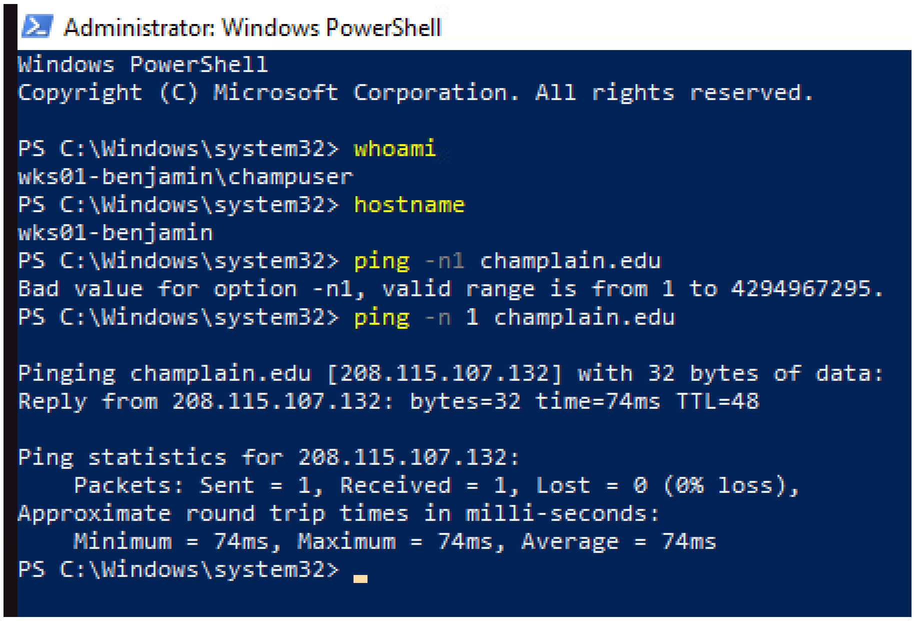
Lab3-1_Segmentation1
SEC-350
Ben W
SP24

Deliverables:

1. Screenshot of internet access on wks01



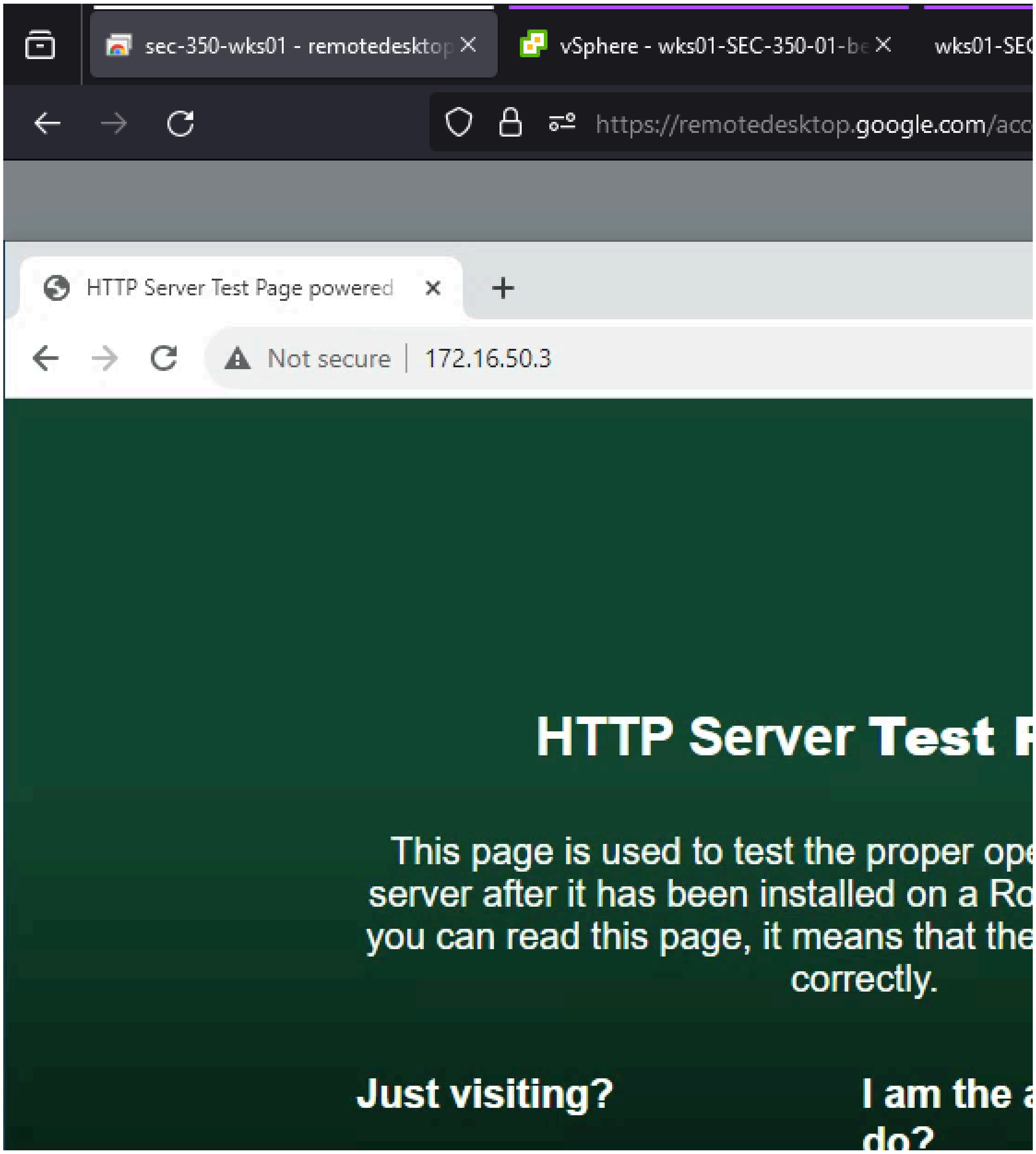
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> whoami
wks01-benjamin\champuser
PS C:\Windows\system32> hostname
wks01-benjamin
PS C:\Windows\system32> ping -n1 champlain.edu
Bad value for option -n1, valid range is from 1 to 4294967295.
PS C:\Windows\system32> ping -n 1 champlain.edu

Pinging champlain.edu [208.115.107.132] with 32 bytes of data:
Reply from 208.115.107.132: bytes=32 time=74ms TTL=48

