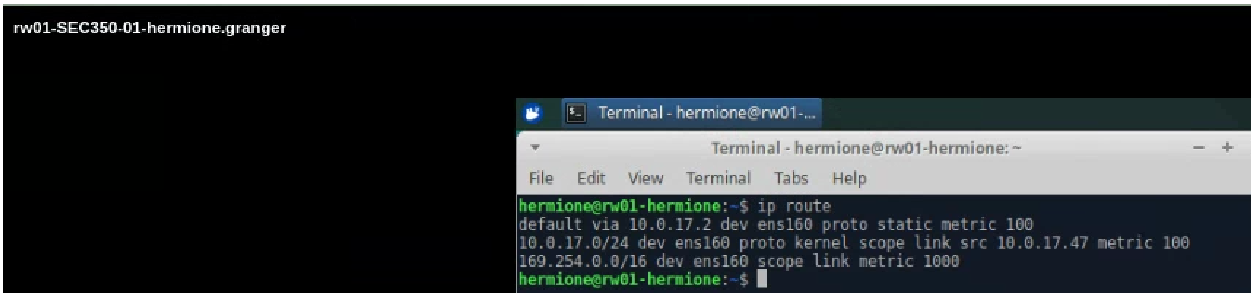
Updated: Sep 29, 2023

Lab 6.1 Port Forwarding and Jump Boxes

> 💣rw01 has a bit too much information about our internal DMZ network. Specifically, rw01 knows the internal routing for our DMZ and used this information to create a static route from SEC350-WAN to the DMZ. A better alternative is to mask the presence of the DMZ altogether with NAT destination rules.

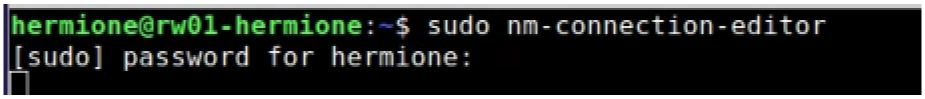
Remove your static route from rw01

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


rw01-SEC350-01-hermione.granger
Terminal - hermione@rw01-...
Terminal - hermione@rw01-hermione: ~
File
Edit
View
Terminal
Tabs
Help

```
hermione@rw01-hermione:~$ 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 10.0.17.47 metric 100
169.254.0.0/16 dev ens160 scope link metric 1000
hermione@rw01-hermione:~$
```

- Can use the “ip route” command to delete routes OR
- Can use the network manager applet - but may need to run it as sudo.



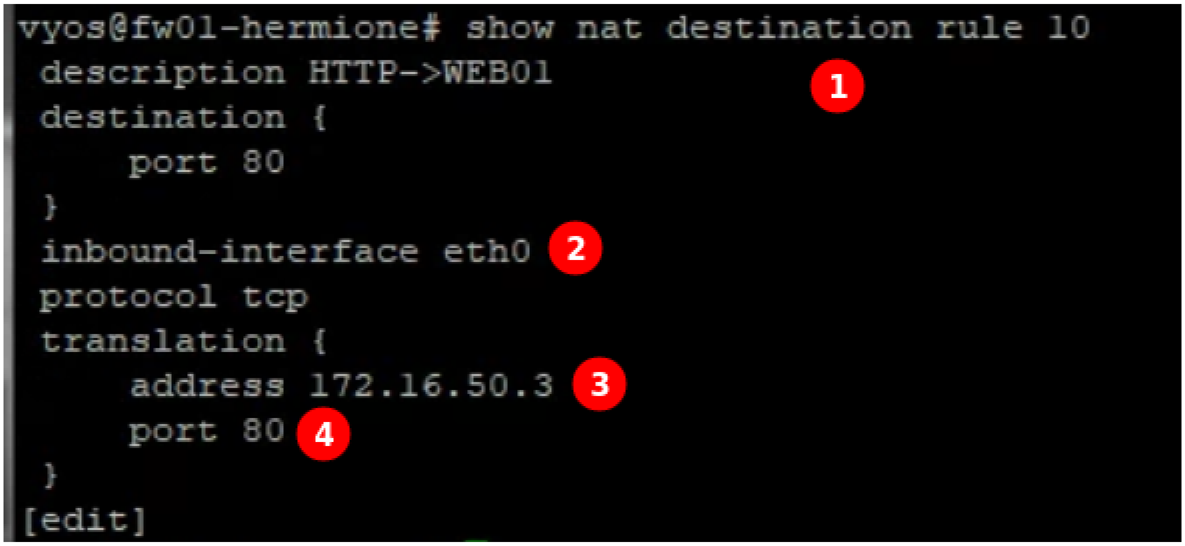
```
hermione@rw01-hermione:~$ sudo nm-connection-editor
[sudo] password for hermione:
```

