**ITOP 2310 - Industry Capstone Project (CRN 12095)**

**Designing Green Leaf IT Security**



*BY – Abhinav, Sanmeet, Pulkit & Tara*

**Table of Content:**

[**1 Project Overview**](#_1._Project_Summary)

[**2 Public Key Infrastructure**](#_2._PKI_(Public)

[**3 Risks**](#_3_Risks:)

[**4 Network Design**](#_4_Network_Infrastructure)

[**4.1 Network Digram**](#_4.1_Network_Diagram:)

[**4.2 Network Segmentation**](#_4.2_Network_Segmentation)

[**4.3 Network Devices**](#_4.3_Network_Devices)

[**5 DHCP**](#_5_DHCP_#)

[**6 DNS**](#_6._DNS)

[**7 Active Directory**](#_7._Active_Directory )

[**8.1 Network Security**](#_ _8._Network)

[**8.2 Wi-Fi**](#_8.2_Wireless_Infrastructure)

[**9 Device Management**](#_9_Device_Management)

[**9.1 SCCM**](#_9.1SCCM)

[**9.2 Intune**](#_9.2_Microsoft_Intune)

[**10 SysLog Server**](#_10_Syslog_Server)

[**11 Cloud**](#_11Cloud_)

## 1. Project Summary

In this project we are going to design a network infrastructure which make this company’s security better and their network more scalable and feasible and in between we are doing penetration testing and vulnerability assessment which helps the company to find the security flaws and they can find the better solutions to prevent from risk and threats .moreover we monitor the network to detect potential security incidents and we develop the procedures and solutions to make it more better . in this We are finding the connectivity, review all policies of the company to know the procedures and application ongoing in a company.

This all begins with thorough assessment, identifying risks, threats, and potential consequences of security breaches. The design phase includes evaluating the current network architecture, incorporating cloud-based resources, and planning for scalability. A strengths and weaknesses analysis covers security, performance, manageability, and cost. The prototype network setup is tested for feasibility and security measures, followed by penetration testing and vulnerability assessment. The existing network is improved based on findings, and recommended equipment is assessed for requirements, redundancy, and scalability. Documentation and training ensure a well-documented, secure, and efficiently managed network. In this project, it concludes with a presentation to stakeholders and the establishment of continuous monitoring for ongoing security and performance reviews.

## 2. PKI (Public Key Infrastructure)

GreenLeaf Technologies has three offices, Head office in San Francisco, California, and branch offices in the New York city and Houston Texas.

The company is using

* Web Servers
* Email Servers
* Active Directory
* File Severs
* Remote Access

So, keeping this in mind, a public key infrastructure will require

**2 Tier CA hierarchy,** Root CA will be implemented in the Main office and will be in offline state. And we will set up 3 issuing CA separated among the three different offices. For redundancy and easy of management

**Green Leaf PKI Solution:**

|  |  |
| --- | --- |
| **PKI Tier Hierarchy** | 2 Tier CA hierarchy |
| **PKI Key Infrastructure Services** | Windows PKI Services |
| **Root CA Name** | GL\_RootCA |
| **Root CA Location** | San Franciso |
| **Root CA Private Key Length** | 4096 bits |
| **Root CA Private Key Storage** | HSM (Hardware Security Module) |
| **Root CA certificate Expiry** | 10 Years |
| **No of Issuing CAs** | 3 |
| **Issuing CA Names** | GL\_SF\_CA, GL\_NY\_CA, GL\_HO\_CA |
| **Issuing CA Locations** | San Fransico, New York, Houston |
| **Issuing CA Private Key Length** | 4096 bits |
| **Issuing CA certificate Expiry** | 2 Years |
| **Templates** | * Webservices * File Encryption * User Authentication * Email Services |

**Windows Public key infrastructure:** We will use the Microsoft CA services as they can work very closely with Active directory and we can take advantage of the Microsoft services, group policy for easy deployment and automated certificate revocation etc.

**Windows Server 2016:** Company is already using the Windows server 2016, So we can just move on with this version, for easier deployment and management

**Private key storage:** It is best if we use HSM (Hardware security Module) for storing private keys. And escrow the private key as backup to one of branch office in HSM, For any extreme situation

**Templates:** We will use webservices, File encryption, User authentication, Email Server certificate templates.

**Separation of duties:** After implementation we will follow the principle of least privilege for the security of the public key infrastructure. We will assign separate admin for the PKI management; A different admin will perform the certificate revocation and issuing etc.

**Configuration for root CA and Issuing CA**

**Root CA: Root** CA will be in power off state, and only needed to be brough online when required. Private key length will be 4096 bit and key will be stored in HSM and backup key will be stored in one its branch office in HSM. Certificate expiry date will be 10 years as we do not want the certificate to expire early, as if the certificate expires after the valid period entire infrastructure will go down. CA will be named Green Leaf Root CA.

**Issuing CAs: We** will set up an Issuing CA in every office for redundancy and for easy management of the PKI. Private keys will be stored in the software and the key length will still be 4096 bits. CA certificate expiry date will be 10 years. Certificates issued by the issuing CA will have an expiry date of 2 years. Issuing CA will be named after the offices they are placed in

**Implementation of PKI in the Company.**

**Transport Layer Security:** Certificates will be used to protect HTTP traffic from the web servers, FTP Traffic from the File Servers. We will also implement the PKI to protect DC LDAP Traffic.

**File Encryption: All** the hard drives whether it is the server, Laptops or computers will have file encryption enabled using the Certificates and Recovery certificates will also be generated to recover the encrypted files.

**Email Services: All** the companies inside email traffic will be done using the PKI. We will use the certificates to protect the emails being exchanged using SMIME protocol.

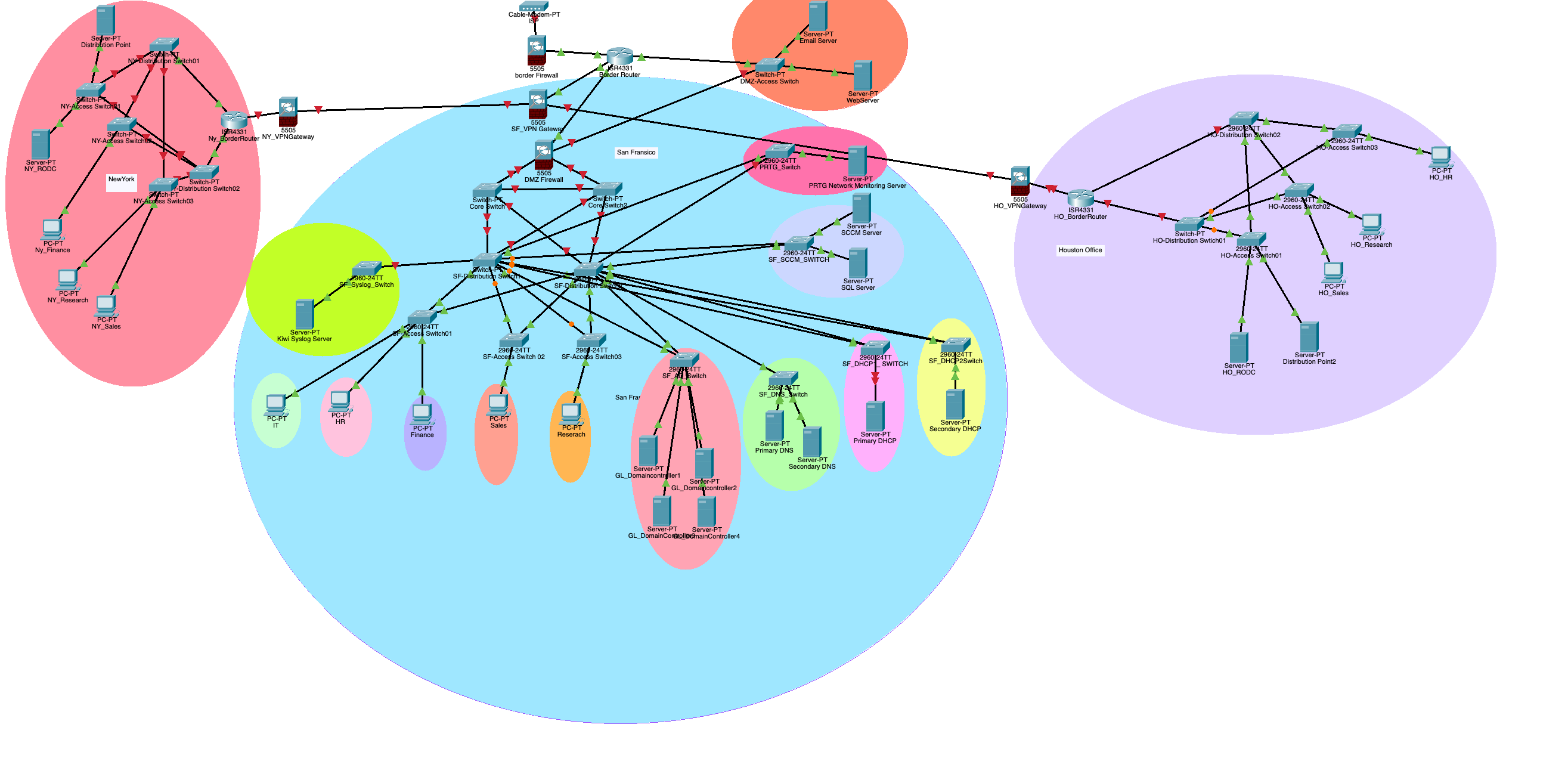
VPN: A user will need to present the certificate to access the company's VPN. As a type of authentication

