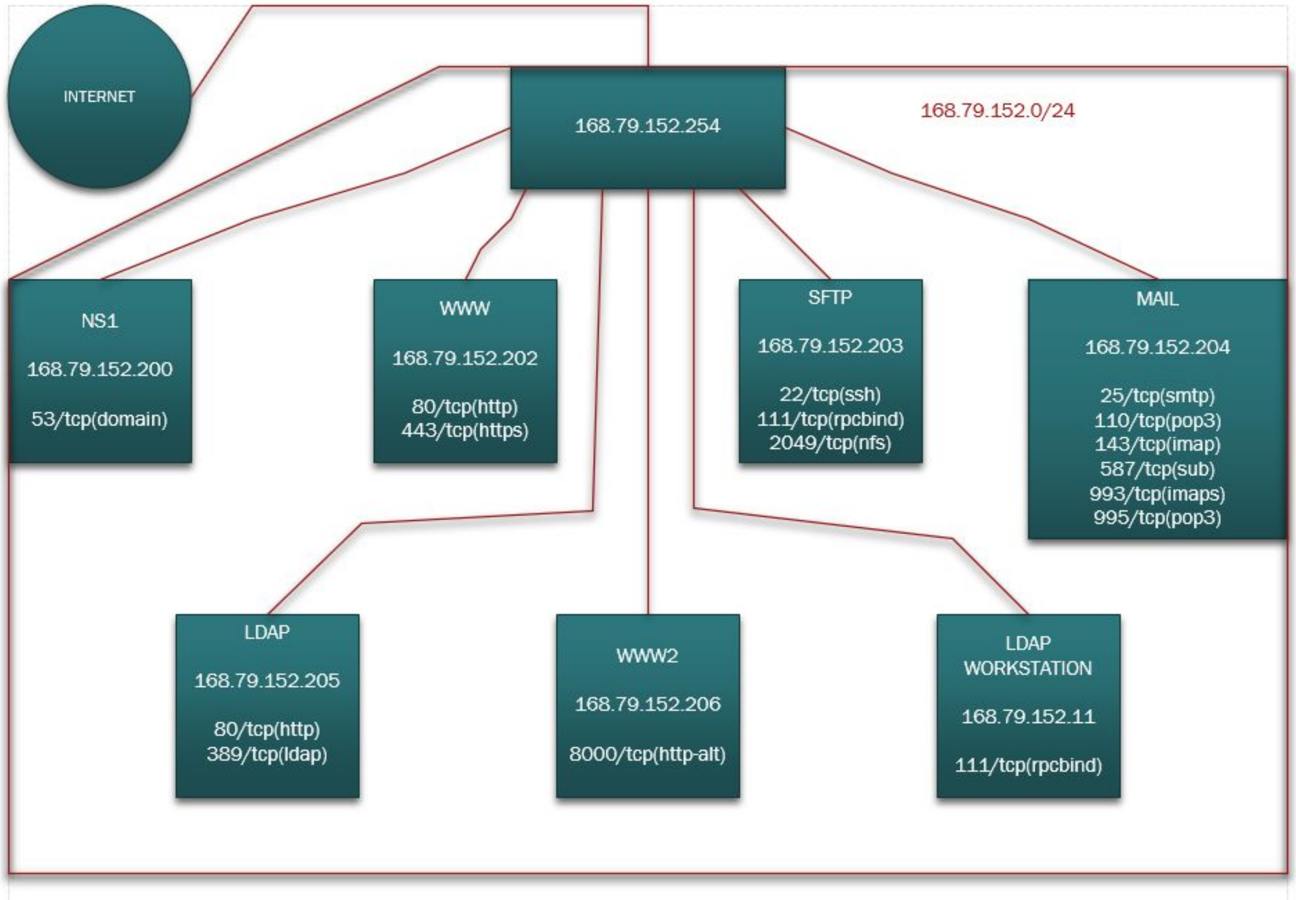
Jonathon schnell
Lab 10

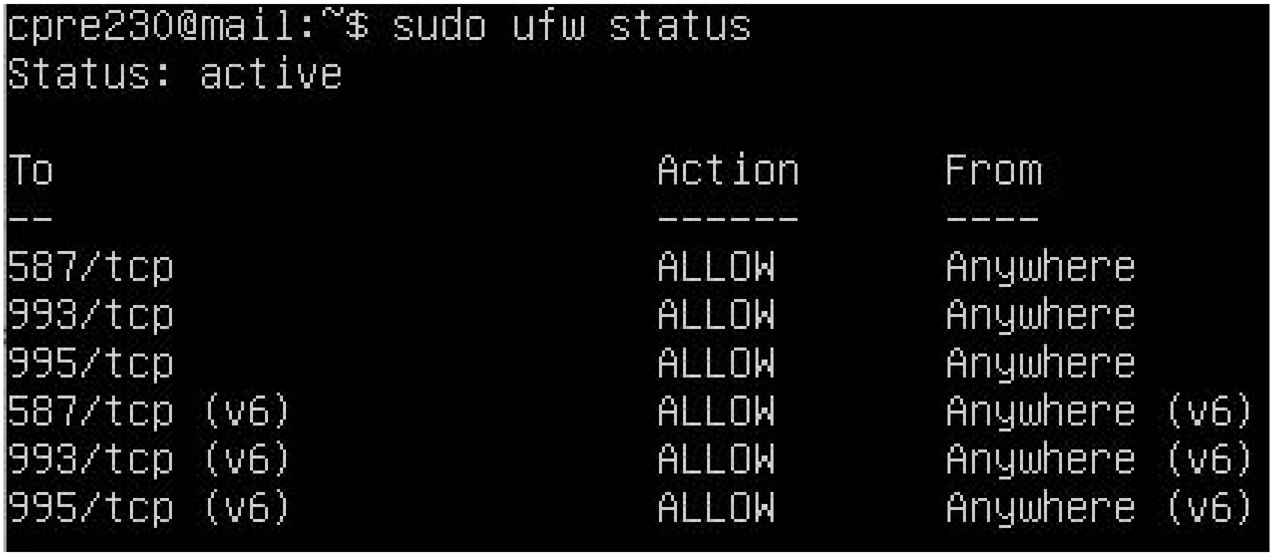
1.

Discovered IP	Open ports/services	Which ports should be open?	Which ports should be public?
168.79.152.200(ns1)	53/tcp(domain)	53/tdp 53/udp	none
168.79.152.202(www)	80/tcp(http) 443/tcp(https)	443/tcp(https)	443/tcp(https)
168.79.152.203(sftp)	22/tcp(ssh) 111/tcp(rpcbind) 2049/tcp(nfs)	22/tcp(ssh) 111/tcp(rpcbind) 2049/tcp(nfs)	none
168.79.152.204(mail)	25/tcp(smtp) 110/tcp(pop3) 143/tcp(imap) 587/tcp(submission) 993/tcp(imaps) 995/tcp(pop3)	587/tcp(submission) 993/tcp(imaps) 995/tcp(pop3)	none
168.79.152.205(ldap)	80/tcp(http) 389/tcp(ldap)	389/tcp(ldap)	none
168.79.152.206(www2)	8000/tcp(http-alt)	8000/tcp(http-alt)	8000/tcp(http-alt)
168.79.152.199(kali)	111/tcp(rpcbind) 3000/tcp(ppp)	111/tcp(rpcbind) 3000/tcp(ppp)	none
168.79.152.254(gateway)	none	none	none
168.79.152.207(ldap workstation)	111/tcp(rpcbind)	111/tcp(rpcbind)	none

2.