Port Forwarding

We've worked with NAT source rules when dealing with traffic from inside the network going out to the WAN. Now we are going to add a NAT destination rule (a.k.a. port forwarding) so that any port 80 traffic coming to our firewall's WAN/eth0 interface will be forwarded on to web01.

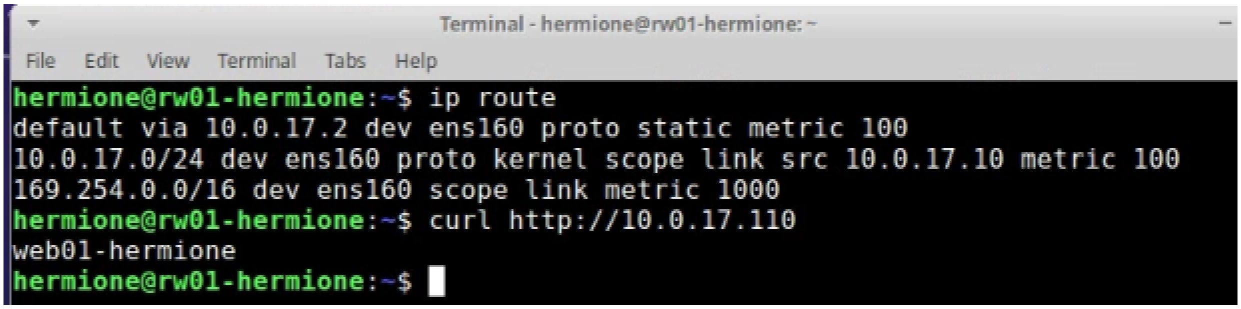
- The destination port refers to the port received by eth0 on fw1
- The inbound interface is eth0/WAN
- The address received is "translated" and forwarded to web01 port 80

Updated: Sep 29, 2023



```
vyos@fw01-hermione# 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]
```

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



Terminal - hermione@rw01-hermione: ~
File Edit View Terminal Tabs Help

```
hermione@rw01-hermione:~$ 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 10.0.17.10 metric 100
169.254.0.0/16 dev ens160 scope link metric 1000
hermione@rw01-hermione:~$ curl http://10.0.17.110
web01-hermione
hermione@rw01-hermione:~$ 
```

