# **Lab: VPN Tunnel**

## **Overview**

**The VPN protocol can be used in several ways; everyday computer users are likely familiar with client VPN services that claim to grant privacy to their customers. Another way to use VPN is to establish a private network connection between two computers (client-server VPN). Today you’ll join two separate networks using IPsec Site-to-Site VPN Tunnelling via pfSense’s built-in IPsec tunnelling capabilities.**

## **Scenario**

**GlobeX needs to establish LAN network connectivity between two sites in order to share mission-critical resources. Both sites have VPN-capable edge routers.**

## **Resources**

* [**Configuring a Site-to-Site IPsec VPN**](https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-s2s-psk.html)
* [**Troubleshooting IPsec VPNs**](https://docs.netgate.com/pfsense/en/latest/troubleshooting/ipsec.html)

## **Objectives**

* **Join two separate LANs using a VPN tunnel**
  + **Use pfSense’s NAT Network mode to simulate an over-internet connection**
* **Successfully ping from one pfSense to a host within the subnet of the remote pfSense**
* **Depict this in a topology diagram**

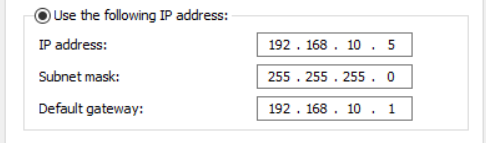
## **Tasks**

### **Part 1: Staging two networks**

* **~~For this lab, you’ll need to deploy a second pfSense VM if you have not done so already.~~**
* **~~The first network should include:~~**
  + **~~pfSense 1~~**
  + **~~Windows 10~~**

***Pfsense A: Going to be used with Windows***

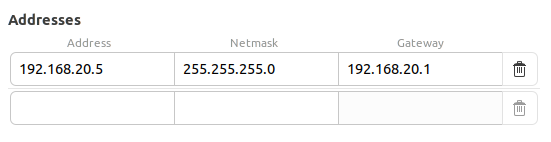
****

****

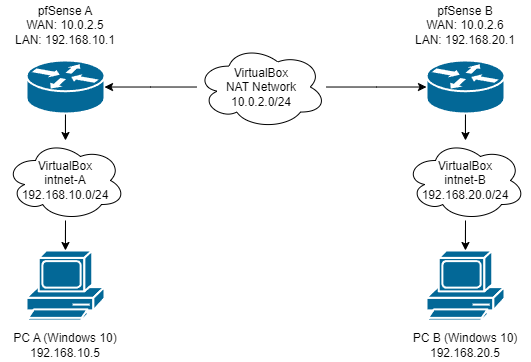
* **~~The second network should include:~~**
  + **~~pfSense 2~~**
  + **~~Any VM with a web browser (Windows 10, Kali, etc.)\~~**

***Pfsense B: Going to be used with linux***

****

****

* **~~The below diagram is an example of how one’s design might turn out:~~**

****

***So far nothing to report, all is as it should be***

### ***Part 2: Configuring pfSense***

***Next, prepare both pfSense devices to handle the VPN connection.***

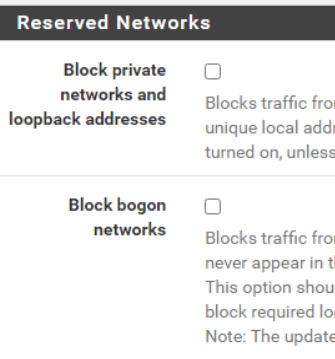
***Include screenshots of each option you configure.***

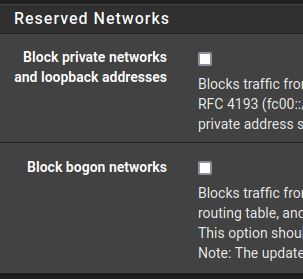
***Hint: in System > General Setup, under webConfigurator, you can change the “Theme” of the web GUI of one pfSense, to make differentiating between your screenshots easier.***

***Disable the default blocking of Private Networks and Bogon Networks to allow pfSense routers to respond to pings on the WAN:***

