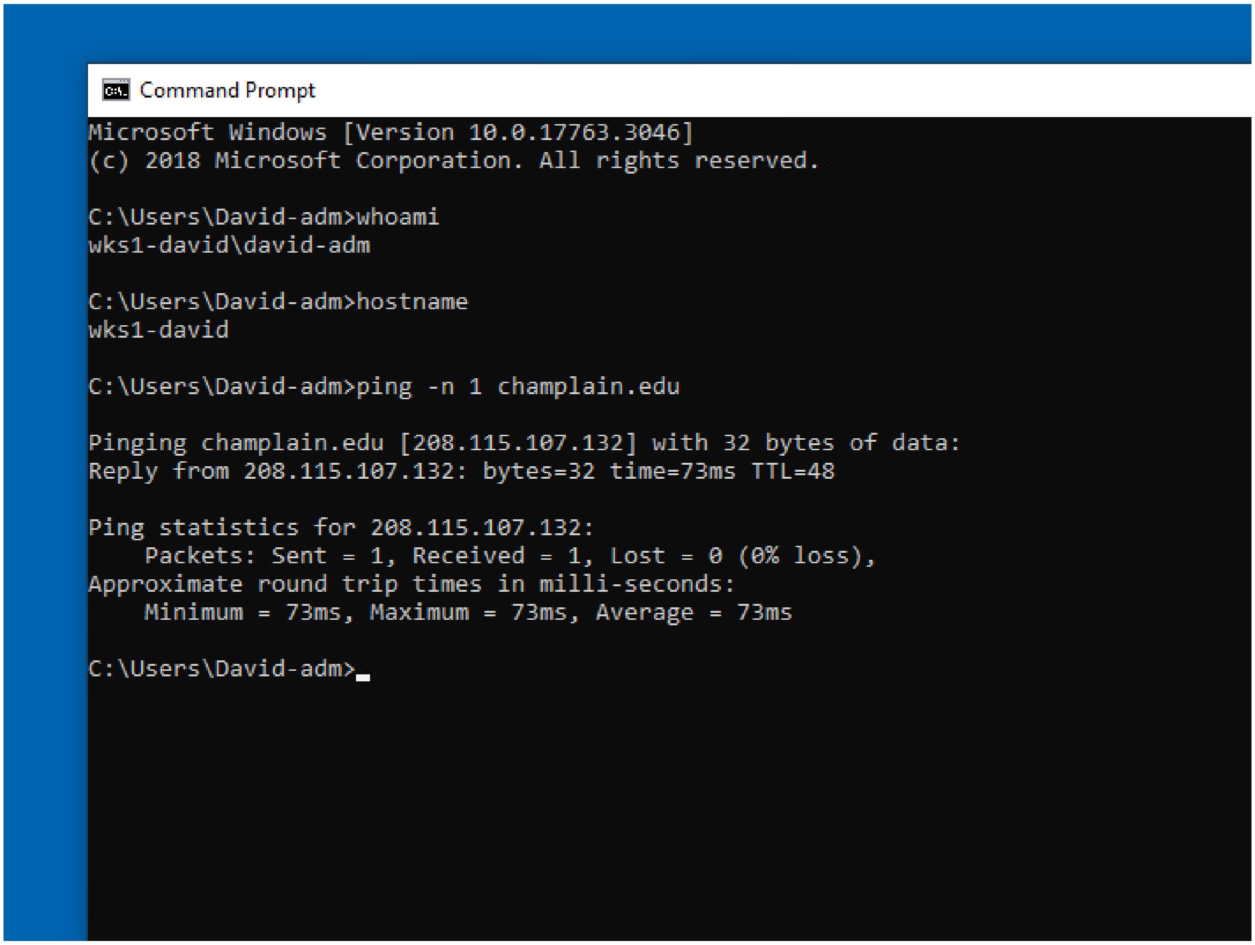
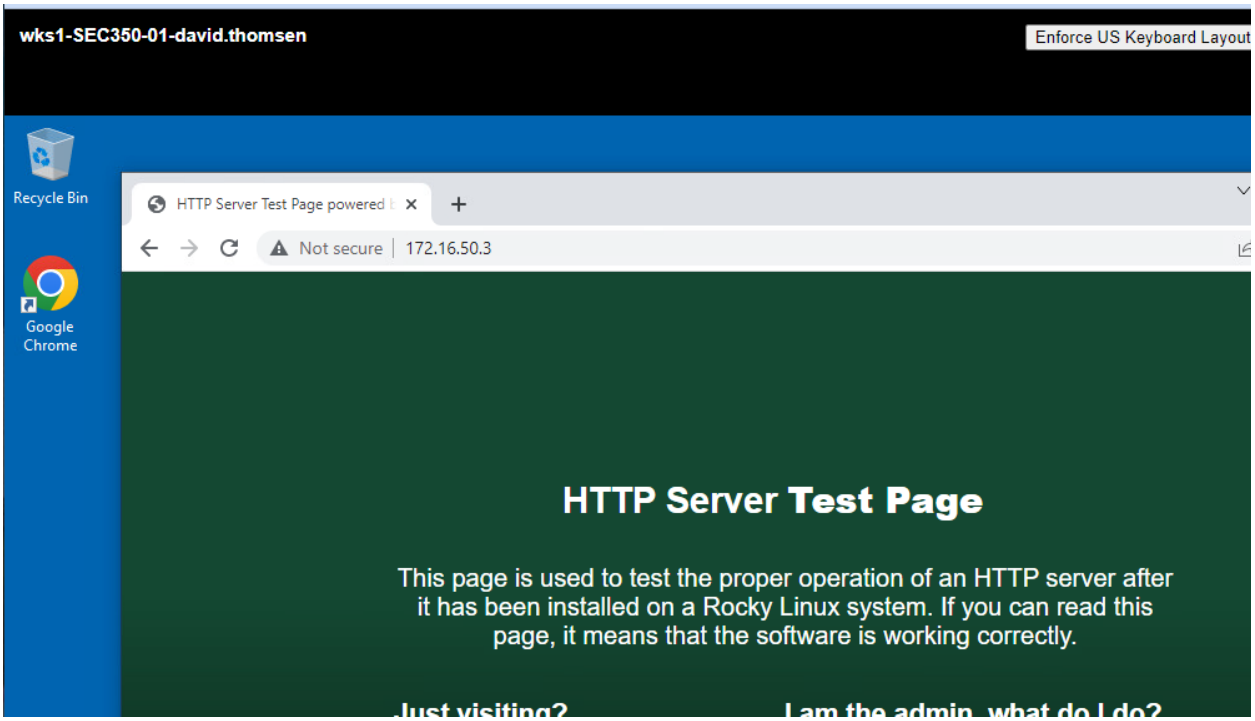
Deliverable 1: You will know you are successful when the following test passes. Provide a screenshot similar (change the IP address) to the one below. From WKS01:

