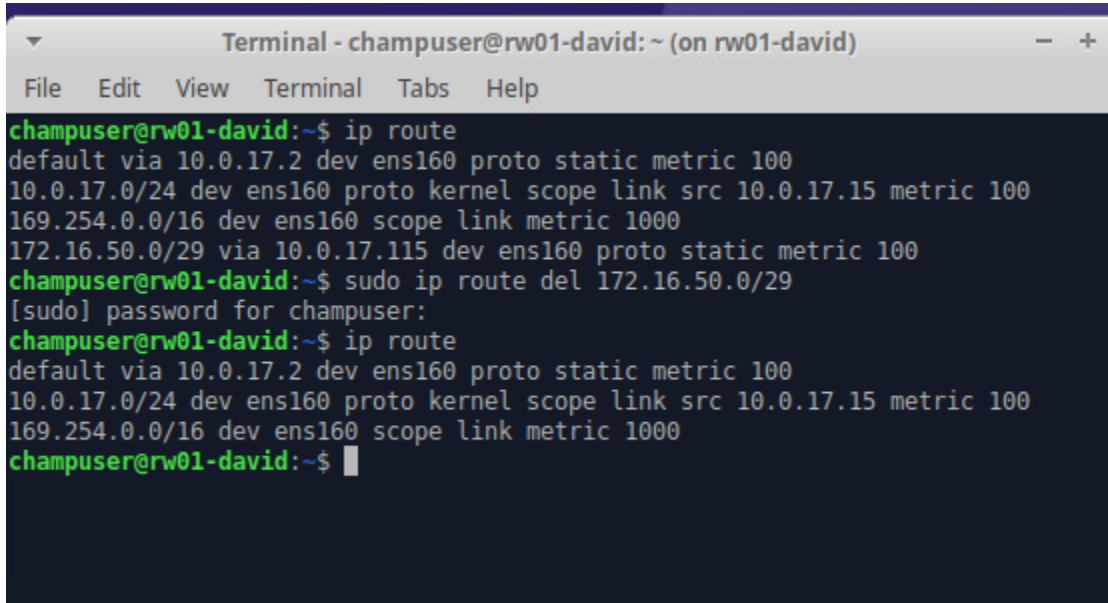


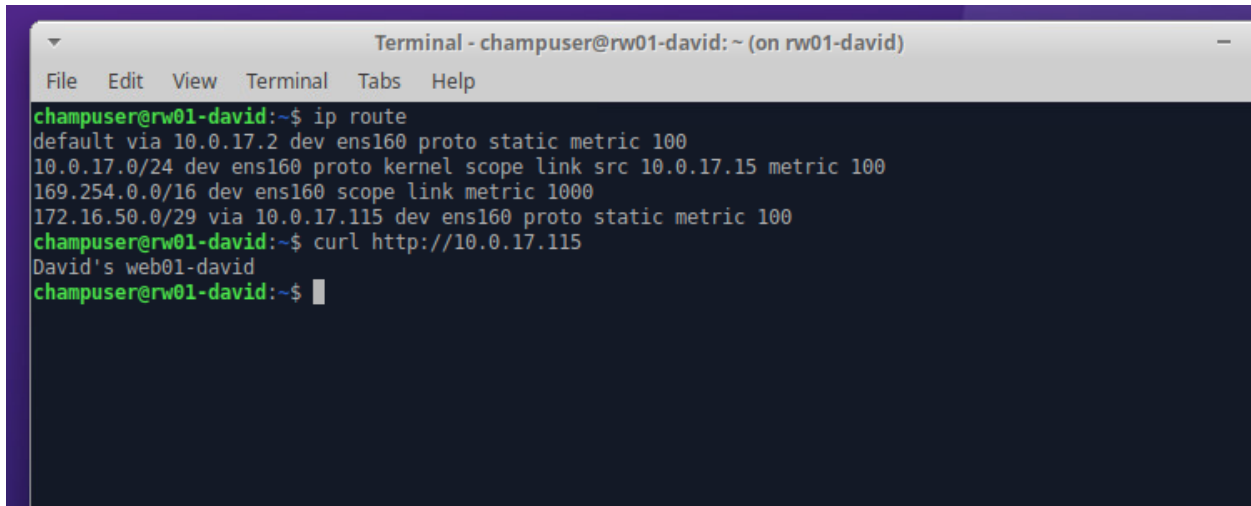
Deliverable 1. Provide a screenshot from rw01 similar to the one below that no longer shows the route to the DMZ network.

A terminal window titled "Terminal - champuser@rw01-david: ~ (on rw01-david)" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the following commands and output:

```
champuser@rw01-david:~$ ip route
default via 10.0.17.2 dev ens160 proto static metric 100
10.0.17.0/24 dev ens160 proto kernel scope link src 10.0.17.15 metric 100
169.254.0.0/16 dev ens160 scope link metric 1000
172.16.50.0/29 via 10.0.17.115 dev ens160 proto static metric 100
champuser@rw01-david:~$ sudo ip route del 172.16.50.0/29
[sudo] password for champuser:
champuser@rw01-david:~$ ip route
default via 10.0.17.2 dev ens160 proto static metric 100
10.0.17.0/24 dev ens160 proto kernel scope link src 10.0.17.15 metric 100
169.254.0.0/16 dev ens160 scope link metric 1000
champuser@rw01-david:~$
```

```
vyos@fw1-david# show nat destination
+rule 10 {
+  description HTTP->WEB01
+  destination {
+    port 80
+  }
+  inbound-interface eth0
+  protocol tcp
+  translation {
+    address 172.16.50.3
+    port 80
+  }
+}
[edit]
vyos@fw1-david#
```

Deliverable 2. Provide a screenshot similar to the one below that shows a curl to your fw01's eth0 interface's IP address.