* ***~~Navigate to Interfaces > WAN, and scroll to the bottom~~***
* ***~~Uncheck the boxes for “Block private networks and loopback addresses” and “Block bogon networks”~~***

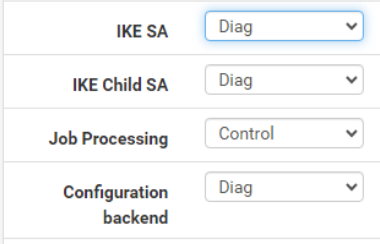
***Windows in Light-Mode, Linux in Dark-Mode***

******

******

***Set logging to verbose so you can see more information about the tunnel’s various handshakes. The steps are:***

* ***~~Navigate to VPN > IPsec, then select then Advanced Settings tab~~***
* ***~~Set IKE SA, IKE Child SA, and Configuration Backend to Diag~~***
* ***~~Set all other log settings to Control~~***
* ***~~Click Save~~***

******

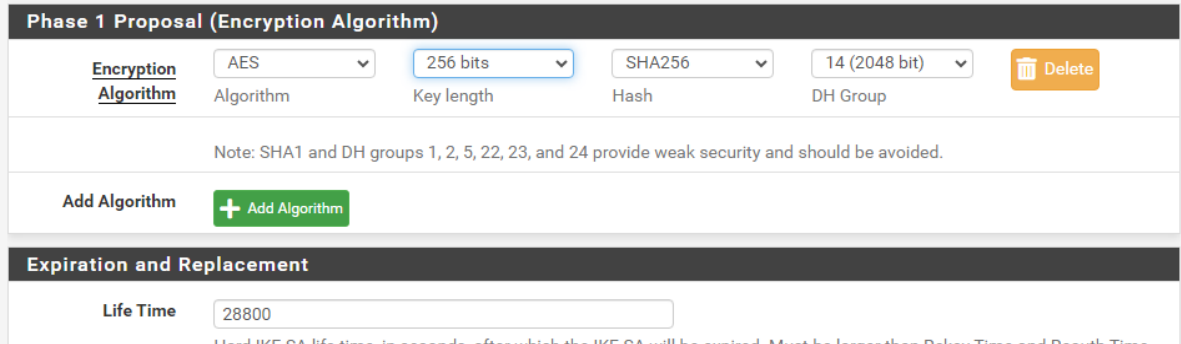
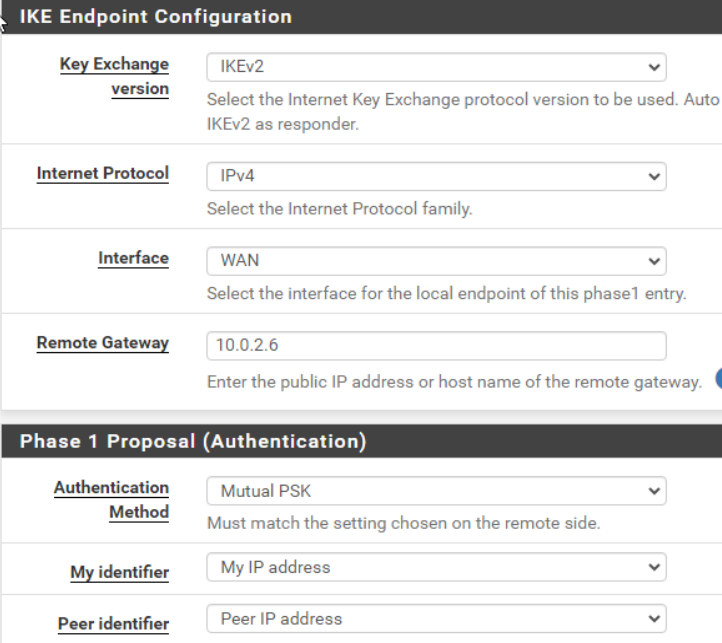
******