Ping statistics for 208.115.107.132:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 74ms, Maximum = 74ms, Average = 74ms
PS C:\Windows\system32> _
```

2. Access to web server from wks01



sec-350-wks01 - remotedesktop
vSphere - wks01-SEC-350-01-be
wks01-SE
https://remotedesktop.google.com/acc
HTTP Server Test Page powered
Not secure
172.16.50.3

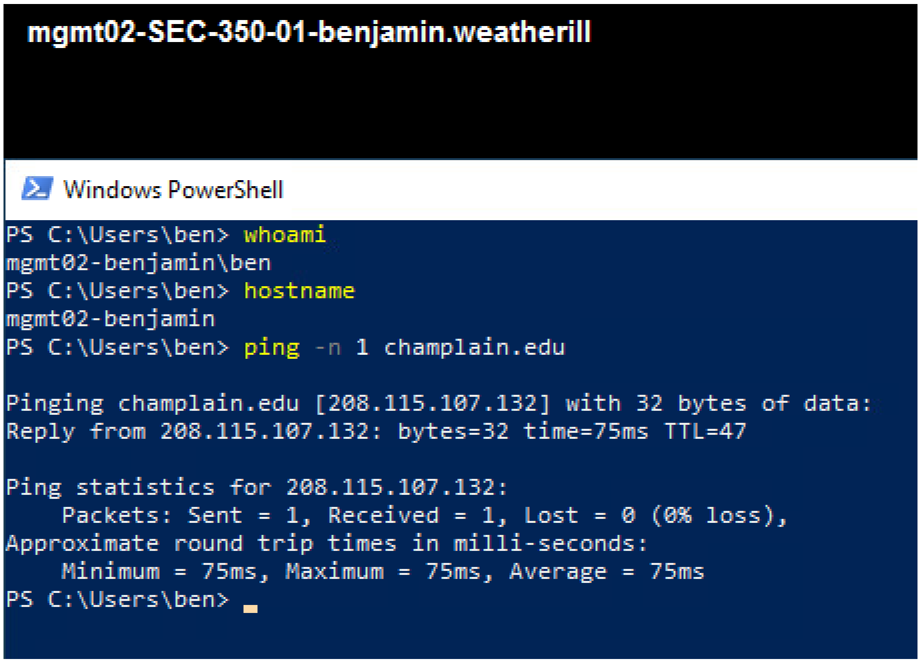
HTTP Server Test F

This page is used to test the proper ope server after it has been installed on a Ro you can read this page, it means that the correctly.

Just visiting?

I am the a do?

3. Mgmt02 connecting to internet

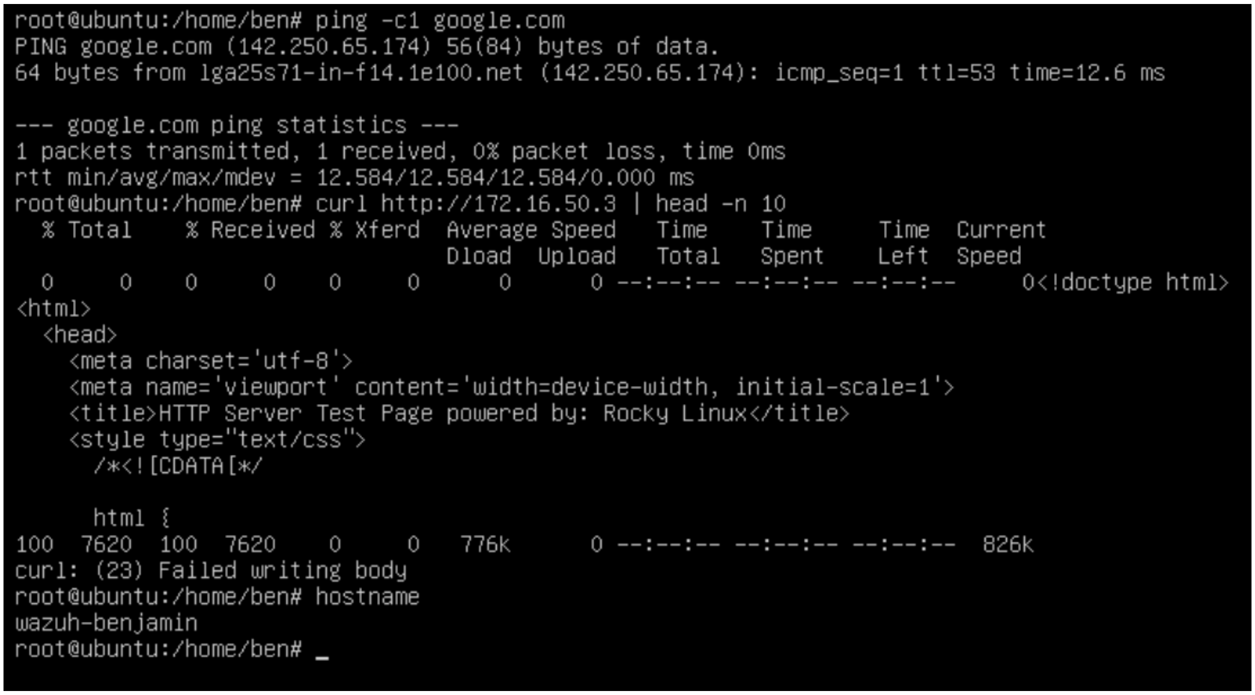


```
PS C:\Users\ben> whoami
mgmt02-benjamin\ben
PS C:\Users\ben> hostname
mgmt02-benjamin
PS C:\Users\ben> ping -n 1 champlain.edu

