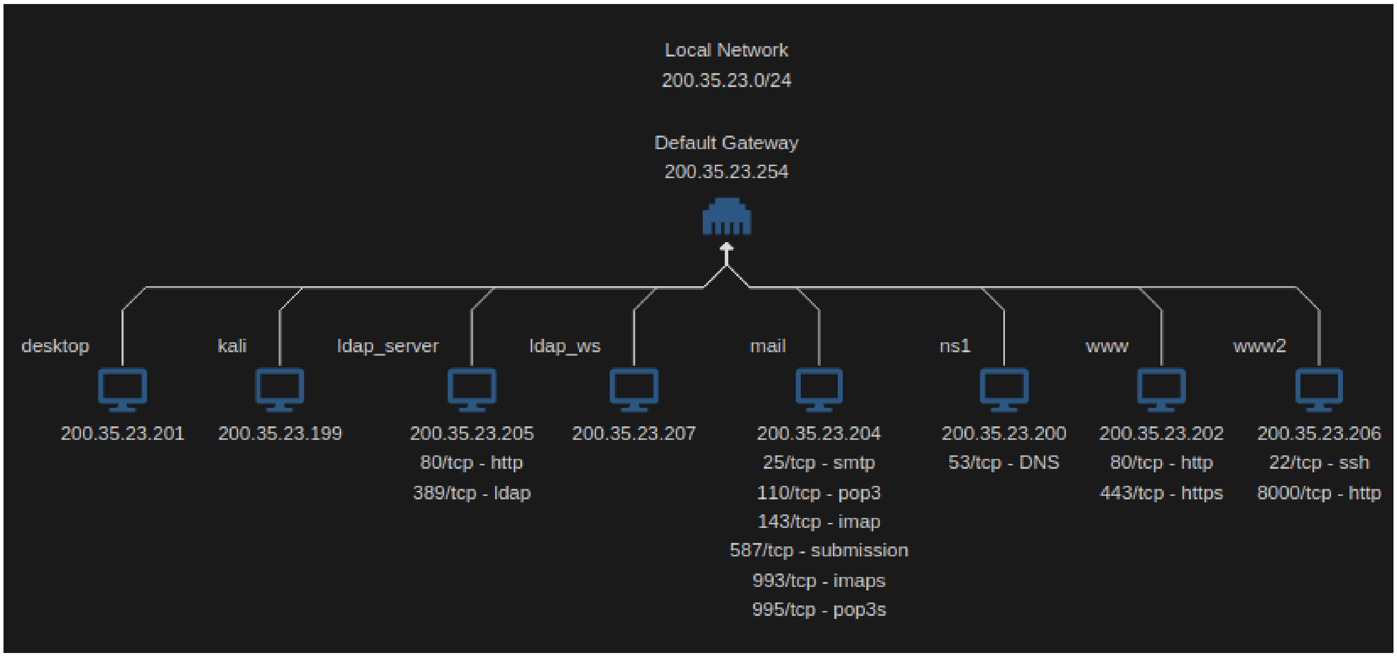
1. Table of FORMATTED nmap results

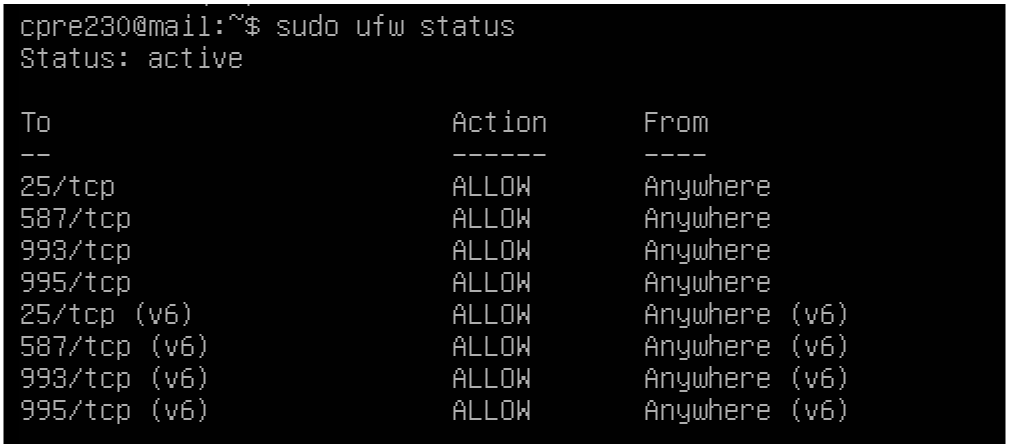
IP	Open Ports	Should(n't) be Open?	Should(n't) be Public?