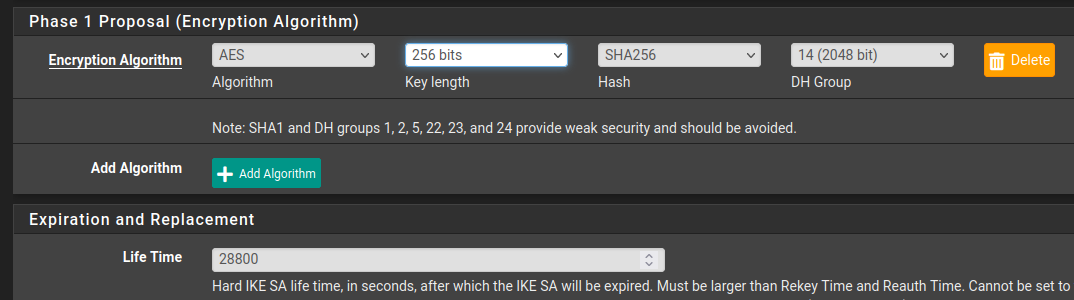
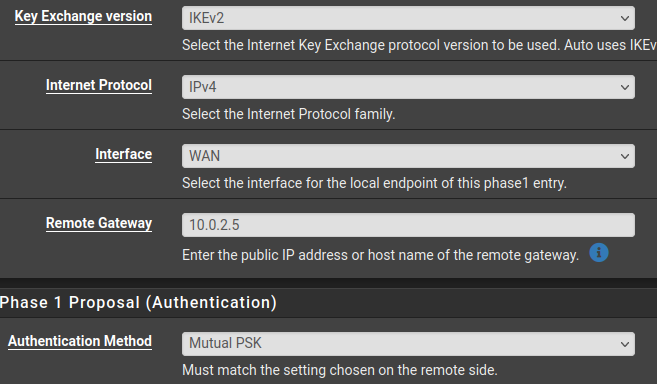
***VPN tunnel specifications:***

***Phase 1***

* ***~~Protocol: IKEv2~~***
* ***~~Interface: WAN~~***
* ***~~Remote Gateway: the WAN IPv4 address of the other router~~***
* ***~~Method: Mutual PSK (Preshared Key)~~***
* ***~~Encryption: AES 256-bit~~***
* ***~~Lifetime: 28800 sec~~***

