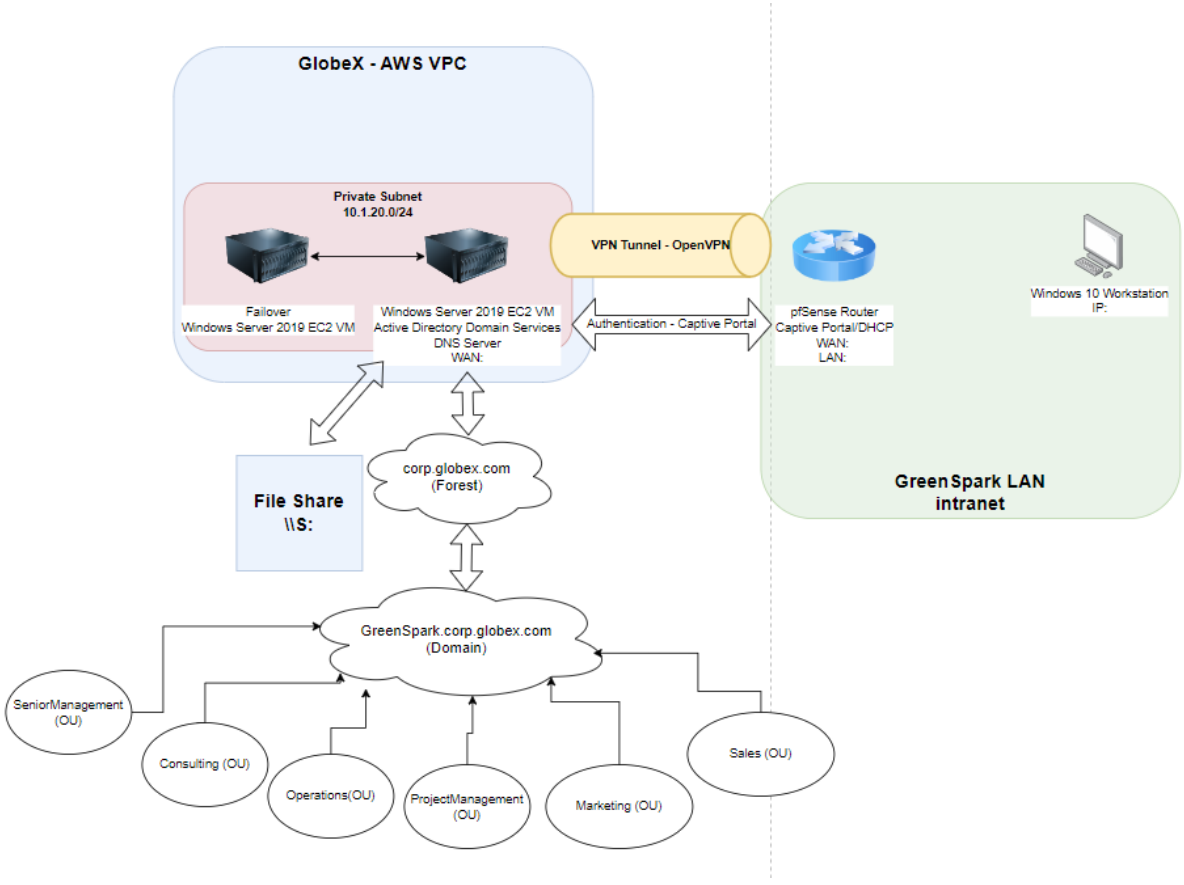
# Network Design

## Network Design Overview

The goal of this network design is to prototype the process of integrating new acquisitions. This particular network is designed to:

- Centrally manage newly acquired IT assets and end-users at GreenSpark through Active Directory
- Establish a security framework utilizing authentication, authorization, and accounting (AAA) that controls access to computer resources, enforces policies, and audits usage.
- Ensure stable, secure access to Globex resources for GreenSpark employees working from their local network
- Provide a modular framework that can be applied to future acquisitions



# Key Components

## AWS VPC with Windows Server 2019

- The Server acts as the host for Globex Active Directory Domain Services, Active Directory, the DNS Server, and File Share system.
- System administrators can manage the security of the network and user account privileges from a centralized location.
- The VPC serves as one end of a VPN Tunnel providing accessibility to end users on GreenSpark's LAN.

## Active Directory on Windows Server 2019

- Active Directory(AD) allows Globex to rapidly establish user accounts in the Globex Domain for newly acquired employees.
- AD provides built in accounting features so Network administrators can monitor account activity
- Using organizational units and group policy objects, Administrators can regulate role-based privileges that limit users ability to access resources outside what their job requires.
- A Captive Portal configured on the GreenSpark local network pfSense router utilizes AD as an authentication database, adding to the security of the network.

Figure 1. Globex Infrastructure (AWS VPC)

| | | |
|---|---|---|
| **Globex VPC (AWS)** | 10.1.0.0/16 | Hosts Globex Resources |
| **____ Subnet** | 10.1.20.0/24 | Private Subnet Shields the Server From Outside Traffic |
| **GlobeX Server (Windows Server 2019)** | 10.1.20.xxx | Handles Globex Domain Services, DNS, FileShare and Authenticates Captive Portal Requests Through Active Directory |
| **Failover Server (Windows Server 2019)** | 10.1.20.201 | Replaces Globex Server in Case of Failure |
| **(2nd Subnet?)** | 10.1.10.0/24 | |
| **Public Gateway** | 10.1.xxx.xxx | Gateway for Open VPN Tunnel |

## Open VPN Tunnel

- The Open VPN Tunnel securely connects the GreenSpark office's local endpoints to Globex VPC resources using AES-256 encryption.

## pfSense Router VM

- The pfSense router establishes the local network for GreenSpark end points
- Provides DHCP services, maintains a secure connection to the Globex VPC via Open VPN
- Hosts a Captive Portal using GlobeX AD to authenticate users, shielding company assets from malicious actors. Captive Portal will provide logs of attempted logins

Figure 2. GreenSpark Infrastructure

| | | |
|---|---|---|
| GreenSpark Network Router (pfSense) | | Establishes OPEN VPN Tunnel with Globex VPC, DHCP, Maintains Firewall, Captive Portal |
| | WAN: 192.168.0.129/24 | |
| | LAN: 10.0.1.1/24 | DHCP Range: 10.0.1.100-10.0.1.200 |
| GreenSpark Workstation (Windows 10) | 10.0.1.104 | Allows users Access to Globex Domain |
| | | |