200.35.23.199	All Closed	All shouldn't	All shouldn't
200.35.23.200	53 - DNS	Should - 53	Should 53
200.35.23.201	All Closed	All shouldn't	All shouldn't
200.35.23.202	80 & 443 - http(s)	Should 443	Should 443
200.35.23.204	25 - smtp 110 - pop3 143 - imap 587 - submission 993 - imaps 995 - pop3s	Should - 25, 587, 993, & 995	Should - 25, 587, 993, & 995
200.35.23.205	80 - http 389 - ldap	Should 80 & 389	All shouldn't
200.35.23.206	22 - ssh 8000 - http	Should - 22 & 8000	Should - 22
200.35.23.207	All Closed	All shouldn't	All shouldn't

2. PROFESSIONAL diagram of initial network

(Accidentally, put 53/tcp instead of 53/udp. I fixed it in the second diagram, but it would have meant recreating this one. Made in yEd.)

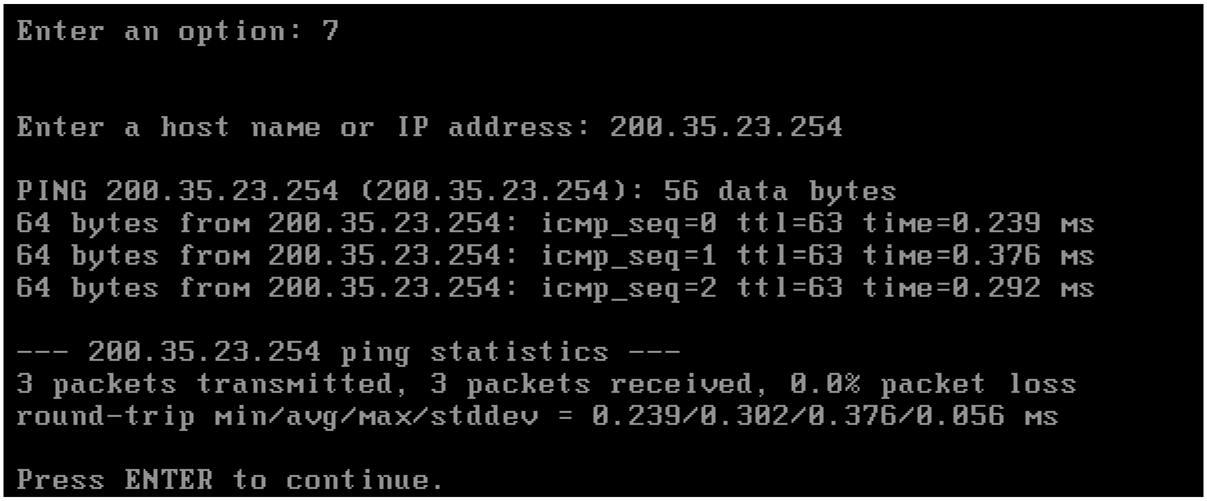


3. UFW screenshot of mail server



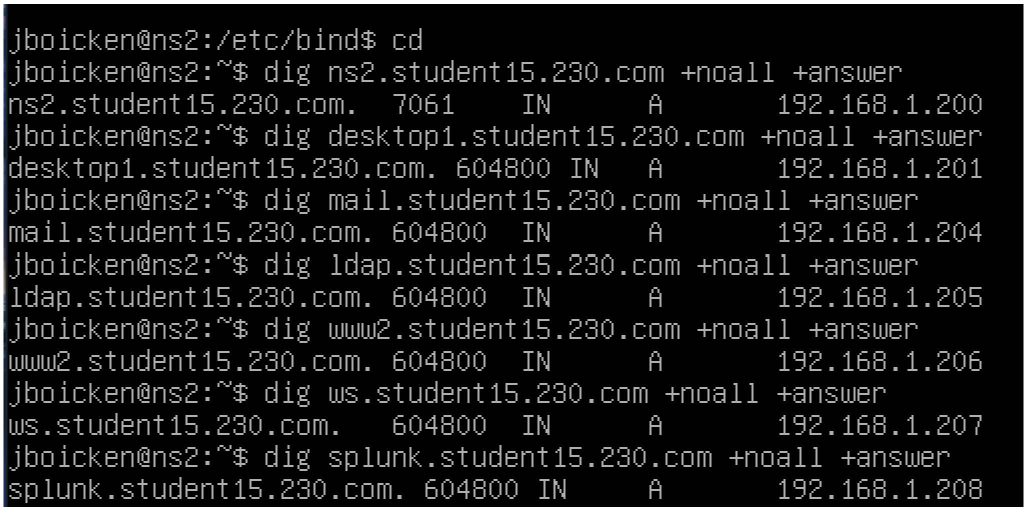
```
cpre230@mail:~$ sudo ufw status
Status: active

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

4. Screenshot of pfSense pinging gateway



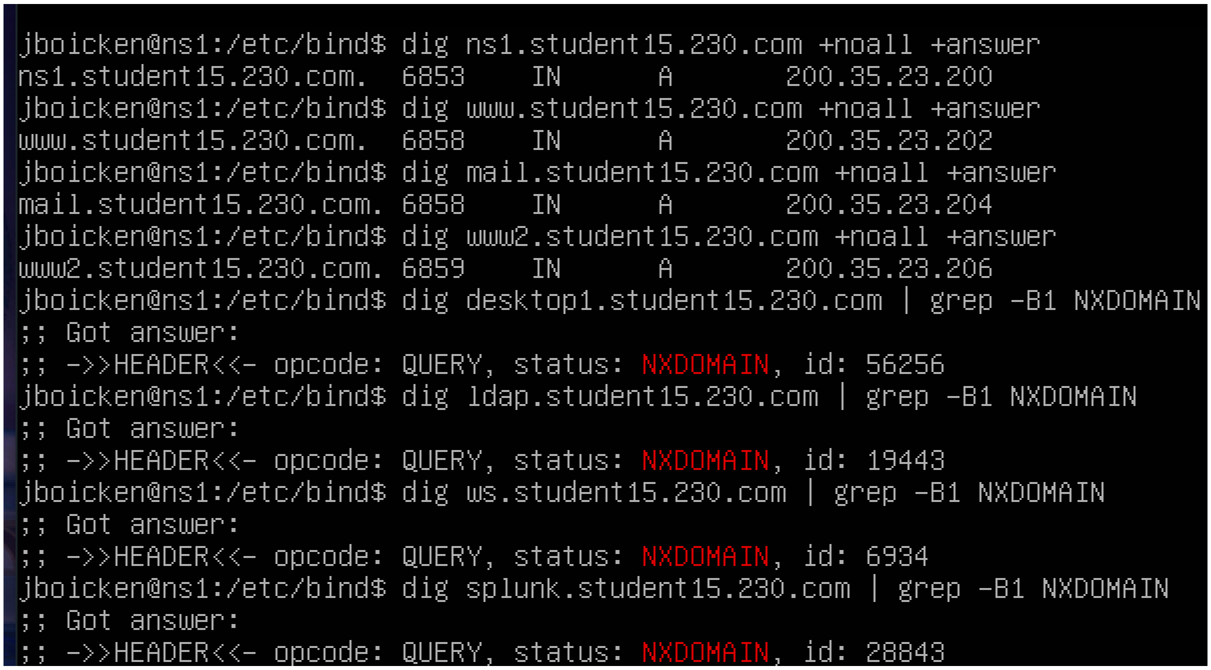
```
Enter an option: 7


Enter a host name or IP address: 200.35.23.254

PING 200.35.23.254 (200.35.23.254): 56 data bytes
64 bytes from 200.35.23.254: icmp_seq=0 ttl=63 time=0.239 ms
64 bytes from 200.35.23.254: icmp_seq=1 ttl=63 time=0.376 ms
64 bytes from 200.35.23.254: icmp_seq=2 ttl=63 time=0.292 ms

--- 200.35.23.254 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 0.239/0.302/0.376/0.056 ms

Press ENTER to continue.