## 3 Risks:

* **Failures and Interruptions:** Current Company network is full single point of failure without any redundant DHCP DNS server, email server, Single Router which is acting as firewall and gateway. If any of these services fail the entire network will go down and companies' entire business will be interrupted. There is no backup DC present, if the Main DC goes down entire green leaf will go down
* **Unpatched Services and Operating System:** the company's devices, from servers to end point devices, have outdated operating systems and have not been patched. Services such as Email Clients and Web Servers have also not been updated. Which leaves a serious security gap for the network. Will create vulnerabilities in the network. Which will result in Network breaches, and Compliance Risks.
* **Flat Network:** Network is not divided into segments; everything is running on a single Vlan. So, if any of the devices is compromised it will result in total loss of the network. There is no segmentation according to the department. All the devices such Laptops, Phones are on the same VLan. It also leaves the network vulnerable to attacks. Flat networks can also contribute to the loss of bandwidth and connectivity issues. Network loops.
* **Severe Lack of Access Control:** Companys current configuration goes against the principles of least privilege. Any account on the network can access any device. And any device can join the network without any barrier. Network Devices such as routers, switches, firewalls have default passwords. There is no ACLs on the File Serves anyone can Read/Write Delete the files in the File Server. This can lead to Data leak, and Data Loss.
* **Unconfigured Firewall:** Firewall is the barrier which separates the network from the public internet. If the firewall is not configured properly. Anyone can easily access the resources. Currently companies' firewalls are acting as a gateway router and firewall and are being used to connect the company's different offices. So, most of the traffic is being transferred from them. But the firewalls are running with default settings such as allow outgoing and incoming traffics are allowed and there is no restriction on the forwarding of the traffic. Unnecessarily open ports which create a serious issue in the network.
* **Lack of Enterprise Hardware:** Company is currently using consumer grade hardware in their network – 2 wireless Access Points, all Switches. These devices are not made while keeping security in mind. And there are less or close to no possibilities for vendor support, firmware updates. These devices are not suitable for company standards and use cases. As these devices lack Access Controls, Centralized Management.
* **No Monitoring Capabilities: From** the company's current network design. They have no visibility of the entire network. There is no centralized log management. No IDS/IPS to detect what is coming and going outside the network. This results in severe issues in troubleshooting the network. Detect Any types of malicious activity such as unauthorized access, Data theft.
* **No Antivirus:**  Company is currently not using any sort of Antivirus. So, there is no way to scan the files which are being brought inside the company's IT infrastructure. We cannot also scan the endpoint devices for any malware trojans. This is a significant issue. As this malware can easily overpower the company's network, Resources can lead to lost control over the network, Data Corruptions.

# 4 Network Infrastructure Design

# 4.1 Network Diagram:



# 4.2 Network Segmentation

Subnetting: we use the Ip address 192.168.0.0/21, which has 2048 addresses. (192.168.0.1 - 192.168.7.254)

Existing Companies network is running on a single vlan we will divide the network depending on departments and management vlan for managing the network devices. Also, we set up an isolated vlan for servers such as dhcp, dns , file server. So that no external traffic can reach this server.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Vlans** | **IP Address Range** | **Subnet** | **Hosts** | **Department** |
| **10** | 192.168.0.1 - 192.168.0.30 | **/27** | **30** | **Managment** |
| **20** | 192.168.0.33-192.168.0.62 | **/27** | **30** | **Human Resource** |
| **30** | 192.168.0.65-192.168.0.94 | **/27** | **30** | **Finance & Accounting** |
| **40** | 192.168.0.129-192.168.0.190 | **/26** | **64** | **IT & Support** |
| **50** | 192.168.1.1-192.168.1.126 | **/25** | **126** | **Research &Development** |
| 60 | 192.168.1.129-192.168.1.254 | **/25** | **126** | Operations |
| 70 | 192.168.2.1-192.168.2.126 | **/25** | **126** | Sales & Marketing |
|  |  |  |  |  |
| 100 | 192.168.6.1-192.168.6.6 | /29 | 6 | DNS |
| 110 | **192.168.6.9-192.168.6.14** | **/29** | **6** | **DHCP1** |
| **120** | **192.168.6.17-192.168.6.22** | **/29** | **6** | **Domain Controllers** |
| **130** | **192.168.6.25-192.168.6.30** | **/29** | **6** | **File Servers** |
| **140** | **192.168.6.33-192.168.6.38** | **/29** | **6** | **Email Servers** |
| **150** | **192.168.6.41-192.168.6.46** | **/29** | **6** | **Webservers** |
|  |  |  |  |  |
| **200** | **192.168.3.1-192.168.3.254** | **/24** | **254** | **Mobile Devices** |
| **210** | **192.168.4.1-192.168.4.254** | **/24** | **254** | **Guest** |
| **220** | **192.168.5.1 - 192.168.5.6** | **/29** | **6** | **Network Monitoring** |
| **230** | **192.168.5.9 - 192.168.5.14** | **/29** | **6** | **DHCP2** |
| **240** | **192.168.5.17-192.168.5.22** | **/29** | **6** | **SysLog** |
| **250** | **192.168.5.25-192.168.5.30** | **/29** | **6** | **SCCM** |

# 4.3 Network Devices

Routers Cisco ASR 1006-X Router

Firewalls FortiGate FG-900G

Core Switch Cisco Catalyst 9600 Series Switch x 2

# Distribution Switch Cisco Meraki MS425-32 Switch

Access Switches: Cisco Catalyst 1000

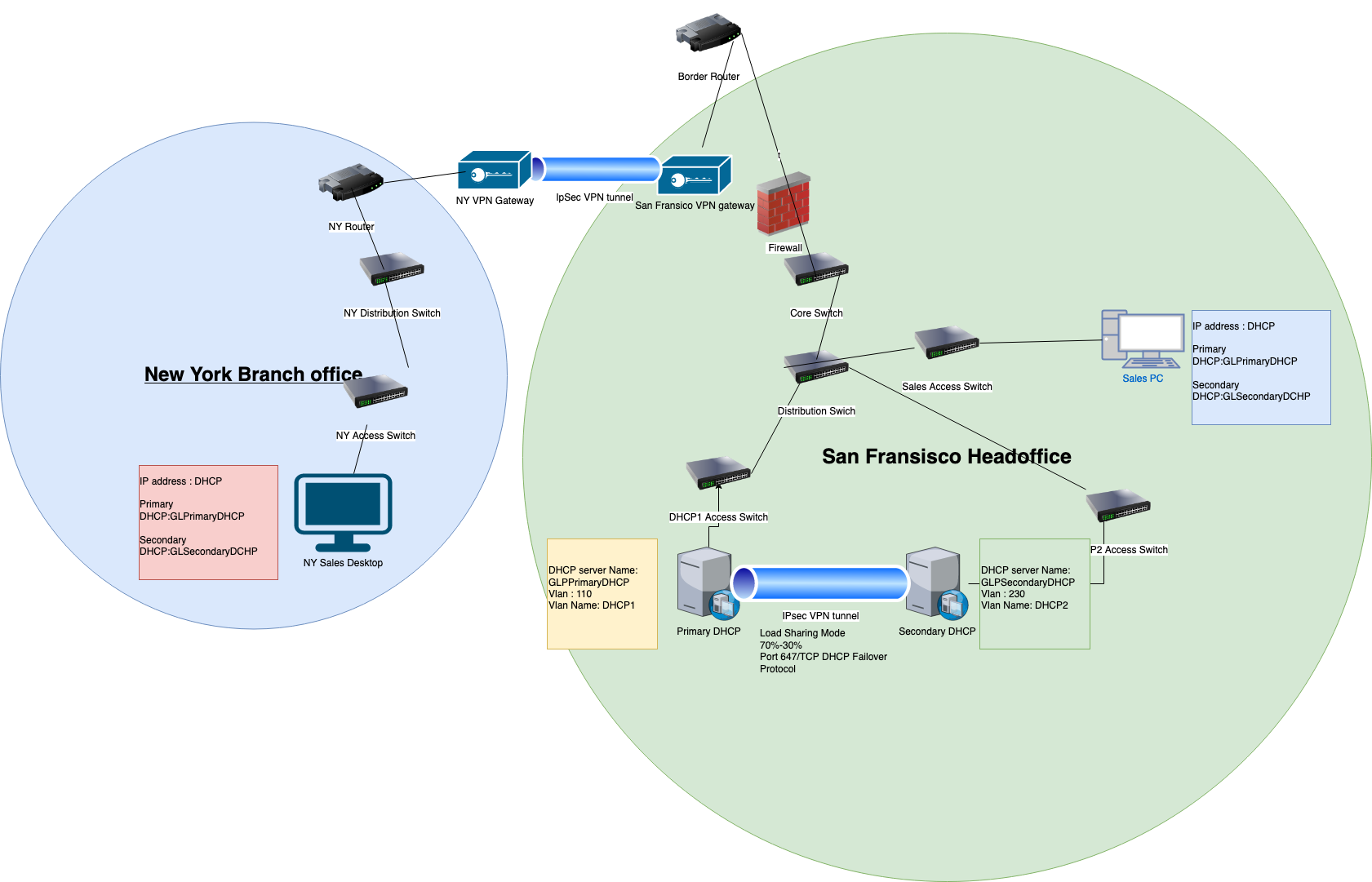
**5 DHCP**

Green Leaf has many devices, and assigning all the devices with Ip address manually is not possible. That why DHCP is very important as it takes the charge of assigning IP addresses to devices manually

For the redundancies we will set up a DHCP failover with a secondary DHCP that serves as backup. This will prevent the DHCP from being a single point of failure.

**Green Leaf DHCP Solution:**

**Diagram:**



|  |  |
| --- | --- |
| No of DHCP Servers | 2 |
| DHCP Server Operating System & DHCP Service | Windows Sever 2016 and Windows DHCP Services |
| DHCP Server Names | * GLPrimaryDHCP * GLSecondaryDHCP. |
| DHCP Server Location | San Fransico Head Office |
| DHCP Server Vlans | 110 & 230 |
| DHCP Server Ip address | * 192.168.6.9-PrimaryDHCP * 192.168.5.9-SecondaryDHCP |
| DHCP Failover Relationship | Load Sharing Mode |
| Fail over Partner | GLSecondaryDHCP |
| Failover Communication | Port 647/TCP DHCP failover Protocol |
| Failover Communication Security | IPsec VPN Tunnel Mode |
| Failover Percentage | * GLPrimaryDHCP: 70% * GLSecondaryDHCP: 30% |

**Servers: No**. Of servers 2 - One primary server and one Secondary Server.

**DHCP server Name:** GLPrimaryDHCP & GLSecondaryDHCP.

**Operating System**: **Microsoft Server 2016,** as it best integrated with other microsoft services and reduces the complexity of managing or integrating it with the network.

**Services: Only** DHCP Services installed on this server as best practices and servers joined with the Active Directory Domain.

Scope:

|  |  |  |
| --- | --- | --- |
| Scope Name | Scope Range | Default Gateway |
| Sales | 192.168.2.1-192.168.2.126 | 192.168.0.1 |
| Operation | 192.168.1.129-192.168.1.254 | 192.168.0.1 |
| Finance | 192.168.0.65-192.168.0.94 | 192.168.0.1 |
| Human Resources | 192.168.0.33-192.168.0.62 | 192.168.0.1 |
| IT | 192.168.0.129-192.168.0.190 | 192.168.0.1 |
| Research | 192.168.1.1-192.168.1.126 | 192.168.0.1 |
| Internal Wireless | 192.168.3.1-192.168.3.254 | 192.168.0.1 |
| Guest Wi-Fi | 192.168.4.1-192.168.4.254 | 192.168.0.1 |

**Scope Name: Scope** Names are assigned with similar name as Vlans name for e.g. vlan 20 has name Human Resource so the scope name will be Human Resource.