Pinging champlain.edu [208.115.107.132] with 32 bytes of data:
Reply from 208.115.107.132: bytes=32 time=75ms TTL=47

Ping statistics for 208.115.107.132:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 75ms, Maximum = 75ms, Average = 75ms
PS C:\Users\ben> _
```

4. Wazuh connected to network, internal and external

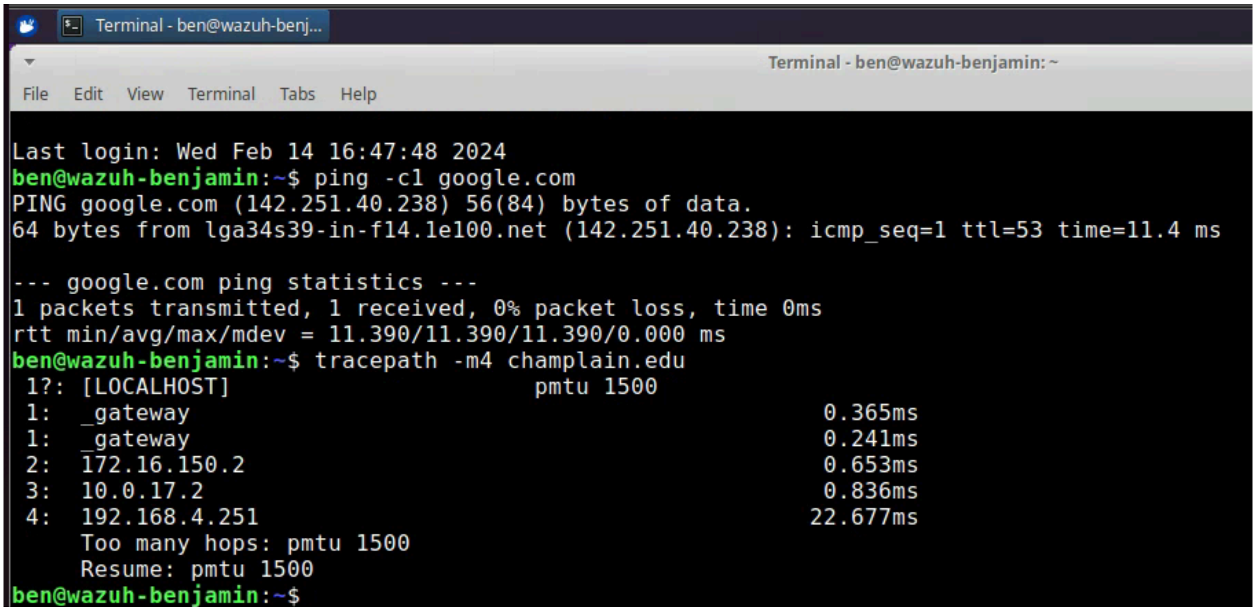


```
root@ubuntu:/home/ben# ping -c1 google.com
PING google.com (142.250.65.174) 56(84) bytes of data.
64 bytes from lga25s71-in-f14.1e100.net (142.250.65.174): icmp_seq=1 ttl=53 time=12.6 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 12.584/12.584/12.584/0.000 ms
root@ubuntu:/home/ben# curl http://172.16.50.3 | head -n 10
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
  0     0    0     0    0     0      0      0 --:--:-- --:--:-- --:--:--     0<!doctype html>
<html>
  <head>
    <meta charset='utf-8'>
    <meta name='viewport' content='width=device-width, initial-scale=1'>
    <title>HTTP Server Test Page powered by: Rocky Linux</title>
    <style type="text/css">
      /*<![CDATA[*/