- show results of the whoami command
- hostname command
- ping champlain.edu



```
Microsoft Windows [Version 10.0.17763.3046]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\David-adm>whoami
wks1-david\david-adm

C:\Users\David-adm>hostname
wks1-david

C:\Users\David-adm>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=73ms 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 = 73ms, Maximum = 73ms, Average = 73ms

C:\Users\David-adm>
```

Deliverable 2: You should also be able to get to your DMZ based web server. Provide a screenshot from WKS01 similar to the one below:


wks1-SEC350-01-david.thomsen
Enforce US Keyboard Layout
Recycle Bin
Google Chrome
HTTP Server Test Page powered b
Not secure
172.16.50.3

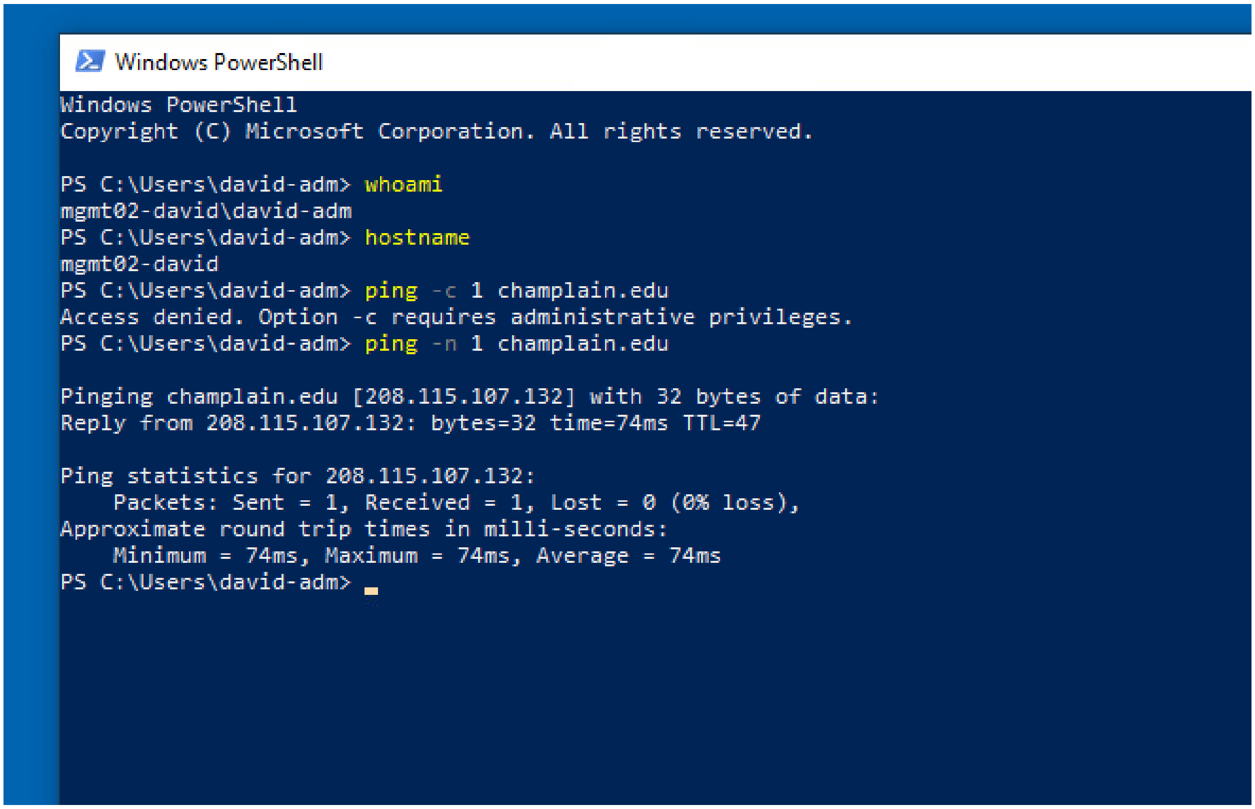
HTTP Server Test Page

This page is used to test the proper operation of an HTTP server after it has been installed on a Rocky Linux system. If you can read this page, it means that the software is working correctly.

Just visiting?

