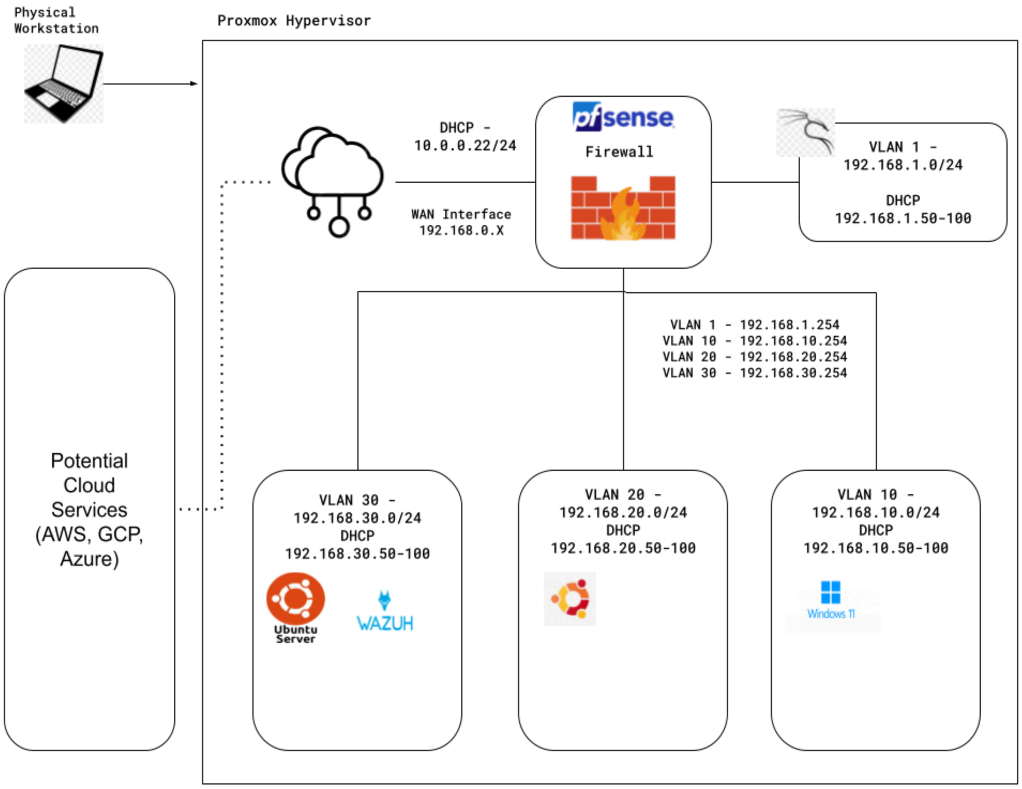
Security Engineering Lab

Status: WIP

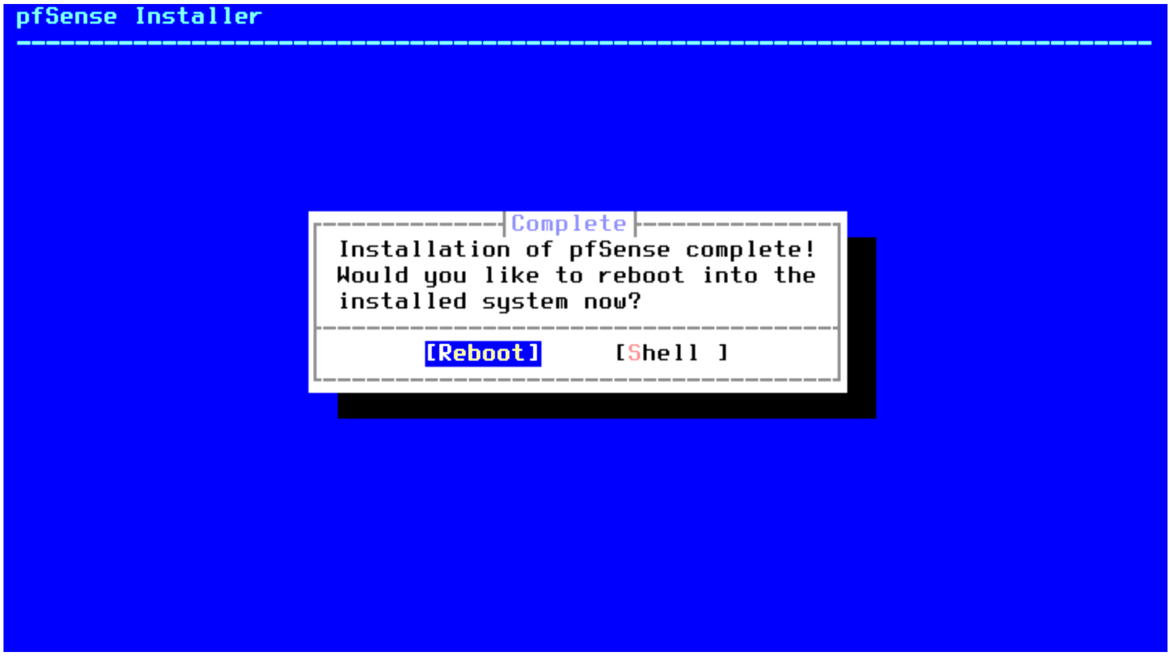
Devices List

- Windows 11 Computers
- AD Server
- Linux Computers
- Firewall
- Wazuh XDR and SIEM solution
- Kali Attack Box