**Scope Range:** All the Scopes are defined. According to the subnet table above with respective vlan names for e.g. scope range for scope human resource will be 192.168.0.33-192.168.0.62.

**Scope Reservation**: All servers, Routers, switches, firewalls have static ip address reserved in their respective scope.

**Exclusion:** All the network address and Broadcast address will be excluded from the DHCP scope.

**Loggings: Logging** feature will be enabled on both DHCP servers. All logs are written to event viewer for trouble shooting purposes.

To avoid duplicating Ip address we will configure the DHCP service to first ping the Ip address to check its status. It's free, it will lease the address.

**Failover Configuration.**

**Failover Relationship:** All the Scopes have a failover relationship. Balanced between GLPrimaryDHCP and GLSecondary DHCP

**Failover Partner Server:** GLSecondary DHCP

**Failover Mode:** the load sharing mode of the Microsoft DHCP failover services is used in failover. In this mode the server will provide IP address to the client devices. And this mode is best suited if the servers are in the same location. Which in case of green leaf, All the core servers will be in the San Franciso.

**Failover Communication:** DHCP servers port tcp 647 are open as they need to communicate persistently. Communication is using DHCP failover protocol. All the communication is happening over IPsec VPN tunnel mode for protection of traffic.

**Failover Load Balance Percentage:** Default Percentage for load balance mode is 50 – 50 %. But we are using 70 – 30 loads with 70% with the GLPrimayDHCP and 30% With GLSecondaryDHCP. Just in case the primary server fails we can transfer all the load to the secondary server.

**Green Leaf DHCP Server Security Solution:**

**DHCP Lease Duration:** All the fixed devices are configured with extended lease of 20 days (about 3 weeks). It helps reduce the network traffic ongoing to DHCP servers and reduce their load.

All Guest and mobile devices have their lease time reduce to 1 hour. It helps free up Ip address from the DHCP pool.

**DHCP IP Conflict:**  Default DHCP Ip address conflict is disabled for all Ip address scope. It will be only enabled for scopes which will take Ip from DHCP pool. Not for scope which have static Ip addressing scheme.

**DHCP Snooping:** It is enabled on the access which connects the DHCP server to the rest of the network. It prevents a rogue DHCP server from going over Ip address.

**Backup DHCP server: It** is very important to back up the DHCP server as it gives ip address to clients on the network. By default, all the backup of dhcp is stored on the local server. So, the backup has been copied to a different server.

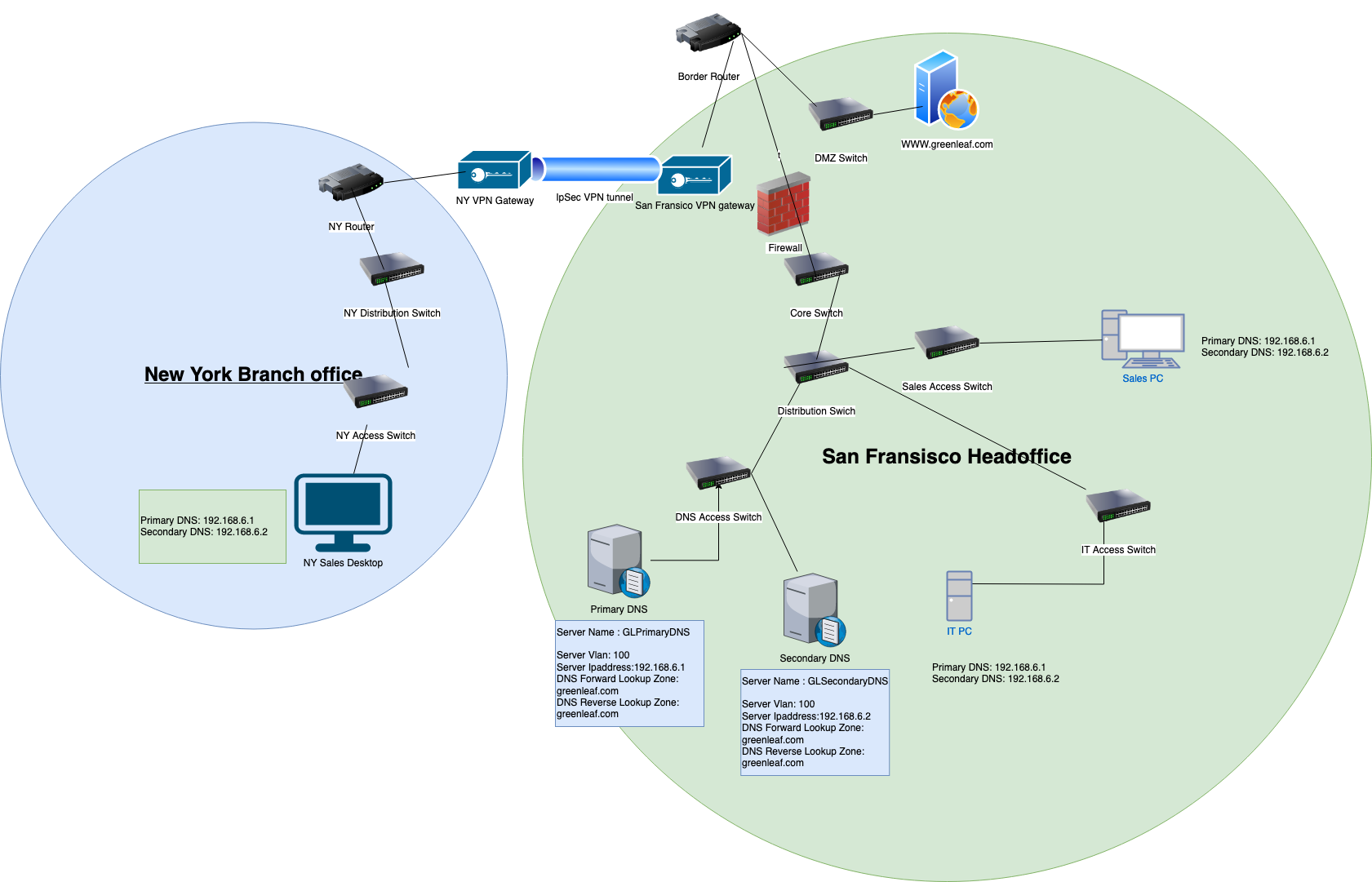
**DHCP MAC Address Filtering: This** feature allows, or block ip address assignment based on the mac address of the clients. It is enabled for all the internal vlans so that no unauthorized devices can join the internal network.

## **6. DNS**

GreenLeaf requires a DNS service which will give naming schemes to all the Ip addresses in the Company. As it is hard to manage just by Ip address. Added a DNS server will provide better management. it is important it is not a single point of failure. So, in the company network infrastructure a primary and secondary DNS server is necessary.

**Green Leaf DNS Solution:**

**Diagram:**



|  |  |
| --- | --- |
| No of Servers | 2 |
| DNS servers Operating System and DNS services | Windows Server 2016 & Microsoft Domain Name Services |
| DNS server Name | GLPrimaryDNS, GLSecondaryDNS |
| Subnet and Vlans | 192.168.6.1-192.168.6.6 & Vlan 100 |
| Static IP address | * GLPrimaryDNS-192.168.6.1 * GLSecondaryDNS-192.168.6.2 |
| Greenleaf DNS Namespace | greenleaf.com |

**Servers:** 1 Primary Server and 1 Secondary server installed at the head office. Each of these servers are joined to the company domains

**Server Names:** GLPrimaryDNS , GLSecondaryDNS

**Networking Configuration:** Vlan 100 & Subnet 192.168.6.1-192.168.6.6.

**Operating Systems:** For better management and integration, we will use the Microsoft server 2016. With Microsoft domain name services installed on each of the servers. No other services is installed on these servers as industry best practice.

**DNS Name Space:** greenleaf.ca is namespace for the top-level domain .ca

greenleaf.com subdomains have been created to logically segregate the greenleaf.com namespace.

* [www.greanleaf.com](http://www.greanleaf.com) This secondary will answer all the webservers' queries.
* email.greenleaf.com this secondary domain will answer all the l emails query.

**DNS Zones:**

**Dns Zone** are very helpful to create a logical separation within the domain namespaces. Dns Zone are stored in a form of zone text file, and it contains all the data of the records and query for the zone.

**Active Directory Integrated Zones:** All the zone files are stored in a text file format on the dns Server locally which is running the domain name services. But with the Active Directory Integrated Zones we can take advantage of the active zone. As in this type of zone all the zones' files are stored in the domain controller with all the advantages of domain controller such as replication, redundancy, simplicity and security.

**2 Active Directory integrated zones have been created as follows**

**Forward Lookup zone:**

greenleaf.com: This is the main domain zone which contains the information about the top-level domain Greenleaf external zone. With all of its subdomain [www.greenleaf.com](http://www.greenleaf.com) and email.greenleaf.com.

**greenleaf.com Zone:**

**Primary DNS:** ns2.greenleaf.com. 192.168.6.1

**Secondary DNS:** ns2.greenleaf.com 192.168.6.2

**External DNS:** cloudflare-name server 1.1.1.1 (Only for the external dns namespace)

**SOA record:** GLPrimaryDNS(Primary Name server) , Email address TTL . This is the first record in on the namerver.

**A record:** [www.greenleaf.com](http://www.greenleaf.com) Webserver Ip address IPv4

**AAAA record:** [www.greenleaf.com](http://www.greenleaf.com) Webserver IPaddress IPv6  
**Mx records:** email.greenleaf.com Mailserver Ipaddress

PTR record: mailserver ipaddress. email.greenleaf.com

**Service ip address**: \_ldap.\_tcp.intgreenleaf.com. IN SRV 0 5 GLDC .intgreenleaf.com

*A secondary zone was created for this zone to reduce the load for the primary zone.*

**Reverse Lookup Zone:** This Zone is needed to query ip address to hostname.

greenleaf.com:

**Primary DNS:** ns2.greenleaf.com. 192.168.6.1

**Secondary DNS:** ns2.greenleaf.com 192.168.6.2

**External DNS:** Cloudflare-name server 1.1.1.1 (Only for the external dns namespace)

**PTR record:** 1 dcipaddress --> ldap.greenleaf.com

**PTR record:**  2 webserveripaddress ---> www.greenleaf.com

**PTR record: 3**. emailserveripaddress --> email.greenleaf.com

**Securing GreenLeaf DNS solution:**

**Secure Dynamic Updates: Client** computers can update their records with DNS server this can lead the server to update unauthorized records from unauthorized hosts. So Active directory integrated have been created. AS they also allow secure dynamic updates. This is further hardened using group policy.