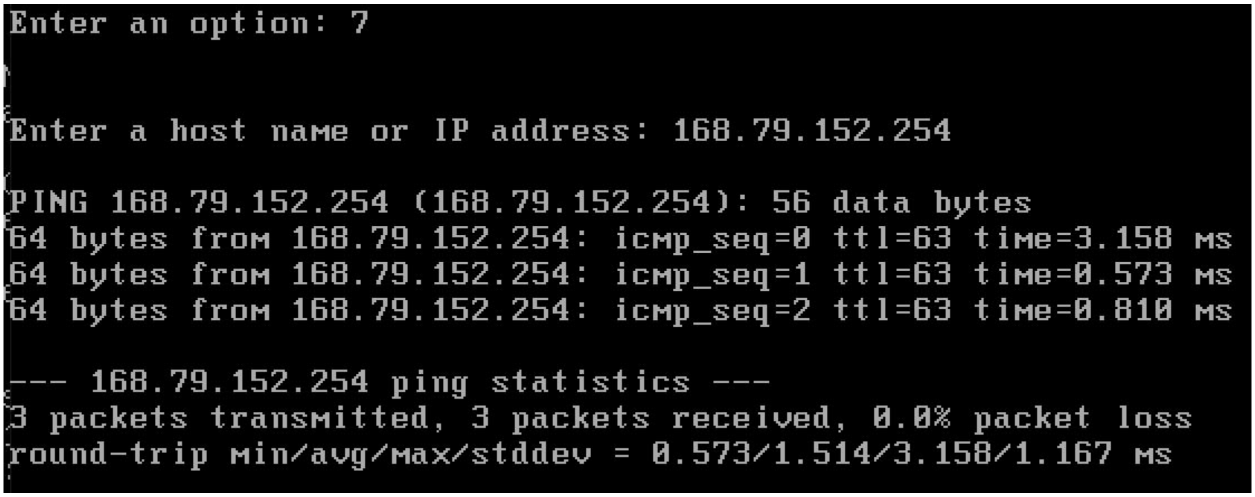


3.



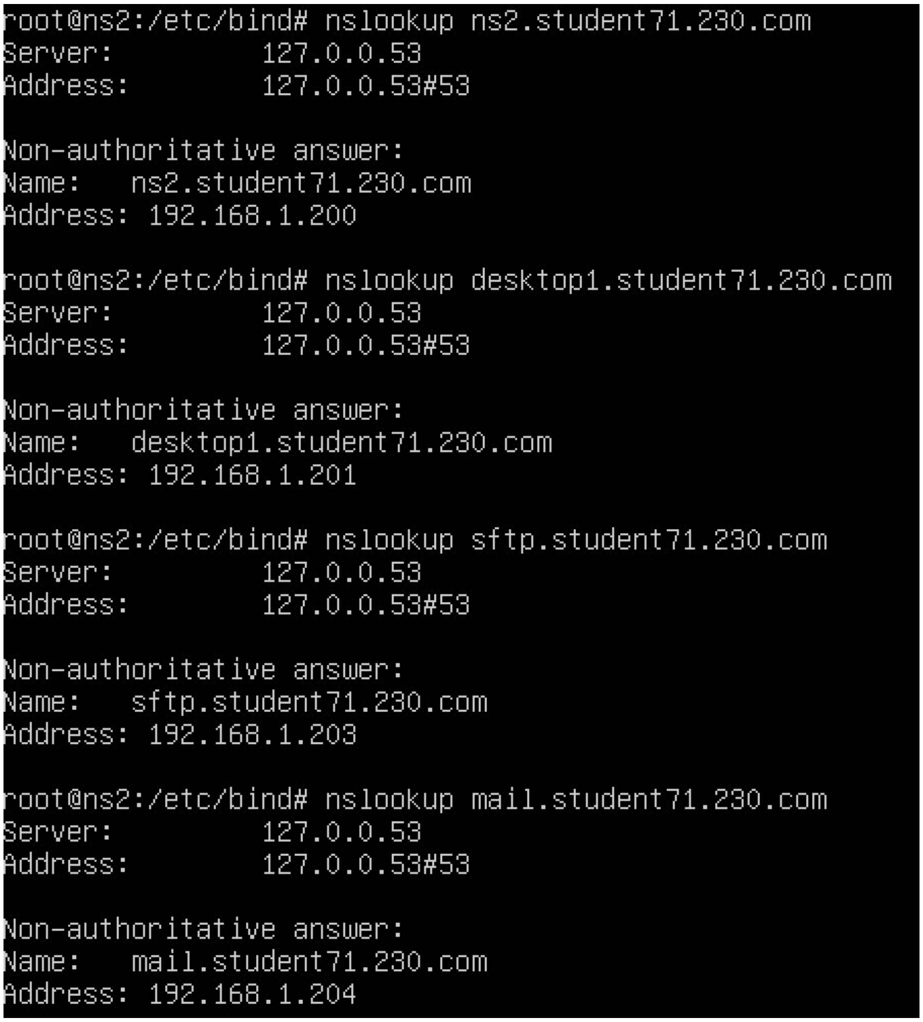
```
cpre230@mail:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
587/tcp                    ALLOW       Anywhere
993/tcp                    ALLOW       Anywhere
995/tcp                    ALLOW       Anywhere
587/tcp (v6)               ALLOW       Anywhere (v6)
993/tcp (v6)               ALLOW       Anywhere (v6)
995/tcp (v6)               ALLOW       Anywhere (v6)
```

4.