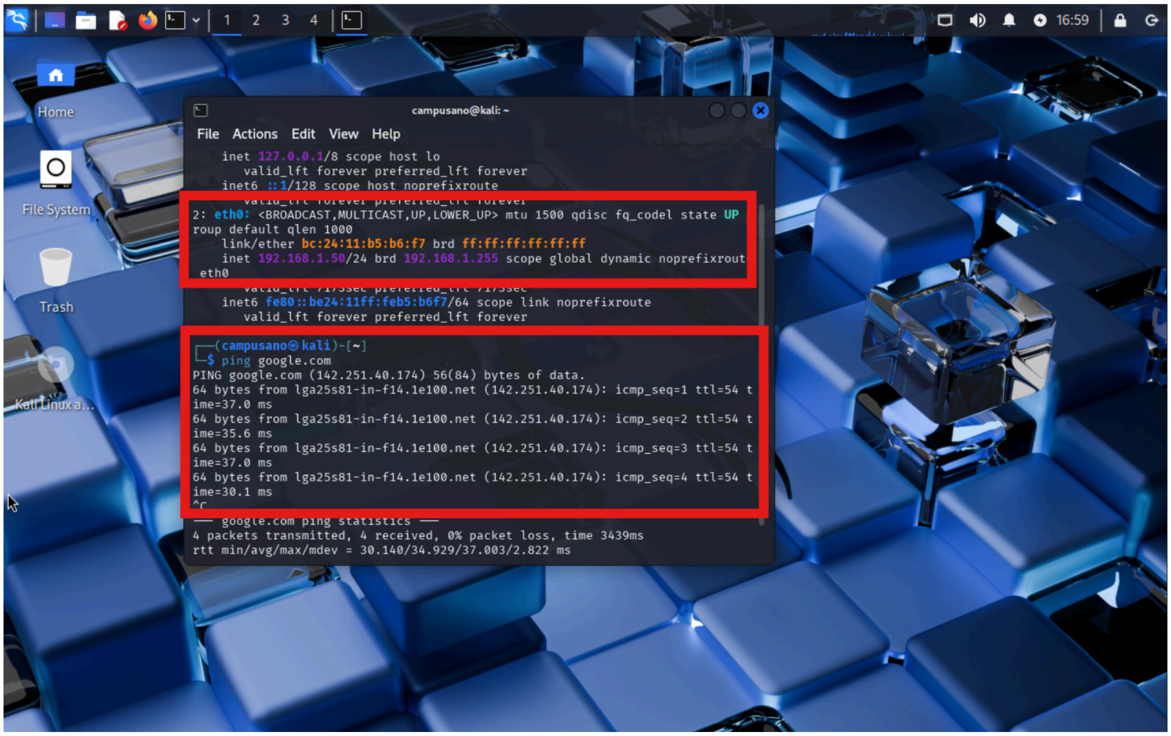
Networking Design



Initial Setup

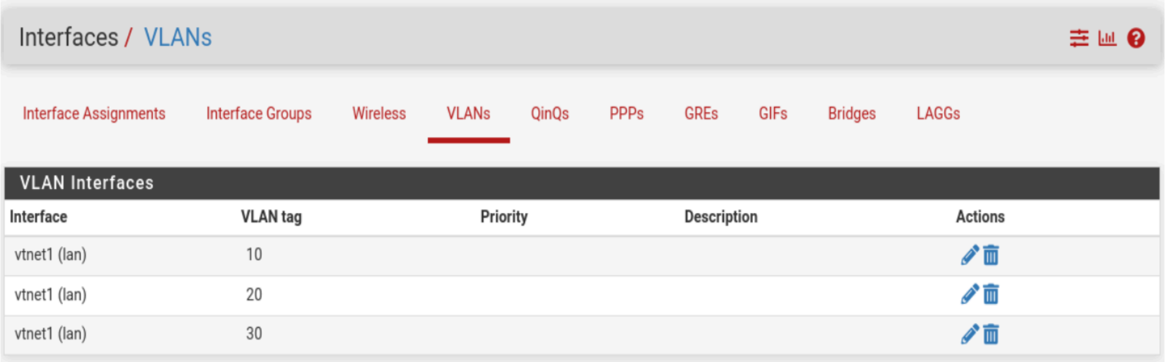
- Install Pfsense for the use of firewall between vlans and home network separation
  - 

    Installation of pfSense complete! Would you like to reboot into the installed system now?
- Create different VLANs for each segment of the network we plan to attack
  - This will also simulate network segmentation when collecting logs and attacking different networks
- Installed Kali, verify we successfully get an IP address to our WAN interface and verified we have internet connectivity



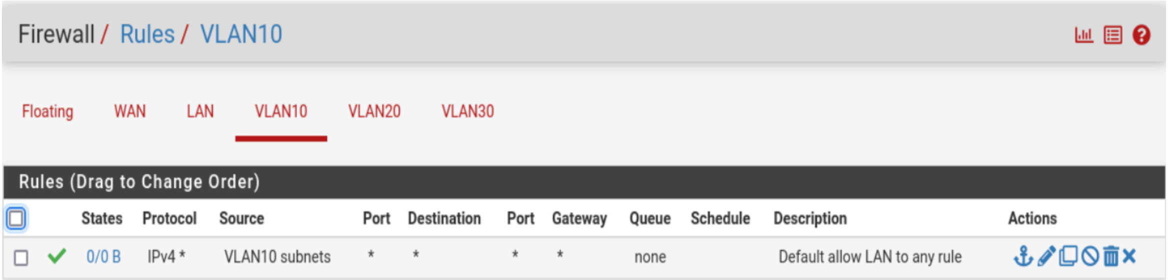
```
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether bc:24:11:b5:b6:f7 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.50/24 brd 192.168.1.255 scope global dynamic noprefixrout
 eth0
       valid_lft 7173sec preferred_lft 7173sec
    inet6 fe80::be24:11ff:feb5:b6f7/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(campusano㉿kali)-[~]
└─$ ping google.com
PING google.com (142.251.40.174) 56(84) bytes of data.
64 bytes from lga25s81-in-f14.1e100.net (142.251.40.174): icmp_seq=1 ttl=54 t
ime=37.0 ms
64 bytes from lga25s81-in-f14.1e100.net (142.251.40.174): icmp_seq=2 ttl=54 t
ime=35.6 ms
64 bytes from lga25s81-in-f14.1e100.net (142.251.40.174): icmp_seq=3 ttl=54 t
ime=37.0 ms
64 bytes from lga25s81-in-f14.1e100.net (142.251.40.174): icmp_seq=4 ttl=54 t
ime=30.1 ms
^C
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3439ms
rtt min/avg/max/mdev = 30.140/34.929/37.003/2.822 ms
```

- Using the Kali Box, we added:
  - All the other VLANs{10..30}
  - Added basic Firewall rules to allow communication between VLANs
  - Configure DHCP and DNS for all VLANs



