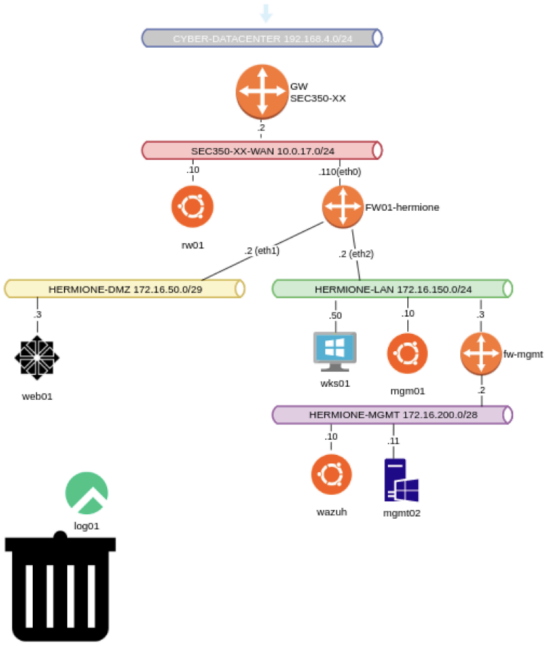
Updated Sep 8, 2023

Lab 3.1 Segmentation 1

In this lab, we are going to segment our network by adding a new firewall and a new network (MGMT). We will retire our log01 server and replace it with a new server on the MGMT network.



Step 1: Configure WKS01

This system will be a Windows 10 VM that represents a typical client in our **internal LAN (SEC-350-LAN).** You should have set the LAN interface on FW1 last week.

Create a named user and add them to the local administrators group. Change the hostname to wks01-yourname. Reboot as necessary.

IP Address: 172.16.150.50
Netmask: 255.255.255.0
Gateway: 172.16.150.2
DNS: 172.16.150.2

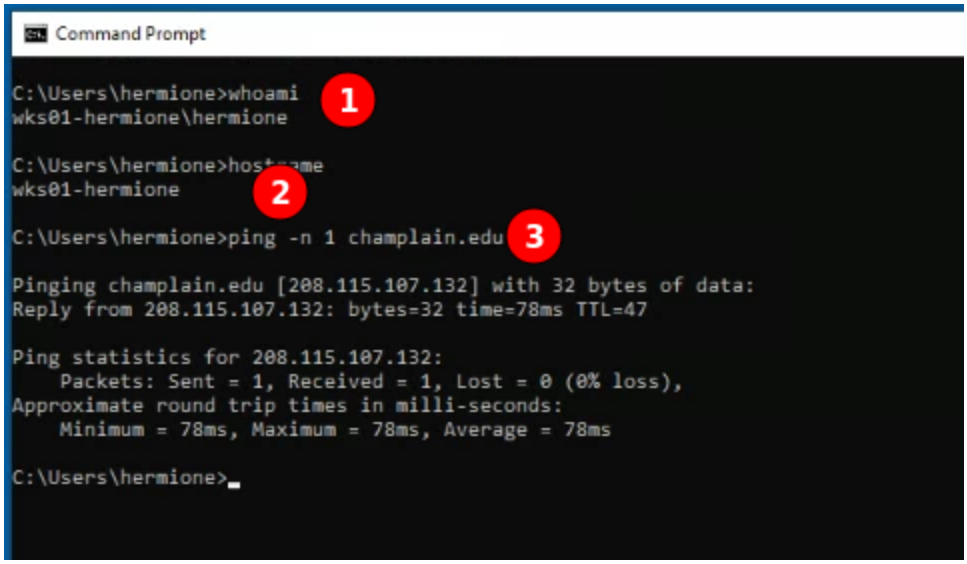
Step 2: Update fw01 - LAN Configuration

In week 1 you created a NAT source rule 10 for the DMZ. In week 2, you created a new NAT source rule **20** for the LAN.

In this lab, create a source rule **30** for NAT FROM MGMT to WAN. Refer to your previous lab or better yet, your tech journal for the correct vyOS syntax.