```

5. Screenshot of all internal entries resolving to internal IP



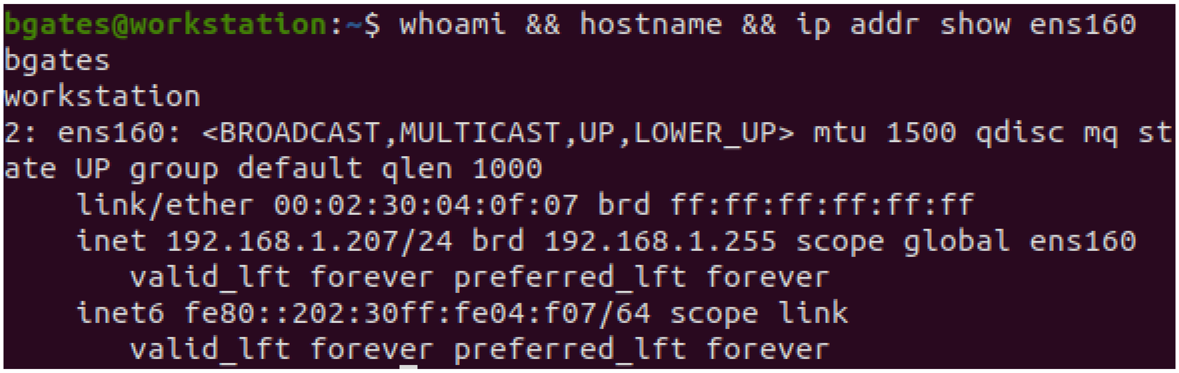
```
jboicken@ns2:/etc/bind$ cd
jboicken@ns2:~$ dig ns2.student15.230.com +noall +answer
ns2.student15.230.com.  7061    IN      A       192.168.1.200
jboicken@ns2:~$ dig desktop1.student15.230.com +noall +answer
desktop1.student15.230.com. 604800 IN   A       192.168.1.201
jboicken@ns2:~$ dig mail.student15.230.com +noall +answer
mail.student15.230.com. 604800  IN      A       192.168.1.204
jboicken@ns2:~$ dig ldap.student15.230.com +noall +answer
ldap.student15.230.com. 604800  IN      A       192.168.1.205
jboicken@ns2:~$ dig www2.student15.230.com +noall +answer
www2.student15.230.com. 604800  IN      A       192.168.1.206
jboicken@ns2:~$ dig ws.student15.230.com +noall +answer
ws.student15.230.com.   604800  IN      A       192.168.1.207
jboicken@ns2:~$ dig splunk.student15.230.com +noall +answer
splunk.student15.230.com. 604800 IN     A       192.168.1.208
```

6. Screenshot of all external entries resolving to external IPs



```
jboicken@ns1:/etc/bind$ dig ns1.student15.230.com +noall +answer
ns1.student15.230.com.  6853    IN      A       200.35.23.200
jboicken@ns1:/etc/bind$ dig www.student15.230.com +noall +answer