***Windows in Light-Mode, Linux in Dark-Mode***

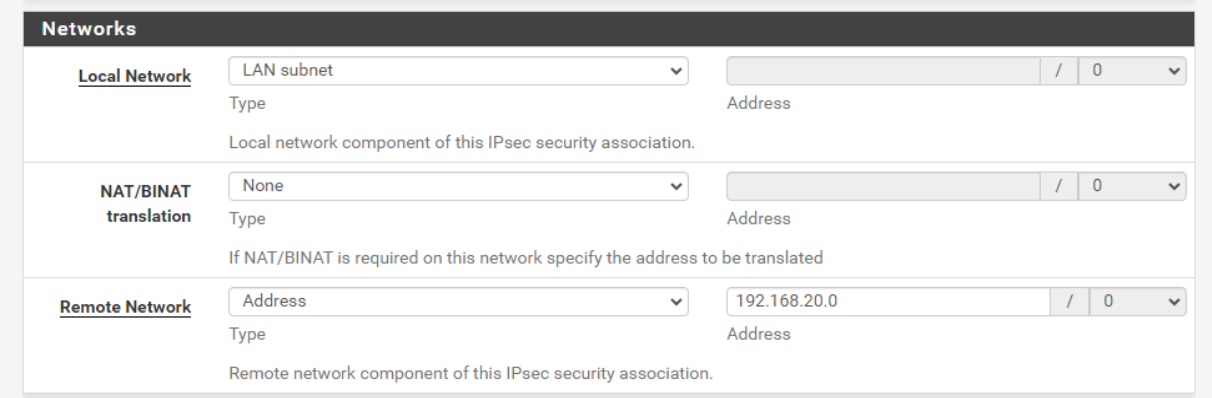
******

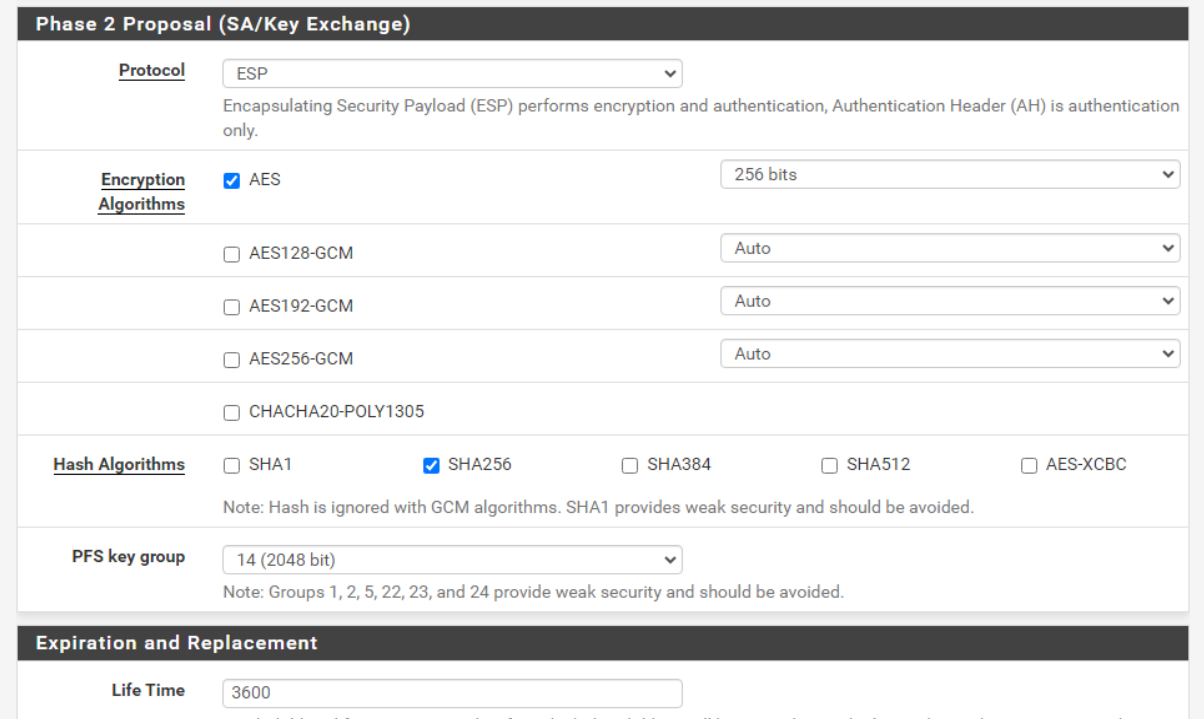
******

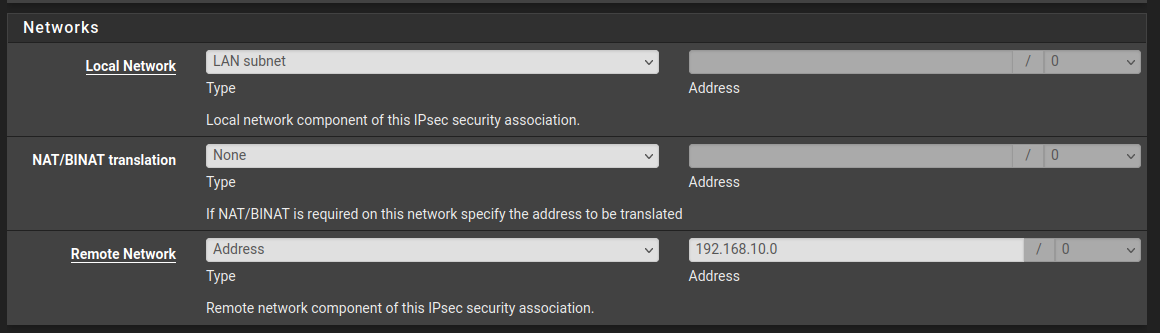
***Phase 2***

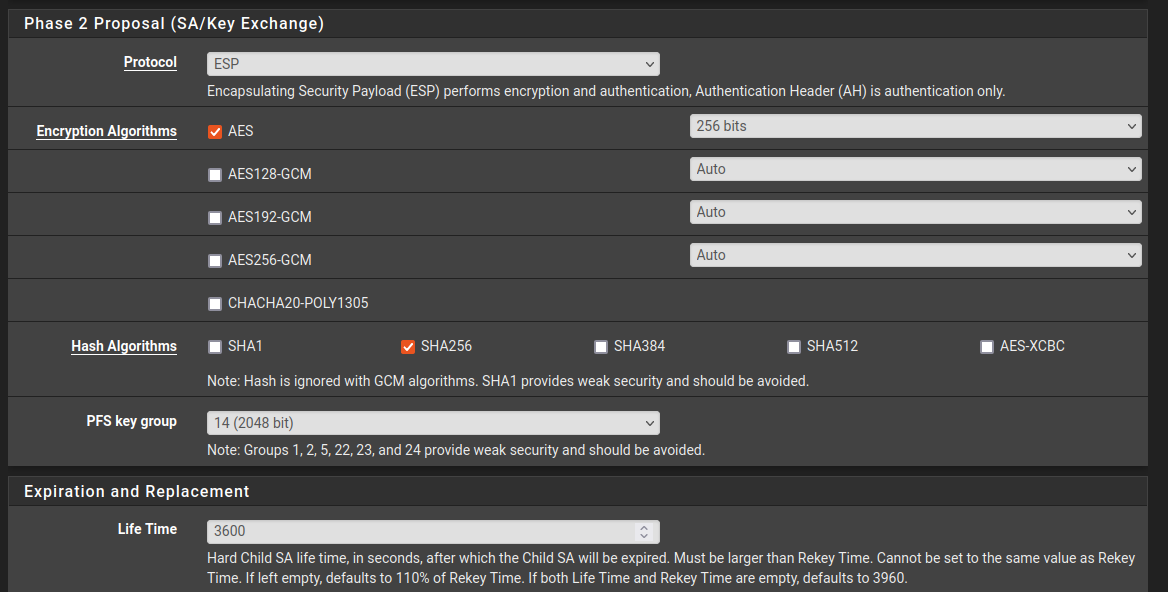
* ***~~Mode: Tunnel IPv4~~***
* ***~~Local Network: LAN subnet~~***
* ***~~Remote Network: the the subnet address of the LAN on the other router  