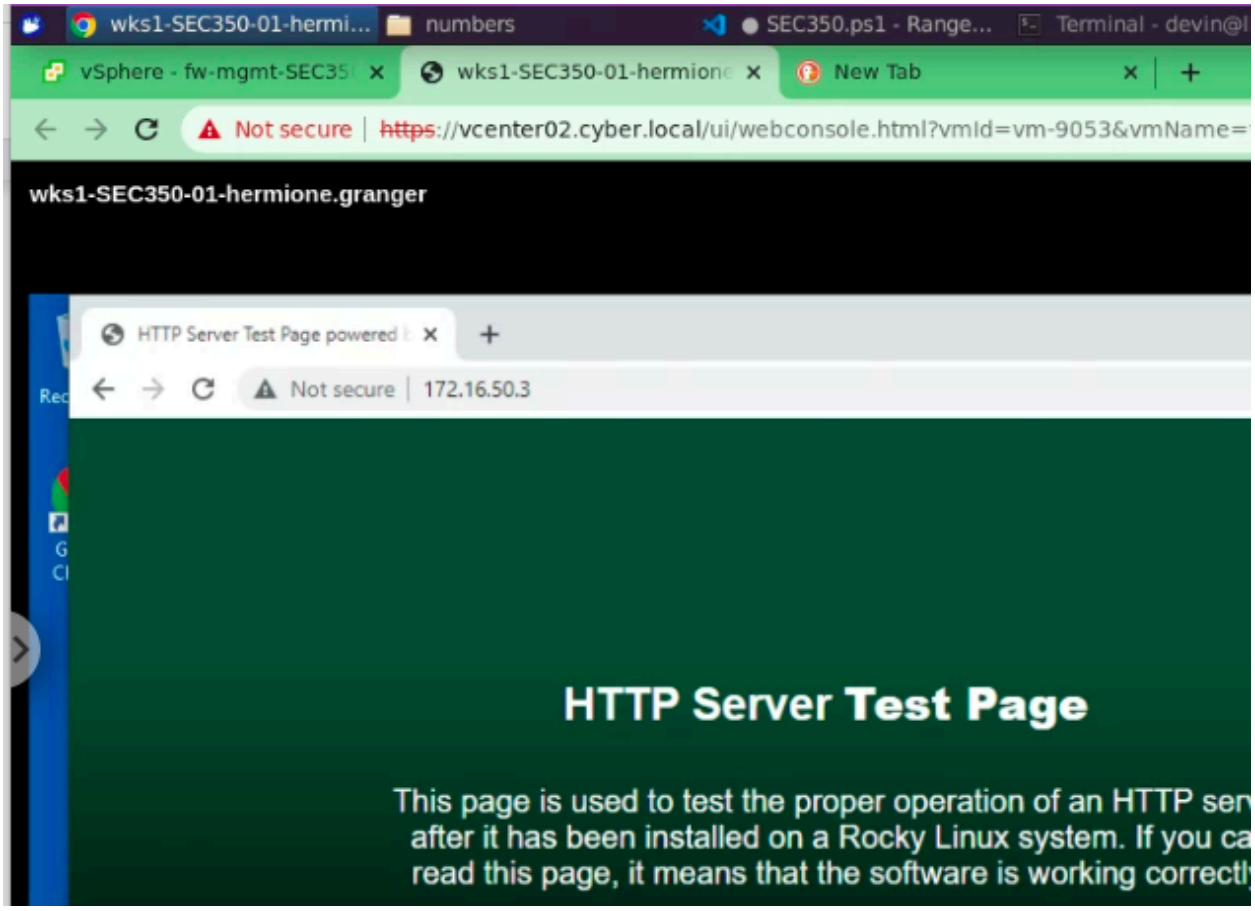
`Deliverable 1: Validate LAN access (you will test MGMT later) Provide a screenshot similar (change the IP address) to the one below. From WKS01:`

