A green leaf logo with plug

Description automatically generated

**GreenLeaf Technologies Inc.**

*Design Document*

|  |
| --- |
| **Prepared By:** |
| Aditi Thakur (000467264) |
| Guneet Sidhu (000461987) |
| Navneet Kaur (000468476) |
| Harnoor Kaur (000467135) |
| Amritjot Kaur (000467826) |

A small island with windmills and buildings

Description automatically generated

**Documentation Information**

|  |  |
| --- | --- |
| Document Title | GreenLeaf Technologies Inc. |
| Document Last Save | October 28, 2024 |

**Document Owner**

|  |  |
| --- | --- |
| **Date of creation** | **Owner** |
| September 09,2024 | Guneet, Aditi, Navneet, Harnoor and Amritjot |

**Document Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author** | **Changes** |
| 1.0 | September 9 |  | Commencement of project |
| 1.1 | September 17 |  | Added details on the current situation, OSI, risks, PKI, and AD |
| 1.2 | September 23 |  | Added details on DNS, Network infrastructure, and AD. |
| 1.3 | September 30 |  | Updated PKI, OSI, AD, and security for Greenleaf Inc. |
| 1.4 | October 7 |  | Review and update documents for PKI, DNS, AD, and network infrastructure |
| 1.5 | October 14 |  | Enhanced the details on DNS, PKI, and network security. Incorporated additional insights on risk management and disaster recovery strategies. |
| 1.6 | October 21 |  | Few revisions on existing services and added Azure cloud solution for GreenLeaf Inc. |
| 1.7 | October 26 |  | Final revision and added Azure cloud solution and DHCP |

[1. Executive Summary 4](#_Toc181645611)

[2. Existing Network Infrastructure 4](#_Toc181645612)

[2.1 Recommendation 4](#_Toc181645613)

[2.2Current Infrastructure 5](#_Toc181645614)

[2.3 Current Network Design 8](#_Toc181645615)

[3. Analysis and Recommendations 10](#_Toc181645616)

[3.1Public Key Infrastructure (PKI) Implementation 10](#_Toc181645617)

[3.2Working on OSI Layers in network design 16](#_Toc181645618)

[3.3Network Infrastructure Design 20](#_Toc181645619)

[3.4 Wi-Fi and Wireless Connections 29](#_Toc181645620)

[3.5 Dynamic Host Configuration Protocol (DHCP) 46](#_Toc181645621)

[3.6 Domain Name System (DNS) 50](#_Toc181645622)

[3.7 Active Directory (AD) 55](#_Toc181645623)

[3.8 Disaster Recovery (DR) 63](#_Toc181645624)

[3.9 Risk Management 64](#_Toc181645625)

# **1. Executive Summary**

GreenLeaf Technologies Inc. is an innovative green startup technology company that develops sustainable energy solutions for residential and commercial clients. Founded in 2015, the company is headquartered in San Francisco (SF), California, with additional offices in New York City (NY) and Houston (HO), Texas. Recently, they received a $40 million investment from an angel investor and their CEO plans to grow the company from 165 employees to 300 and relocate to larger offices to accommodate the growth.

To support this growth, a new scalable and secure network infrastructure is essential.

# **2. Existing Network Infrastructure**

Numerous issues plague the current network infrastructure, such as out-of-date hardware, inadequate firewall policies, a lack of network segmentation, inadequate monitoring and incident response, and a lack of redundancy for essential services. These restrictions put the firm at risk for downtime, performance snags, and security breaches, all of which could have a detrimental effect on day-to-day operations.

**2.1 Recommendation**

To address these issues, the network team comes up with a new detailed network plan including recommendations that meet the proposed requirement.

* A blend of cloud-based services (for scalability, flexibility, and disaster recovery) and on-premises hardware (for core operations and vital services). With this hybrid approach, the business may take advantage of the cloud infrastructure's scalability and cost-effectiveness while still keeping control over important data.
* Security will be greatly increased by implementing stringent access controls, network segmentation, intrusion detection/prevention systems (IDS/IPS), and next-generation firewalls.
* To separate network traffic, VLANs will be employed (e.g., employee devices, guest networks and server access). This will create a safe and isolated environment for various kinds of devices. By limiting the attack surface and preventing network congestion, this segmentation will enhance security as well as performance.
* Redundancy will be used in the configuration of critical services like DNS, DHCP, and firewalls to guarantee that services continue to function even in the case of a hardware failure. Further, defense against disruptions can be provided via failover solutions and cloud-based backups.
* In order to give real-time visibility into network traffic and system performance, network monitoring tools will be implemented. Long downtimes will be avoided and speedier problem-solving capabilities will be possible.
* Our disaster recovery plan will make use of cloud-based services for replication and backup. Critical data and services can be promptly restored in the case of a significant outage or disaster, reducing the impact on business operations.

**Conclusion**

The network that GreenLeaf Technologies now has is insufficient for the company's growth and increasingly intricate activities. The company's growth and security posture are seriously jeopardized by the performance, security, scalability, and redundancy flaws that have been found. These issues are addressed by the suggested network redesign, which adds more advanced security protocols, scalable modern infrastructure, and better network management tools. In addition to accommodating GreenLeaf's expanding workforce, this new design will guarantee that the business's operations continue to be safe, dependable, and expandable for many years to come.

**2.2Current Infrastructure**

A close-up of a company's information

Description automatically generated

|  |  |
| --- | --- |
| **San Francisco HQ Offices** | |
| Department | Employees |
| Research &Development (R&D) | 20 |
| Sales & Marketing | 30 |
| Operations | 30 |
| IT & Support | 20 |
| Human Resources | 10 |
| Finance & Accounting | 15 |

|  |  |
| --- | --- |
| **New York Offices** | |
| Department | Employees |
| Operations | 10 |

|  |  |
| --- | --- |
| **Houston Office** | |
| Department | Employees |
| R&D | 20 |

|  |  |
| --- | --- |
| **Remote Users** | |
| Department | Employees |
| Sales | 10 |

**Server**

A server is a computer that provides information to other computers called “clients” on the computer network. There are a couple of servers used in our current infrastructure which are as follows:

|  |  |  |
| --- | --- | --- |
| **Server used** | **Operating system** | **Quantity** |
| Email Server | Windows Server 2016, Exchange | 1 |
| DNS Server | Windows Server 2016 | 1 |
| DHCP Server | Windows Server 2016 | 1 |
| Domain Controller | Windows Server 2008 | 1 |
| Web Server | Linux, Apache | 1 |
| File Server | Windows Server 2016 | 2 |

**Network Equipment**

Physical devices that allow hardware on a computer network to interact and communicate with one another.

|  |  |  |
| --- | --- | --- |
| **Network Equipment used:** | **Quantity** | **Comments** |
| Wireless Access Points | 4 | consumer-grade, without enterprise features |
| Switches | 6 | unmanaged, no VLAN support |
| Firewall | 3 | single vendor, low-end models |

**Workstations**

Workstations are personal computers or desktop systems employees use to perform daily tasks, such as working on documents, accessing software, or communicating with others. They are typically more powerful than standard home computers.

|  |  |  |
| --- | --- | --- |
| **Devices** | **Operating System** | **Quantity** |
| Desktop Computers | Windows 10 | 130 |
| Laptops | MacOS | 30 |
| Desktop Computers | Linux | 10 |

**Wireless Devices**

Wireless devices are gadgets like smartphones, tablets, and laptops that connect to the internet or other networks without physical cables.

|  |  |  |
| --- | --- | --- |
| **Devices** | **Operating System** | **Quantity** |
| Smartphones | iOS and Android | 40 |
| Tablets | iOS and Android | 25 |

**Network Equipment Models**

|  |  |  |
| --- | --- | --- |
| **Network Equipment Models** | | |
| Role | Location | Brand of Model |
| Firewall | SF Firewall (Firewall\_SF) | Netgear ProSafe FVS318G |
| Firewall | NY Firewall (Firewall\_NY) | ZyXEL USG20-VPN |
| Firewall | HO Firewall (Firewall\_HO) | Cisco ASA 5506-X |
| Switches | Switch A (SF) | TP-Link TL-SG1024D-24 Ports  (Consumer-Grade) |
| Switches | Switch B (SF) | D-Link DGS-1024D – 24  Ports  (Consumer-Grade) |
| Switches | Switch C (SF) | Netgear GS324 – 24  Ports  (Consumer Grade) |
| Switches | Switch D (NY) | Cisco Catalyst 2960-L Series (WS-C2960L-24TS-LL) – 24 ports (Low-end enterprise) |
| Role | Location | Brand of Model |
| Firewall | SF Firewall (Firewall\_SF) | Netgear ProSafe FVS318G |
| Firewall | NY Firewall (Firewall\_NY) | ZyXEL USG20-VPN |
| Firewall | HO Firewall (Firewall\_HO) | Cisco ASA 5506-X |
| Switches | Switch A (SF) | TP-Link TL-SG1024D-24 Ports  (Consumer-Grade) |
| Switches | Switch B (SF) | D-Link DGS-1024D – 24  Ports  (Consumer-Grade) |