**Zone Transfer:** Zone transfer is method which allows a client to query All the zone records from the authoritative zone. This is a serious vulnerability. So, Zone transfer has been narrowed down to only specific Ip addresses. All other clients request a zone transfer.

**Maintains:** Regular updates for the operating system and DNS services software have been scheduled. To reduce the attack vectors for the DNS server.

**DNSSEC- Domain Name System Security Extensions** provides data integrity and prevents attacks like DNS snooping. It uses PKI for strong authentication and data integrity. So, this feature has been enabled. It is using company's PKI to maintain a chain of trust till root server.

*A MX records have been signed using the DNSSEC*

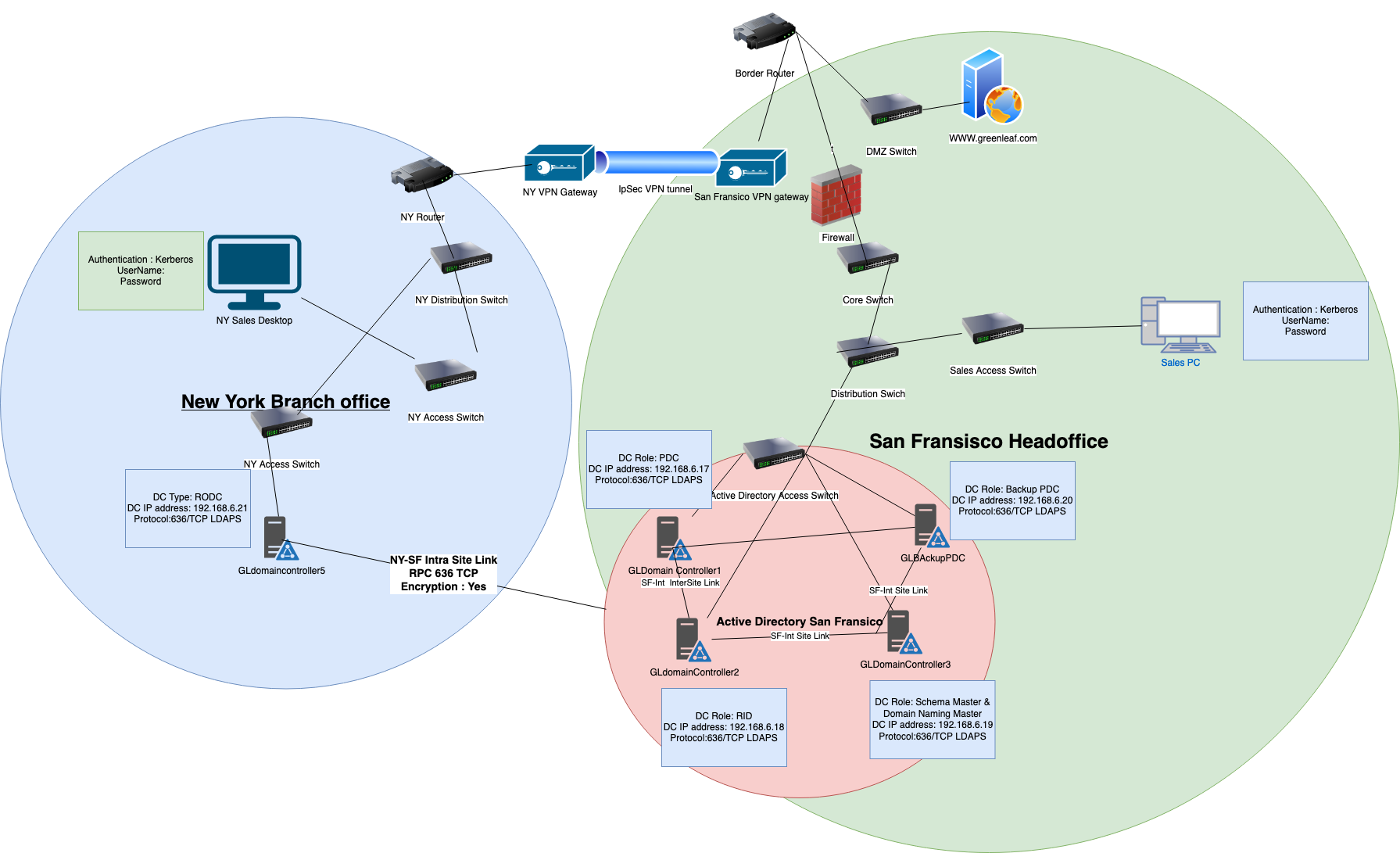
**DNS Transaction Signature (TSIG):** This feature allows secure traffic between DNS servers. So, this feature is being used to protect traffic between GLPrimaryDNS and GLSecondaryDNS . This feature uses a shared secret key method. This helps securing information between the DNS server and Zone transfer traffic.

DNS over HTTPS: DNS protocol like all other fundamental protocols is vulnerable as there is no security for authentication and Traffic is transmitted in clear traffic. So, to protect the DNS traffic from being spoofed we are using Transport layer security to protect DNS traffic.

## 7. Active Directory

For Centralized Management of the companies IT infrastructure, we use an Active Directory Which will also handle user identification. Active Directory consists of Active Directory domains, Forests, Schema and Data store.

**Green Leaf Active Directory Solution:**



**Green Leaf Active Directory Logical Structure:**

**Forest:** greenleaf.com

**Domains:** greenleaf.com

**Organizational Units:**

Sales

Marketing

Research

IT

Human Resources

Finance

**Security groups:**

Network Administrators

Active Directory Administrators

DNS and DHCP Administrators

Managers

System Administrators

**Active Directory Physical Structure:**

**San Fransico Office:** greenleaf.com

|  |  |
| --- | --- |
| **No of Domain Controllers** | 4 |
| **Type of Domain Controllers** | Read & Write Domain Controllers |
| **Domain Controllers Names** | * GLdomaincontroller1 * GLdomaincontroller2 * GLdomaincontroller3 * GLBackupPDC. |
| **Domain Controllers Location** | San Fransico |
| **Domain Controllers Vlans & Subnets** | 120 & 192.168.6.17-192.168.6.22 |
| **Domain Controllers Static Ip address** | * 192.168.6.17 - GLdomaincontroller1 * 192.168.6.18 - GLdomaincontroller2 * 192.168.6.19 - GLdomaincontroller3 * 192.168.6.20 - GLBackupPDC |
| **Domain Controllers Ports** | * 636/TCP LDAPS * 53/TCP/UDP DNS * 3269/TCP Secure Global Catalog * 88-TCP/UDP Kerberos |
| **Domain Controllers Roles** | * GLdomaincontroller1-PDC * GLdomaincontroller2-RID * GLdomaincontroller3-Schema Master and Domain Naming Master * GLBackupPDC- Backup PDC server |
| **Replication Site** | San Fransisco |
| **Replication Site** Link | * SF-Int Inter-Site * NY-SF Intra-Site * HO-SF Intra-site |
| **Replication Schedule** | 30 Min |
| **Replication Protocol & Security** | RPC Protocol-TCP 636 and TCP 3269 |

**Global Catalog:** the Sans Fransico are read and write domain controllers. 2 of them are configured as global catalog. There is no disadvantage in making 2DCs as global catalog. And it also increases performance so global catalog feature have been enabled on the all the DC. DC with role PDC is not set as Global Catalog to reduce traffic on it.

**Primary Domain Controller (PDC):** GLDomaincontroller1 is set up as the PDC. This server has the highest specification among all the other DCs. PDC in the Forest is responsible for Account Passwords, Logins etc. So, this Server needs to be online 24x7. If this server goes down. No one will be able to login. A Standby DC has been configured GLBackupPDC. For the PDC in the San Fransico Office for backup purposes.

RID: GLDomaincontroller2 has been assigned the role of RID master. These DC is responsible for replicating domain controller in the same domain.

**Schema Master and Domain Naming Master:** GLDomainController3 has been assigned the role of Schema Master and Domain Master.

**Replication Site**: San Fransico

**Replication Site Link:** 1. **SF-In**t Inter-Site This link is setup for replication between all the DC present in San Fransico.

2. NY-SF & HO-SF Intra-site Link is setup for replicate head office with branch office.

Replication Schedule: Replication Interval is Set to 30 and to save bandwidth the Replication schedule is reduced during peak hours of the company to save bandwidth and latency.

**Replication Protocol:** RPC Remote Procedure Calls over TCP/IP as SMTP is degraded protocol and does not suit company security policy.

**Branch New York Office, Houston, Texas office**

AS this branch office lack the physical security and IT expertise. A Read only domain Controller is placed there. This site is linked to the San Fransico Headquarter. As read only domain controller holds all the objects records but no-account passwords. But no changes can be made to it.

**New York Office:**

|  |  |
| --- | --- |
| **No of Domain Controllers** | 1 |
| **Type of Domain Controllers** | Read Only |
| **Domain Controllers Names** | GLdomaincontroller5 |
| **Domain Controllers Location** | New York |
| **Domain Controllers Vlans & Subnets** | 120 & 192.168.6.17-192.168.6.22 |
| **Domain Controllers Static Ip address** | 192.168.6.21 - GLdomaincontroller5 |
| **Domain Controllers Ports** | * 636/TCP LDAPS * 53/TCP/UDP DNS * 3269/TCP Secure Global Catalog * 88-TCP/UDP Kerberos |
| **Replication Site** | New York |
| **Replication Site** Link | NY-SF Intra-Site |
| **Replication Schedule** | 30 Min |
| **Replication Protocol & Security** | RPC Protocol-TCP 636 and TCP 3269 |

**Houston, Texas:**

|  |  |
| --- | --- |
| **No of Domain Controllers** | 1 |
| **Type of Domain Controllers** | Read Only |
| **Domain Controllers Names** | GLdomaincontroller6 |
| **Domain Controllers Location** | Houston |
| **Domain Controllers Vlans & Subnets** | 120 & 192.168.6.17-192.168.6.22 |
| **Domain Controllers Static Ip address** | 192.168.6.22 - GLdomaincontroller6 |
| **Domain Controllers Ports** | * 636/TCP LDAPS * 53/TCP/UDP DNS * 3269/TCP Secure Global Catalog * 88-TCP/UDP Kerberos |
| **Replication Site** | Houston |
| **Replication Site** Link | HO-SF Intra-Site |
| **Replication Schedule** | 30 Min |
| **Replication Protocol & Security** | RPC Protocol-TCP 636 and TCP 3269 |

**Green Leaf Active Diretory Security Solution**

**Software and Service Updates:** A Regular Update Schedule has been set for updating the Operating System, Active Directory Domain Services and other software running on DC. All the updates go through the patch management lifecycle as defined in the company patch management policy.