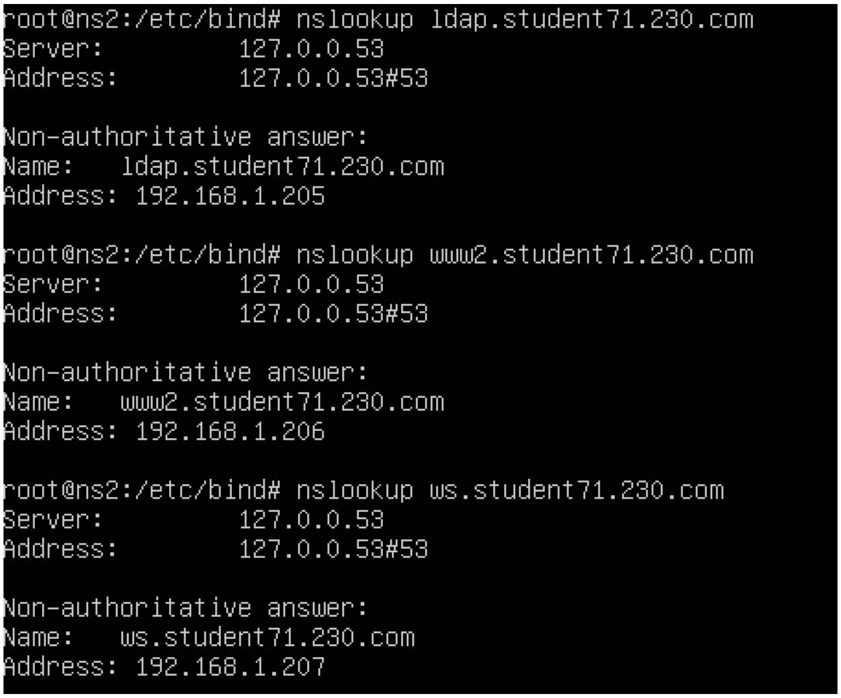


```
Enter an option: 7

Enter a host name or IP address: 168.79.152.254

PING 168.79.152.254 (168.79.152.254): 56 data bytes
64 bytes from 168.79.152.254: icmp_seq=0 ttl=63 time=3.158 ms
64 bytes from 168.79.152.254: icmp_seq=1 ttl=63 time=0.573 ms
64 bytes from 168.79.152.254: icmp_seq=2 ttl=63 time=0.810 ms

--- 168.79.152.254 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.573/1.514/3.158/1.167 ms
```

5.

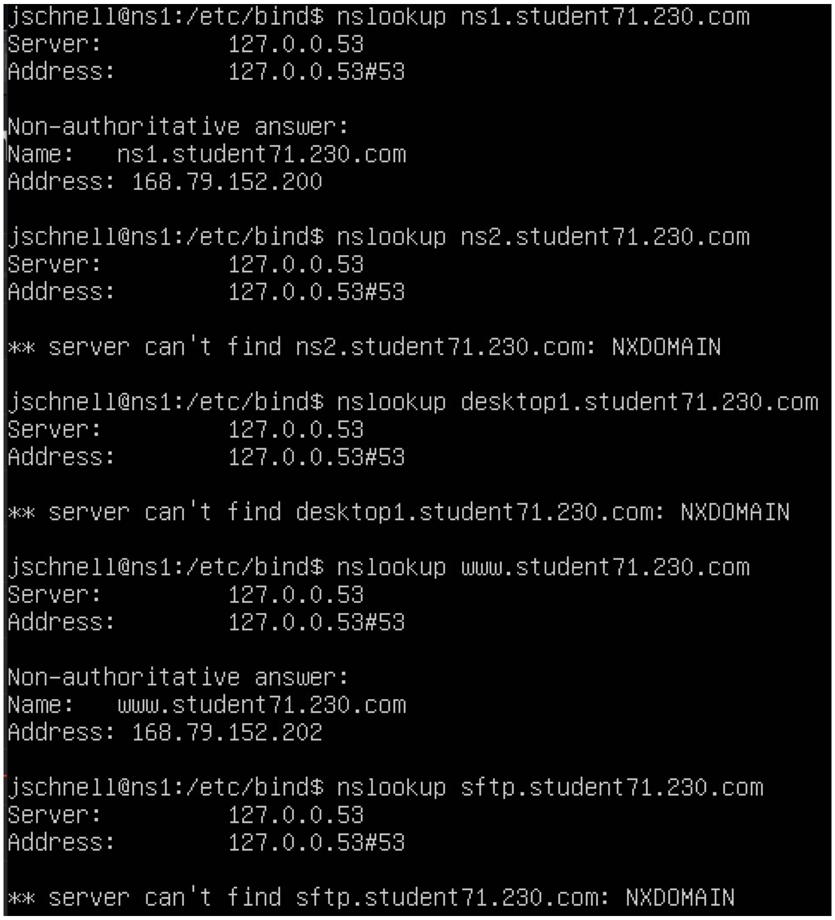


```
root@ns2:/etc/bind# nslookup ns2.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns2.student71.230.com
Address: 192.168.1.200

root@ns2:/etc/bind# nslookup desktop1.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   desktop1.student71.230.com
Address: 192.168.1.201

root@ns2:/etc/bind# nslookup sftp.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   sftp.student71.230.com
Address: 192.168.1.203

root@ns2:/etc/bind# nslookup mail.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   mail.student71.230.com
Address: 192.168.1.204
```