The Jump Box

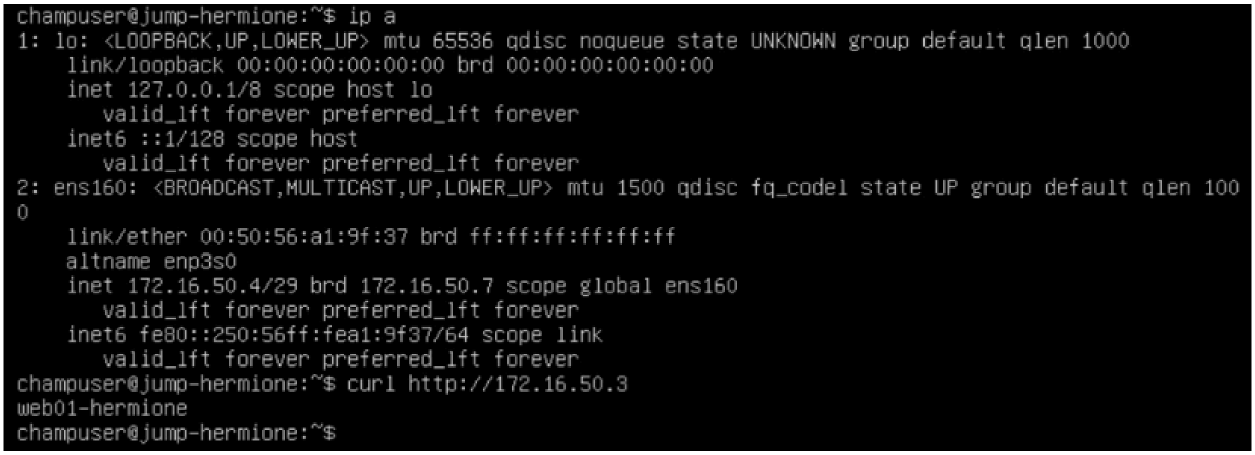
💡A Jump Box is a system, normally exposing SSH, RDP or a VPN port to a less secure network. It is typically located within a DMZ and is used as an initial access point for remote administration. Once authenticated to the Jump Box, you can leverage its position in the network to pivot to internal systems (so can an attacker). It is regularly used in industry when someone needs network access. The Jump Box needs to be resistant to Bruteforce password attacks and be watched like a hawk. Its access to internal networks should be restricted to what it needs and no more. We are going to deploy one of these to the DMZ for our external web admin to use when administering the web server.

Updated: Sep 29, 2023

```
Deliverable 3.  Configure jump to have the following characteristics
```

- `Network: DMZ Network`
- `IP Address: 172.16.50.4/29`
- `hostname: jump-`*`yourname`*
- `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
```



```
champuser@jump-hermione:~$ 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 100
0
    link/ether 00:50:56:a1:9f:37 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:fea1:9f37/64 scope link
       valid_lft forever preferred_lft forever
champuser@jump-hermione:~$ curl http://172.16.50.3
web01-hermione
champuser@jump-hermione:~$
```

💡Use Case: We have a remote admin (yourname-jump) coming from rw01 and they need access to web01 via jump. This access should not be enforced by password but rather an SSH key. Think very hard about how best to get your public key. to jump. You should not type it out because there is a nearly 100% chance you will introduce a typo.

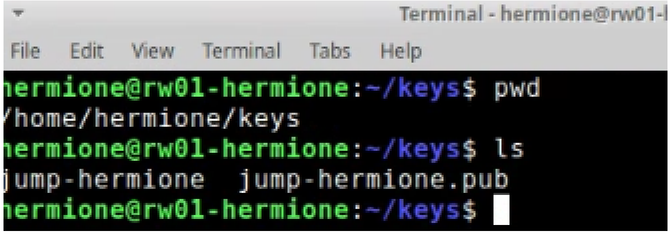
Firewalls and SSH

1. Adjust the firewall rules from LAN-TO-DMZ such that mgmt01 can ssh into any server on the DMZ.
2. Make sure that fw01 is only listening for SSH on the LAN interface (172.16.150.2) and not on all interfaces (0.0.0.0/0)

Key Generation on rw01

On rw01, create a dedicated keypair that will only be used for ssh access to jump. make sure to name the keypair something other than the default and add a comment indicating its purpose. Make sure to add a passphrase when prompted.

Updated: Sep 29, 2023