**2.3 Current Network Design**

|  |
| --- |
| All servers are on the same subnet, without proper segmentation. |
| No VLANs were implemented, leading to unnecessary broadcast traffic. |
| No redundancy or failover mechanisms are in place for critical services (DHCP, DNS, email). Outdated server operating systems and unpatched software, expose the network to potential security risks. |
| Lack of proper network access controls, allowing unauthorized devices to connect to the network. |
| Insufficient firewall policies, exposing internal resources to the internet |

**Internet Connection and Firewalls**

|  |
| --- |
| Each location (SF, NY, and HO) has an ISP connection and is equipped with a low-end, single-vendor firewall, which also acts as a router. |
| SF Firewall (Firewall\_SF) is connected to the ISP and the VPN tunnel to NY and the WAN connection to HO. |
| NY Firewall (Firewall\_NY) is connected to the ISP and the VPN tunnel to SF. |
| HO Firewall (Firewall\_HO) is connected to the ISP and the WAN connection to SF. |

**Switches**

|  |
| --- |
| SF: Firewall\_SF connects to Switch A, which further connects to Switches B and C. |
| NY: Firewall\_NY connects to Switch D. |
| HO: Firewall\_HO connects to Switch E, which further connects to Switch F. |

**Servers**

|  |
| --- |
| All in SF, on the same subnet, without proper segmentation. |
| All servers are connected to Switch A. |

# **3. Analysis and Recommendations**

**3.1Public Key Infrastructure (PKI) Implementation**

As GreenLeaf Technologies is expanding from 165 to 300 employees and moving into larger offices, the company needs a secure way to protect its network and sensitive information. Public Key Infrastructure (PKI) is a highly effective solution for securing communications, authenticating users and devices, and protecting sensitive data. PKI uses digital certificates to establish trust between users, devices, and services across the network.

**PKI Deployment Across Three Locations**

**PKI Components:**

* Certificate Authority (CA): Issues and manages digital certificates.
* Registration Authority (RA): Acts as the verifier of certificates but does not issue them.
* Digital Certificates: These certify the ownership of a public key by the named subject.
* Public and Private Keys: The core of encryption; public keys are shared while private keys are kept secure.
* Certificate Revocation List (CRL): A list of revoked certificates to maintain security.

**Locations and Role of PKI:**

* **San Francisco (Headquarters)**:
* **VLAN 100 – PKI VLAN (Root CA)**
* This is the **Root CA** location. The Root CA will be kept **offline** (disconnected from the network) to protect it from attacks.
* The Root CA will only be used to sign and issue certificates to the Intermediate CAs in New York and Houston. After setup, it will remain offline for security reasons.
* **New York (Branch)**:
* **VLAN 150 - PKI VLAN (Intermediate CA)**
* Hosts an **Intermediate CA** that will handle the day-to-day certificate operations for the New York office.
* The Intermediate CA will issue certificates for devices, servers, VPN connections, and users in the New York office. VPN clients for remote workers will be authenticated using certificates issued by the Intermediate CA.
* **Houston (Branch)**:
  + **VLAN 200 - PKI VLAN (Intermediate CA)**
  + Similar to New York, Houston will have its own **Intermediate CA**.
  + The Houston Intermediate CA will issue certificates for internal servers, user devices, and secure communications between employees in Houston.

**PKI Architecture**

The organization will implement a **Two-Tier PKI Architecture** which strikes a balance between security, scalability, and manageability in our proposal. This model involves:

**Why 2-Tier Architecture?**

We have chosen a 2-tier PKI system over 1-tier and 3-tier because it provides an ideal balance between security, efficiency, and manageability for our organization. In a 1-tier PKI, there’s only one Certificate Authority (CA), the Root CA, that handles all operations, including issuing, managing, and revoking certificates. While this setup may seem simple, it presents a significant risk. If the Root CA is ever compromised, the entire system collapses. Every certificate issued would become invalid, leading to a complete breakdown of trust across all systems, and you’d need to reissue all certificates from scratch. Additionally, as our organization grows and more certificates are needed, the Root CA will become overloaded, causing delays and inefficiencies in issuing and managing certificates. Thus, a 1-tier system lacks both scalability and security.

A 3-tier PKI adds another layer with Issuing CAs that distribute certificates. While it offers even more separation, it’s unnecessary for a company of our size. The added complexity of managing three layers does not provide enough benefit to justify the overhead. A 2-tier system offers sufficient security without making operations too complicated. In conclusion, a 2-tier PKI offers the right balance of security, efficiency, and scalability. It keeps the Root CA safe, distributes the workload efficiently across Intermediate CAs, and avoids the unnecessary complexity of a 3-tier system. This makes it an ideal choice for our organization’s needs.

A diagram of a plant

Description automatically generated

**VLAN Implementation**

Let’s consider VLANs for servers in all three locations.

A diagram of a company

Description automatically generated

**VLAN segmentation** plays a key role in protecting Greenleaf’s network by isolating critical systems and ensuring that only authorized users can access sensitive resources:

* **PKI VLAN Protection**: The **Root CA** in **VLAN 100** and the **Intermediate CAs** in **VLAN 150** (New York) and **VLAN 200** (Houston) are isolated in their own VLANs. Only IT admins from their corresponding **Admin VLANs** (VLAN 30, 160, 210) can interact with these sensitive systems, reducing the risk of unauthorized access.
* **Department Segmentation**: Each department (e.g., Finance, Sales, R&D) operates within its own VLAN to limit lateral movement in case of compromise.
* **Firewall and Access Control Lists (ACLs)** While VLANs segment the network, **firewalls** and **Access Control Lists (ACLs)** provide the necessary security rules to control which devices and users can access specific network segments. This ensures that even if devices are in the same network, only authorized traffic is allowed to reach sensitive areas like the **PKI VLAN** or **VPN servers**.
* **Firewalls** are configured to restrict access to the **PKI VLANs** so that only IT administrators can reach the **Root CA** or **Intermediate CAs**.
* **ACLs** provide additional granular control over what types of traffic are allowed between VLANs. For example, only devices in **VLAN 30 (IT Admin)** can communicate with the **Root CA** in **VLAN 100**.

**Practical Use Cases for PKI in an Organization’s Network**

### **VPN Setup Using PKI for Secure Remote Access**

**VPNs** are used to securely connect remote users and Greenleaf offices. Each office has its own **VPN server** hosted in a dedicated VLAN, and access to the VPN is managed through **PKI certificates**.

* **Issue Certificates**: The **Intermediate CAs** in New York and Houston issue **certificates** for users and VPN servers. These certificates are required for authentication.
* **Install Certificates on VPN Servers**: Each **VPN server** in **VLAN 110 (SF)**, **VLAN 160 (NY)**, and **VLAN 210 (HO)** has its certificate installed to secure all communication.
* **Establish VPN Connections**: When a remote user or a user from another office tries to connect, the VPN server verifies the user's **certificate**. If the certificate is valid, the VPN server establishes an **encrypted tunnel** using **AES-256 encryption**.

#### **Example of VPN Protection**:

A remote user working from home attempts to access the network in **San Francisco**. The **VPN server** in **VLAN 110** checks the user’s certificate, and if authenticated, it allows the connection. All communication is encrypted to prevent unauthorized access or interception of sensitive data.

### **Email Server Configuration and Protection**

**Email servers**, located in **VLAN 120 (SF)**, **VLAN 170 (NY)**, and **VLAN 220 (HO)**, handle internal communications. These servers use **S/MIME certificates** issued by the **Intermediate CAs** to encrypt and authenticate emails.

* **S/MIME Certificate Setup**: Each email server uses **S/MIME certificates** to ensure that all emails sent within and between offices are encrypted and secure.
* **Email Server Protection**: The email servers are isolated in their respective VLANs, preventing unauthorized access from other departments.

#### **Example of Email Security**:

When an employee in **Houston** sends an email to someone in **New York**, the email is encrypted by the **Houston email server** using an **S/MIME certificate**. The email can only be decrypted by the recipient’s email server, ensuring that even if the email is intercepted, it remains secure.

##### **Server Authentication**

Internal servers, such as database, email, and file servers, will use certificates to encrypt and authenticate communications.

* **SSL/TLS for Data Encryption**: **SSL/TLS certificates** will be issued to servers, securing communications between them. For example, data transmitted between the New York and Houston servers will be encrypted, preventing unauthorized access.
* **Server-to-Server Authentication**: When two servers (e.g., email and database servers) communicate, they will use SSL/TLS certificates to mutually authenticate, ensuring that only valid servers are part of the communication.

##### **Device Authentication**

To ensure that only authorized devices connect to the network, each device (laptops, mobile phones, etc.) will receive a device certificate.

* **Certificate-Based Authentication**: Devices in New York and Houston will be issued unique certificates signed by the Intermediate CA. When a device attempts to connect to the network, its certificate will be validated.
* **Wi-Fi Access**: Wi-Fi access points will require certificate-based authentication to ensure that only devices with valid certificates can access the company network.

##### **Internal Web Application Security**

Internal web applications, such as HR portals and inventory systems, will be secured using SSL/TLS certificates.

* **Secure Access to Web Apps**: Each web application will have a certificate to secure access through HTTPS. Users in all locations will access internal apps via encrypted connections, preventing data leaks.
* **User Authentication**: Web applications will authenticate users using client certificates, ensuring that only authorized personnel can access sensitive systems.