**Principle of Least Privilege:** Under no circumstances is any user allowed to login to any DC. For Least privilege at least 2 administrators must be present in case there is need to access the domain controllers. The Access must be properly documented.

**Monitoring:** A Mirror port is configured on the Switch which connects the DC to rest of the network for continuous monitoring of the traffic. Logging has been enabled on all the Domain Controllers. Copies of all the logs are also transferred to a central Location on Syslog Server. For centralized monitoring and auditing of all the DC.

**LDAPS:** LDAP Light-weight directory protocol transfer data in plain text without any authentication mechanism. So, to secure the LDAP traffic. LDAP Signing and Binding has been enabled for the traffic and in place of LDAP LDAPS is being used to encrypt the LDAP traffic.

**Securing Replication Site & Links:** Site Links work on the RPC Remote Procedure Call Is used to replicate the Data among domain controllers within a site and in between sites. RPC Encryption has been enabled to protect the traffic between domain Controllers.

**Network Security:** All the Domain Controllers are put in a separate VLan. To isolate them from the rest of the network. further lock down the traffic to only Active Directory related traffic to reach the Domain Controllers.

**Backup:** Regular Synchronized and Asynronized Backup have been Schedule for Active Directory Database. 2 On Site backup and one offsite Backup.

**Antivirus:** All Domain controllers are installed with the Companys Antivirus software for protection again Malwares, Viruses , Spyware.

**Read Only Domain Controllers:** Branch Office of Green Leaf does not possess adequate security measures for protecting Read-Write Domain controllers. So, for enhanced security RODC has been placed. RODC contains all objects of AD except the Account passwords.

# **8. Network Security**

**8.1 Access Control**

**Role Based Access Control:**

**Access Control Model:** RBAC (Role Based Access Control)

**Roles:** Active Directory Security Groups

**Network Devices:** Routers, Core Switches , Distribution Switches, Access Switches, Firewalls

Authentication: Active Directory LDAP (Kerberos) + Hardware Security Key

**Security Group Name:** Network Administrators

**Local Accounts:** Disabled

**Active Directory**

Devices: Domain Controllers

**Authentication:** Active Directory LDAP(Kerberos) + Hardware Security Key

Security Group Name: Active Directory Administrators

Local Account: Partially Disabled, protected with very strong password and MFA (It is hard to eliminate the full effect of the local administrative account.)

**Domain Name System**

**DNS Servers:**

**Authentication:** Active Directory LDAP(Kerberos)+ Hardware Security Key

**Security Group Name:** DNS Administrators

Local Account: Partially Disabled, protected with very strong password and MFA(It is hard to eliminate the full effect of the local administrative account.)

**DHCP**

**DHCP Servers:**

**Authentication:** Active Directory LDAP(Kerberos)+ Hardware Security Key

**Security Group Name:** DHCP Administrator

Local Account: Partially Disabled, protected with very strong password and MFA (It is hard to eliminate the full effect of the local administrative account.)

**Workstations**

**Devices:** All Desktop Clients

**Authentication:** Active Directory LDAP(Kerberos)+ Hardware Security Key

**Security Group Name:** Desktop Administrators

**Responsibilities:** Group policy management, Access Management, Software and Service updates.

**Network Devices** such as switches, Routers , Firewalls are denied access to all the clients and users. Only Administrator which have been assigned to the network administrator security group can access the network devices and make changes to it. All the network devices can be accessed using only the ldap protocol and the local administrator account credentials are saved securely and are to be used only when necessary.

Active Directory: AD Administrator Security group have been created and only users attached to this role security group can access the domain controllers and make changes to it. Local admin account of the domain controllers is locked down using group policy and are protected using secure credentials

**DNS: DNS** Administrator Security Group has been created. All the administrators in this security can make changes to the domain controller, perform maintains. Make Zone transfers, Create Zones.

**DHCP:** DHCP Administrator Security Group. All the users in the security group can manage the DHCP servers, Create Scopes, Manage the Ip address reservation and do maintaince on the DHCP server.

**Access Control List**

**Network Structure:** Segmentate logically using VLANs

**Greenleaf Departments ACLs:** Isolated from each other (No Department can talk to each other.). Traffic is not allowed to be routed from one department to another.

**Internet Traffic:** No Direct internet Access for internal clients. All internet traffic goes forward to the proxy server.

DNS ACL: Only DNS Query and other traffic is allowed.

Active Directory ACL: Traffic related to Active Directory is allowed and only from trusted internal clients

**DHCP:** Traffic such request ip address or giving address is allowed.

External Access Control List: Explicit Deny (All traffic is denied by default)

**The entire network has been logically segmented into different VLANS. For better security and management. This also helps control the traffic flow to the vlans.**

**All Company Departments** have been assigned their own VLANs. So better Security traffic that goes into this vlans are for their respective departments. All the Departments are isolated from each other. No Client device in this vlan is allowed to access to other Vlans.

**Internet Traffic:** Direct Internet Access for all the internal Clients have been denied which means no internal client is allowed to access the internet directly.

**DNS Traffic:** All the DNS servers have been assigned to a separate VLAN with its own subnet. So for better performance and Security. Only Traffic related to DNS or DNS query from client is allowed to reach the DNS VLAN rest all traffic is denied. Except for the number of clients which are used to do maintains to the DNS servers.

**Active Directory Traffic: All** the Domain Controllers are grouped together in an AD VLan. 2 of these domains' controllers are Read Only and are set up at branch offices. To increase the network speed and to tighten the security to make sure no one can send malicious traffic to the Domain controllers, only LDAP traffic is allowed to reach the domain controllers. As domain controllers need to talk to each other. Traffic from another Domain is also allowed for this VLANS.

**DHCP Traffic:** As DHCP only purpose is to assign IP addresses when a client requests an Ip address from the server. So, there is no need for other network requests to reach this server, this reduces the attack surface. Only a DHCP traffic, or a client request is allowed to reach DHCP server. As for providing access for maintains and other tasks. Only Certains clients with ip address are allowed to remote connect into the server is done through role-based access.

**Network Monitoring Solution**

**Centralized Network Monitoring Solution:** PRTG Network Monitor

**Servers Name:** GL\_SF\_Monitor

Vlan: 220

**Subnet:** 192.168.5.1-192.168.5.6

**Locations:** San Francisco

**GL\_SF\_Monitor:**

Role: Monitor All the devices

**Capabilities:** SSH, DNS, LDAP , DHCP, ICMP Disk Space, Device Health, Device RAM, Device Process.

**Traffic Capture**

**TAP:**

**Garland Technology Network TAPs**

**Type:** Passive

**No of Taps:** 5

**Locations:** 1. 2 TAPS with VPN gateways connecting Head office with branch office.

2. 2 TAPS on the Access Switches connecting the DNS and Active Directory.

3. 1 Tap with the access switch connecting the file servers.

**SPAN Port Analyzer:**

**Monitored Ports:**

1. Active Directory Access Switch Port

2. DNS Switch Port

3. File Servers Switch Ports

4. Departments Access Switch Port

All the mirrored traffic will be sent to the PRTG Network Monitor for analyzing.

SPAN is used for detecting any suspicious traffic as it completely copies the entire traffic. It is also useful for performance monitoring.

**Firewalls:**

**San Fransico Office** *FortiGate FG-91G*

**Border Firewall:** FortiGate FG-900G

**Firewall Name :** GL\_BRFirewall

**Firewall Configuration:**

**Allowed Incoming :**  Default Policy Explicit Deny

1. HTTP/HTTPS Traffic

2. Email Traffic

3. VPN traffic from remote clients

**Outgoing Traffic:** Default Policy is allowing all the outgoing traffic is allowed.

**Coke Firewall :** FortiGate FG-900G

**Firewall Name:** GL\_CokeFirewall

**Firewall Configuration:**

**Incoming Traffic:** Explicit Deny (All traffic is denied)

**Traffic from remote Clients**

**Required:** Authentication

**Authentication Method:** RADIUS Server.

**Authentication Protocol**: EAP-TLS

**Authentication Policy**: Device Location, Device Service Pack Level, Device Mac address , User Authentication , User role.

**Outgoing Traffic:** Explicit Deny

Traffic to the Bastion Server used to manage the All the devices in the DMZ zone.

**DMZ Zone:** *This zone has been created between the Border and Coke Firewall. As this zone consist of public facing Devices.*

**DMZ zone Devices: 1** Webserver, 1 Email Server, 1 Bastion Server.

**Webserver :** This server is hosting the Green Leaf company Website [www.greenleaf.com](http://www.greenleaf.com)

**Email Server**: This server is hosting exchange server for the Greenleaf.

**Bastion Server:** This server consists of the only remote management solution which connects to the webserver and email server. This server is heavily monitored.

**Branch Offices Houston and NewYork**

**Houston Firewall:** Fortigate FG-900G

**Firewall Name:** GL\_HO\_Firewall

**Firewall Configuration:** This firewall is also acting as a VPN gateway to connect it to the headquarters in San Fransico.

Incoming: Explicit Deny, only traffic from the headquarter is allowed. No traffic from public internet is allowed

**Allowed Traffic**

1. VPN Traffic.

2. SSH traffic

3. DNS/ DHCP traffic

4. Active Directory Traffic

5. ICMP traffic

**Outgoing:** Explicit Deny, All the traffic is routed to the headquater forward Proxy server.

**Allowed Traffic:**

1. HTTP/HTTPs traffic

2. DNS/DCHP Traffic

3 Active Directory Traffic.

**Newyork Firewall:** Fortigate FG-900G

**Firewall Name:** GL\_NewYork\_Firewall

Firewall Configuration: This firewall is also acting as a VPN gateway to connect it to the headquarters in Sanfransico.