```
ermione@rw01-hermione:~/keys$ pwd
/home/hermione/keys
ermione@rw01-hermione:~/keys$ ls
jump-hermione  jump-hermione.pub
ermione@rw01-hermione:~/keys$ 
```

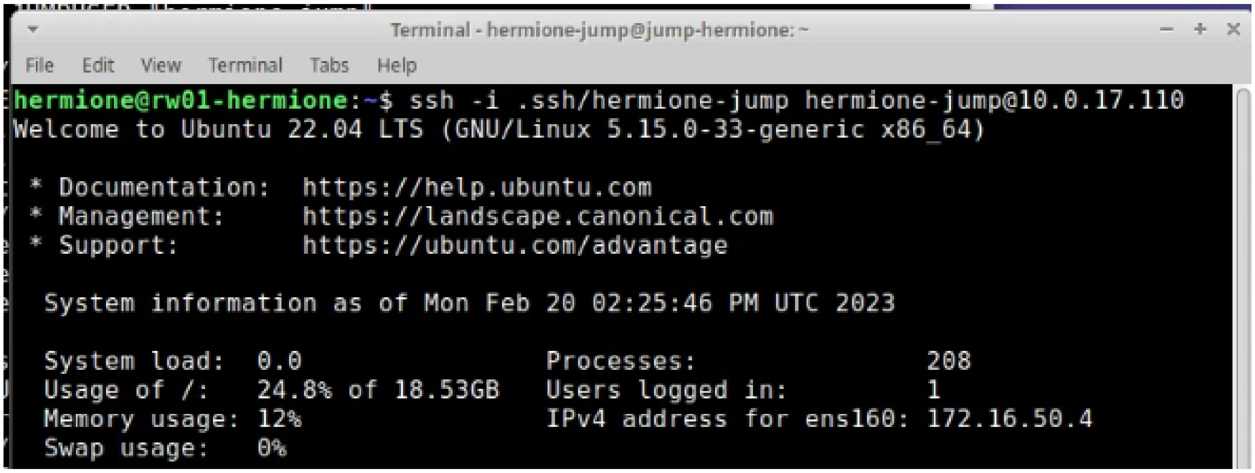
Passwordless User on jump

Figure out how to create a passwordless user called yourname-jump on jump. Figure out how to copy over the public component of the jump keypair you just created on rw01 to new users .ssh/authorized_keys file. Make sure to document this in your tech journal. This will require some research and likely a lot of troubleshooting to make happen.

Port Forward TCP/22 -> Jump

- Create a port forward for tcp/22 on the firewall and have it redirected to jump
- Adjust WAN-TO-DMZ to allow SSH from WAN into jump
- Attempt your SSH from web01 to your fw01's eth0 address. Make sure to tell ssh which keys to use.

💡You might get a message indicating the remote host identification has changed. If so, this is because the destination IP was once associated with vyos/ssh and not jump/ssh. The fix is to remove the ~/.ssh/known_hosts file on rw01.


Terminal - hermione-jump@jump-hermione: ~
File Edit View Terminal Tabs Help

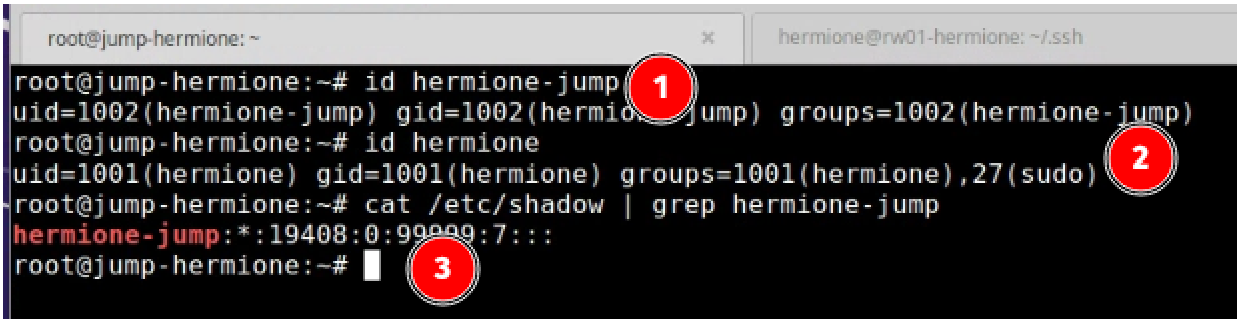
```
hermione@rw01-hermione:~$ ssh -i .ssh/hermione-jump hermione-jump@10.0.17.110
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-33-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Mon Feb 20 02:25:46 PM UTC 2023