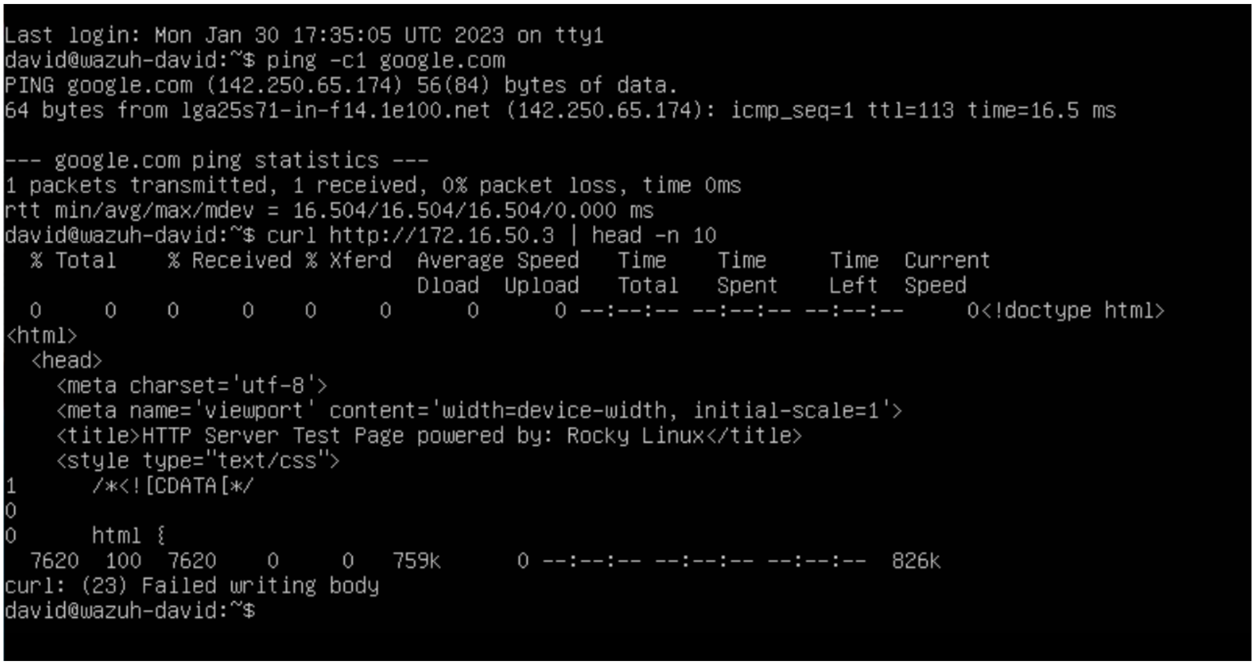
I am the admin, what do I do?