**Incoming:** Explicit Deny, Only traffic from the headquater is allowed. No traffic from public internet is allowed

Allowed Traffic

1. VPN Traffic.

2. SSH traffic

3. DNS/ DHCP traffic

4. Active Directory Traffic

5. ICMP traffic

Outgoing: Explicit Deny, All the traffic is routed to the headquater forward Proxy server.

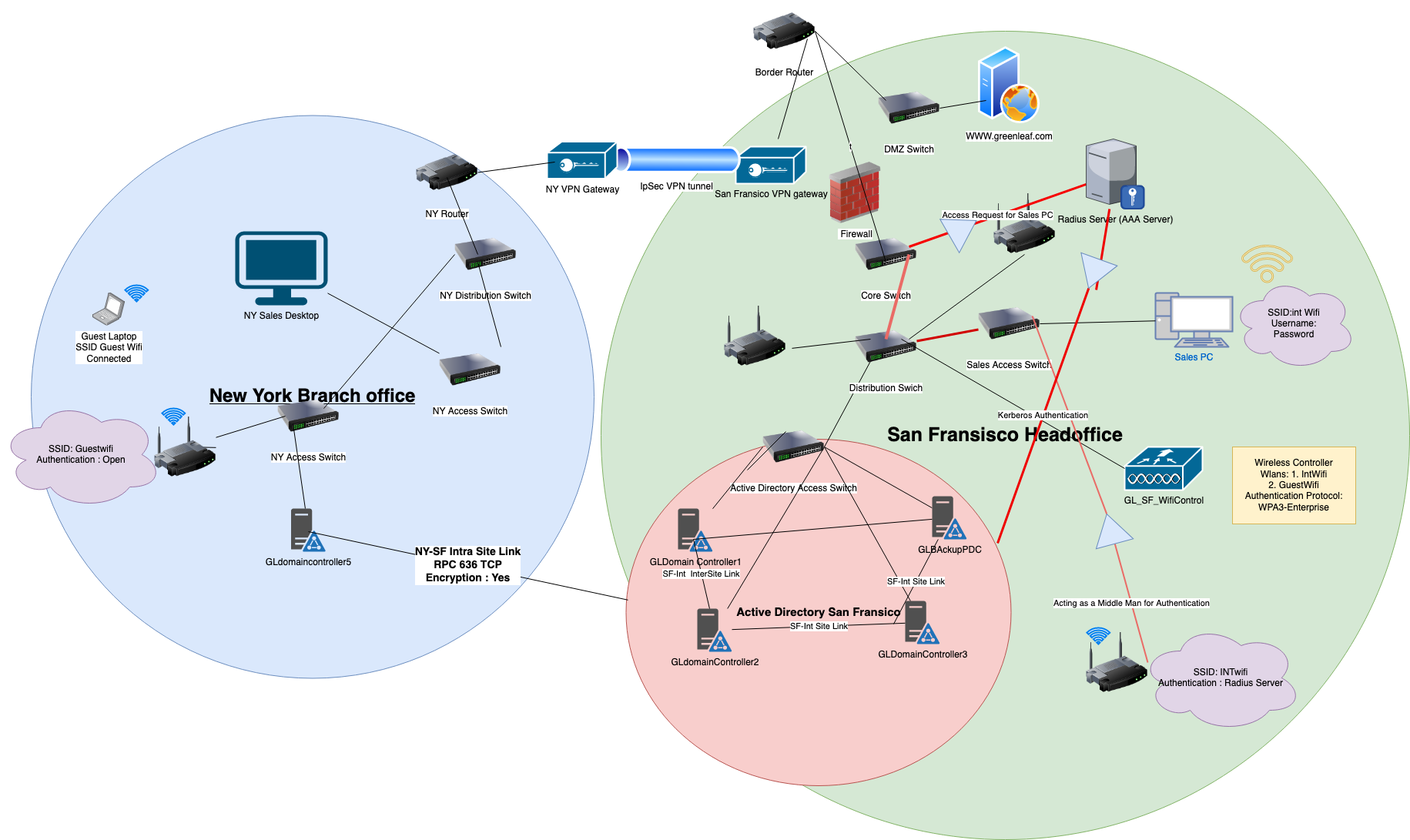
Allowed Traffic:

1. HTTP/HTTPs traffic

2. DNS/DCHP Traffic

3 Active Directory Traffic.

# **8.2 Wireless Infrastructure**



**San Fransisco:**

**Wireless Infrastructure**

Wireless Devices:

1 Wireless Controller, 6 Access Points

1 Radius Server

**Configuration:**

**VLAN: 10**

**Subnet 192.168.0.1-192.168.0.30**

**Wireless Controller Name:** GL\_SF\_WifiControl

**No of Controllers:** 1

**Wireless Access Points:** GL\_SF\_WA1 , GL\_SF\_WA2, GL\_SF\_WA3, GL\_SF\_WA4, GL\_SF\_WA5, GL\_SF\_WA6.

No of Wireless LANS(WLANS): 2

**Internal WLAN:** 300 – IntWifi

**SSID:** Hidden

Subnet: 192.168.3.1-192.168.3.254

ACL: No Internet Access.

Authentication: Required

**Wireless Authentication Protocol:** WPA3-Enterprise

**Wireless Authentication:** EAP- TLS with Radius Server

**Guest WLAN: 310** – GuestWifi

**Subnet:** 192.168.4.1-192.168.4.254

**ACL:** Internet Access Only, All other connection deny

**SSID:** Visible

Authentication: Not Required

**Houston Office:**

Wireless Infrastructure

**2 Wireless Access Points:**

**Configuration:**

No of Wireless Access Points: 2

Wireless Access Points: GL\_HO\_WA1 GL\_HO\_WA2

**No of Wireless LANS(WLANS):** 2

**Internal WLAN:** 300 – IntWifi

SSID: Hidden

**Subnet:** 192.168.3.1-192.168.3.254

**ACL:** No Internet Access.

Authentication: Required

**Wireless Authentication Protocol:** WPA3-Enterprise

Wireless Authentication: EAP- TLS with Radius Server

**Guest WLAN: 310** – GuestWifi

**Subnet: 192.168.4.1-192.168.4.254**

**ACL:** Internet Access Only, All other connection denied.

**Newyork Branch Office.**

Wireless Infrastructure

**2 Wireless Access Points:**

**Configuration:**

No of Wireless Access Points: 2

Wireless Access Points: GL\_NY\_WA1 GL\_NY\_WA2

**No of Wireless LANS(WLANS):** 2

**Internal WLAN:** 300 – IntWifi

SSID: Hidden

**Subnet:** 192.168.3.1-192.168.3.254

**ACL:** No Internet Access.

Authentication: Required

**Wireless Authentication Protocol:** WPA3-Enterprise

Wireless Authentication: EAP- TLS with Radius Server

**Guest WLAN: 310** – GuestWifi

**Subnet: 192.168.4.1-192.168.4.254**

**ACL:** Internet Access Only, all other connection denied.

**1 Wireless Controller** has been placed at the San Francisco Office Which will manage all the Access Points Across entire company network. It provides better management, scalability , visibility on a centralized platform and reduces the chance of Rogue Access Point attack.

**2 Wireless LAN** have been created to segment the company's wireless infrastructure. Internal WLANs will follow the companies ACLS and will not allow any internet traffic. Guest wlan will only be allowed internet access. Connection to internal host will be denied.

**WPA3** Being the latest technology in wireless security is best for protecting company wireless network. WPA3-Enterprise integrates the Active directory login which follows company access policy of RBAC.

**EAP-TLS (Extensible Access Protocol)** It a industry standard protocol used for remote authentication. EAP can also be used with Wireless technology for authentication too.

Using **Radius Server** allows the user to authenticate against the Active Directory. And fulfill the requirement of Authentication, Authorization and Accounting.

*New York and Houston Branch Office Lacks the Security and Expertise to manage the Wireless Controllers. So, no Wireless Controllers have been set up.*

## 9 Device Management

## 9.1SCCM

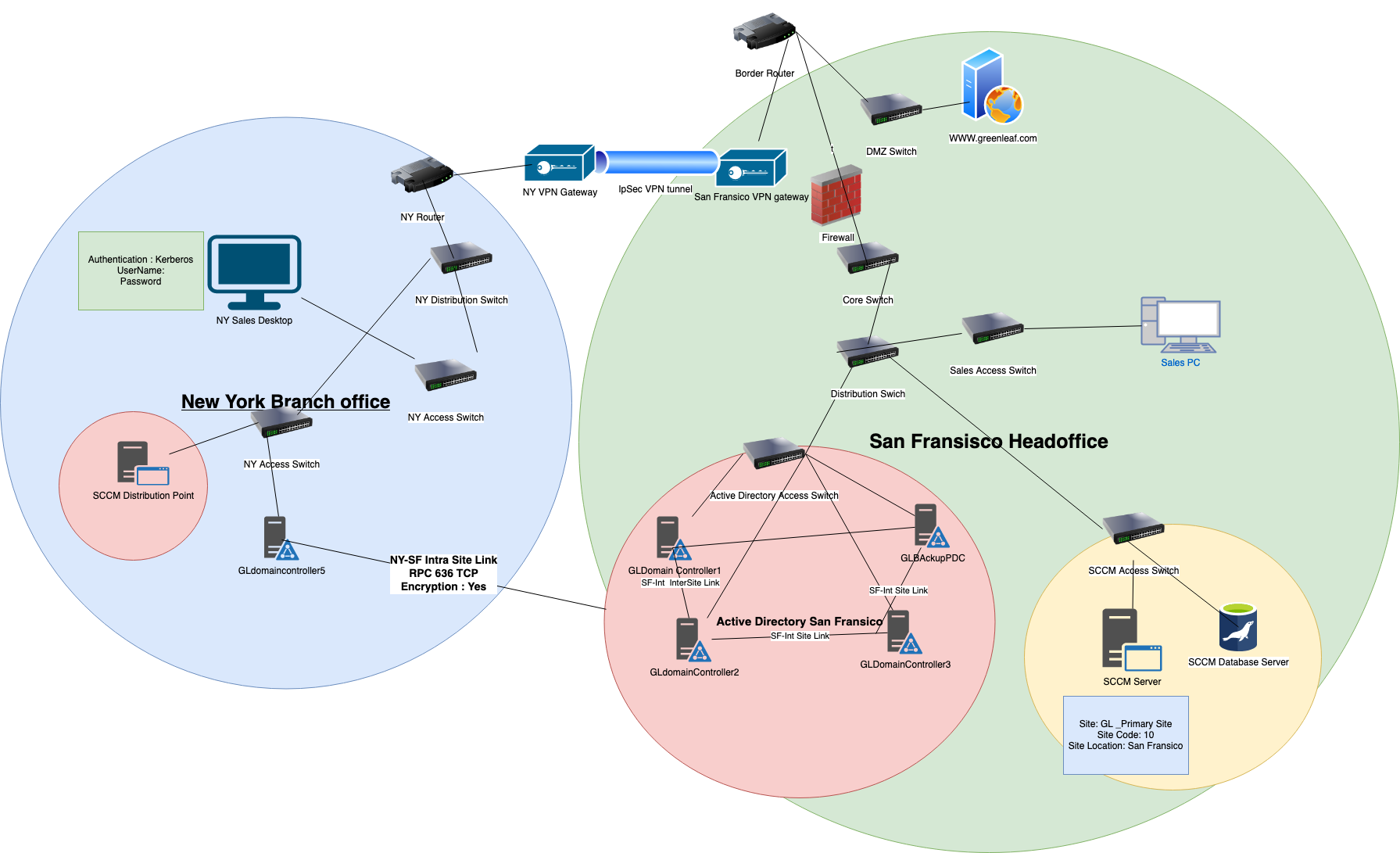
System Center Configuration Manager is a Centralized Management tool. It helps manage and monitor devices. It is best suited for windows devices. As it removes the need to manually do updates, Install Application or Deploy operating systems.