**Key Security Measures in PKI Implementation**

Implementing PKI across multiple locations (Houston, San Francisco and New York) brings challenges in ensuring secure communication, certificate management, and data integrity.

**Root CA Security**

* **Physical Security**: The Root CA will be kept offline and stored in a secure, access-controlled environment at the San Francisco HQ. Only authorized personnel can access the Root CA, and it will be powered on only for certificate-signing operations.
* **Hardware Security Module (HSM)**: The Root CA will be stored in an HSM, which provides physical and cryptographic protection to private keys, ensuring they cannot be extracted, even if physical access is gained.

**Certificate Issuance and Lifecycle Management**

* **Intermediate CAs**: Intermediate CAs in New York and Houston will handle day-to-day certificate issuance. Each certificate issued to devices, users, or systems will include an expiration date and revocation information.
* **Key Protection**: Private keys associated with issued certificates will be stored using hardware tokens or software-based encryption to ensure they are not compromised.

**Certificate Revocation**

* **Certificate Revocation Lists (CRLs)**: Each Intermediate CA will maintain a CRL to revoke certificates that are compromised, expired, or no longer needed. The CRL will be regularly updated and propagated across all locations to ensure real-time certificate validation.
* **Online Certificate Status Protocol (OCSP)**: OCSP servers will be set up to provide real-time certificate status checks, ensuring that invalid or revoked certificates are not trusted.

##### **Encryption for Data Transmission**

* **AES-256 Encryption**: All data transmitted between the three locations will be encrypted using AES-256, one of the most secure encryption standards, ensuring data integrity and confidentiality.

**3.2Working on OSI Layers in network design**

Greenleaf Technologies Inc. has three office locations in **San Francisco (SF)**, **New York (NY)**, and **Houston (HO)**, and the network design and functionality need to support each location's requirements. Here's how the OSI model will function and how the network will be managed and secured in all three locations based on the infrastructure provided:

**San Francisco (SF) - Main Office**

* **Departments**: R&D (40 employees), Sales & Marketing (50 employees), Operations (40 employees), IT & Support (30 employees), Human Resources (15 employees), Finance & Accounting (25 employees).
* **Primary Role**: Main hub with centralized resources including all company servers (e.g., file servers, email server, web server, DHCP, DNS, and Domain Controller).

**Network Design for San Francisco:**

1. **Physical Layer (Layer 1)**:
   * The backbone network for the office will use **CAT6 Ethernet cabling** for high-speed connectivity (1000 Mbps).
   * Wireless devices will connect via **two wireless access points** for coverage throughout the office.
2. **Data Link Layer (Layer 2)**:
   * Switches A, B, and C will handle traffic within the office, connecting servers and workstations.
   * **VLANs will be implemented** to separate different departments and servers, reducing unnecessary broadcast traffic.
3. **Network Layer (Layer 3)**:
   * The **Firewalls (Net gear Prostate FVS318G)** will connect the office to the internet and establish a **VPN tunnel to NY** and a **WAN connection to HO**, ensuring secure inter-office communication.
   * The IP addressing scheme will be **managed using DHCP** from the Windows Server 2016.
4. **Transport Layer (Layer 4)**:
   * The firewall will implement policies to handle **secure data transport** (TCP/IP), while **IPSec VPN tunnels** will encrypt inter-office data transfers.
5. **Security**:
   * Firewall policies will be applied to control incoming/outgoing traffic, ensuring **intrusion detection and prevention**.
   * Regular **patch updates** will be scheduled to address vulnerabilities and maintain up-to-date network equipment.
6. **Management**:
   * **Centralized monitoring** will be performed from the San Francisco office, ensuring real-time network performance tracking and security alerting for all locations.

**New York (NY) - Remote Office**

* **Departments**: Operations (20 employees), Sales & Marketing (20 employees).

**Network Design for New York:**

1. **Physical Layer (Layer 1)**:
   * Wired connections will use **Switch D (Cisco Catalyst 2960-L)**, with wireless coverage provided by a **Netgear WAC104 access point**.
2. **Data Link Layer (Layer 2)**:
   * Similar to SF, VLANs will be used to separate departments within the NY office, ensuring **network efficiency** and limiting traffic between unrelated departments.
3. **Network Layer (Layer 3)**:
   * The **Firewall\_NY (ZyXEL USG20-VPN)** will connect to both the internet and the **VPN tunnel to SF**, ensuring secure communication with headquarters.
   * All devices will use **private IP addressing**, with DHCP services handled centrally from SF.
4. **Security**:
   * Firewall policies will ensure secure access control, protecting internal resources from unauthorized internet traffic.
   * Any traffic between NY and SF will be secured via **IPSec VPN**, preventing external interference.
5. **Management**:
   * Remote management of the NY office will be handled from SF via centralized monitoring tools. Regular **remote audits** and updates will be conducted to ensure security compliance.

**Houston (HO) - R&D Office**

* **Departments**: R&D (35 employees), Operations (20 employees), Sales & Marketing (15 employees).

**Network Design for Houston:**

1. **Physical Layer (Layer 1)**:
   * Wired and wireless devices in HO will connect through **Switch E and F (HP OfficeConnect 1920S and Ubiquiti UniFi Switch)**, and wireless access will be provided via **Linksys LAPN600**.
2. **Data Link Layer (Layer 2)**:
   * As with the other offices, VLANs will segregate departments, reducing broadcast domain issues and improving security.
3. **Network Layer (Layer 3)**:
   * The **Firewall\_HO (Cisco ASA 5506-X)** will connect to the WAN link between SF and HO, ensuring continuous communication with SF.
   * Devices in the HO office will be assigned IPs from a **central DHCP service**, ensuring a unified address plan.
4. **Security**:
   * The firewall will enforce strict access policies, and the WAN connection to SF will be secured with **encrypted protocols**.
   * Regular penetration testing will be performed to identify potential vulnerabilities.
5. **Management**:
   * HO office will be monitored remotely via SF’s centralized monitoring infrastructure. Any performance issues or incidents will trigger **alerts for immediate action**.

**Inter-Office Connectivity & Management:**

* **Inter-Office Connections**:
  + The **IPsec VPN tunnel** between NY and SF will ensure encrypted traffic between these locations, supporting secure data exchange for Operations and Sales teams.
  + The **WAN connection between HO and SF** will allow for secure R&D collaboration between these locations.
* **Centralized Monitoring & Incident Response**:
  + All offices will be monitored through **centralized tools**, allowing for real-time detection of potential issues like network downtime, security incidents, or performance bottlenecks.
  + A **network operations center (NOC)** based in SF will receive alerts from **firewalls and monitoring systems** like LibreNMS, allowing for swift response to incidents.
* **Security Protocols**:
  + Each location will have its **firewall with policies tailored** to control both incoming and outgoing traffic.
  + Regular **security audits and vulnerability assessments** will be performed, ensuring that firewall rules are effective, and the network remains compliant with security best practices.

**3.3Network Infrastructure Design**

Implementing a comprehensive network infrastructure for GreenLeaf Technologies Inc. across three locations—San Francisco (SF), New York (NY), and Houston (HO)—requires meticulous planning, design, and execution.

**Network Design**

A hybrid network model combining on-premises infrastructure with cloud-based resources. The topology includes:

* **Core Layer**: Centralized in the SF office with high-performance switches and servers.
* **Distribution Layer:** Managed switches at each branch handling VLANs and inter-VLAN routing.
* **Access Layer:** Wireless access points and edge devices connecting end-users.

**IP Addressing Scheme**

**Private IP Addressing (RFC 1918):**

* SF Office: 10.0.0.0/16
* NY Office: 10.1.0.0/16
* HO Office: 10.2.0.0/16

**Subnetting:**

Allocate subnets for different departments within each location.

**Example for SF Office:**

* R&D: 10.0.10.0/24
* Sales & Marketing: 10.0.20.0/24
* Operations & IT: 10.0.30.0/24
* Finance & HR: 10.0.40.0/24

**VLAN Design and Segmentation**

VLANs (Virtual Local Area Networks) segregate network traffic to enhance security and reduce congestion.

**Headquarters (San Francisco)**

1. **VLAN 10 - R&D:** Isolate research and development traffic for security and resource allocation.
2. **VLAN 20 - Sales & Marketing:** Separate sales and marketing to manage bandwidth and sensitive data.
3. **VLAN 30 - Operations:** Dedicate a VLAN for operational traffic to streamline processes.
4. **VLAN 40 - IT & Support:** Provide IT and support teams with a separate VLAN to manage network resources and troubleshooting.
5. **VLAN 50 - HR:** Secure HR-related data with a dedicated VLAN for privacy compliance.
6. **VLAN 60 - Finance & Accounting:** Ensure financial transactions are isolated for enhanced security.

**New York (Operations)**

1. **VLAN 70 - Operations:** Connect NYC operations seamlessly with headquarters, maintaining workflow consistency.

**Houston (R&D)**

1. **VLAN 10 - R&D:** Mirror VLANs for R&D to ensure cohesive research efforts across locations.

**Remote Users (Sales)**

1. **VLAN 80 - Remote Access:** Allocate a VLAN for remote users to securely connect to the network via VPNs.