Deliverable 3. On mgmt02, provide a screenshot similar to the following one



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

PS C:\Users\david-adm> whoami
mgmt02-david\david-adm
PS C:\Users\david-adm> hostname
mgmt02-david
PS C:\Users\david-adm> ping -c 1 champlain.edu
Access denied. Option -c requires administrative privileges.
PS C:\Users\david-adm> 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=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 = 74ms, Maximum = 74ms, Average = 74ms
PS C:\Users\david-adm> _
```

Deliverable 4. On Wazuh, provide a screenshot similar to the one below that shows your correct hostname, named administrative (sudo) user logged in and able to ping google.com and curl your web server.

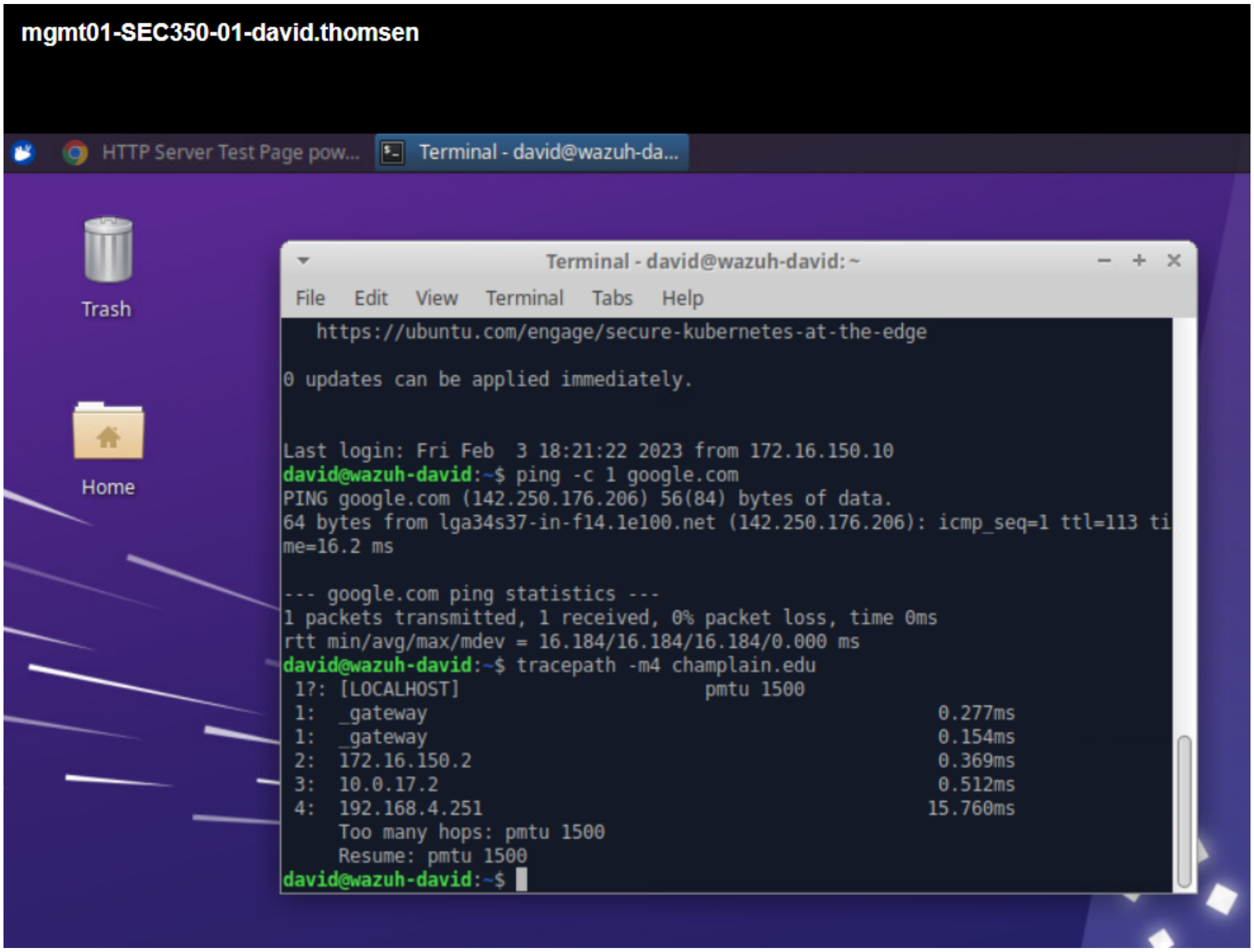