www.student15.230.com.  6858    IN      A       200.35.23.202
jboicken@ns1:/etc/bind$ dig mail.student15.230.com +noall +answer
mail.student15.230.com. 6858    IN      A       200.35.23.204
jboicken@ns1:/etc/bind$ dig www2.student15.230.com +noall +answer
www2.student15.230.com. 6859    IN      A       200.35.23.206
jboicken@ns1:/etc/bind$ dig desktop1.student15.230.com | grep -B1 NXDOMAIN
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 56256
jboicken@ns1:/etc/bind$ dig ldap.student15.230.com | grep -B1 NXDOMAIN
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 19443
jboicken@ns1:/etc/bind$ dig ws.student15.230.com | grep -B1 NXDOMAIN
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 6934
jboicken@ns1:/etc/bind$ dig splunk.student15.230.com | grep -B1 NXDOMAIN
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 28843
```

7. Screenshot of successful WS migration
    a. `whoami && hostname && ip addr show ens160`



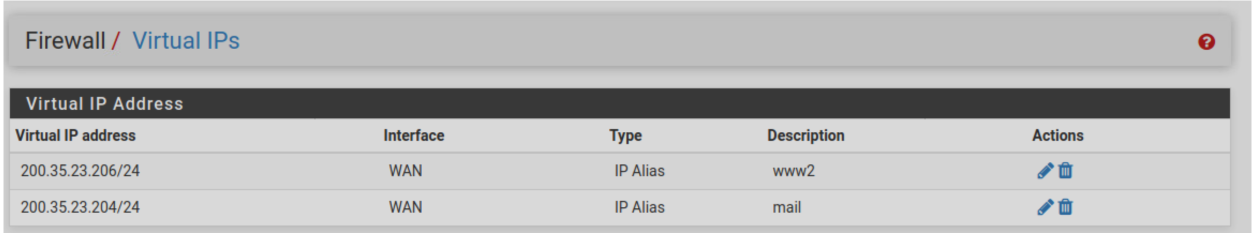
```
bgates@workstation:~$ whoami && hostname && ip addr show ens160
bgates
workstation
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq st
ate UP group default qlen 1000