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



Updated Sep 8, 2023

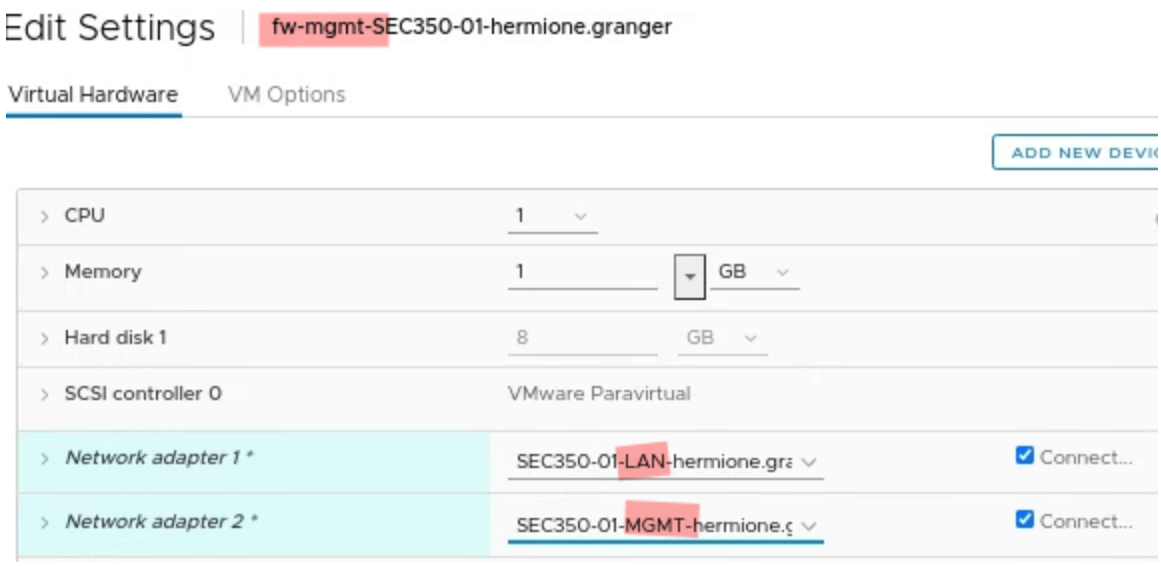
`Deliverable 2:  You should also be able to get to your DMZ based web server from WKS01.  Provide a screenshot from WKS01 similar to the one below:`



Step 3: Configure fw-mgmt

The Management Firewall is going to separate the main LAN production network from the systems used by administrators to manage this network (MGMT). You will configure the two interfaces as shown below.

Updated Sep 8, 2023



Configure your fw-mgmt firewall's hostname with interface descriptions and interface addresses:
eth0: LAN-172.16.150.3/24
eth1: MGMT-172.16.200.2/28
NOTE: MGMT is using a /28!

Note that the SEC350-LAN Interface is on 172.16.150.3 (.2 is already used by fw01). The firewall's SEC350-MGMT interface will be assigned an IP of 172.16.200.2 (FYI: different segment == different subnet). Don't forget to remove the default dhcp address from eth0.

```
vyos@fw-mgmt-hermione:~$ show interfaces
Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down
Interface        IP Address                        S/L  Description
---------        ----------                        ---  -----------
eth0             172.16.150.3/24                   u/u  SEC350-LAN
eth1             172.16.200.2/28                   u/u  SEC350-MGMT
lo               127.0.0.1/8                       u/u
                 ::1/128
vyos@fw-mgmt-hermione:~$ _
```

Set the following (refer to Tech Journal):

- gateway next-hop (static route)
- name server to your fw01's LAN interface address (172.16.150.2).
- set dns forwarding such that requests are allowed from your management subnet and management interface.

Step 4: Configure mgmt02

mgmt02 is a windows server, place this on your management segment (check your adapter in vcenter!)
IP Address: 172.16.200.11

Netmask: 255.255.255.240 (yes this is a /28)
Gateway: 172.16.200.2
DNS: 172.16.200.2

Add a named administrative user and change the hostname.

Step 5: RIP on FW1 and FW-MGMT

> 💡Rather than double NAT from MGMT to LAN and LAN to WAN we will implement RIP which will greatly simplify the routing from MGMT to LAN. It will also increase our visibility for sensors outside of the MGMT network.

We are going to configure fw1 and fw-mgmt in such a way that they know of each other's attached networks. This should be a refresher from NET150 and NET215 however we will be using vyos and not packet tracer.