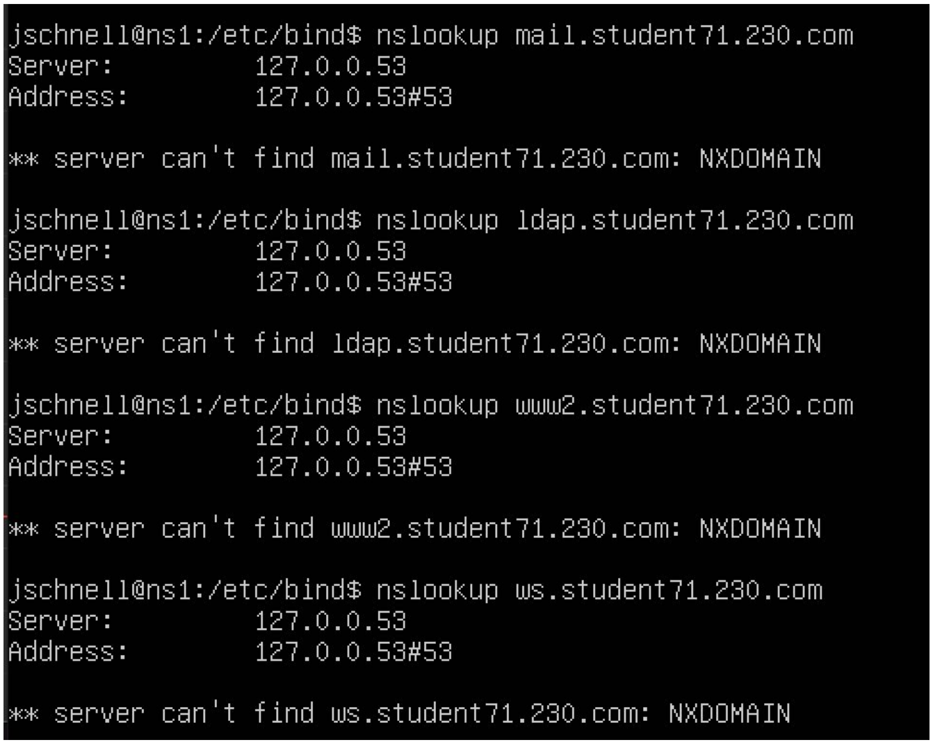


```
root@ns2:/etc/bind# nslookup ldap.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ldap.student71.230.com
Address: 192.168.1.205

root@ns2:/etc/bind# nslookup www2.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www2.student71.230.com
Address: 192.168.1.206

root@ns2:/etc/bind# nslookup ws.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ws.student71.230.com
Address: 192.168.1.207
```

6.