    link/ether 00:02:30:04:0f:07 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.207/24 brd 192.168.1.255 scope global ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::202:30ff:fe04:f07/64 scope link
       valid_lft forever preferred_lft forever
```

8. Discussion of pros/cons of port forwarding only vs virtual IPs and port forwarding

Pros of Virtual IPs over just forwarding	Cons of Virtual IPs over just forwarding
- Allows connections of the same port ranges to multiple machine through different IPs - Allows forwarding of port range to port per machine instead of port range to machine - Can be used to allow multiple connections at once	- Uses up an ip address on the higher network (our XX.XX.XX.0/24) - More resource intensive on the machine - Adds complexity to the firewall's functions and network

9. Screenshots (2) of Virtual IP config page and NAT Forwarding page

Virtual IPs:

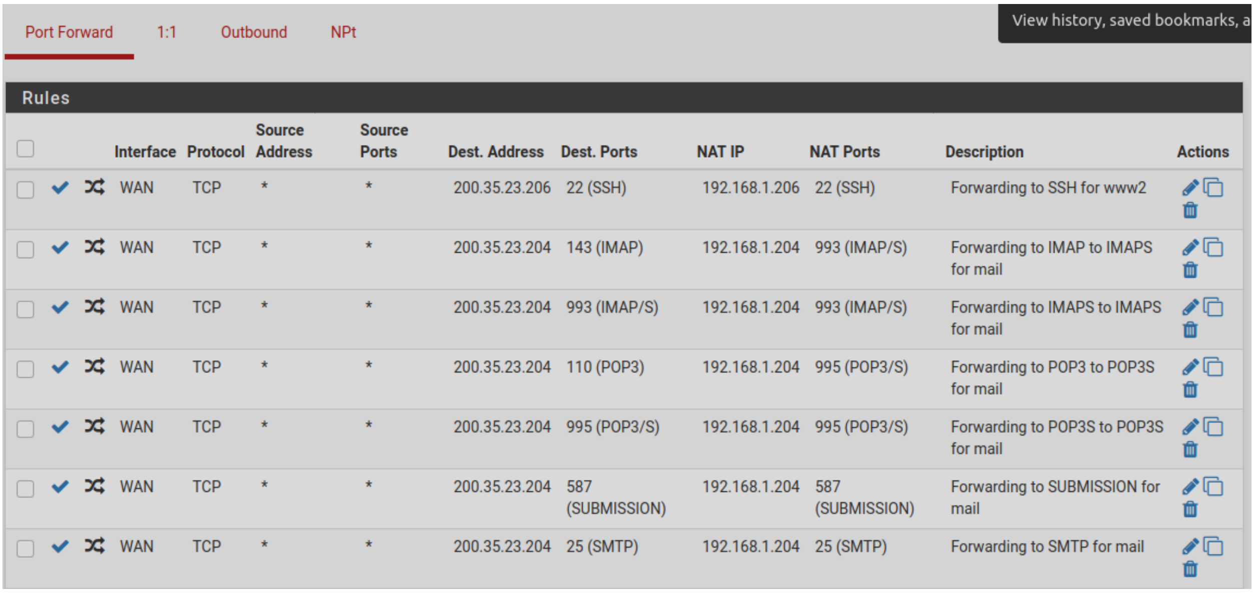


Firewall / Virtual IPs

Virtual IP Address

Virtual IP address	Interface	Type	Description	Actions
200.35.23.206/24	WAN	IP Alias	www2	
200.35.23.204/24	WAN	IP Alias	mail	

Port Forwarding:

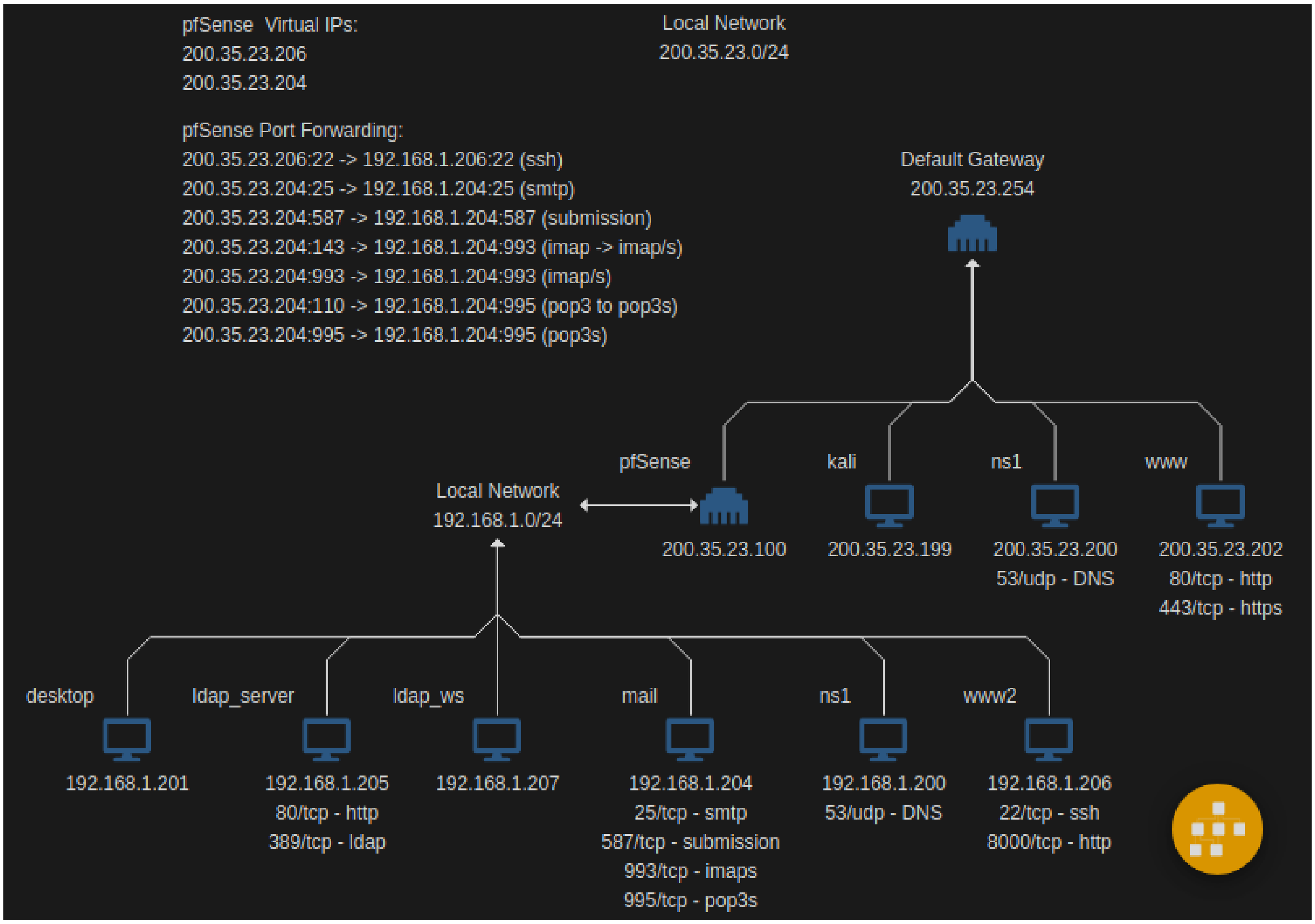


Rules

☐		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
☐	✓	WAN	TCP	*	*	200.35.23.206	22 (SSH)	192.168.1.206	22 (SSH)	Forwarding to SSH for www2	