**Additional Considerations**

* **Guest VLAN:** For non-employees or temporary users who need internet access without touching the main network.
* **Management VLAN:** For network management devices and traffic to ensure control and monitoring.

Implementing these VLANs helps in segmenting network traffic, reducing congestion, and enhancing security across Greenleaf’s locations and remote connections.

**Selecting Network Devices**

Selecting the appropriate network devices is crucial for building an efficient, secure, and scalable network infrastructure.

***Firewalls***

**Requirements**

Next-Generation Firewall (NGFW) capabilities, VPN support, high throughput.

**Devices**

* SF Office: Cisco Firepower 2110 NGFW
* NY Office: Cisco Firepower 1010 NGFW
* HO Office: Palo Alto PA-220 NGFW

***Switches***

**Requirements**  
Managed, Layer 3 capabilities, VLAN support, PoE (if needed for devices like IP phones).

**Devices**

* SF Office: 1x Cisco Catalyst 9200 Series
* NY Office: 1x Cisco Catalyst 9200 Series
* HO Office: 1x Cisco Catalyst 9200 Series

***Wireless Access Points (APs)***

**Requirement** Enterprise-grade, support for 802.11ax (Wi-Fi 6), centralized management.

**Devices**

* SF Office: 2x Cisco Meraki MR42
* NY Office: 2x Cisco Meraki MR42
* HO Office: 2x Cisco Meraki MR42

***Servers***

**Requirements**

High performance, virtualization support, redundancy.

**Devices**

SF Office: 7x Dell PowerEdge Servers running VMware

***WAN Devices***

**Requirements**

SD-WAN capability, secure and reliable connectivity.

**Devices**

* + SF Office: Cisco SD-WAN powered by Viptela
  + NY & HO Offices: Compatible SD-WAN edge devices

**Additional Devices**

* + Network Management: Centralized management solution (e.g., Cisco Meraki Dashboard)
  + Backup Power: Uninterruptible Power Supplies (UPS) for critical devices

**Cabling and Physical Setup**

**Cabling Infrastructure**

* + Internal Cabling: Use CAT6 or higher for Ethernet connections within each office.
  + Backbone Cabling: Utilize Fiber Optic Cables for high-speed connections between switches and firewalls.
  + Patch Panels: Organize cabling in server rooms using patch panels for easy management.

**Physical Layout**

**Server Room Setup:**

* + Centralized in the SF office.
  + Ensure proper cooling and ventilation.
  + Implement cable management racks and trays.

**Office Layout:**

* + Position switches strategically to minimize cable lengths and ensure coverage.
  + Install wireless APs in optimal locations to ensure full Wi-Fi coverage.

**Network Diagram**

The network diagram for all three locations would show:

**San Francisco (SF Office)**

- Firewall: Cisco Firepower 2110 connects to the Internet and WAN link to NY/HO offices.

- Switches: 2 x Cisco Catalyst 9200 handles all internal connections (computers, servers, VLANs).

- Servers: Dell PowerEdge servers for DHCP, DNS, email, and file sharing.

- VLANs: Department-specific segmentation (R&D, Sales, IT, etc.).

- Wi-Fi: 2 x Cisco Meraki MR42 for wireless coverage.

**New York (NY Office)**

- Firewall: Cisco Firepower 1010 connects to the Internet and VPN tunnel to the SF office.

- Switch: Cisco Catalyst 9200 for internal connections.

- VLANs: Separate VLANs for Sales and Operations.

- Wi-Fi: 2x Cisco Meraki MR42.

**Houston (HO Office)**

- Firewall: Palo Alto PA-220 connects to the Internet and WAN link to the SF office.

- Switches: 1 x Cisco Catalyst 9200.

- VLANs: Separate VLANs for R&D, Sales, and Operations.

- Wi-Fi: 2 x Cisco Meraki MR42.

**Inter-Office Communication:**

- VPN Tunnels: Secure IPsec VPN connections between SF, NY, and HO to allow seamless, secure communication across all locations.

**Network Diagram**

A diagram of a network

Description automatically generated

**KEY COMPONENTS OF NETWORK DIAGRAM**

This network diagram represents the planned setup for Greenleaf Technologies Inc. as it expands its workforce and office locations.

**1.** **Cloud Connections**: Three clouds in the diagram are linked to each office & cloud service to support the hybrid model by using both on-premises hardware and cloud services.

**2. Routers and Switches**: There are multiple routers and Layer 3 switches to connect and manage traffic between different parts of the network and the cloud to manage routing between offices, cloud, and internal servers.

**3. PCs, Laptops, and Wireless:** PCs and laptops are connected through wired connections or wireless access points respectively providing flexibility and mobility for employees.

**4. Servers**: The diagram includes several servers to host internal services like file storage or company applications. These are connected directly to switches to ensure fast access.

**5.** **Active Directory (AD):** The AD server manages user accounts, and device permissions and only provides authorized users to access the company’s resources. That is, if an employee tries to log in, AD checks their credentials and decides if they are allowed in.

**6. DNS Server**: DNS is like the phonebook of the network—it converts easy-to-remember names (e.g.: fileserver.greenleaf.local) into the actual location (IP addresses) of servers, making it easier for employees to find what they need without remembering numbers.

**7. PKI Server**: PKI acts as the security guard for the network. PKI handles security by issuing digital certificates for secured communications over encrypted emails, secure VPN, or safe web access.

**8. Wireless and Wired Access**: The design shows both wired and wireless networks for different devices. Wireless access points are spread throughout the network, allowing laptops and mobile devices to connect.

**LAN Connectivity**

LAN connects computers and devices within each location, to facilitate communication, resource sharing, and centralized management. It is set up during initial network deployment or even when we need to expand the office space by adding more departments (when needed).

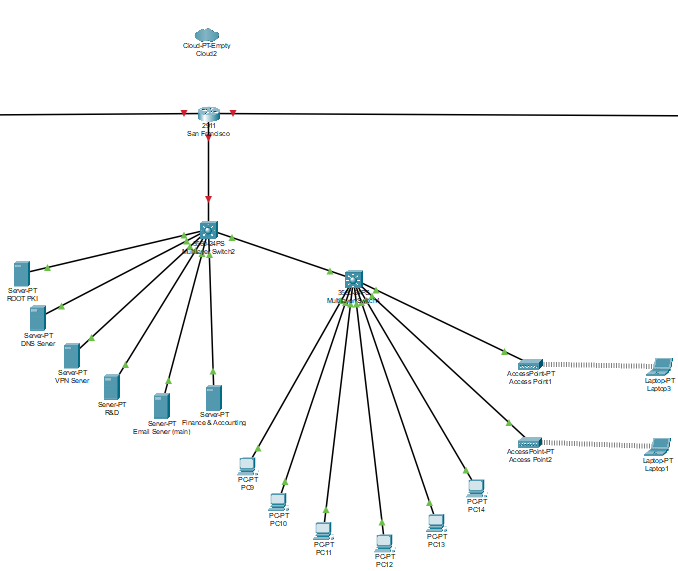
**Locations:**

* San Francisco (Headquarters): Connects multiple departments (R&D, Sales, Operation, etc.)
* New York (Operations): Supports operations-focused devices.
* Houston (R&D): Connects research and development staff and resources.

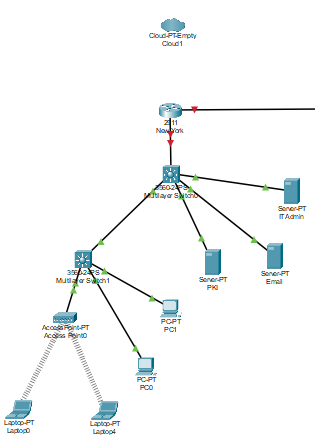
**Importance –** As we know LAN helps to provide high-speed internet connectivity for quick access to resources, enables the sharing of assets like printers and servers, reduces the need for individual internet connections (cost-effective), and segments internal traffic, allowing tighter security controls.

**Security –** We have placed switches, ethernet, VLANs, and tools to monitor and optimize LAN performance. This will ensure reliability, security, and efficiency in all locations individually.

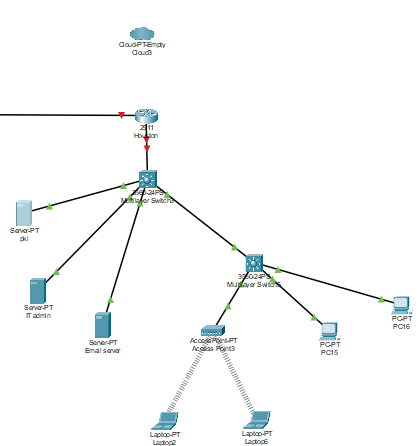
**SAN FRANCISCO (HEADQUARTERS)**



**NEW YORK**



**HOUSTON**



**WAN Connectivity**

WAN connects multiple LANs across geographically separated locations i.e. San Fransico, Houston, and New York, as per this project, allowing data and communication flow.