VLAN Interfaces

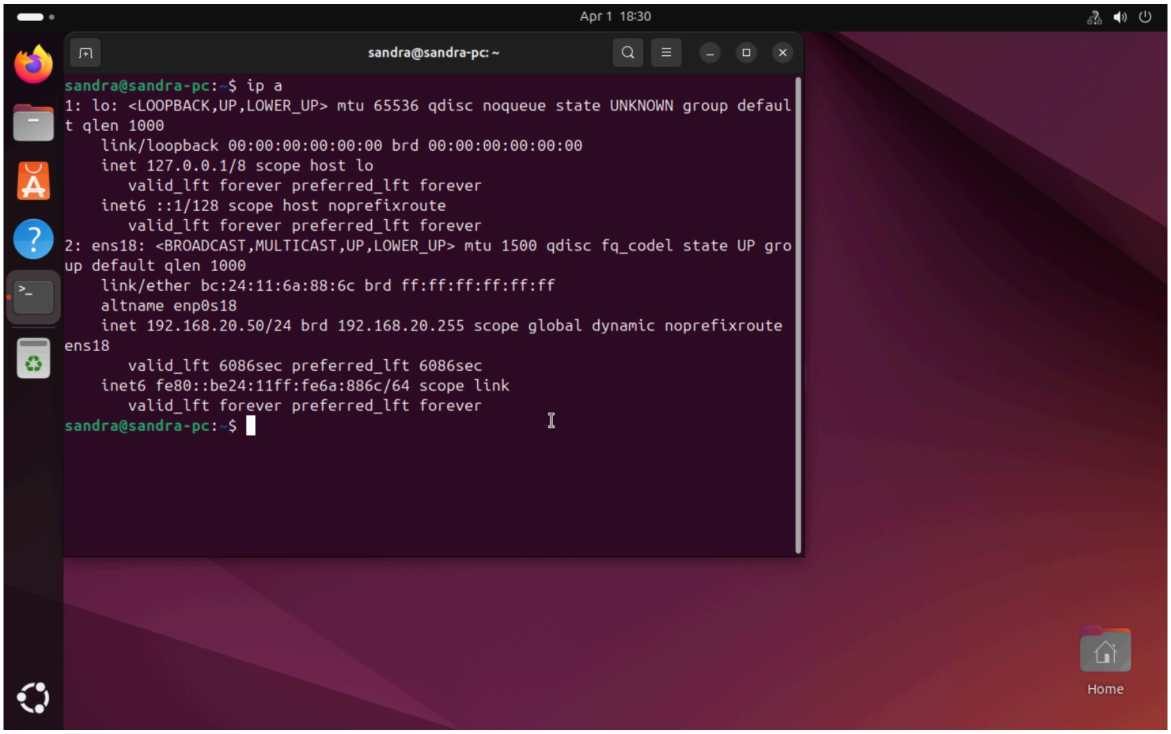
Interface	VLAN tag	Priority	Description	Actions
vtnet1 (lan)	10			
vtnet1 (lan)	20			
vtnet1 (lan)	30			



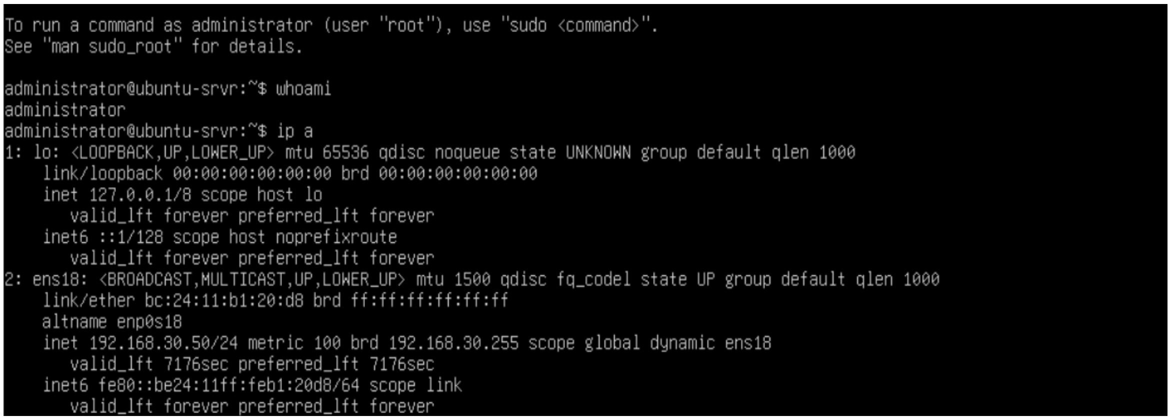
Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0/0 B	IPv4 *	VLAN10 subnets	*	*	*	*	none		Default allow LAN to any rule	

- Finalized the installation of our ubuntu endpoint, correctly assigned to VLAN 20