  This is a subnet address address, e.g. 10.0.2.0/24, which is different from a gateway address such as 10.0.2.1~~***
* ***~~Protocol: ESP~~***
* ***~~Encryption: AES 256-bit~~***
* ***~~PFS Key Group: 14 (2048 bit)~~***
* ***~~Lifetime: 3600 sec~~***

***Windows in Light-Mode, Linux in Dark-Mode***

******

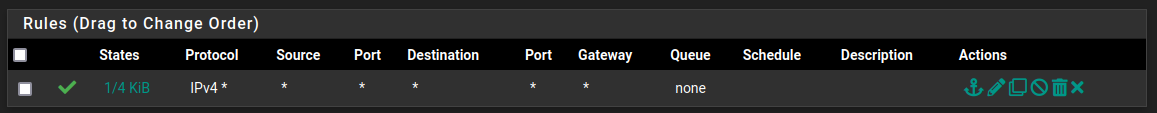
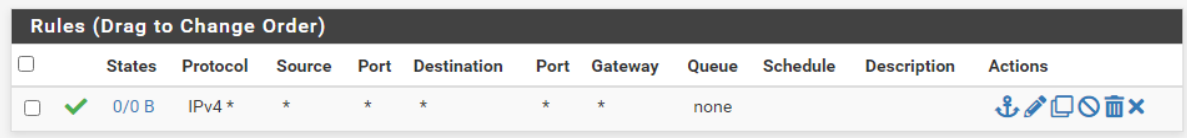
******