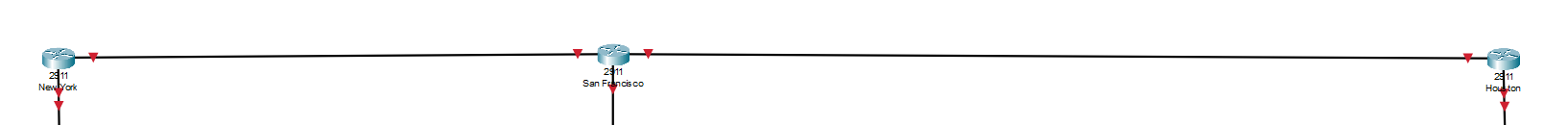
We set it up during the initial network design phase while expanding to different locations. Regular updates are made after accessing and testing the network to improve bandwidth and support new applications or increased traffic.

The central hub for WAN is San Fransisco which further connects to New York and Houston offices through which they share resources and information. This allows all locations to access centralized applications, databases, and resources maintained at the headquarters. Furthermore, this facilitates real-time communication and collaboration and ensures data and application availability across different regions.

This will need routers and dedicated WAN links, such as MPLs, and Internet VPNs, to the connected locations.

**Importance**— Implementing WAN connectivity will facilitate efficient and secure communication and enable resource sharing between geographically dispersed offices.

**Security** – VPNs are encrypted to secure data transmission over the WAN, protecting unauthorized access. Furthermore, network monitoring tools will track performance and reliability, ensuring efficient WAN operation across locations.



**3.4 Wi-Fi and Wireless Connections**

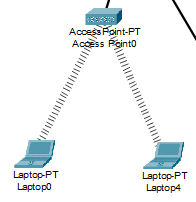
Wi-Fi and Wireless connections are essential for providing mobile and flexible network access without physical cables, facilitating connectivity for devices such as laptops, tablets, and smartphones.

Wi-Fi networks are deployed during the initial phase of designing office infrastructure or expanding office spaces. We would need to regularly update the Wi-Fi in order to enhance coverage, speed, and security, especially when new technology standards emerge (eg. Wi-Fi 6).

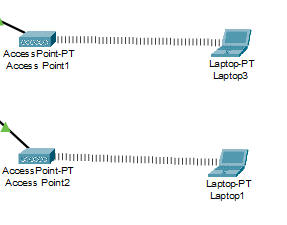
**Importance** – We will deploy access points in strategic locations to maximize coverage and minimize dead zones in all locations to ensure complete coverage. This will enable employees to work from different locations within the office without being tethered to a desk. Furthermore, this will reduce the cost of extensive cabling, lowering installation and maintenance costs.

**Security** – Separate SSIDs or VLANs should be used for guest access and internal traffic to enhance security. Implementation of WPA3 encryption and strong authentication protocols to protect the wireless network.

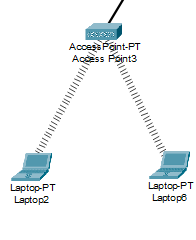
**NEW YORK**



**SAN FRANCISCO**



**HOUSTON**



**Email and Cloud Services**

These services are essential for communication, collaboration, and data storage, allowing employees to send messages and access shared resources online. These need to be deployed when centralizing communication and data storage along with periodic updates which we will need to do to new features, security enhancements, or increased usage.

As the central hub, San Fransisco will be managing email servers and cloud resources. However, the branches (New York and Houston) will access their cloud services for collaboration and email for communication and the remote users will be able to use them remotely from any location.

**Importance** – Streamlines communication and collaboration, accessibility from remote locations, and scalability are the features that are enhanced with the use of email and cloud services.

To implement email and cloud services in the project infrastructure, we will need cloud-based solutions like Microsoft 365 or Google Workspace for reliability and easy management with time collaboration tools and data storage.

**Security** – Data is protected with encryption, secure access controls, and regular backups.

A white background with black lines

Description automatically generated

**VPN**

A secure, encrypted connection over the internet that allows remote users and branch offices to access the corporate network securely.

We will be installing a VPN while connecting branch offices to the headquarters and regular updates will be made to enhance security and performance while remote connectivity is involved.

Here too, San Fransisco will control the central management of the VPN. Along with this, these will also be used in branch offices for secure access to shared resources and applications at headquarters.

**Importance** – VPN also ensures consistency at all locations and allows remote users to access the network and resources.

For this, we will need VPN software for remote users and configure VPN servers at headquarters.

**Security** – Use of strong encryption protocols like IPsec or SSL/TLS for secure data transmission. This will allow only authorized users to gather information.

**Use of WAN, LAN for Network Security**

**WAN (Wide Area Network)**

Wide Area Networks (WANs) connect geographically dispersed locations, enabling communication and data sharing. In the case of GreenLeaf Technologies, the WAN connects San Francisco, New York, and Houston.

**Wide Area Network**

**Intrusion Prevention**

**Firewalls**

**Encryption**

**DLP**

**Security Considerations for WAN Connections**

1. **Encryption:**
   * **VPN Tunnels:** Use secure VPN protocols like IPsec or OpenVPN to encrypt data transmitted over the WAN. This prevents unauthorized access and data interception.
   * **Configuration:** Configure VPN tunnels with strong encryption ciphers (e.g., AES-256) and authentication mechanisms.

**How VPN Tunnels Work**

1. **Authentication:** When a user attempts to connect to the VPN, they are prompted for credentials (username/password or other authentication factors).
2. **Encryption:** Once authenticated, the VPN client establishes a secure tunnel with the VPN server. All data transmitted through this tunnel is encrypted using a strong encryption algorithm (like AES-256).
3. **Data Transmission:** Encrypted data is transmitted over the public network, making it difficult for unauthorized parties to intercept or understand.
4. **Decryption:** Upon reaching the destination network, the VPN server decrypts the data, allowing it to be accessed by authorized users.

**Benefits of VPN Tunnels**

* **Security:** Protects data from unauthorized access and eavesdropping.
* **Remote Access:** Enables employees to securely connect to the corporate network from remote locations.
* **Site-to-Site Connections:** Can be used to connect multiple office locations securely.

**VPN Protocols**

* **IPsec:** A widely used standard for VPN tunnels, offering strong security features and interoperability.
* **OpenVPN:** An open-source VPN protocol known for its flexibility and ease of use.

**In the context of GreenLeaf Technologies, VPN tunnels can be used to:**

* **Connect remote employees:** It will allow employees in New York and Houston to securely access the corporate network.
* **Connect between offices:** It will establish secure connections between the San Francisco, New York, and Houston offices for data sharing and collaboration.
* **Protect sensitive data:** Encrypt data transmitted over the WAN to prevent unauthorized access.

**FIREWALLS**

**Firewalls** act as a security barrier between a network and an external network (like the internet). They examine network traffic and filter packets based on predefined rules, blocking unauthorized access and malicious attempts.

**Firewalls:** Cisco ASA, Palo Alto Networks Next-Generation Firewall and Fortinet FortiGate

**Firewall Placement**

* **Boundary Firewalls:** Deploy firewalls at the network perimeter of each location (San Francisco, New York, Houston). This allows them to control traffic entering and exiting the network.

**Firewall Configuration**

1. **Rule Creation:** Define rules to specify which traffic is allowed or blocked. These rules can be based on factors like:

**Specific Locations:**

* **San Francisco:** Deployed a firewall at the connection point between the internal network and the internet connection.
* **New York:** Placed a firewall at the network boundary to protect the New York office from external threats.
* **Houston:** Implement a firewall at the Houston office's internet connection point.
  + **Source and destination IP addresses:** Control traffic based on the source and destination networks.
  + **Ports:** Allow or block traffic on specific ports (e.g., HTTP, HTTPS, FTP).
  + **Protocols:** Specify protocols (TCP, UDP, ICMP) to allow or block.
  + **Applications:** Control traffic for specific applications (e.g., web browsing, email).

1. **Default Deny:** Implemented a "default deny" policy, which blocks all traffic that doesn't explicitly match an allow rule.
2. **Logging:** Enabled logging to monitor firewall activity and identify potential security incidents.

**Firewall Rules for GreenLeaf Technologies**

* **Inbound Traffic:**
  + Allow incoming traffic from authorized external networks (e.g., VPN connections, business partners).
  + Block traffic from known malicious IP addresses or networks.
  + Restrict incoming traffic to specific ports used by legitimate applications.
* **Outbound Traffic:**
  + Allow outbound traffic to authorized destinations (e.g., internet, cloud services).
  + Block outbound traffic to known malicious destinations or for unauthorized applications.
  + Implement rate limiting to prevent excessive outbound traffic.

**Firewall Rule Configuration**

* **Rule Sets:**
  + **Location:** Configure firewall rules at the network perimeter devices (e.g., routers, firewalls).
  + **Granularity:** Create specific rules to allow or block traffic based on source/destination IP addresses, ports, protocols, and applications.
  + **Examples:**
    - Allow incoming traffic from authorized VPN connections and known business partners.
    - Restrict incoming traffic to specific ports used by legitimate applications.
    - Allow outbound traffic to authorized destinations (e.g., internet, cloud services).
    - Block outbound traffic to known malicious destinations or for unauthorized applications.

**Intrusion Prevention**

* **Location:** Enable intrusion prevention features within firewalls or dedicated IPS devices.
* **Configuration:**
  + **Signature-Based Detection:** Use pre-defined signatures to detect known attack patterns.
  + **Anomaly Detection:** Monitor network traffic for unusual behavior that might indicate an attack.
  + **Response Actions:** Configure the IPS to take actions like blocking traffic, logging alerts, or resetting connections.