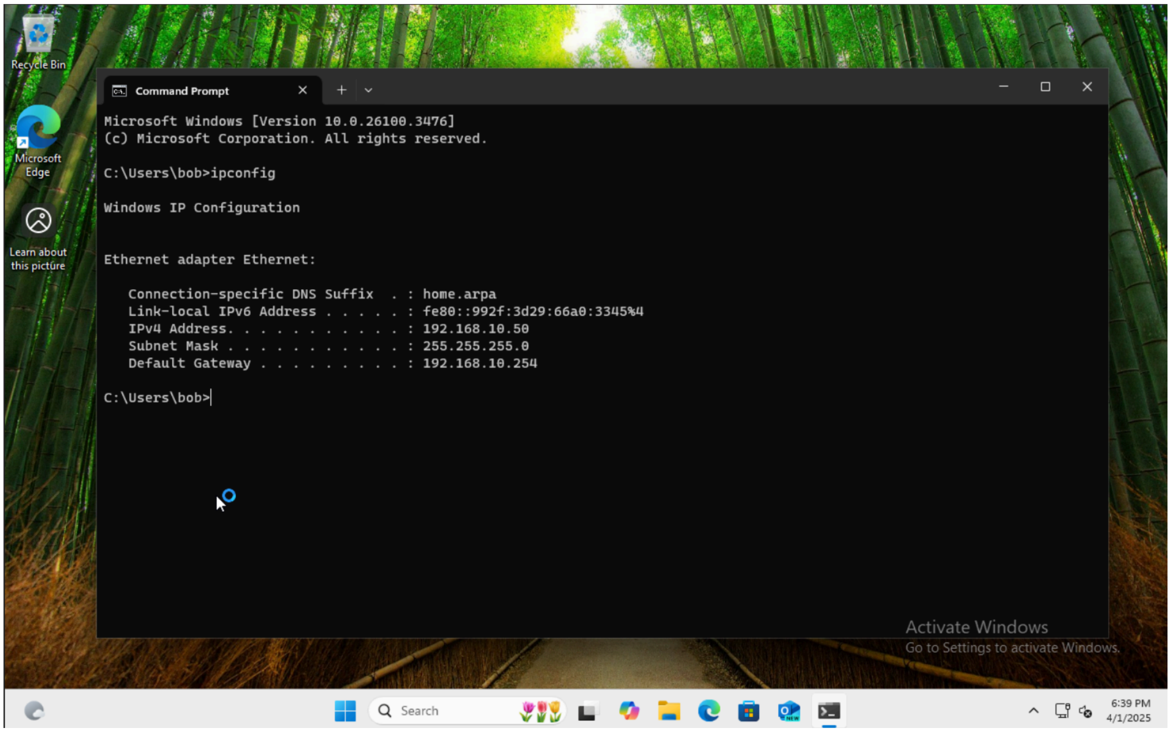
- 

```
sandra@sandra-pc:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t 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 noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP gro
up default qlen 1000
    link/ether bc:24:11:6a:88:6c brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.20.50/24 brd 192.168.20.255 scope global dynamic noprefixroute
ens18
       valid_lft 6086sec preferred_lft 6086sec
    inet6 fe80::be24:11ff:fe6a:886c/64 scope link
       valid_lft forever preferred_lft forever
sandra@sandra-pc:~$
```

- Finalized the installation of Ubuntu server, this server will host wazuh and our log aggregation systems, most likely elastic search. It is correctly configure on VLAN 30
  - 

```
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

administrator@ubuntu-srvr:~$ whoami
administrator
administrator@ubuntu-srvr:~$ 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 noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:b1:20:d8 brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 192.168.30.50/24 metric 100 brd 192.168.30.255 scope global dynamic ens18
       valid_lft 7176sec preferred_lft 7176sec
    inet6 fe80::be24:11ff:feb1:20d8/64 scope link
       valid_lft forever preferred_lft forever
```

- Same for our windows 11 endpoint that will collect data from. We are using different systems to learn log aggregation and collection from different sources



```
Microsoft Windows [Version 10.0.26100.3476]
(c) Microsoft Corporation. All rights reserved.

C:\Users\bob>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : home.arpa
   Link-local IPv6 Address . . . . . : fe80::992f:3d29:66a0:3345%4
   IPv4 Address. . . . . . . . . . . : 192.168.10.50
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.254

C:\Users\bob>
```

○

●