On fw01, enable RIP on eth2(LAN) and advertise the DMZ Network

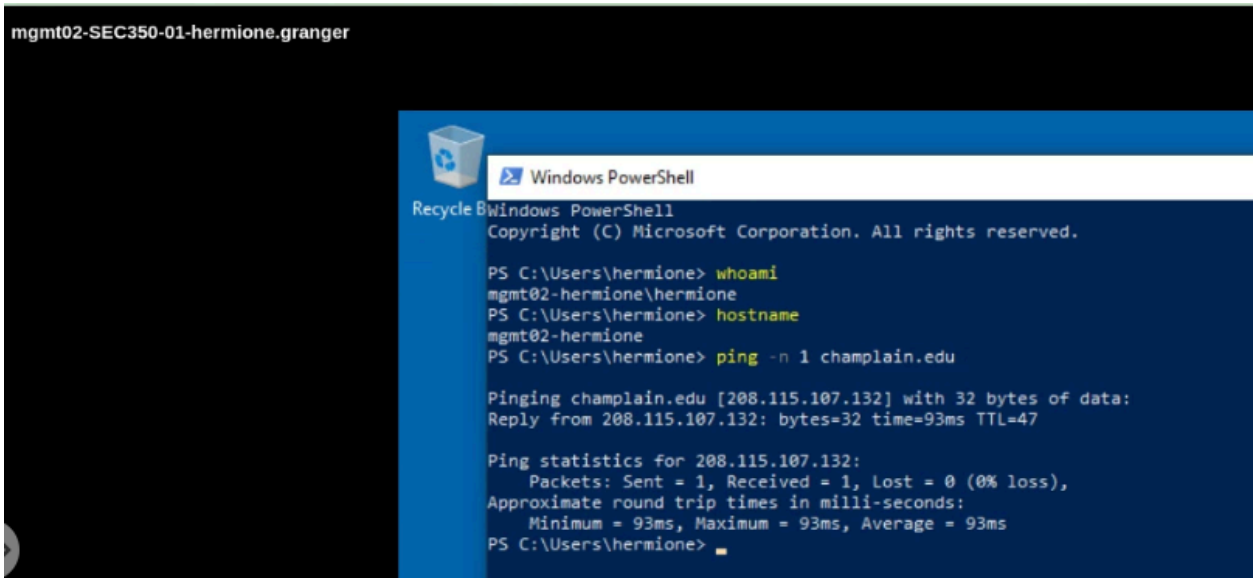
```
set protocols rip interface eth2
#share routes to the DMZ
set protocols rip network 172.16.50.0/29
```

On fw-mgmt, Enable RIP on eth0(LAN) and advertise the MGMT network

```
set protocols rip interface eth0
#share routes to the management network
set protocols rip network '172.16.200.0/28'
```

On fw01, you should have already allowed NAT traffic from the MGMT network (rule 30).

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



Step 6: Shutdown log01

Say goodbye to your syslog server, if you are done with all previous labs, feel free to turn it off. We are going to configure a new box called wazuh that will capture security relevant logs from configured systems.

Step7: Configure server wazuh

Wazuh is a new ubuntu server. Configure it on the **SEC350-MGMT** network with the following address information. It may take some time to boot because it's looking for a non-existent dhcp server.

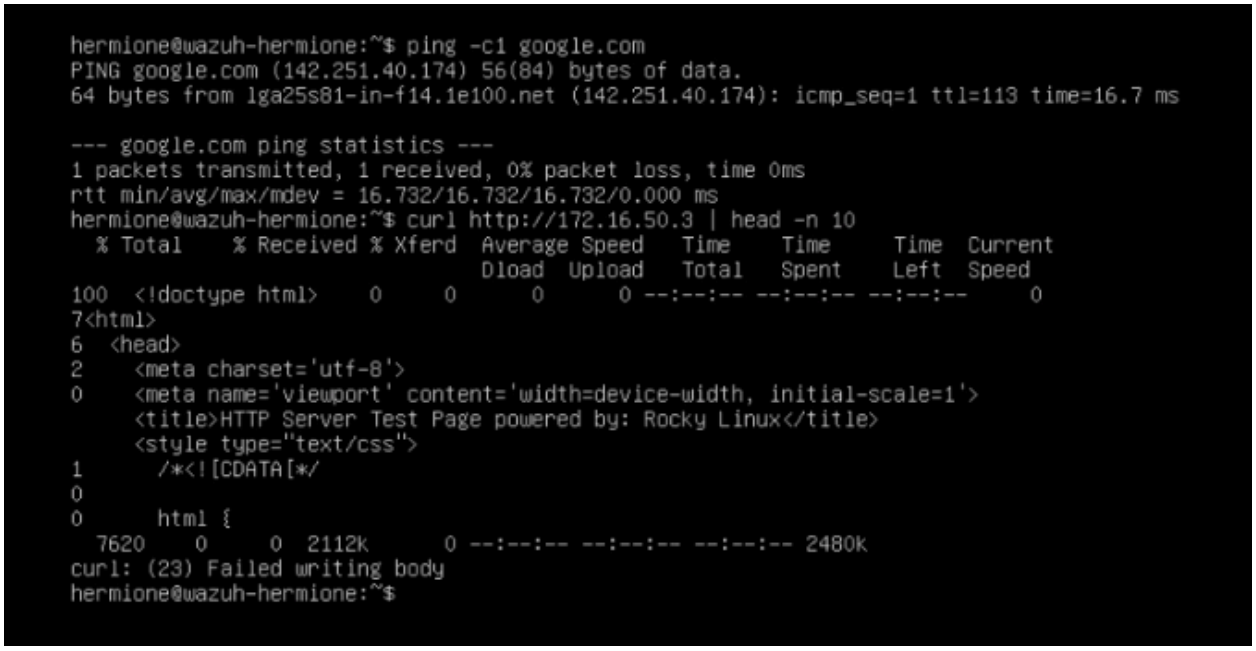
If you've not used netplan yet, welcome (it's fun)!
(Hints:

- /etc/netplan/00-installer-config.yaml is the config file
- When researching, use instructions with "routes: -to: default …." instead of Gateway4 (that is deprecated)
- sudo netplan apply
- IP info

  IP: 172.16.200.10/28
  Gateway: 172.16.200.2
  DNS: 172.16.200.2

Set hostname: wazuh-yourname

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.



Step 8: Update client logging configurations

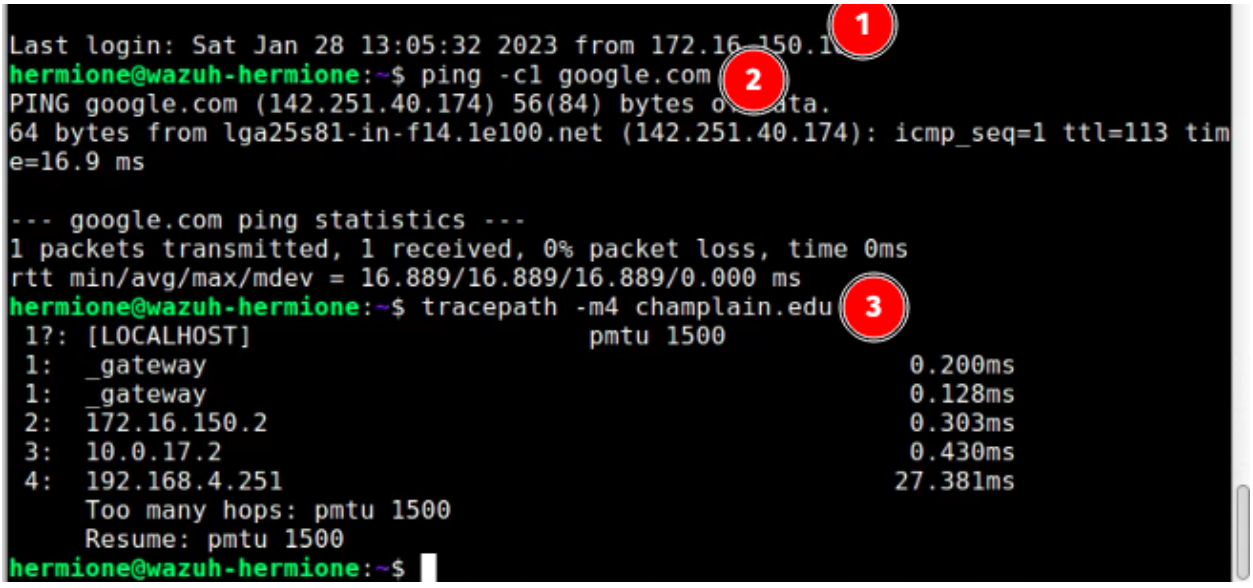
💡fw01 and web01 have stale syslog configurations because we have decommissioned log01. Remove those log forwarding messages from the vyos syslog configuration and the web01 client configuration. In the near future, our wazuh agents will forward specific messages (instead of all of them)