```
Last login: Mon Jan 30 17:35:05 UTC 2023 on tty1
david@wazuh-david:~$ ping -c1 google.com
PING google.com (142.250.65.174) 56(84) bytes of data.
64 bytes from lga25s71-in-f14.1e100.net (142.250.65.174): icmp_seq=1 ttl=113 time=16.5 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 16.504/16.504/16.504/0.000 ms
david@wazuh-david:~$ 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">
1      /*<![CDATA[*/
0
0      html {
  7620  100  7620    0     0   759k      0 --:--:-- --:--:-- --:--:--  826k
curl: (23) Failed writing body
david@wazuh-david:~$
```

Deliverable 5. On mgmt1, provide a screenshot similar to the one below showing:

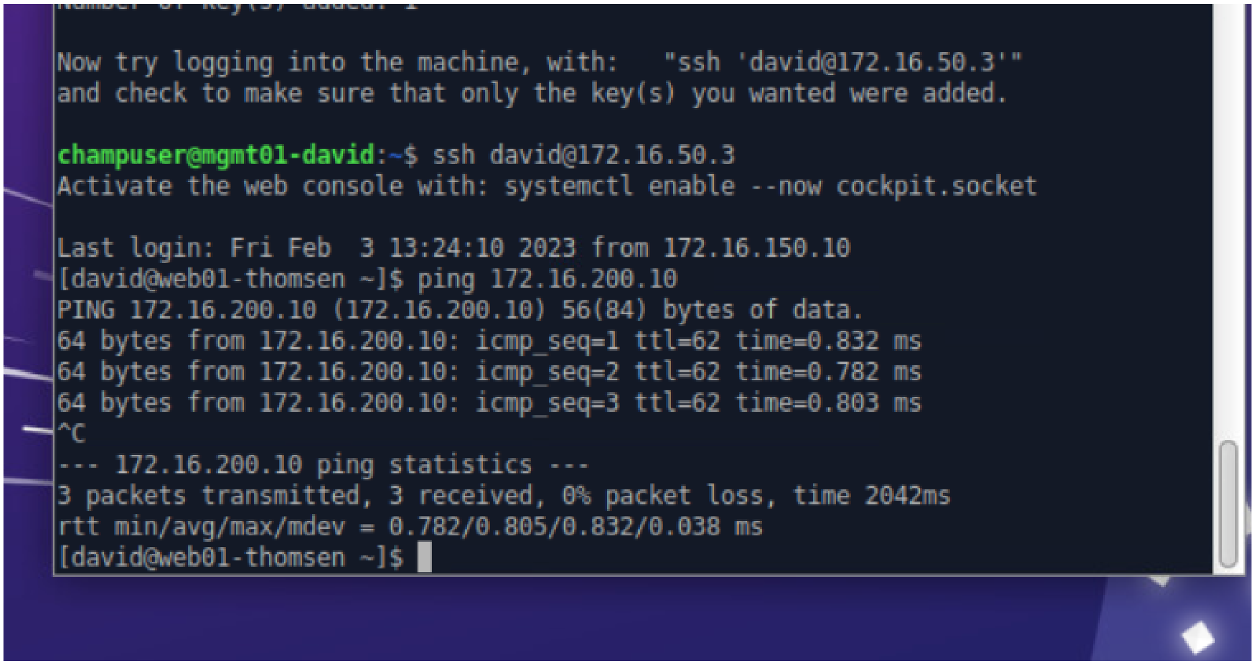
- ssh from mgmt1 on LAN to wazuh on MGMT
- another ping to google
- traceroute to champlain.edu with 4 hops

-


mgmt01-SEC350-01-david.thomsen
HTTP Server Test Page pow...
Terminal - david@wazuh-da...
Trash
Home
Terminal - david@wazuh-david: ~
File
Edit
View
Terminal
Tabs
Help

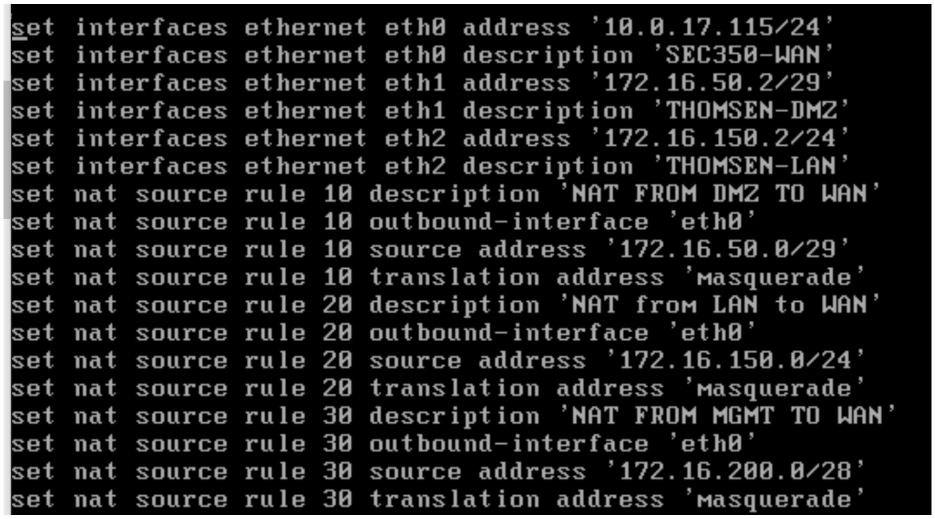
```
   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

0 updates can be applied immediately.