GreenLeaf has large number of windows devices integrated with Active Directory. By introducing System Center Configuration, we reduce the need to manually update or deploy applications or operating systems.

**No of Windows Clients:** 130

**No of MacOS Clients**: 30

**SCCM Solution For GreenLeaf for Management of Devices**



|  |  |
| --- | --- |
| No of Servers : | 4 |
| Server Types | * SCCM Core Server * Microsoft Sql Server * 2 Deployment Point Servers |
| SCCM core Servers Name | * GL\_SCCMServer * GL\_SCCMDB |
| Servers Location : | San Fransico |
| Servers VLAn | 2540 |
| Servers Subnet | 192.168.5.25-192.168.5.30 |
| SCCM | Configurations |
| Site Name: | GL\_Primary Site |
| Site Code: | 10 |
| Site Location: | San Fransico |
| No of Distribution Point: | 2 |
| Location: | * New York * Houston |
| Distribution Point Names: | * GL\_NYDP * GL\_HODP |

**On Boarding Clients**

**Group Policy to Deploy the SCCM Client Package:** All the clients which are part of Group Policy Management will join the green leaf infrastructure using GPO which will deploy the client packages to the Clients and install the package. Make the clients automatically join the SCCM Primary Site

**Network Discovery:** Clients which do not support Group Policy Management such as MacOS clients will join the SCCM Primary Site through network discovery by deploying SCCM Client Packages through Network and installing them.

**SCCM Usage in Company for Device Management**

**Hardware Inventory:** SCCM is used for inventory the number of windows and MacOS clients in the company as SCCM only supports this 2 types of devices. So all of windows and MacOS devices are being accounted using SCCM.

**Software Inventory:** SCCM has the feature of creating a software library through which all the clients on SCCM can download the software. This feature removes the issue of unwanted software being installed on the computer. As SCCM acts as a software repository.

*Software Inventory of SCCM in Green Leaf:*

* *Microsoft Office Suite*
* *Adobe Suite*
* *Java SDK*

**Software Updates:** One of the Core Features of SCCM is patch management. Greenleaf has a good number of windows and mac devices. It needs a solution to update the services and operating system of the devices. As doing it manually is not possible and. Software updates need to be schedule at a particular time of day to not interrupt work.

**Endpoint Protection:** SCCM can endpoint protection by deploying policies for detecting malware, viruses and spyware. This feature is being used in Company SCCM to detect any Malware, Viruses and Spyware by regularly scanning endpoints automatically.

**Security for green leaf SCCM server and Deployment points**

**Authentication and Access Security:** All SCCM servers such as Database servers, Core sever, and Deployment are authenticated using Kerberos authentication protocol with multi-factor authentication and Access is only given to the system administrators security groups and all the access is accounted.

**TLS-SSL:** Sccm uses HTTP and SMB for traffic between the server and the client for deploying software updates and deploying applications. So, to protect the SCCM traffic TLS-SSL is used to upgrade the unsecured protocols using companies PKI solution

**IPSec Tunnels:** IPSec VPN tunnels are set up to protect the traffic between the SCCM server, SCCM database and deployment points.

**Logging:** All the activity of devices is being logged and all the criticial and important logs are being sent to centralized Syslog server for centralized management.

**Updates and Maintains:** SCCM servers require regular updates for the service and updates for operating systems. Regular update policy has been made. To make sure SCCM servers get regular patches. The backup of the Servers has been configured to be stored in a centralized location.

## **9.2 Microsoft Intune**

Green Leaf has good numbers for end devices such as Android phones, iPhone, Linux, Mac and windows laptop. It is not possible to manage all the devices manually. And company supporting remote work. So, it is very important to extend company security infrastructure to support remote. That is where Microsoft Intune comes into play.

Intune is a cloud-based endpoints and application management system. It provides many features such as device enrollment, device policy, device health, remote wipe, conditional access controls, application management. This solution is a part of Microsoft 365 and can integrate with SCCM.

Intune, with its capability, will allow the company to provide access to company data to users from outside company premises and further secure the client's endpoints devices. By managing the device health, Antivirus, automatic software updates.

**Intune Solution for Device Management**

**No of Mobile Phones: 75**

**No of Linux devices 10**

**No of Mac devices 30**

**No of Windows Devices: 13**

*A SCCM Server with 2 Deployment Points already present with Windows Devices and MacOS currently enrolled.*

**GreenLeaf Requirements for Intune:**

* Remote Wipe
* VPN profile
* Device Heatlh such as Software update status, Antivirus
* Applications – Outlook, SharePoint, OneDrive, Adobe Suite, Antivirus Software

**Intune domain: greenleaf.onmicrosoft.com**

**Deployment Model:** **Co-management Model,** in this model Intune and SCCM Work Together to manage devices. This model allows Company to manage devices using Intune while keeping their on-premises infrastructure. In this Model the Windows devices are enrolled with SCCM and Intune Side by Side.

**Users and Groups:** Company is already using Active Directory Users and Groups. But Intune does not Support Hierarchy. So, Some Changes still needs to be made before migrating them to Intune.

*Following are the groups:*

* Sales
* Human Resource
* Research
* Finance
* IT
* Administrator Group This group is responsible for device enrollment , Security and application policy and Device updates, VPN Policy.

*Intune Supports Role Based Access Controls, But Different from Active Directory Security Groups. It uses Tags which can be assigned to users for giving access to make changes.*

*Following are the Role. Tags created.*

* Device Management Administrator
* Application Management Admin
* Endpoint Security Admin
* VPN and Authentication Admin.

**Enrolling GreenLeaf Devices to Intune**

**Intune uses Intra ID for device enrollment**. And every single device enrolled in Intune will have a separate ID.

**SCCM enabled Devices:** These devices still need to be enrolled with the Intune Intra ID Service for centralized management. Intune automatically enrolls them after a co-management feature has been enabled within SCCM and Intune.

**Other Devices (Linux, iPhone, Android):** IT-driven enrollment method is used. In this method all the devices are enrolled at the initial setup of all the devices and are assigned Intra ID.

**Defining Intune policies for device Managment**

**Email Security Policy:** Protecting the outlook app. Prevent devices from forwarding emails to personal emails, downloading attachments, Take screenshots of company emails.

**Device Security Policy:**

Minimum of 8 characters PIN for Devices.

Prevent Backups to personal clouds of the devices

Requirement of Antivirus installed.

**Application Control Policy:**

Automatic Updates of Applications and Software

Disabled Access to public googles play and other app stores,

Disabled Copy and Paste from companies' applications

**Compliance Policy:**

**Device Health:** If all the policies defined are fulfilled device is said to be in health state. If device is not fulfilling all the above policy device is lose access to company data till it meets the requirements

**Remote Wipe Policy:**

**In the case of device Lost**.

- *Device is locked*

*- Device loses all access to company data and network.*

*- If device is found, Device needs to reach compliance state then device is reenrolled.*

**In the case of device Lost.**

*- Device is locked*

*- Device is wiped clean*

**Intune Device Profiles for Green Leaf Devices**

**VPN Profile:**

*Preconfigured with certificate in the VPN profile of the device so. Users just have connected to VPN to access the company network.*

Preconfigured Settings: Profile Name

Device Name

Server Address

Issued Certificate

VPN protocol

**Email Profile:** *This profile allows the device to automatically connect to the company exchange server.*

**Preconfigured Settings:**  Profile Name

Device Name

Issued Certificate

Email Server Address:

SMTP port:

IMAP port:

## 10 Syslog Server

GreenLeaf has a large network infrastructure including routers, switches, firewalls, Servers providing critical services, Mobile Devices, Laptops. All these devices generate logs. But it is nearly impossible to look at each device's logs. So, the company needs a centralized platform for collecting logs. And using those logs to troubleshoot issues or detect any breaches. We use **Kiwi Syslog server from solar winds**. Which is a centralized managed log server. It collects data from all the devices on the network. Format the logs depending on rules and filters to provide useful information and give alerts.

