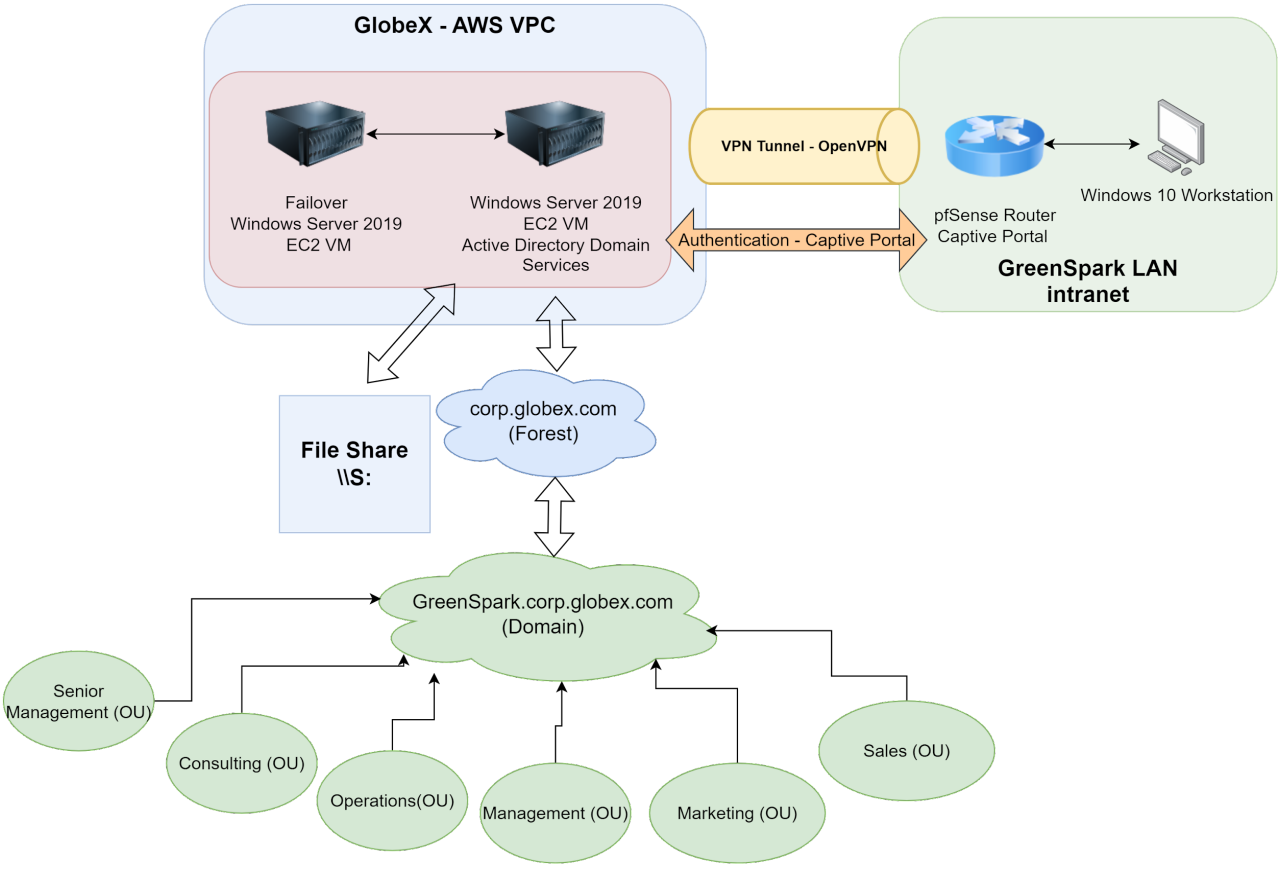
Network Design

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
Private Subnet	10.1.20.0/24	Private Subnet Shields the Server From Outside Traffic
GlobeX Server (Windows Server 2019)	10.1.20.2	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
Public Gateway	10.100.100.91	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)	WAN: 192.168.0.129/24 LAN: 10.0.1.1/24 DHCP Range: 10.0.1.100-10.0.1.200	Establishes OPEN VPN Tunnel with Globex VPC, DHCP, Maintains Firewall, Captive Portal
GreenSpark Workstation (Windows 10)	10.0.1.104	Allows users Access to Globex Domain

Figure 3. pfSense Router - Reserved IPs

LAN:	Purpose
10.0.1.0	Network Address
10.0.1.1	PfSense Router
10.0.1.255	Broadcast Address
10.0.1.10-10.0.1.50	Reserved IP Range, Space for Future Subnetting if Desired

Security Policies

Active Directory (Domain Controller on Windows Server on AWS VPC)

- Group Policy Objects (GPO) are applied to organizational units (OU) based on department. GlobeX applied GPOs to all non-technical Greenspark employees that do the following:
    - Restrict user access to Control Panel, protecting key configurations on the PC
    - Restrict user access to Command Prompt and the user execution of scripts
        - Note: GlobeX Admins can still access Command prompt through RDP

AWS VPC

- AWS configured to block all external traffic to ports by default
- GlobeX configured the following ports to be open to facilitate consistent, secure accessibility of resources including:
    - Port: 1194 (Open VPN), 443 (HTTPS)

pfSense Router

- GreenSpark users authenticated through the Captive Portal do not have the ability to change the configuration of the pfSense. Only GlobeX admins can make changes.
- pfSense firewall will have the following rules
    - Inbound Firewall Rules:
        - Allow Active Directory Traffic:
            - Protocol: TCP/UDP
            - Port: 389 (LDAP), 636 (LDAPS)
        - Allow DNS Traffic:
            - Protocol: TCP/UDP
            - Port: 53
        - Allow Kerberos Traffic:
            - Protocol: TCP/UDP
            - Port: 88
        - Allow NTP Traffic:
            - Protocol: UDP
            - Port: 123
        - Allow HTTP Traffic:
            - Protocol: TCP
            - Port: 80
        - Allow HTTPS Traffic:
            - Protocol: TCP
            - Port: 443
        - Allow RDP Traffic:
            - Protocol: TCP/UDP
            - Port: 3389
        - Allow ICMP Traffic:
            - Protocol: ICMP
    - Outbound Firewall Rules:

- Allow Outbound Traffic for Established Connections:
  - Protocol: TCP/UDP
  - State: Established
- Allow Outbound DNS Traffic:
  - Protocol: TCP/UDP
  - Port: 53
- Allow Outbound HTTP and HTTPS Traffic:
  - Protocol: TCP
  - Port: 80, 443
- Allow Outbound NTP Traffic:
  - Protocol: UDP
  - Port: 123
- Allow Outbound VPN (Open VPN) Traffic:
  - Protocol: UDP
  - Port: 1194