☐	✓	WAN	TCP	*	*	200.35.23.204	143 (IMAP)	192.168.1.204	993 (IMAP/S)	Forwarding to IMAP to IMAPS for mail	
☐	✓	WAN	TCP	*	*	200.35.23.204	993 (IMAP/S)	192.168.1.204	993 (IMAP/S)	Forwarding to IMAPS to IMAPS for mail	
☐	✓	WAN	TCP	*	*	200.35.23.204	110 (POP3)	192.168.1.204	995 (POP3/S)	Forwarding to POP3 to POP3S for mail	
☐	✓	WAN	TCP	*	*	200.35.23.204	995 (POP3/S)	192.168.1.204	995 (POP3/S)	Forwarding to POP3S to POP3S for mail	
☐	✓	WAN	TCP	*	*	200.35.23.204	587 (SUBMISSION)	192.168.1.204	587 (SUBMISSION)	Forwarding to SUBMISSION for mail	
☐	✓	WAN	TCP	*	*	200.35.23.204	25 (SMTP)	192.168.1.204	25 (SMTP)	Forwarding to SMTP for mail	

10. Network diagram of final (migrated) network

(Made in yEd. Orange circle on the bottom is just an overlay element to reformat the diagram.
I also messed up and named ns2 as ns1.)



pfSense Virtual IPs:
200.35.23.206
200.35.23.204

pfSense Port Forwarding:
200.35.23.206:22 -> 192.168.1.206:22 (ssh)
200.35.23.204:25 -> 192.168.1.204:25 (smtp)
200.35.23.204:587 -> 192.168.1.204:587 (submission)
200.35.23.204:143 -> 192.168.1.204:993 (imap -> imap/s)
200.35.23.204:993 -> 192.168.1.204:993 (imap/s)
200.35.23.204:110 -> 192.168.1.204:995 (pop3 to pop3s)
200.35.23.204:995 -> 192.168.1.204:995 (pop3s)