Last login: Fri Feb  3 18:21:22 2023 from 172.16.150.10
david@wazuh-david:~$ ping -c 1 google.com
PING google.com (142.250.176.206) 56(84) bytes of data.
64 bytes from lga34s37-in-f14.1e100.net (142.250.176.206): icmp_seq=1 ttl=113 ti
me=16.2 ms

--- google.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 16.184/16.184/16.184/0.000 ms
david@wazuh-david:~$ tracepath -m4 champlain.edu
 1?: [LOCALHOST]                      pmtu 1500
 1:  _gateway                                             0.277ms
 1:  _gateway                                             0.154ms
 2:  172.16.150.2                                         0.369ms
 3:  10.0.17.2                                            0.512ms
 4:  192.168.4.251                                       15.760ms
     Too many hops: pmtu 1500
     Resume: pmtu 1500
david@wazuh-david:~$ 
```

Deliverable 6. A screenshot similar to the one below shows a ping from web01 to wazuh.

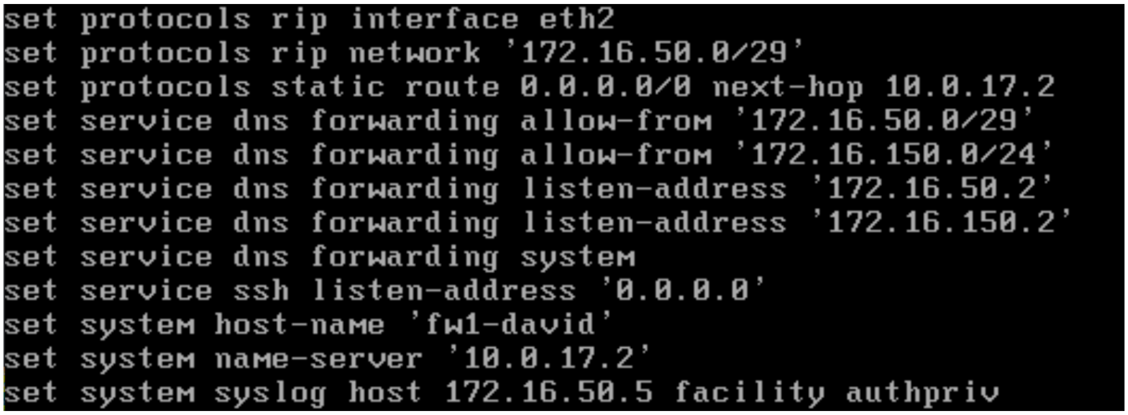


```
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'david@172.16.50.3'"
and check to make sure that only the key(s) you wanted were added.