  System load:  0.0               Processes:               208
  Usage of /:   24.8% of 18.53GB   Users logged in:         1
  Memory usage: 12%               IPv4 address for ens160: 172.16.50.4
  Swap usage:   0%
```

Updated: Sep 29, 2023

```
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.
```

Create an account for the internal admin

So the external user gets into jump using an ssh key, you will still want to manage jump via SSH from mgmt01. Make sure you have a named administrative user so you can login as something other than champuser. When you are done you should have a remote unprivileged passwordless user called yourname-jump, a privileged (sudo) user called yourname. You can check your work with something like:

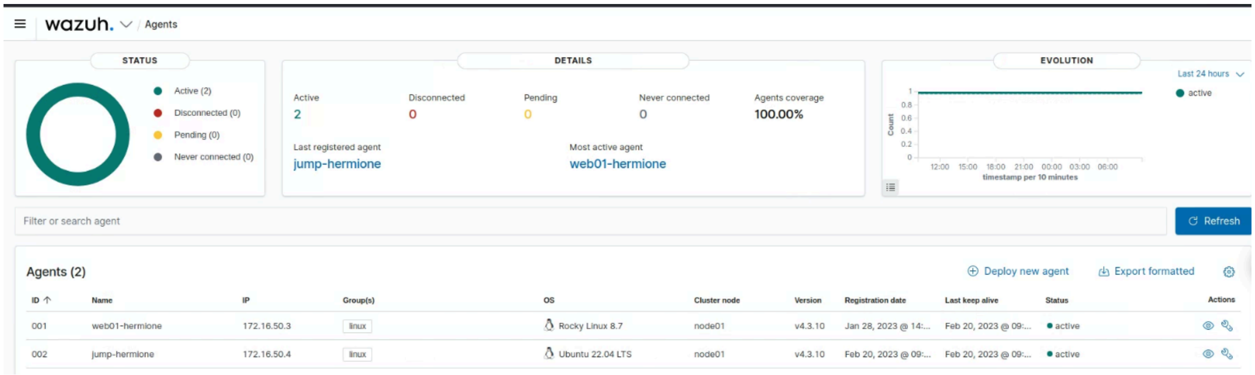


```
root@jump-hermione:~# id hermione-jump
uid=1002(hermione-jump) gid=1002(hermione-jump) groups=1002(hermione-jump)
root@jump-hermione:~# id hermione
uid=1001(hermione) gid=1001(hermione) groups=1001(hermione),27(sudo)
root@jump-hermione:~# cat /etc/shadow | grep hermione-jump
hermione-jump:*:19408:0:99999:7:::
root@jump-hermione:~# 
```

1. Shows that yourname-jump is not a member of any privileged group
2. yourname is a sudo user
3. yourname-jump has no password entry in /etc/shadow.

Wazuh agent on Jump

```
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.
```



Active	Disconnected	Pending	Never connected	Agents coverage
2	0	0	0	100.00%

Last registered agent
jump-hermione

Most active agent
web01-hermione

Agents (2)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status
001	web01-hermione	172.16.50.3	linux	Rocky Linux 8.7	node01	v4.3.10	Jan 28, 2023 @ 14:...	Feb 20, 2023 @ 09:...	● active
002	jump-hermione	172.16.50.4	linux	Ubuntu 22.04 LTS	node01	v4.3.10	Feb 20, 2023 @ 09:...	Feb 20, 2023 @ 09:...	● active

Updated: Sep 29, 2023

Journal

Deliverable 6. Tech Journal that covers:

- Netplan configuration, ideally this is a link to your SYS265 tech journal article.
- Port Forwarding and firewall adjustments for vyos
- Creation of a passwordless user on jump
- Key based ssh to the jump box
- Agent installation on jump

Deliverable 7. Reflection. What gave you issues in the lab and how did you overcome them? Note, this reflection can be either placed in your journal or can be submitted as part of the lab submission.