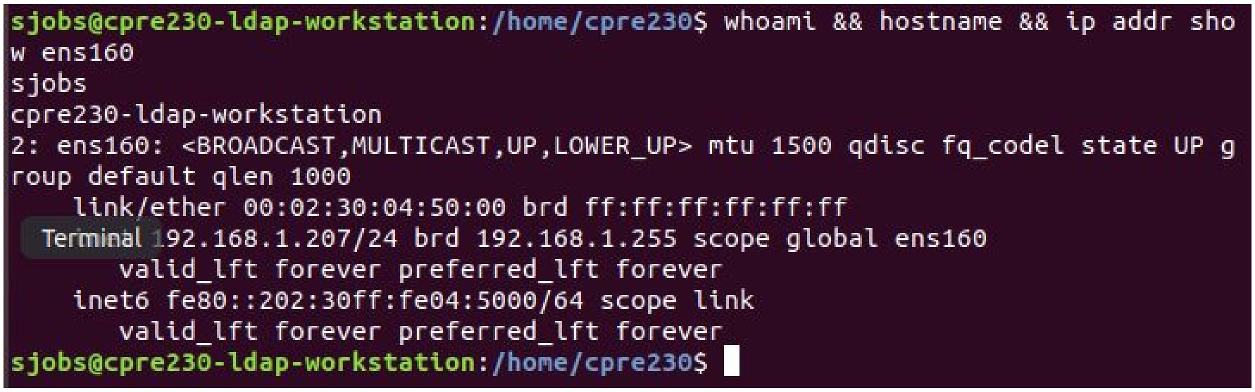


```
jschnell@ns1:/etc/bind$ nslookup ns1.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   ns1.student71.230.com
Address: 168.79.152.200

jschnell@ns1:/etc/bind$ nslookup ns2.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find ns2.student71.230.com: NXDOMAIN

jschnell@ns1:/etc/bind$ nslookup desktop1.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find desktop1.student71.230.com: NXDOMAIN

jschnell@ns1:/etc/bind$ nslookup www.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.student71.230.com
Address: 168.79.152.202

jschnell@ns1:/etc/bind$ nslookup sftp.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find sftp.student71.230.com: NXDOMAIN
```



```
jschnell@ns1:/etc/bind$ nslookup mail.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find mail.student71.230.com: NXDOMAIN

jschnell@ns1:/etc/bind$ nslookup ldap.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find ldap.student71.230.com: NXDOMAIN

jschnell@ns1:/etc/bind$ nslookup www2.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find www2.student71.230.com: NXDOMAIN

jschnell@ns1:/etc/bind$ nslookup ws.student71.230.com
Server:         127.0.0.53
Address:        127.0.0.53#53

** server can't find ws.student71.230.com: NXDOMAIN
```

7.

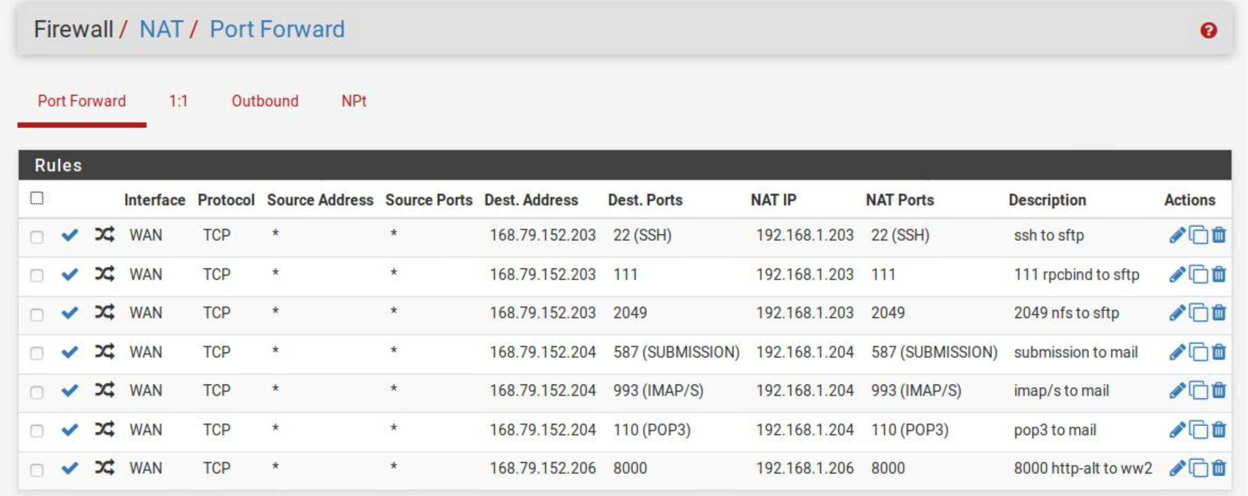


```
sjobs@cpre230-ldap-workstation:/home/cpre230$ whoami && hostname && ip addr sho
w ens160
sjobs
cpre230-ldap-workstation
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:02:30:04:50:00 brd ff:ff:ff:ff:ff:ff
  Terminal 192.168.1.207/24 brd 192.168.1.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::202:30ff:fe04:5000/64 scope link
       valid_lft forever preferred_lft forever
sjobs@cpre230-ldap-workstation:/home/cpre230$
```

