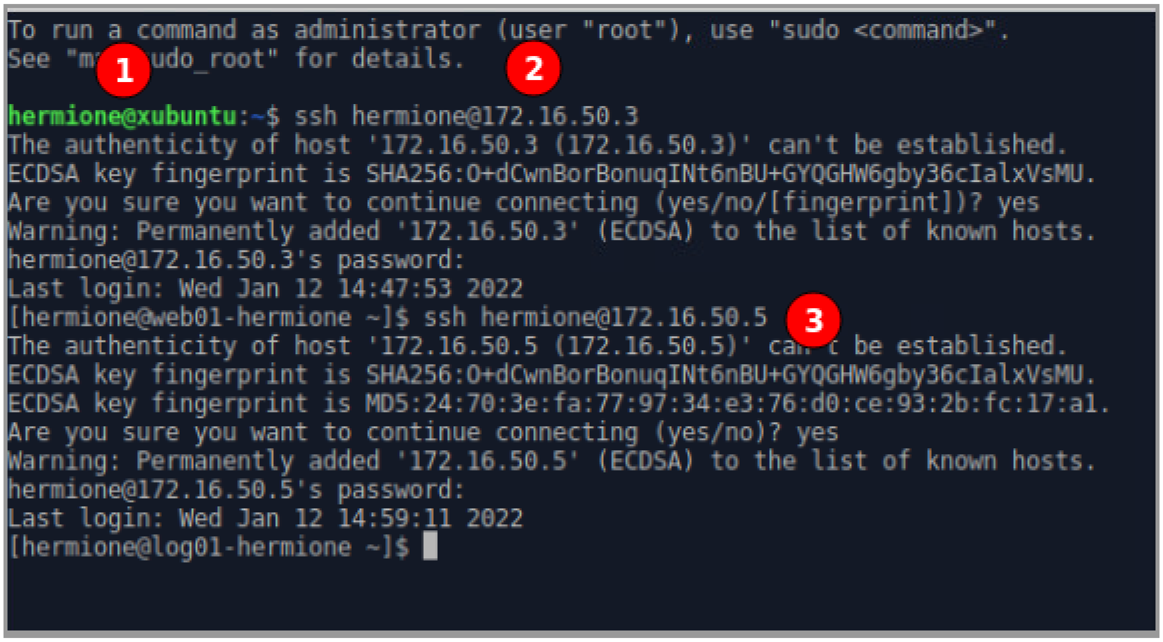


```
[hermione@log01-hermione ~]$ sudo tail /var/log/messages
Jan 12 15:10:35 localhost firewalld[824]: WARNING: AllowZoneDrifting is enabled. This is considered
an insecure configuration option. It will be removed in a future release. Please consider disabling
it now.
Jan 12 15:11:29 localhost systemd: Starting Cleanup of Temporary Directories...
Jan 12 15:11:29 localhost systemd: Started Cleanup of Temporary Directories.
Jan 12 15:11:50 log01-hermione systemd: Stopping System Logging Service...
Jan 12 15:11:50 log01-hermione rsyslogd: [origin software="rsyslogd" swVersion="8.24.0-57.el7_9.1" x
-pid="1206" x-info="http://www.rsyslog.com"] exiting on signal 15.
Jan 12 15:11:50 log01-hermione systemd: Stopped System Logging Service.
Jan 12 15:11:50 log01-hermione systemd: Starting System Logging Service...
Jan 12 15:11:50 log01-hermione rsyslogd: [origin software="rsyslogd" swVersion="8.24.0-57.el7_9.1" x
-pid="1764" x-info="http://www.rsyslog.com"] start
Jan 12 15:11:50 log01-hermione systemd: Started System Logging Service.
Jan 12 15:14:06 web01-hermione test: TESTFROMWEB01TOLOG01
[hermione@log01-hermione ~]$
```

rw01->SSH->web01->SSH->log01

From rw01, use a SSH session to login to web01, from that SSH session login to log01.

Deliverable 8: Provide a screenshot that shows this layered ssh session. It should look similar to this:



```
To run a command as administrator (user "root"), use "sudo <command>".
See "m    udo_root" for details.

hermione@xubuntu:~$ ssh hermione@172.16.50.3
The authenticity of host '172.16.50.3 (172.16.50.3)' can't be established.
ECDSA key fingerprint is SHA256:O+dCwnBorBonuqINt6nBU+GYQGHW6gby36cIalxVsMU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.16.50.3' (ECDSA) to the list of known hosts.
hermione@172.16.50.3's password:
Last login: Wed Jan 12 14:47:53 2022
[hermione@web01-hermione ~]$ ssh hermione@172.16.50.5
The authenticity of host '172.16.50.5 (172.16.50.5)' can't be established.
ECDSA key fingerprint is SHA256:O+dCwnBorBonuqINt6nBU+GYQGHW6gby36cIalxVsMU.
ECDSA key fingerprint is MD5:24:70:3e:fa:77:97:34:e3:76:d0:ce:93:2b:fc:17:a1.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.16.50.5' (ECDSA) to the list of known hosts.
hermione@172.16.50.5's password:
Last login: Wed Jan 12 14:59:11 2022
[hermione@log01-hermione ~]$
```

💡 The next two deliverables assume you have a tech journal github repository. Begin construction of a SEC350 area. See the course home page for your instructor's github handle. If your repository is private, make sure to add your instructor as a collaborator.

Deliverable 9. VYOS Tech Journal Entry. Create a standalone article on vyos. Make sure you document those commands used during this course of this lab like setting the hostname, interfaces, gateway,dns, nat and dns forwarding Provide a link.

Deliverable 10. syslog Tech Journal Entry Take notes on the configuration steps necessary to create a syslog server and a syslog client. Provide a link.