******

******

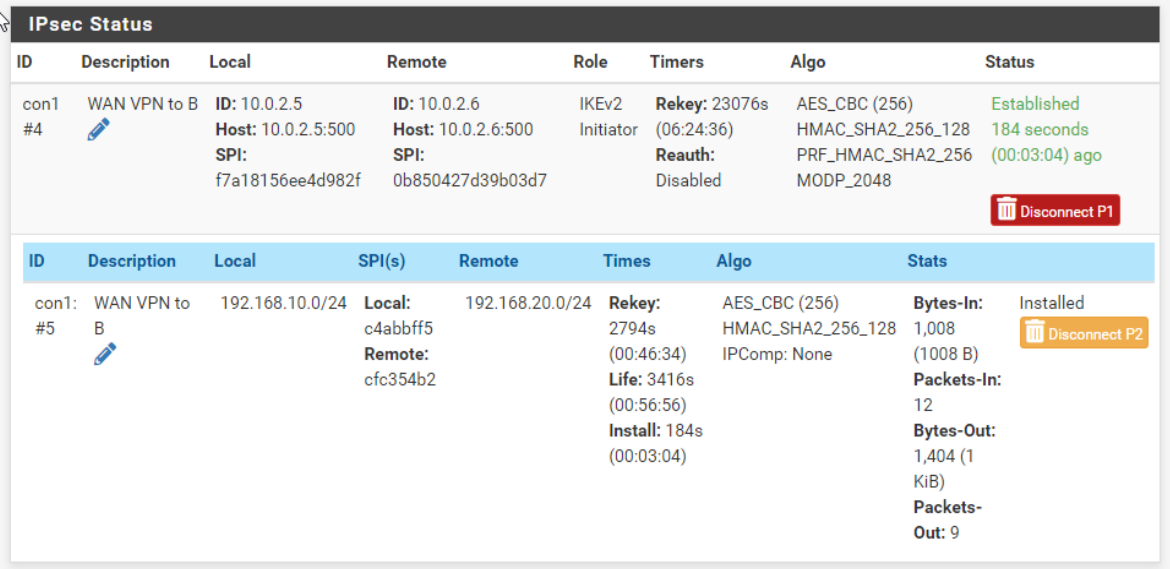
***Firewall Rule specification:***

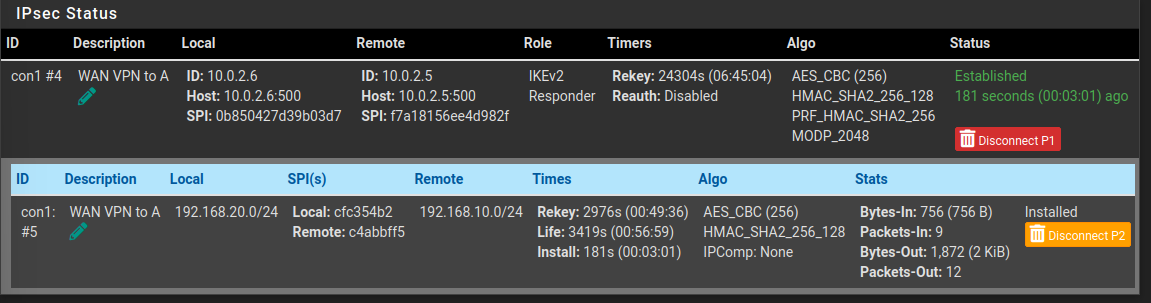
* ***~~Create corresponding rules on WAN and IPsec:~~***
  + ***~~Action: Pass~~***
  + ***~~Protocol: Any~~***
  + ***~~Source: Any~~***
  + ***~~Destrination: Any~~***

******

***Attempt to verify connectivity:***

* ***~~Navigate to Status > IPsec~~***
* ***~~Press “Connect P1 and P2”~~***
* ***~~The status screen should indicate “Established” for P1 and “Installed” for P2~~***