8.
Port forwarding only is typically used when only one public ip address is available. Different port requests from the internet can be forwarded to the correct internal ip. This is known as network address translation or NAT. And advantage of port forwarding is it is easier to configure and does not require a range of external ip addresses. Anyone can setup port forwarding to access an internal network from the internet for services such as ssh and ftp or game servers. All of these services can have different internal ip's but the firewall of router will automatically send requests for ssh to the ssh server and ftp requests to the ftp server.

Virtual ips and port forwarding are commonly used together when a public ip network range is available. This is also known as network address translation or NAT. an advantage of using a virtual ips is load balancing can be performed to help large platforms run smoother for users. Virtual ips also offer more flexibility in network configuration.

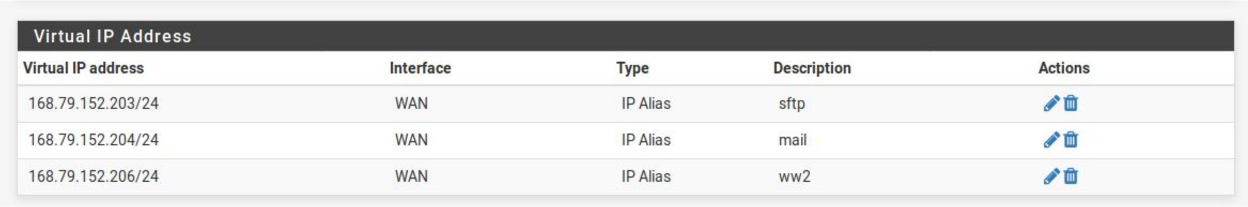
9.



