- A clear, written explanation and justification your network design.
    - Include a table or chart of network infrustructure and configuration details (yes, this will overlap with your topology -- you must document your network in both ways):
        - Subnets and their uses
            - Include Subnet Masks, CIDR addresses, etc.

Internal Network

Device(s)	Subnet Address	DHCP Range	Reserved IP address	NAT
PFsense router	10.0.5.0/24	10.0.5.100 -10.0.5.250	10.0.5.99	15.0.1.0/24

VPC

Device(s)	IP Address	Subnet Address	DHCP Range	Static IP
Window Server/	44.211.220.193	10.1.0.0/16	None Applicable	Yes
Internet Gateway		192.168.1.0/24	N/A	No
Outside Customer Gateway	34.193.147.83		N/A	Yes
Inside Customer Gateway		169.254.252.194/ 30	N/A	Yes

- Internal Network Firewall Rules:
- WAN:
    - Allows TCP IPv4
- LAN:
    - Allows TCP IPv4
- Virtual Private Cloud and EC2 instance Security Groups:
    - Allows ICMP IPv4

    - Allows SSH traffic
    - Allows RDP
    - Allows UDP traffic

PFsense router:

- Route all incoming traffic from the Window Server and internet to a desired end user.

Captive Portal:

- A way to create access for new users. Allows end users privileges to access the internet using log-in credentials. This request is sent to Windows Server.

AWS VPC:

- Secure elastic private cloud environment.

VPN tunnel:

- Allows packets being sent between the Internal network and VPC to be encrypted.

AWS EC2 Window Server 2019 instance:

- Represents Globex centralized server.
- Acts as DNS server for all connected users
    - A service to look up websites with certain domain names to provide for the end user.

Windows Active Directory:

- A service to provide new users with accounts, passwords, a domain name, and shared files.

Internal Gateway:

- Acts as a virtual router for the VPC.