**List of Green Leaf Devices**

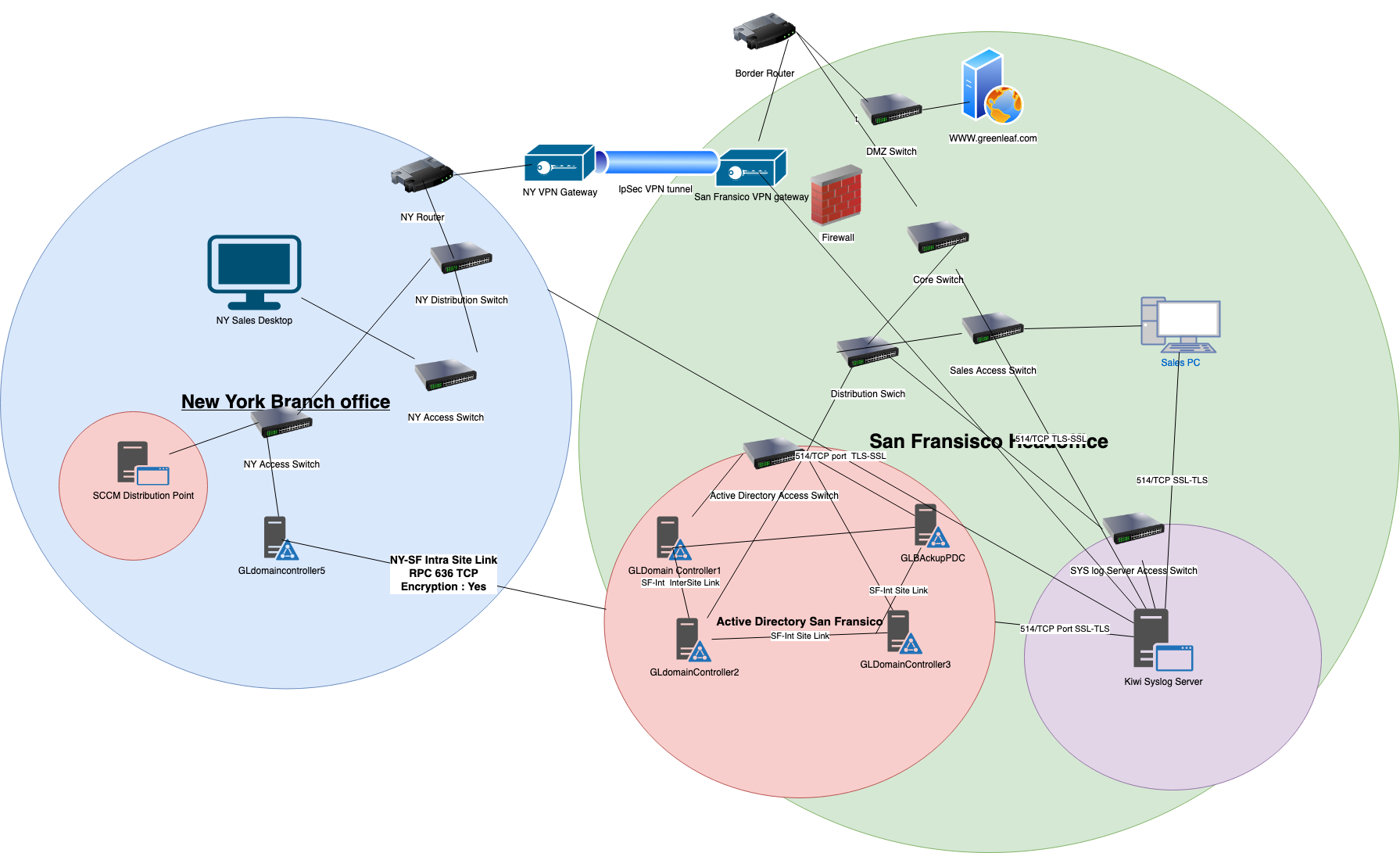
**Network Devices:** Routers, Switches, Firewalls, Wireless Controller, VPN gateways.

**Servers:** DNS, DHCP, Domain Controllers, Email Server, SCCM servers, Webservers

**Mobile Devices:** Intune Log

**Special Devices:** PRTG Monitoring Solution

**Syslog Model for Centralized Log Management**



**Client Devices Configuration**

**Network Devices:**

|  |  |
| --- | --- |
| **Type of Devices** | Network Devices |
| **Protocol and Port** | 514/TCP |
| **Syslog Server Name** | GL\_Syslog |
| **Syslog Server Ip address** | 192.168.5.17 |
| **Push or Pull Mode** | Push |
| **Severity Criteria** | Critical & Important |
| **Logs Format** | JSON (Java Object Notation) |
| **Types of Logs being send** | * Logging attempts * Configuration Changes * Device Online Status * Device Crash |

**Server Logs:**

|  |  |
| --- | --- |
| **Type of Devices** | Servers |
| **Protocol and Port** | 514/TCP |
| **Syslog Server Name** | GL\_Syslog |
|  |  |
| **Syslog Server Ip address** | 192.168.5.17 |
| **Push or Pull Mode** | Push |
| **Severity Criteria** | Critical & Important |
| **Logs Format** | JSON (Java Object Notation) |
| **Types of Logs being send** | * System Disk Storage * System RAM Usage * System Network Usage * Failed Logging Attempts * Admin Account Login * Remote Logging Attempts via SSH * System Crash |

**Mobile Devices:**

|  |  |
| --- | --- |
| **Type of Devices** | Intune |
| **Protocol and Port** | 514/TCP |
| **Syslog Server Name** | GL\_Syslog |
| **Syslog Server Ip address** | 192.168.5.17 |
| **Push or Pull Mode** | Pull |
| **Severity Criteria** | Critical & Important |
| **Logs Format** | JSON (Java Object Notation) |
| **Types of Logs being send** | * Failed Logging Attempts * Admin Account Login * Devices With Bad Health * Intune Policy Changes |

**Special Devices : PRTG Monitoring Solution**

|  |  |
| --- | --- |
| **Type of Devices** | PRTG Monitoring Solution |
| **Protocol and Port** | 514/TCP |
| **Syslog Server Name** | GL\_Syslog |
| **Syslog Server Ip address** |  |
| **Push or Pull Mode** | Pull |
| **Severity Criteria** | Critical & Important |
| **Logs Format** | JSON (Java Object Notation) |
| **Types of Logs being send** | All the Logs |

**Kiwi Syslog Server:**

|  |  |
| --- | --- |
| Syslog Software | Kiwi Syslog Server |
| Operating System | Microsoft Windows Server 2016 |
| No of Servers | 1 |
| Server Locations | San Fransico |
| Server Name | GL\_Syslog |
| Server Ip address | 192.168.5.17 |
| Server Subnet | 192.168.5.17-192.168.5.22 |
| Server Vlan | 240 |
| Server Ports | 514/TCP |
| Logs Filters | * Multiple Failed Login Attempts in sort amount of time * Servers disk space getting full * High Usuage of RAM in the Servers * Suspecius Traffic From the Server * Multiple Failed Attempts to access sensitive file * Network Device Up and Down * Low Priority Messages |

**Alerts and Actions Scheme**

1. **Multiple Failed Login Attempts:** Alert Level Critical, Immediately Send a Email to all the system Administrator and record the event and send the event to SIEM server for analysis
2. **Server Disk Space getting full:** Alert level important, Create a alert on its web interface with warning
3. **Multiple Failed Attempts to access sensitive file:** Alert Level Critical, immediately notify all the Administrators via email
4. **Low Priority Messages:** Direct the Messages to SIEM for analysis

**Rotation and Archiving Scheme**

**Log File Locations**: GL\_Syslog

**Log rotation:** Configured for a new file every 5 days

**Archiving:** Logs older then 60 days (about 2 months) are automatically compressed and Achieved moved to Cloud for Storage

**Retention Policy:** All the Achieved logs file are retained and kept for up to 1 year and for important logs file they are achieved for up to 5 years For Retention of Logs cloud is very suitable with its multi-tier storage of file at very low cost and flexibility.

**Security for Greenleaf Syslog Solution**

SSL-TLS and IPsec VPN tunnel: Secure Logs Transmission using TLS-SSL. All the logs transmitted are encrypted and All the devices are configured to send logs over secure tunnels. All the Traffic is send over a TCP connection within a VPN tunnel as default UDP port is not secure

Authentication and Access: Integrating it with the Companies Active Directory for Multifactor and Role based Access. Using Kerberos for authentication

**Full Disk Encryption: Bit** Locker is used to encrypt the file system where logs are stored. And all the logs are backed up to the cloud in encrypted format

**Network Segmentation:** The Kiwi Server is placed in a separate vlan and Firewall rules are set up for it to receive traffic from source only at 514 TCP port. And SSH traffic is locked down to certain clients.

**Kiwi Server Web Access** is used over HTTPS not HTTP for security.

11Cloud

**Hybrid Cloud Model: A** hybrid cloud model is a cloud adoption model in which a company runs some part of its infrastructure in the cloud and some part is run on-premises. By using this model, a company takes advantage of cloud flexibility, redundancy, Scaling capabilities and Global Reach.

As Green Leaf is a new start-up company with most of its services running on premises. It is not possible to move to cloud directly. So, for green leaf a hybrid solution is a better way to go and then in future green leaf can completely adopt the cloud for running its services.

**Azure Express Route:** Green Leaf is leveraging the Microsoft Azure Express Route to extend its capabilities to clouds. Express Route provides the company with a direct point to point connection to the Azure network. Green Leaf is using this service to connect to the resources running on the cloud.

Azure Blob Storage: Green leaf is leveraging Azures Blob Storage for long term and short-term retention of logs backup for compliance and troubleshooting. As blob storage provides file retention policy, redundancy and long-term storage at cheap price. Company is taking advantage of this policy for storing it slogs

|  |  |
| --- | --- |
| Container Name | GreenleafLogs |
| Storage Account Name | Greenleaf |
| location | Canada |

**Azure File Share:** This Azure Service allows greenleaf to replace all the file servers on premises. And move to cloud for file management. This Azure file share is a headless technology. It integrates with company Active Directroy for access controls. And need a Entra Connect sync server for file syncronization. It offers access control, strict logging and redundancy with failover features

|  |  |
| --- | --- |
| Azure Storage Account | Greenleaf |
| Azure file Share | greenleafFS |
| Regional Redundancy | Yes |
| Local Redundancy | Yes |
| VPN Gateway | IPsec tunnel mode at 415/tcp |
| Active Directory Services | Greenleaf.com |
| Active Directory Services Location | San Fransisco |
| Intra File Sync Server | greenleafFSync |
| Intra File Sync Server Location | San Fransisco |

Green Leaf Cloud Adoption RoadMap:

**Phase 1: Current Solution**

* Azure Blob Storage : Backing up logs to the blob storage for long term retention
* Azure File Share: Replacing on-premises file server
* Azure Express Route: Connecting On-premises to Azure cloud Network

**Phase 2: Azure Virtual Machines & Networking Services**

* Running company public website on the cloud.
* Exchange Server on the cloud
* 5 Azure Virtual Machines Server on Cloud
* Azure VPN service for connecting all the offices of green leaf to cloud
* Azure Firewall for protecting all the VMs on the cloud

**Phase 3: Azure Active Directory, Azure Kubernetes Service**

* Replacing On-premises Active Directory with the cloud.
* Running containerized application by taking advantages of Azure Kubernetes services.

**Phase 4: Azure Database Services:**

Replacing all the on-premises database servers and putting them on the savety net of the cloud

**Thank You**