champuser@mgmt01-david:~$ ssh david@172.16.50.3
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Fri Feb  3 13:24:10 2023 from 172.16.150.10
[david@web01-thomsen ~]$ ping 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=0.832 ms
64 bytes from 172.16.200.10: icmp_seq=2 ttl=62 time=0.782 ms
64 bytes from 172.16.200.10: icmp_seq=3 ttl=62 time=0.803 ms
^C
--- 172.16.200.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2042ms
rtt min/avg/max/mdev = 0.782/0.805/0.832/0.038 ms
[david@web01-thomsen ~]$
```

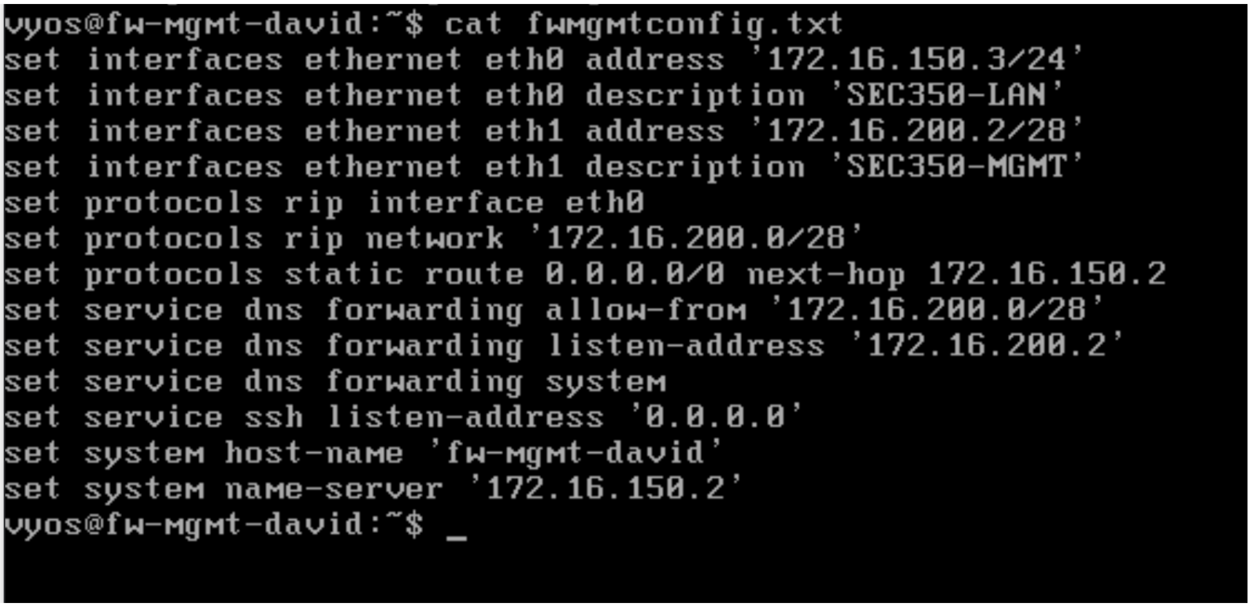
Deliverable 7. export the firewall configurations at the end of week 3 for fw-mgmt and fw1. The following command line will provide the most usable format. Provide screenshots or links to your firewall configurations in github.



```
set interfaces ethernet eth0 address '10.0.17.115/24'
set interfaces ethernet eth0 description 'SEC350-WAN'
set interfaces ethernet eth1 address '172.16.50.2/29'
set interfaces ethernet eth1 description 'THOMSEN-DMZ'
set interfaces ethernet eth2 address '172.16.150.2/24'
set interfaces ethernet eth2 description 'THOMSEN-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 20 description 'NAT from LAN to WAN'
set nat source rule 20 outbound-interface 'eth0'
set nat source rule 20 source address '172.16.150.0/24'
set nat source rule 20 translation address 'masquerade'
set nat source rule 30 description 'NAT FROM MGMT TO WAN'
set nat source rule 30 outbound-interface 'eth0'
set nat source rule 30 source address '172.16.200.0/28'
set nat source rule 30 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 'fw1-david'
set system name-server '10.0.17.2'
set system syslog host 172.16.50.5 facility authpriv
```



```
vyos@fw-mgmt-david:~$ cat fwmgmtconfig.txt
set interfaces ethernet eth0 address '172.16.150.3/24'
set interfaces ethernet eth0 description 'SEC350-LAN'
set interfaces ethernet eth1 address '172.16.200.2/28'
set interfaces ethernet eth1 description 'SEC350-MGMT'
set protocols rip interface eth0
set protocols rip network '172.16.200.0/28'
set protocols static route 0.0.0.0/0 next-hop 172.16.150.2
set service dns forwarding allow-from '172.16.200.0/28'
set service dns forwarding listen-address '172.16.200.2'
set service dns forwarding system
set service ssh listen-address '0.0.0.0'
set system host-name 'fw-mgmt-david'
set system name-server '172.16.150.2'
vyos@fw-mgmt-david:~$ _
```