      html {
100  7620  100  7620    0     0   776k      0 --:--:-- --:--:-- --:--:--  826k
curl: (23) Failed writing body
root@ubuntu:/home/ben# hostname
wazuh-benjamin
root@ubuntu:/home/ben# _
```

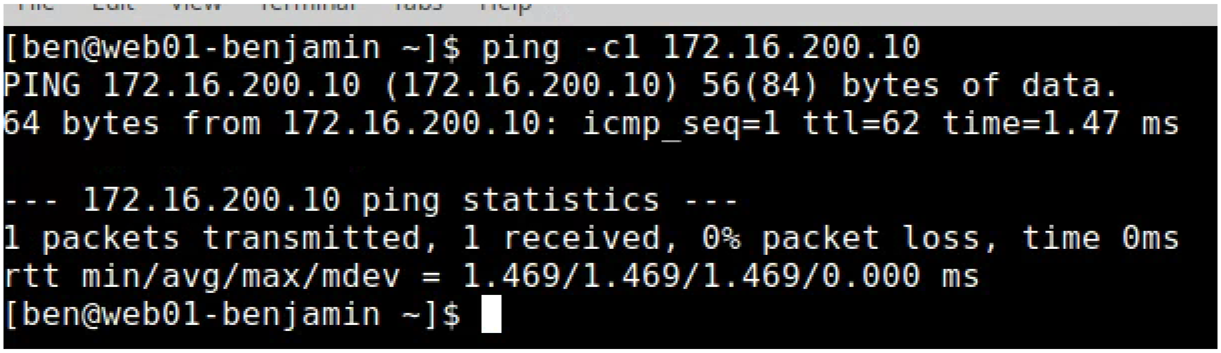
5. Wazuh connected


Terminal - ben@wazuh-benj...
Terminal - ben@wazuh-benjamin: ~
File Edit View Terminal Tabs Help

```
Last login: Wed Feb 14 16:47:48 2024
ben@wazuh-benjamin:~$ ping -cl google.com
PING google.com (142.251.40.238) 56(84) bytes of data.
64 bytes from lga34s39-in-f14.1e100.net (142.251.40.238): icmp_seq=1 ttl=53 time=11.4 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 11.390/11.390/11.390/0.000 ms
ben@wazuh-benjamin:~$ tracepath -m4 champlain.edu
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway                                            0.365ms
 1:  _gateway                                            0.241ms
 2:  172.16.150.2                                        0.653ms
 3:  10.0.17.2                                           0.836ms
 4:  192.168.4.251                                      22.677ms
     Too many hops: pmtu 1500
     Resume: pmtu 1500
ben@wazuh-benjamin:~$
```

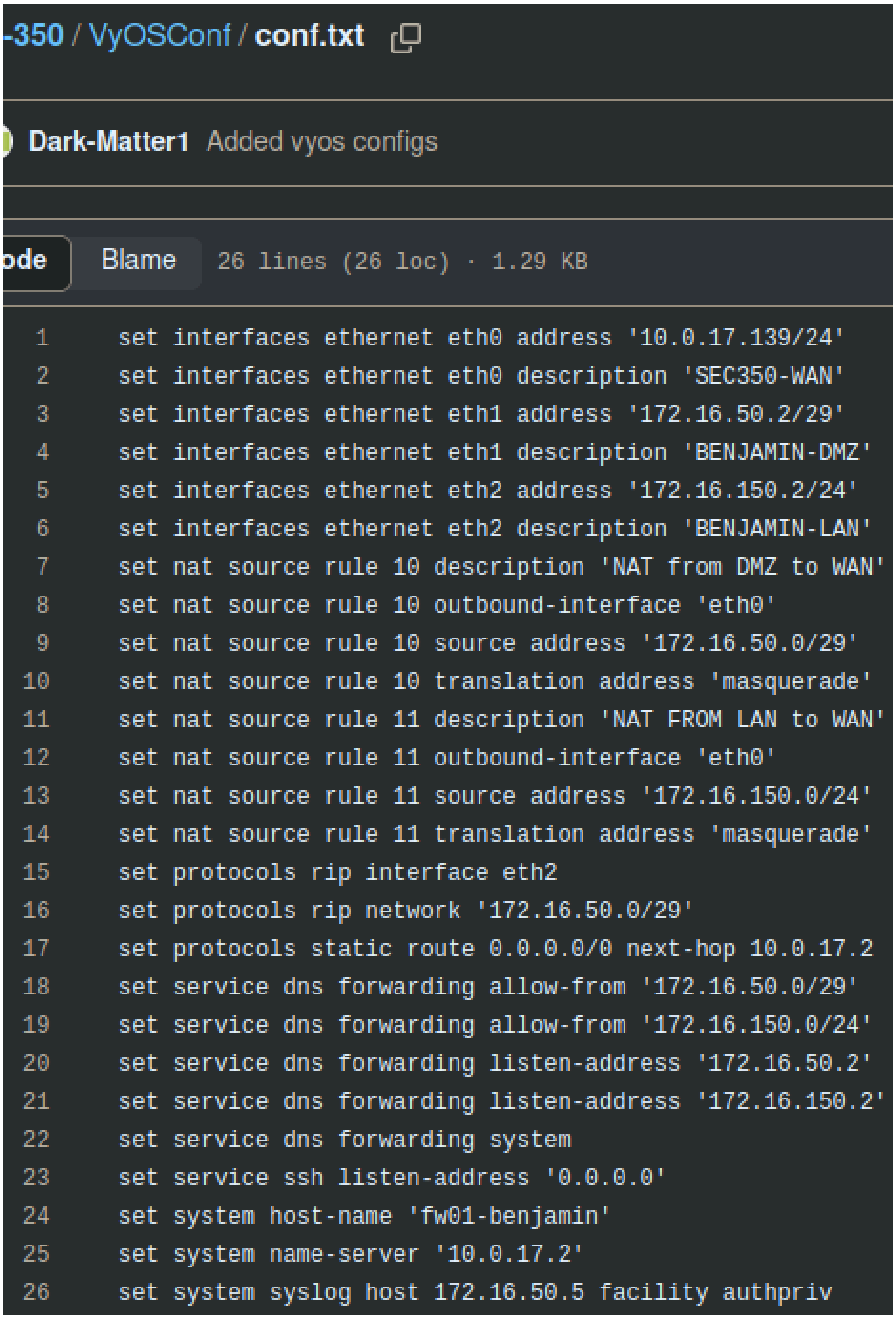
6. Web01 pinging wazuh



