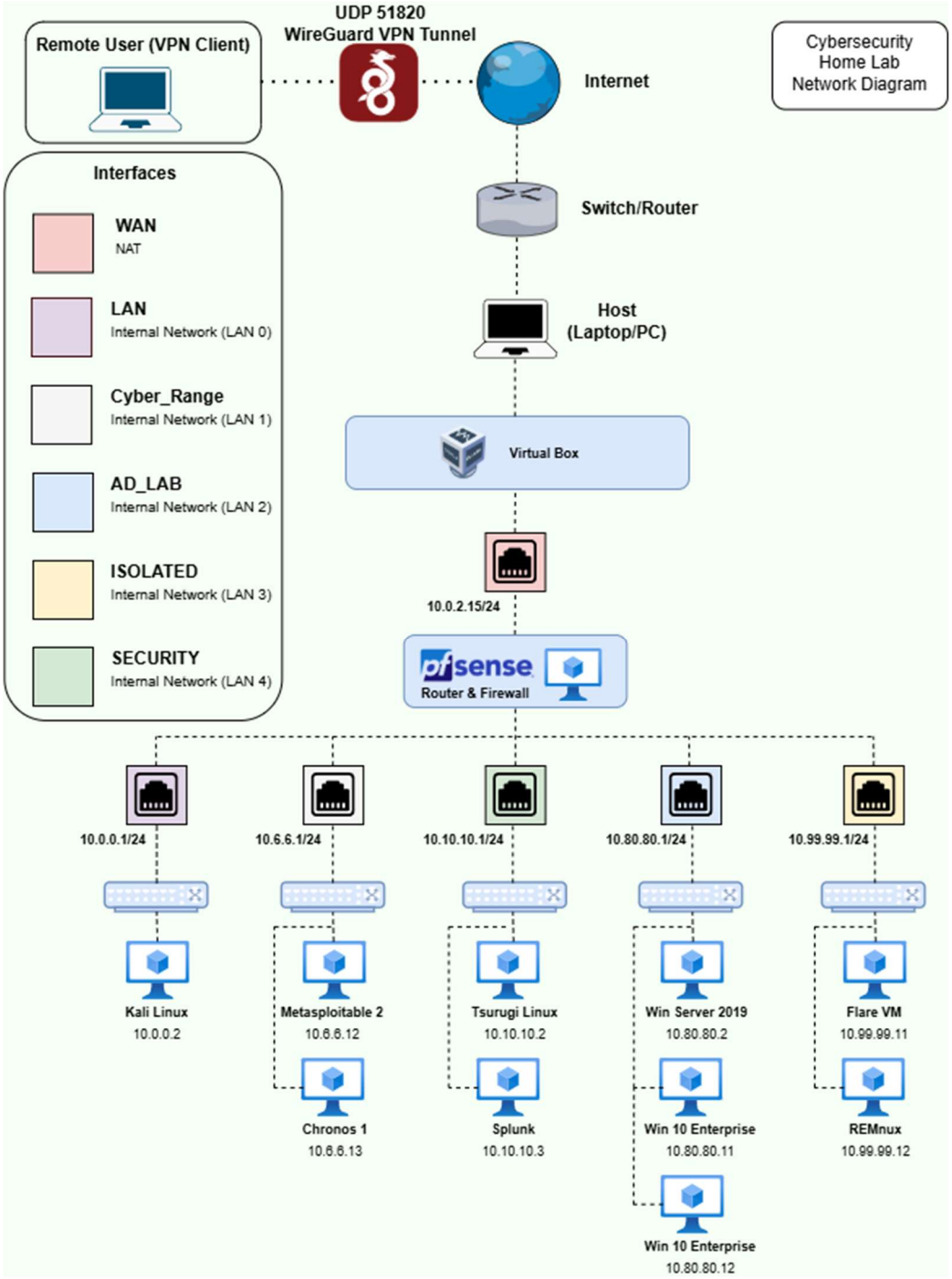
Milestone 1 – Network Design and Documentation

1) *Planned Network Setup and Components*

The planned network is shown in the following diagram. The design simulates a segmented cybersecurity home lab that's secured by a centralized firewall and VPN gateway.



2) ***Components:***

- ***Internal VMs:***
  Multiple VMs exist in this network. All of them lie behind pfSense and are segmented into different subnets (LAN, CYBER_RANGE, SECURITY, AD_LAB, and ISOLATED).

  Each subnet is designed with a purpose and contains operating systems tailored to the function. For example, penetration testing systems are in the CYBER_RANGE subnet, monitoring tools in the SECURITY subnet, and Windows infrastructure inside the AD_LAB subnet.

- ***Remote User:***
  This represents a user that is outside the internal network. It would connect over the internet to the pfSense WAN interface, using a VPN tunnel, which in this case, is WireGuard. After the user is authenticated, it will gain access to the internal resources that the firewall rules allow.

- ***Firewall Solution Choice: pfSense***
  pfSense is an open-source firewall platform that includes strong ACL and firewall rule support. It includes NAT support for internal internet access, supports VPN sources like WireGuard, and maintains good logging for blocked traffic and rules.

- ***Virtualization Platform: VirtualBox***
  VirtualBox is a virtualization platform that works best for this project. It is easy to create different network segments (LAN1 – 4) using VirtualBox. It allows NAT support for WAN testing ensuring internal isolation for security. Additionally, pfSense can have multiple NICs attached.

- ***VPN software: WireGuard***
  WireGuard is a modern VPN tool that has strong cryptography and is easy to configure. It uses UDP port 51820, making it good for this kind of environment.

  To configure WireGuard:
  1) We would install and enable WireGuard on pfSense.
  2) Once installed, we would be able to create a VPN tunnel interface.
  3) We would define the VPN subnet for the clients connecting to it.
  4) Create a key pair for both the pfSense server and the remote user.
  5) We would add the remote user as a peer on pfSense.
  6) Import the client configuration into the remote user's WireGuard client
  7) Estasblish a VPN connection to pfSense via WAN over UDP port 51820

After connection, the remote user's access is controlled through firewall rules, ensuring segmentation and security enforcement.

3) ***Key Network Policies:***

- ***NAT: Outbound NAT Policy***
  Internal subnets are private and not routable on the internet. pfSense will conduct outbound NAT on the WAN interface. This means that when an internal VM attempts to access the internet, its IP address will be translated to the pfSense WAN address. This avoids internal IP address ranges from being exposed when reaching external resources and services.

- ***ACLs: Default Deny; Permit only needed traffic:***
  - ICMP filtering (Ping):
    - Block Echo requests from WAN into internal networks
    - Allow ICMP within internal networks
    - Allow echo requests from internal networks to WAN
  - SSH (TCP 22):
    - Block SSH from WAN to internal networks
    - Allow SSH within internal networks
    - Allow SSH only over a VPN if needed for remote administration
  - HTTP(S) (TCP 80/TCP 443):
    - Allow HTTP(S) from specific sources (VPN subnet, LAN)
    - Block WAN access to internal web servers
  - FTP (TCP 21):
    - Block FTP from WAN
    - Allow FTP internally or through a VPN

- ***VPN Configuration***
  Type: Remote Access VPN
  Protocol: WireGuard
  Port: UDP 51820
  Authentication: Private/Public Key Pairs
  Access policy: VPN users only get access to approved subnets and hosts

- ***Logging/Alerting (pfSense/IDS/IPS)***
  Enable firewall logging on key rules:
  - Blocked WAN -> internal network connections
  - Blocked ICMP from WAN
  - Blocked SSH attempts

- VPN connection events
- IDS/IPS support for packet monitoring

Logs can then be reviewed through pfSense.