**Data Loss Prevention (DLP)**

* **Data Classification:**
  + Classify data based on sensitivity levels (e.g., confidential, proprietary, public).
  + Tag or label data accordingly.
* **DLP Solutions:** Deploy DLP solutions at network gateways, endpoints, and cloud environments.
* **Rule Configuration:** Define rules to detect and block actions like:
  + Unauthorized data transfers (e.g., copying sensitive files to USB drives)
  + Sensitive data being sent to unauthorized recipients
  + Violations of data privacy regulations

**3.5 Dynamic Host Configuration Protocol (DHCP)**

DHCP plays a crucial role in automating the assignment of IP addresses across the organization's network, ensuring efficient connectivity for all devices in the San Francisco headquarters and branch offices in New York and Houston. By dynamically allocating IP addresses, DHCP minimizes manual configuration errors and enhances operational efficiency, particularly important as the company scales from 165 to 300 employees. Additionally, local DHCP servers in each branch provide redundancy, reduce latency in IP address assignment, and support network segmentation, thereby improving overall security and management of the expanding network infrastructure.

Here main reasons for needing DHCP in the GreenLeaf Technologies Inc. project:

* **Automated IP Management**: DHCP automatically assigns IP addresses to devices, reducing the need for manual configuration.
* **Efficiency and Time Savings**: It speeds up the process of connecting new devices to the network, minimizing the risk of errors.
* **Centralized Control**: DHCP provides centralized management of IP address allocations across multiple locations.
* **Scalability**: As GreenLeaf expands, DHCP allows for easy integration of new devices without complicated setups.
* **Dynamic IP Allocation**: Devices can receive new IP addresses as needed, facilitating mobility and remote access for employees.
* **Conflict Prevention**: It helps prevent IP address conflicts, ensuring reliable network connectivity for all devices.

A screenshot of a computer

Description automatically generated

**DHCP Setup for GreenLeaf Technologies Inc.**

Dynamic Host Configuration Protocol (DHCP) automates IP address assignment within the network, ensuring devices receive IP addresses without manual configuration.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | **San Francisco** |  |  |
| **VLAN** | **Description** | **IP Address Range** | **Subnet Mask** | **Default Gateway** |
| 10 | R&D | 10.0.10.1 - 10.0.10.254 | 255.255.255.0 | 10.0.10.1 |
| 20 | Sales & Marketing | 10.0.20.1 - 10.0.20.254 | 255.255.255.0 | 10.0.20.1 |
| 30 | Operations | 10.0.30.1 - 10.0.30.254 | 255.255.255.0 | 10.0.30.1 |
| 40 | IT & Support | 10.0.40.1 - 10.0.40.254 | 255.255.255.0 | 10.0.40.1 |
| 50 | HR | 10.0.50.1 - 10.0.40.254 | 255.255.255.0 | 10.0.50.1 |
| 60 | Finance & Accounting | 10.0.60.1 - 10.0.40.254 | 255.255.255.0 | 10.0.60.1 |
|  |  |  |  |  |
|  |  | **New York (Operations)** |  |  |
| **VLAN** | **Description** | **IP Address Range** | **Subnet Mask** | **Default Gateway** |
| 70 | Operations | 10.0.70.1 - 10.0.70.254 | 255.255.255.0 | 10.0.70.1 |
|  |  |  |  |  |
|  |  | **Houston (R&D)** |  |  |
| **VLAN** | **Description** | **IP Address Range** | **Subnet Mask** | **Default Gateway** |
| 80 | R&D | 10.0.80.1 - 10.0.80.254 | 255.255.255.0 | 10.0.80.1 |

Having DHCP functionality in each branch ensures efficient, reliable, and secure network operations across all locations.

**Steps to Implement DHCP**

1. **Server Selection**:
   * Choose a dedicated server (physical or virtual) to run the DHCP service.
   * Ensure the server has adequate resources and is connected to the network.
2. **Install DHCP Server Software**:
   * Install DHCP server software (e.g., Windows Server DHCP role, ISC DHCP for Linux) on the chosen server.
3. **Configure DHCP Scopes**:
   * Define DHCP scopes for each location and VLAN:
     + Set IP address ranges
     + Exclude reserved IP addresses for static devices like servers.
4. **Set Lease Duration**:
   * Determine lease times based on device types:
     + Shorter leases for mobile devices.
     + Longer leases for desktops.
5. **Configure DHCP Options**:
   * Set options for default gateway (router IP), DNS servers, and other essential network information.
6. **Enable DHCP Relay (If needed)**:
   * In branch locations, set up DHCP relay agents on routers to forward requests back to the main DHCP server.
7. **Implement Security Measures**:
   * Enable DHCP snooping on network switches to prevent rogue servers.
   * Set up access control lists (ACLs) to restrict access to the DHCP server.
8. **Testing**:
   * Test the DHCP configuration by connecting devices and checking if they receive the correct IP addresses.
   * Verify network connectivity and check DHCP logs for errors.
9. **Monitoring and Maintenance**:
   * Regularly monitor DHCP logs for issues and performance.
   * Adjust scopes, options, and leases as needed, especially during growth phases.

This setup ensures efficient IP distribution across all GreenLeaf locations, supporting growth and operational efficiency.

**DHCP in Other Branches**

1. **Local Traffic Management**: Reduces latency by providing quicker responses to IP requests.
2. **Redundancy**: Ensures IP address assignment continues if the connection to the main office fails.
3. **Independent Operation**: Allows branches to manage their own devices without relying on centralized services.
4. **Load Balancing**: Distributes DHCP requests across servers to reduce the load on the main server.
5. **Network Segmentation**: Supports specific configurations for unique VLANs or address ranges at each location.
6. **Enhanced Security**: Enforces branch-specific security policies for better protection.

Overall, branches will enhance the DHCP network's performance, redundancy, and security while ensuring each location can operate effectively and independently.

**SECURITY MEASURES**

To servers at both headquarters and branch locations, implement the following measures:

1. **DHCP Snooping**: Prevent unauthorized DHCP servers by enabling DHCP snooping on switches.
2. **Access Control Lists (ACLs)**: Restrict DHCP traffic to trusted devices and networks.
3. **Network Segmentation**: Isolate DHCP servers in a secure VLAN to enhance security.
4. **Network Access Control (NAC)**: Ensure only authorized devices can connect and request IP addresses.
5. **Regular Updates**: Keep DHCP server software up to date to address vulnerabilities.
6. **Logging and Monitoring**: Track requests and monitor for suspicious activity.

**3.6 Domain Name System (DNS)**

The DNS (Domain Name System) in GreenLeaf Technologies Inc.'s network, spanning **San Francisco (SF)**, **New York (NY)**, and **Houston (HO)**, will be structured and managed to ensure efficient name resolution, redundancy, and fault tolerance across all three locations. And most importantly we will place a **single DNS server per location** Here’s how it will function:

**1. Distributed DNS Server in San Francisco (SF)**

* **Location**: San Francisco hosts the primary DNS server (Windows Server 2016).
* **Primary Role**: The DNS server in SF will handle **name resolution** for internal network services and external domains. It is responsible for translating domain names (like www.greenleaf.com) into IP addresses used by devices across the network.
* **Implementation**:
  + The DNS server is centralized in SF, allowing it to manage DNS records for all internal resources, such as file servers, email servers, and web servers.
  + It will be configured with **forward lookup zones** for internal domains and may use **DNS forwarding** to external DNS providers for external domain queries (e.g., public websites).A screenshot of a computer

    Description automatically generated
  + **Redundancy** will be ensured by setting up secondary DNS servers in NY and HO to handle requests if the primary DNS in SF fails.

**Most importantly why we are using distributed DNS?**

**Ans: Geographical Distribution:**

* The company operates in three geographically distant locations: San Francisco, New York, and Houston. A distributed DNS setup would allow each office to have its own DNS server, reducing latency and improving performance for employees at each site.

1. **DNS Replication and Secondary Servers in NY and HO**

We will be using **2-way replication.** Because of the following reason:

* **Multiple Update Locations**: With a two-way replication setup, both primary and secondary DNS servers can accept updates. This flexibility is important for organizations like Greenleaf that may have multiple departments or teams needing the ability to make DNS changes from different locations (e.g., San Francisco, New York, and Houston).
* **Local Changes**: If a specific office needs to make a DNS change, it can do so on its local server without waiting for updates from a centralized location. This can be particularly useful in situations where the network is distributed.
* **Synchronization:** For Greenleaf Technologies, a **two-way DNS** replication strategy is recommended across its three locations—San Francisco (SF), New York (NY), and Houston (HO)—to ensure that DNS records are synchronized efficiently and reliably. This setup allows DNS servers in each office to accept updates, facilitating quick local changes and improving redundancy; if one server fails, the others can continue to serve DNS queries without interruption. By deploying **Active Directory Integrated Zones** for Windows DNS or using secure zone transfers for BIND, Greenleaf can maintain consistent and up-to-date DNS records across all locations, ultimately enhancing performance and reliability for its expanding workforce and customer base.
* **New York (NY)** and **Houston (HO)** will both have secondary DNS servers, replicating the DNS zones from SF.