```
[ben@web01-benjamin ~]$ ping -cl 172.16.200.10
PING 172.16.200.10 (172.16.200.10) 56(84) bytes of data.
64 bytes from 172.16.200.10: icmp_seq=1 ttl=62 time=1.47 ms

--- 172.16.200.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 1.469/1.469/1.469/0.000 ms
[ben@web01-benjamin ~]$
```

7. Config files in GitHub


-350 / VyOSConf / conf.txt
Dark-Matter1 Added vyos configs
ode
Blame
26 lines (26 loc) · 1.29 KB

```
set interfaces ethernet eth0 address '10.0.17.139/24'
set interfaces ethernet eth0 description 'SEC350-WAN'
set interfaces ethernet eth1 address '172.16.50.2/29'
set interfaces ethernet eth1 description 'BENJAMIN-DMZ'
set interfaces ethernet eth2 address '172.16.150.2/24'
set interfaces ethernet eth2 description 'BENJAMIN-LAN'
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'
set nat source rule 11 description 'NAT FROM LAN to WAN'
set nat source rule 11 outbound-interface 'eth0'
set nat source rule 11 source address '172.16.150.0/24'
set nat source rule 11 translation address 'masquerade'
set protocols rip interface eth2
set protocols rip network '172.16.50.0/29'
set protocols static route 0.0.0.0/0 next-hop 10.0.17.2
set service dns forwarding allow-from '172.16.50.0/29'
set service dns forwarding allow-from '172.16.150.0/24'
set service dns forwarding listen-address '172.16.50.2'
set service dns forwarding listen-address '172.16.150.2'
set service dns forwarding system
set service ssh listen-address '0.0.0.0'
set system host-name 'fw01-benjamin'
set system name-server '10.0.17.2'
set system syslog host 172.16.50.5 facility authpriv
```

https://github.com/benjamin-weatherill/SEC-350/blob/main/VyOSConf/conf.txt