Firewall / NAT / Port Forward

Rules

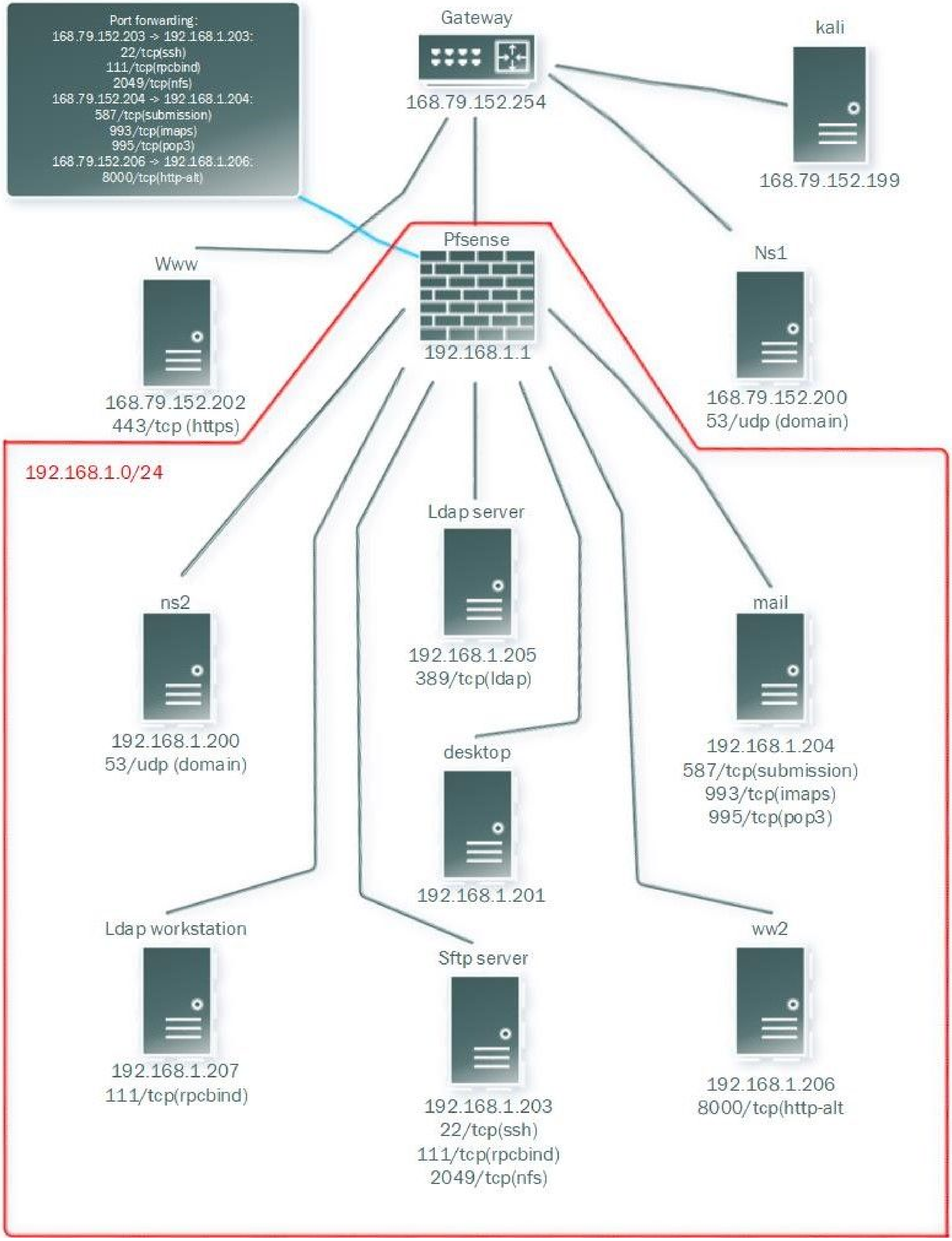
□			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	⇄	WAN	TCP	*	*	168.79.152.203	22 (SSH)	192.168.1.203	22 (SSH)	ssh to sftp	✎⧉🗑
□	✓	⇄	WAN	TCP	*	*	168.79.152.203	111	192.168.1.203	111	111 rpcbind to sftp	✎⧉🗑
□	✓	⇄	WAN	TCP	*	*	168.79.152.203	2049	192.168.1.203	2049	2049 nfs to sftp	✎⧉🗑
□	✓	⇄	WAN	TCP	*	*	168.79.152.204	587 (SUBMISSION)	192.168.1.204	587 (SUBMISSION)	submission to mail	✎⧉🗑
□	✓	⇄	WAN	TCP	*	*	168.79.152.204	993 (IMAP/S)	192.168.1.204	993 (IMAP/S)	imap/s to mail	✎⧉🗑
□	✓	⇄	WAN	TCP	*	*	168.79.152.204	110 (POP3)	192.168.1.204	110 (POP3)	pop3 to mail	✎⧉🗑
□	✓	⇄	WAN	TCP	*	*	168.79.152.206	8000	192.168.1.206	8000	8000 http-alt to ww2	✎⧉🗑



Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
168.79.152.203/24	WAN	IP Alias	sftp	✎🗑
168.79.152.204/24	WAN	IP Alias	mail	✎🗑
168.79.152.206/24	WAN	IP Alias	ww2	✎🗑

10.


Port forwarding:
168.79.152.203 -> 192.168.1.203:
22/tcp(ssh)
111/tcp(rpcbind)
2049/tcp(nfs)
168.79.152.204 -> 192.168.1.204:
587/tcp(submission)
993/tcp(imaps)
995/tcp(pop3)
168.79.152.206 -> 192.168.1.206:
8000/tcp(http-alt)
Gateway
168.79.152.254
kali
168.79.152.199
Pfsense
192.168.1.1
Www
168.79.152.202
443/tcp (https)
Ns1
168.79.152.200
53/udp (domain)
192.168.1.0/24
Ldap server
192.168.1.205
389/tcp(ldap)
ns2
192.168.1.200
53/udp (domain)
mail
192.168.1.204
587/tcp(submission)
993/tcp(imaps)
995/tcp(pop3)
desktop
192.168.1.201
Ldap workstation
192.168.1.207
111/tcp(rpcbind)
Sftp server
192.168.1.203
22/tcp(ssh)
111/tcp(rpcbind)
2049/tcp(nfs)
ww2
192.168.1.206
8000/tcp(http-alt