******

******

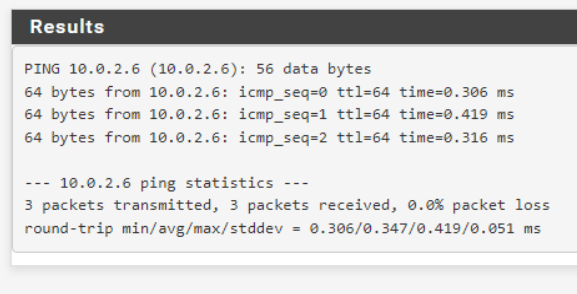
***I didn’t pay enough attention on the ‘NAT Network’ portion of class, but it was really easy to figure out. Otherwise they connected flawlessly.***

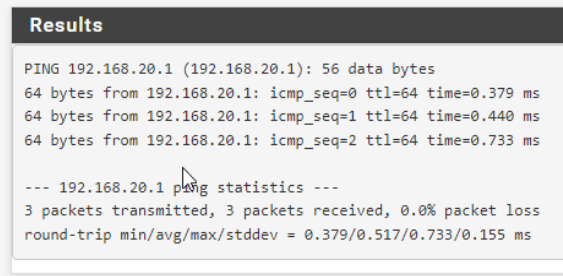
***To troubleshoot connectivity, analyze the IPsec logs for clues as to what may be holding back connectivity from succeeding. Use search engines and reference the Netgate forums for help in evaluating where any misconfigurations could be.***

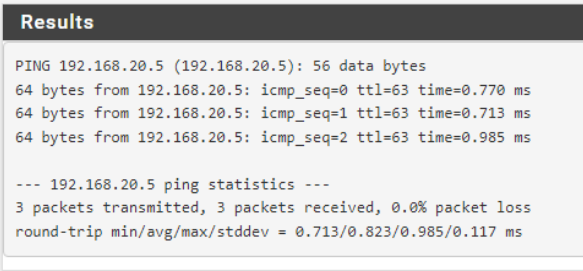
***Attempt to ping both the WAN IP and the LAN IP of the remote pfSense:***

* ***~~From pfSense:~~***
  + ***~~Navigate to Diagnostics > Ping~~***
  + ***~~Hostname: the LAN IPv4 address of the other router~~***
  + ***~~Source Address: LAN~~***