**Purpose**:

* + These secondary servers will ensure that each location can resolve internal and external domain names without always relying on SF, reducing latency and dependency on a single point of failure.
  + In case of **network issues** or **SF server downtime**, NY and HO will continue to have access to up-to-date DNS records for internal name resolution through the **replicated zones**.

**3. DNS Queries and Resolution Flow**

* **Internal Queries**: When a device in any office (SF, NY, or HO) needs to resolve an internal domain (like file.greenleaf.local):
  + The request is first sent to the **local DNS server** (primary in SF, secondary in NY/HO).
  + If the DNS server has the record, it responds with the IP address.
  + If the record is not found, the query will be forwarded to the **primary DNS in SF** (if the local server is a secondary DNS).
* **External Queries**: For public domains (e.g., www.google.com):
  + The DNS server forwards the query to external DNS resolvers (such as Google DNS or the ISP's DNS) to resolve public domain names.

**4. DNS Redundancy and Load Distribution**

* **Primary-Secondary Setup**:
  + **Primary DNS** in SF will have full read/write access to DNS records, handling updates, deletions, and additions of internal DNS records.
  + **Secondary DNS** servers in NY and HO will receive **zone transfers** from SF, ensuring consistency across all locations. They act as read-only copies for internal domain queries.
* **Failover Mechanism**:
  + If the primary DNS server in SF fails, NY and HO will continue to resolve internal DNS queries using their secondary servers.
  + This provides resilience in the network by preventing **service disruption** in case the SF office experiences downtime.

**5. DNS Security**

* **DNSSEC (DNS Security Extensions) Implementation:**
* **SF:** The primary DNS server for the organization is in San Francisco, where most of the network infrastructure, including servers and workstations, reside. Implementing DNSSEC at this location will protect DNS queries from being tampered with, ensuring that domain name resolutions for both internal and external services are secured. The DNSSEC protocol will add a layer of cryptographic signatures to verify that DNS responses haven't been altered.
* **NY and HO:** These locations will rely on the central DNS in SF but could have local DNS caching servers to reduce latency. Implementing DNSSEC across all locations ensures that DNS responses passed between locations are authenticated and secured, mitigating the risk of DNS spoofing or cache poisoning attacks.
* **Access Control for DNS Record Updates**
* **SF**: Given that the main DNS server is housed in San Francisco, implementing strict access control mechanisms here is crucial. Only authorized devices and personnel from the IT department should have the ability to update DNS records. This will prevent unauthorized modifications, ensuring that rogue devices or attackers cannot introduce malicious DNS entries. Access control policies can be enforced via network access control (NAC) and role-based access control (RBAC).
* **NY and HO**: Though these offices may not house primary DNS servers, ensuring access control over DNS services (such as local DNS caching or internal DNS services) is still important. Limiting who can access and modify DNS settings in these locations reduces the chance of an insider threat or a compromised device altering DNS configurations maliciously.

**6. DNS Load Balancing**

* **Geographical Distribution**: DNS queries from NY and HO can be directed to their **local secondary servers** first to reduce latency, only querying the SF DNS server if necessary.
* **Performance Optimization**: This setup will ensure faster internal name resolution across the company’s distributed offices, reducing potential network traffic and improving response times for DNS lookups.

**Small diagram which illustrates how DNS will work in all three locations:**

A diagram of a server

Description automatically generated

Furthermore, we have chosen to migrate **DNS** to **Azure Cloud**:

**Why Migrate DNS to Azure Cloud**

1. **Scalability**:
   * Azure DNS automatically scales to handle increased queries, suitable for a growing workforce and customer base.
2. **High Availability**:
   * Built-in redundancy ensures minimal downtime, critical for GreenLeaf's multi-location operations.
3. **Integration:**
   * Seamless integration with other Azure services (e.g., Azure VMs, VNets).
4. **Cost Efficiency**:
   * Reduce on-premises hardware maintenance costs by leveraging Azure’s pay-as-you-go model.
5. **Security:**
   * DNSSEC prevents spoofing and man-in-the-middle attacks.
   * Role-based access control (RBAC) in Azure ensures only authorized changes are made.
6. **Performance:**
   * Azure’s globally distributed DNS infrastructure offers low-latency responses.

**When to Migrate DNS to Azure Cloud**

1. **Company Growth:**
   * As GreenLeaf scales from 165 to 300 employees, a scalable DNS infrastructure ensures reliability.
2. **Hybrid Cloud Adoption:**
   * With plans to integrate on-premises and Azure resources, DNS on Azure streamlines name resolution.
3. **Redundancy and Disaster Recovery**:
   * Azure DNS provides high availability and geo-redundancy, crucial for disaster recovery.
4. **Operational Efficiency:**
   * Outdated DNS servers in the current setup make Azure migration timely.
5. **Security Enhancements:**
   * Features like DNSSEC in Azure secure DNS traffic.

**How to Migrate DNS to Azure Cloud**

1. **Planning**:
   * **Assess Current DNS Setup**: Review DNS servers (Windows Server 2016 in San Francisco, New York, and Houston).
   * **Identify Critical Zones**: Determine which DNS zones (internal and external) need migration.
   * **Choose Azure DNS**:
     + **Public DNS**: For external domains.
     + **Private DNS**: For internal resources and name resolution across Azure VNets.
2. **Prepare Azure DNS**:
   * **Create DNS Zones**: Set up corresponding zones in Azure DNS.
   * **Configure Virtual Networks**: For private DNS zones, ensure Azure VNets align with internal subnets.
   * **Set Up Forwarders**: Configure Azure DNS to forward external queries to public resolvers.
3. **Migration Process:**
   * Export current DNS zone data from on-premises servers.
   * Import zone data into Azure DNS using tools like PowerShell or Azure Portal.
   * Test zone integrity and ensure all records are present and functional.
4. **Hybrid Integration (Optional):**
   * Use **Azure DNS Private Resolver** for hybrid setups to resolve names between on-premises and Azure environments.
5. **Cutover:**
   * Change authoritative nameservers for external zones to Azure DNS nameservers.
   * Update internal configurations to use Azure DNS for resolution.
6. **Testing & Validation:**
   * Verify name resolution for all domains.
   * Test failover scenarios and monitor performance.

**3.7 Active Directory (AD)**

Active Directory Design for GreenLeaf Technologies Inc.

In this project, GreenLeaf Technologies Inc., Active Directory provide solutions for user authentication, authorization, and management across every location (San Francisco (SF) HQ, New York (NY), and Houston (HO)). As the business is expanding from 165 to 300 employees, AD is using efficient procedures for handling user credentials, security policies, and permissions. Although, it supports scalability, centralizes access control, and generates security through features such as Group Policy, role-based access, and authentication across the network infrastructure.

Given GreenLeaf Technologies’ scale requirements and expansion, a **Hybrid Active Directory model** would be recommended as it is quite suitable for organizations. The model will combine on-premises AD for internal services, which is important for compliance, latency-sensitive operations and security as well. Hence, this model integrates on-premises Active Directory with Azure Active Directory (Azure AD) which allows scalability, cloud services, and secure remote access for remote users.

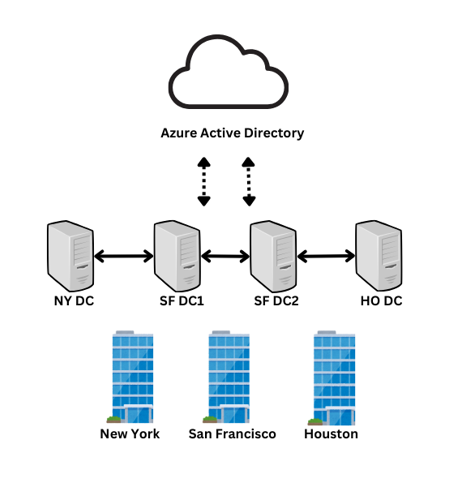
1. **Active Directory Server Design:**

* **Domain Controllers:** San Francisco will act as *Domain Controller 1* **(DC1)** (main data centre for authentication), and on the other hand, *Domain Controller 2* **(DC2)** (for redundancy and failover).
* **Sub-Domains:** For local authentication, redundancy, file sharing, and reducing latency, both offices in New York (NY) and Houston (HO) are working as sub-domains (ADC) (Additional Domain Controllers).

1. **Servers for Active Directory Setup:**

* **San Francisco (SF) HQ:** San Francisco (HQ) includes Domain Controller 1 and Domain Controller 2 for backup.
* **New York (NY) (Sub Domain):** 1 Additional Domain Controller (ADC) (Windows Server 2022).
* **Houston (HO) (Sub Domain):** 1 Additional Domain Controller (ADC) (Windows Server 2022).

The Image below illustrates the intended diagram:



Positioning Domain Controller:

* **San Francisco (HQ):** The DC1 & DC2 will enclose at the Headquarters (HQ). This server will handle the larger part of authentication and account management for the continuous organization. However, these Domain Controllers will hold FSMO (Flexible Single Master Operations) roles **(RID, PDC Emulator, Infrastructure Master, Schema Master, and Domain Naming Master)**.
* **New York (NY):** This site has its own Domain Controller to reduce authentication latency, ensuring local requests are managed without burdening the headquarters.
* **Houston (HO):** In a similar manner, Houston will have one Domain Controller to manage local traffic.
* **LOCATION:** For NY and HO, in each office’s respective data centre, secured within VLAN 20 and 30 for AD services.