- On web01, remove your rsyslog dropin configuration from /etc/rsyslog.d
- On fw1, remove syslog host 172.16.50.5 setting from configuration (Hint: delete…)

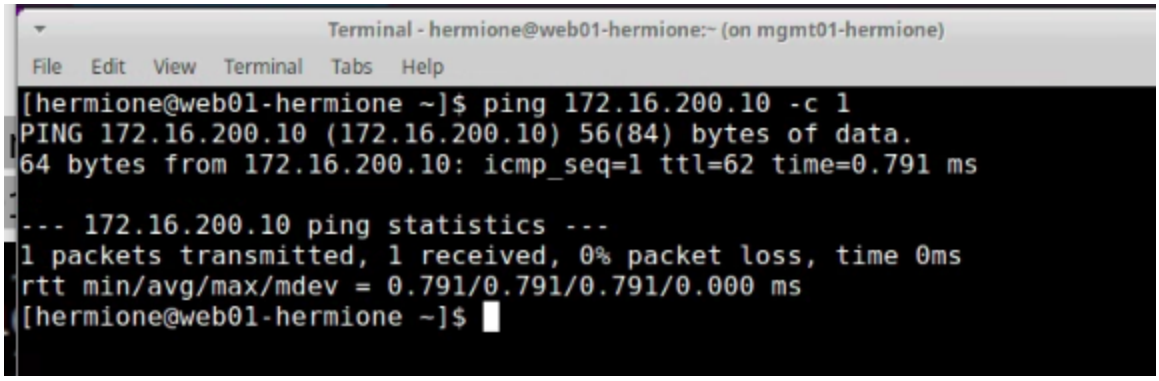
`Deliverable 5. On mgmt1, provide a screenshot similar to the one below showing:`

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

💡Take a hard look at the traceroute, visualize the hops from mgmt->lan->wan->internet



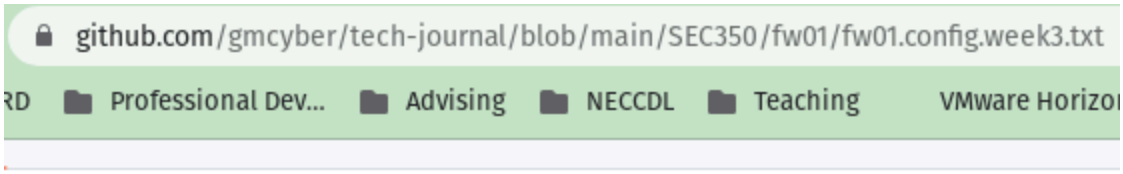
Deliverable 6. A screenshot similar to the one below that shows a ping from web01 to wazuh.



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.

```
show configuration commands | grep -v "syslog
global\|ntp\|login\|console\|config\|hw-id\|loopback\|conntrack"
```

Updated Sep 8, 2023



main **tech-journal** / SEC350 / fw01 / **fw01.config.week3.txt**

gmcyber week3 sec350

1 contributor

30 lines (30 sloc) | 1.52 KB

```
1  set interfaces ethernet eth0 address '10.0.17.110/24'
2  set interfaces ethernet eth0 description 'SEC350-WAN'
3  set interfaces ethernet eth1 address '172.16.50.2/29'
4  set interfaces ethernet eth1 description 'HERMIONE-DMZ'
5  set interfaces ethernet eth2 address '172.16.150.2/24'
6  set interfaces ethernet eth2 description 'HERMIONE-LAN'
7  set nat source rule 10 description 'NAT FROM DMZ to WAN'
8  set nat source rule 10 outbound-interface 'eth0'
```

main **tech-journal** / SEC350 / fw-mgmt / **fw-mgmt.week3.txt**

gmcyber week3 sec350

1 contributor

13 lines (13 sloc) | 625 Bytes

```
1  set interfaces ethernet eth0 address '172.16.150.3/24'
2  set interfaces ethernet eth0 description 'HERMIONE-LAN'
3  set interfaces ethernet eth1 address '172.16.200.2/28'
4  set interfaces ethernet eth1 description 'HERMIONE-MGMT'
5  set protocols rip interface eth0
6  set protocols rip network '172.16.200.0/28'
7  set protocols static route 0.0.0.0/0 next-hop 172.16.150.2
```