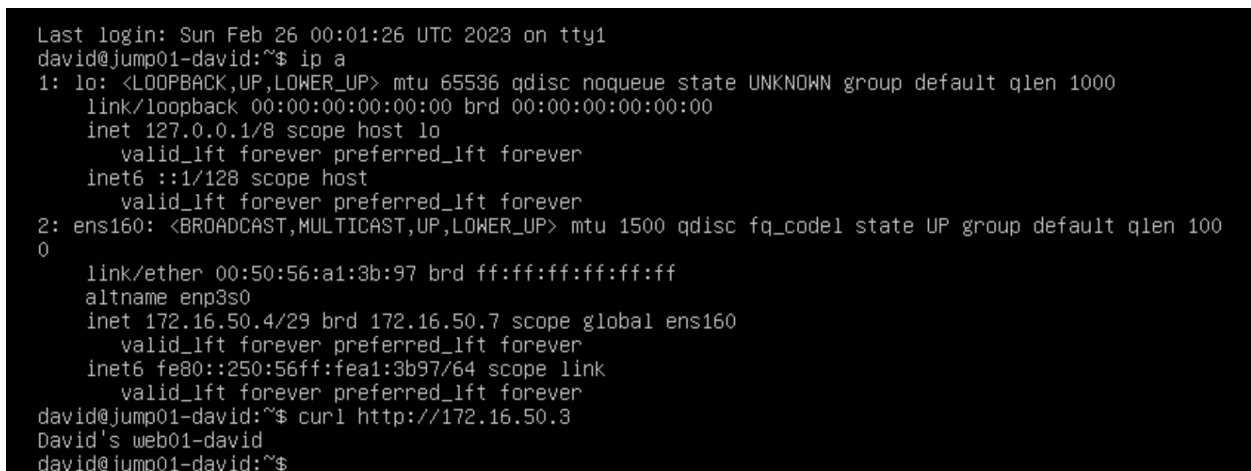


```
Terminal - champuser@rw01-david:~ (on rw01-david)
File Edit View Terminal Tabs Help
champuser@rw01-david:~$ ip route
default via 10.0.17.2 dev ens160 proto static metric 100
10.0.17.0/24 dev ens160 proto kernel scope link src 10.0.17.15 metric 100
169.254.0.0/16 dev ens160 scope link metric 1000
172.16.50.0/29 via 10.0.17.115 dev ens160 proto static metric 100
champuser@rw01-david:~$ curl http://10.0.17.115
David's web01-david
champuser@rw01-david:~$
```

Deliverable 3. Configure jump to have the following characteristics

- Network: DMZ Network
- IP Address: 172.16.50.4/29
- hostname: jump
- secure champuser by changing the default password

Provide a screenshot similar to the one below that shows the IP address, and a curl to jump's nextdoor neighbor, web01



```
Last login: Sun Feb 26 00:01:26 UTC 2023 on tty1
david@jump01-david:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default 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 fq_codel state UP group default qlen 1000
    link/ether 00:50:56:a1:3b:97 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 172.16.50.4/29 brd 172.16.50.7 scope global ens160
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:fea1:3b97/64 scope link
        valid_lft forever preferred_lft forever
david@jump01-david:~$ curl http://172.16.50.3
David's web01-david
david@jump01-david:~$
```

Deliverable 4. Provide a screenshot similar to the one above that shows a passwordless login from rw01 to jump via tcp/22 directed to fw01's eth0 IP address.

```
champuser@rw01-david:~$  
champuser@rw01-david:~$ ssh david-jump@10.0.17.115  
Enter passphrase for key '/home/champuser/.ssh/id_rsa':  
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-33-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
System information as of Sat Feb 25 11:28:54 PM UTC 2023  
  
System load:  0.0                Processes:            211  
Usage of /:   24.9% of 18.53GB   Users logged in:     2  
Memory usage: 12%                IPv4 address for ens160: 172.16.50.4  
Swap usage:   0%  
  
0 updates can be applied immediately.  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Sat Feb 25 23:25:00 2023 from 10.0.17.15  
david-jump@jump01-david:~$
```

Note I was able to get this working however, I made the keys on the champuser account rather than my named account.

```
minal - root@jump01-da...  
File Edit View Terminal Tabs Help  
root@jump01-david:~# id david-jump  
uid=1002(david-jump) gid=1002(david-jump) groups=1002(david-jump)  
root@jump01-david:~# id david  
uid=1001(david) gid=1001(david) groups=1001(david),27(sudo)  
root@jump01-david:~# cat /etc/shadow | grep david-jump  
david-jump::19408:0:99999:7:::  
root@jump01-david:~#
```

Deliverable 5. Figure out how to install the wazuh agent on jump. Note, you can pull the deb package down to mgmt01, scp it to jump and then execute the installation command against the agent installation package. In this way, you don't have to open up the DMZ-to-WAN firewall. Provide a screenshot showing the successful registration of your jump server's agent.