A screenshot of a computer

Description automatically generated

Sites are designed to manage network load efficiently. However, it performs replication between Domain controllers that are geographically separated.

Sales Team: It is a Remote users’ team, in which users will authenticate through Azure AD. This framework allows secure, remote access to internal resources via VPN or conditional access policies in Azure.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Location | Server Role | FSMO Roles | Operating System | VLAN Assign | Purpose | Other Configuration |
| San Francisco  (HQ) | Domain Controller 1 (DC 1) | RID Master, PDC Emulator | Windows Server 2022 | VLAN 10 | Main data centre for authentication and account management | Azure connected in Active Mode |
| San Francisco (HQ) | Domain Controller 2 (DC 2) | Schema Master, Domain Naming Master, Infrastructure Master | Windows Server 2022 | VLAN 10 | Redundancy and failover for DC 1 | Azure AD connected in staging mode |
| New York (NY) | Additional Domain Controller (ADC) | None | Windows Server 2022 | VLAN 20 | Handles local authentication and reduces latency | Read Only Domain Controller (RODC) |
| Houston (HO) | Additional Domain Controller (ADC) | None | Windows Server 2022 | VLAN 30 | Handles local authentication and reduces latency | Read Only Domain Controller (RODC) |

The given table outlines the Active Directory structure across multiple sites, detailing the distribution of roles, redundancy measures, network configuration, and cloud integration to ensure high-level security, efficient authentication, and streamlined management of resources across its expanding locations.

To synchronize the on-premises Active Directory (AD) infrastructure described in the table with Azure Active Directory Domain Services (Azure AD DS):

1. **San Francisco (Headquarter)- DC -1:** This DC will carry RID Master and PDC Emulator roles that are very important for handling domain-wide duties like object identifiers and Time synchronization. However, this DC is connected in Active Mode to Azure AD, so it constantly syncs charges to Azure AD such as user accounts, group policies, etc. Azure AD Connect is used to sync the on-premises user directory and credential information with Azure AD, ensuring that user data is consistent across both places.
2. **San Francisco (Headquarter)-DC-2:** It carries Schema Master, Domain Naming Master, and Infrastructure Master features, ensuring that overall AD schema and domain structure are well maintained. Moreover, for Azure connection, Connected to Azure AD in staging mode, means, DC acts as a failover for DC 1’s connection. If DC 1 goes offline, DC2 will take over the responsibilities of Azure AD. This ensures a high availability of synchronization.
3. **New York and Houston (ADCs) (Additional Domain Controllers):**
4. These are Read-Only Domain Controllers (RODC), as they hold a read-only copy of the AD. They are also used for local authentication to reduce latency but also not to make any variations to the AD database directly.
5. Azure AD Sync: Since RODCs do not write changes, they do not synchronize directly to Azure AD. Instead changes in AD database come from writable DCs such as DC1 and DC2 in San Francisco. Any updates made at HQ will be synced to Azure AD, and then those changes are reflected in RODCs for local authentication.

**Synchronization Process for Azure AD:**

Azure AD Connect: this tool is configured on DC1 **(Primary)** and DC2 **(in staging mode)**, to continuously sync on-premises AD with Azure AD, such as User accounts, Groups and Memberships, Password hashes for SSO and Azure-based services, and security policies. However, by default, Azure AD Connect syncs changes every 30 minutes, but this can be customized depending on the company’s needs.

**Replication setup:**

Type of Replication: Multi-master replication using the Knowledge Consistency Checker (KCC).

Sites and Services Configuration:

Hub-and-spoke topology: The DC 1 in San Francisco acts as the hub, while New York and Houston DCs are spokes. Any updates and changes for an account are initiated in the SF centre and spread to all other sites.

Replication occurs intra-site every 15 minutes within the same location, and inter-site every 3 hours between locations using IP-based replication.

Site Links: A VPN tunnel will be used for inter-office replication between San Francisco (SF), New York (NY), and Houston (HO). The tunnel will protect the replication traffic.

**VLAN for AD Design:**

* Increasing security, a dedicated VLAN for AD services will be created.
* VLAN will keep apart the AD services from other network traffic, ensuing that only authorized devices can interact with the Domain Controllers.

San Francisco (HQ): VLAN 10 (AD Traffic)

New York (NY): VLAN 20 (Sub-domain AD traffic)

Houston (HO): VLAN 30 (Sub-domain AD traffic)

All network traffic within these VLANs will be kept under control by firewall rules to prevent unauthorized access.

**Security arrangement for AD Servers:**

1. **Physical Security:**

* All servers will be bound in the secure server room in each office with biometric access controls.
* Servers will have UPS systems and Redundant cooling systems to protect against power failures or overheating.

1. **Network security:**

* IPsec is used for security purposes, and for secure communication between Domain Controllers across sites.
* Firewalls: Firewalls will be deployed to secure access between the AD network and other subnets. Each location will have a firewall with rules to avoid unauthorized access/traffic from reaching the Domain Controllers.
* Network Access Control (NAC): To limit down network approach only to authorized devices within the AD VLAN.
* Monitoring: Executing security monitoring with an Intrusion Detection System (IDS) and Security Information and Event Management (SIEM) to track unusual activities and prevent breaches, and any brute-force attacks.

**Server Location:** All the Domain Controllers (DCs), DNS, and DHCP servers will be in a dedicated server room at the HQ, providing climate control, biometric access, and redundant power supplies to ensure uninterrupted operation. For this, we can implement some security measures for Active Directory such as Multifactor Authentication (MFA), Group Policy Objects (GPOs), Regular Patching, and Continual Backup.

* MFA: Azure AD MFA will help users authenticate, especially for remote and high-privilege users.
* GPOs: Strict GPOs will impose security guidelines like increase password complexity, account lockout and software restrictions.
* Regular Patching: Regularly upgrade AD servers with security patches and monitor for vulnerabilities.
* Backups: A powerful backup system will be in place to back up AD data both on-premises and in the cloud to recover from potential data leakage.

**For Backup and Disaster Recovery (DR):** As AD is analytical to the company’s operations, a strong backup and disaster recovery plan is necessary to implement.

**Backup Strategy:** Execute daily backups for AD and store in both on-premises storage and Azure Backup, ensuring the ability to restore information in case of data corruption.

**Disaster Recovery:** In case of catastrophic failure, the whole AD setup can be put back either to new on-premises infrastructure or completely in Azure, allowing the companies to keep going with business continuity.

**3.8 Disaster Recovery (DR)**

Disaster Recovery (DR) encompasses the strategies and processes necessary for restoring operations promptly after any disruption, such as cyberattacks, hardware failures, or other unforeseen events. A tailored approach is essential for each operational office to ensure minimal downtime and continuity of services.

**San Francisco (HQ)**

**Role**: The central hub for critical servers, including DNS, DHCP, email, and file servers.

**Backup & Replication**: Implement regular backups of critical data locally and in the cloud, utilizing Azure Backup. Establish replication of all essential servers to an offsite or cloud-based environment to ensure rapid recovery.

**Failover Mechanism:** Implement robust failover solutions for critical services to guarantee uninterrupted operations during server failures.

**New York Office**

**Role**: Key operational center that relies on services hosted in the headquarters San Fransico.

**VPN Backup**: Establish backup VPN tunnels to ensure continuous connectivity in case of primary connection failures.

**Local Redundancy:** Maintain local backups for essential departmental data, with replication to Azure Cloud for additional recovery assurance.

**Houston Office**

**Role**: Focused on Research & Development (R&D) and requires high availability for innovative projects.

**Cloud-based DR**: Implement cloud based disaster recovery solutions, such as Azure Site Recovery, to replicate research data and systems securely.

**Data Preservation**: Ensure daily backups of critical data are stored in multiple locations, with appropriate measures in place to protect sensitive information.

**Cross Location Strategies**

**Geographical Replication**: Ensure data from the HQ is replicated to both operational offices, enabling them to serve as recovery locations for one another through cloud solutions.

**Regular DR Drills:** Conduct periodic disaster recovery drills to simulate failures, test recovery procedures, and ensure employee readiness.

**3.9 Risk Management**

Risk Management involves identifying, assessing, and mitigating potential risks across all locations. Each site will have a tailored strategy to address physical and cybersecurity risks.

**San Francisco (HQ)**

**Cybersecurity Risks**: Implement robust firewalls and Intrusion Prevention Systems (IPS) to guard against unauthorized access.

**Physical Risks:** Ensure critical systems are equipped with uninterruptible power supplies (UPS) and backup generators for continuous operations.

**Vendor Management:** Partner with trusted vendors to guarantee the reliability and security of critical infrastructure.

**New York Office**

**Cybersecurity Risks:** Focus on remote access control and VPN security, utilizing strong encryption for data in transit and enforcing multifactor authentication (MFA).

**Downtime Risks:** Mitigate the impact of potential connectivity losses with backup VPNs or software defined WAN (SDWAN) solutions.

**Houston Office**

**Cybersecurity Risks:** Protect sensitive research data with encryption and role-based access control (RBAC).

**Data Integrity:** Regularly backup data to offsite locations to preserve the integrity of critical information.