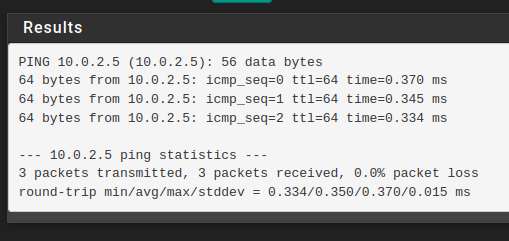
***Pfsense A - Pings***

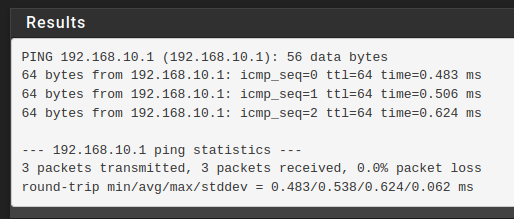
******

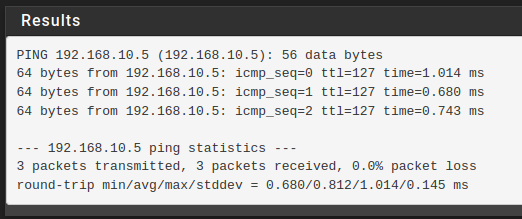
******

******

***pfsense B - Pings***

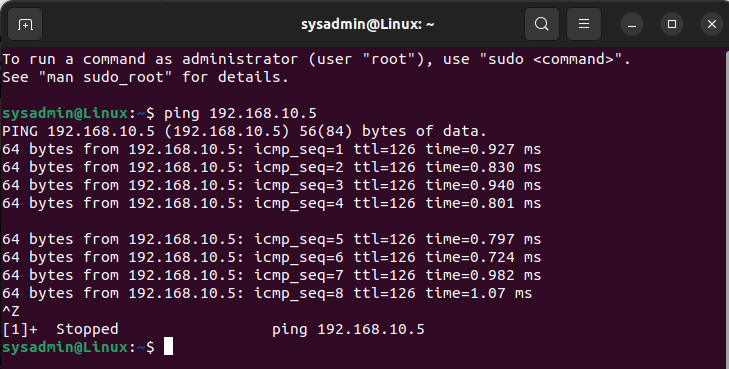
******

******

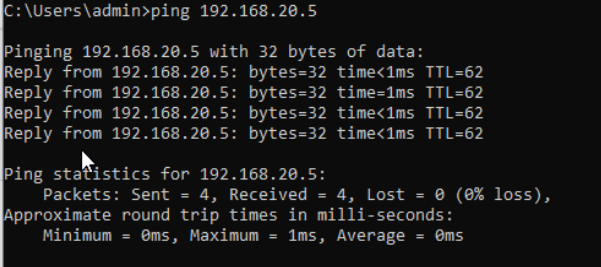
******

* ***~~From a host computer, use the terminal ping command as you normally would.~~***

***From Linux:***

******

***From Windows:***

******

***If you’ve correctly shared your subnets in Phase 2, and allowed traffic in your various firewall rules, you should be able to ping the remote router’s subnet/LAN address. If not, tinker with your configuration some more.***

***Don’t worry about getting your assets in each LAN to ping over the tunnel just yet; we’ll get to that in the next lab.***

***Include a screenshot of your VPN configuration screen and validate successful connectivity by analyzing pfSense status indicators and system logs. Include screenshots that indicate successful VPN tunnel connectivity.***

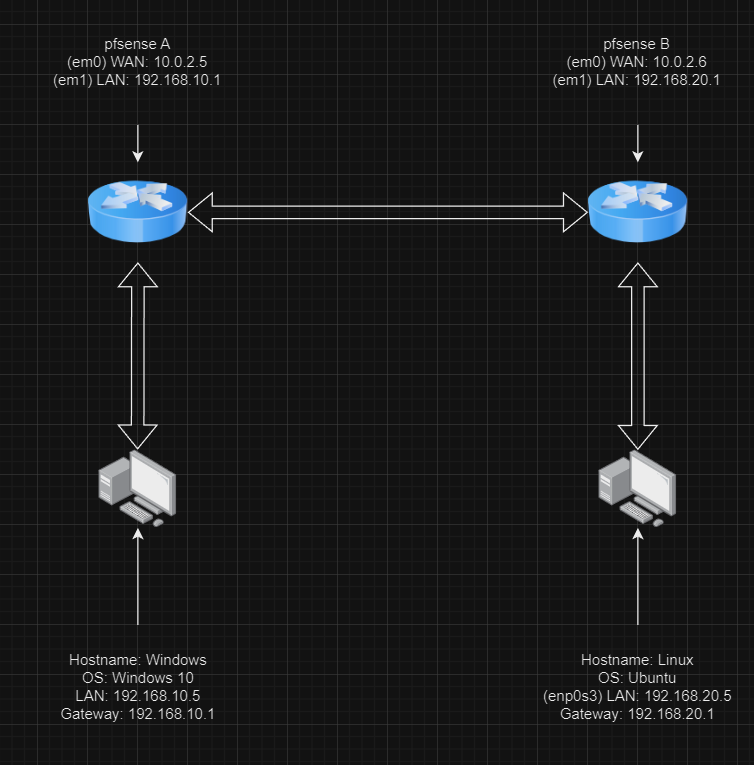
### ***Part 3: Topology***

***Use Draw.io to to create a network topology similar to the diagram above.***

***For each device on the network, include:***

* ***~~IP addresses for each NIC~~***
* ***~~Host names~~***
* ***~~Host Operating Systems~~***

***Include a screenshot of your topology here, and save your topology for use in the future. You will need it for the next lab.***

******

***Leave your VirtualBox network as-is! You’ll need it for next class, so don’t delete anything (especially that VPN tunnel)!***

***I did it all, there wasn’t any weird steps I had to do (except disable windows firewall)***