Network Security Final Project

Table of Contents

[FINAL PROJECT 3](#_Toc163727765)

[Description 3](#_Toc163727766)

[Responsibilities and Tasks 3](#_Toc163727767)

[Minutes of Meeting 4](#_Toc163727768)

[Network Topology 5](#_Toc163727769)

[ Overview 6](#_Toc163727770)

[Network Segmentation 7](#_Toc163727771)

[ Subnetting 7](#_Toc163727772)

[ Zones 8](#_Toc163727773)

[Router 10](#_Toc163727774)

[Switch 10](#_Toc163727775)

[DDoS Protection 11](#_Toc163727776)

[SD-WAN 11](#_Toc163727777)

[Firewall 14](#_Toc163727778)

[Certificate Authority (CA) 16](#_Toc163727779)

[NAC 18](#_Toc163727780)

[IPS/IDS 20](#_Toc163727781)

[Site-to-Site VPN 22](#_Toc163727782)

[Remote Access VPN 25](#_Toc163727783)

[Access Points 26](#_Toc163727784)

[Servers In Server Farm 26](#_Toc163727785)

[Wireless Network 29](#_Toc163727786)

[High Availability 29](#_Toc163727787)

[Threat Assessments 30](#_Toc163727788)

[Security Audits & Penetrating testing 31](#_Toc163727789)

[Security Policies 34](#_Toc163727790)

[ZTNA 35](#_Toc163727791)

[NIST Framework 36](#_Toc163727792)

[Conclusion 37](#_Toc163727793)

# FINAL PROJECT

## Description

The project aims to design and implement a highly secure network architecture for a corporate headquarters and two branch offices. The network topology is meticulously crafted to ensure robust protection against cyber threats while facilitating seamless communication and efficient operations across all locations. At the heart of the network lies the headquarters, serving as the central hub for inter-branch connectivity and external communication. It is equipped with advanced security measures, including redundant firewalls, network access control (NAC), and intrusion detection/prevention systems (IDS/IPS), to safeguard critical assets and data against potential breaches and vulnerabilities.

Each branch office is seamlessly integrated into the network, benefiting from secure inter-branch connections via site-to-site VPN and MPLS technologies. The network architecture at the branches mirrors that of the headquarters, featuring redundant firewalls, core switches, and distribution switches to ensure reliability and resilience.

Key components of the network include a DMZ zone for hosting public-facing web and application servers, an inside zone for company devices, a server farm for critical infrastructure services, and a guest zone for providing Wi-Fi access to visitors. These zones are carefully segmented and protected by robust security measures to minimize the risk of unauthorized access and data breaches. By implementing this highly secure network architecture, the organization can mitigate cyber threats, maintain regulatory compliance, and safeguard its reputation and business continuity. The project represents a proactive approach to cybersecurity, prioritizing the protection of sensitive information and ensuring the integrity and availability of network resources.

## Network Topology

A diagram of a computer network

Description automatically generated with medium confidence

A diagram of a computer network

Description automatically generated

## Overview

The network topology chart maps out a detailed layout of an enterprise's digital communications framework, featuring a central command center (HQ) and satellite branches. This setup is intricately outfitted with various devices and protective mechanisms that knit together to foster a secure and streamlined flow of information across the organization. Delving into the diagram reveals a sophisticated interplay of elements and processes:

**Headquarters (HQ):**

* The HQ's main router is the guardian of internet connectivity, directing data across the internal MPLS network and ensuring secure connections through the VPN.
* A specialized DDoS protection layer shields the entire network, acting as a digital bulwark against volumetric cyber threats.
* The firewall is the definitive sentinel, delineating the network's secure precincts and regulating traffic through the network's internal byways, known as VLANs.
* The core switch at HQ serves as the central hub, a juncture point where data streams are dispersed to their rightful destinations across the organizational web.

**Security and Compliance Nexus:**

* The NAC reinforces the network's defences, granting access solely to verified devices.
* The IDS/IPS keeps a vigilant watch over data transit, thwarting potential incursions and unsanctioned activities.
* Within HQ lies the server farm, a robust repository hosting an array of critical servers, each serving pivotal roles from data backup to security and asset oversight.

**Zonal Structure:**

* The Inside Zone carves out specialized enclaves within the HQ for varying service and server activities.
* Like a borderland, the DMZ facilitates external access to services while maintaining a quarantine from the internal sanctum.
* The Guest Zone caters to visitors, offering them a portal to the internet while shielding the internal network's core.

**Branch Outposts:**

* Branches 1 and 2 mirror the HQ's structural essence, each possessing its routers and firewalls, all orchestrated to maintain internal harmony and secure communication conduits.
* VLANs are the threads in the tapestry, segmenting traffic flow to maintain order and efficiency within each branch.

**Connective Tissue:**

* The MPLS veins provide a rapid and stable conduit for inter-site communication, ensuring data courses swiftly between the network's extremities.
* The VPN pathways offer an encrypted alternative for data travel, wrapping communications in a secure envelope over the internet.

**Protective Services:**

* The WAF within the DMZ stands as a digital shield, guarding web applications against a spectrum of cyber threats.
* A suite of server services - from authentication protocols to endpoint defences and resource tracking - forms a comprehensive security matrix.

**Network Vigilance:**

* Network monitoring systems persistently survey the network's pulse, poised to detect and rectify any anomalies in the digital stream.

**Auxiliary Components:**

* Wi-Fi networks, scattered across the VLANs, extend the reach of connectivity, unshackling devices from wired constraints.
* Backup systems anchor the server farm, ensuring an unbreakable chain of data custody and swift restoration capabilities.
* Management systems like MDM and Patch Manager are device integrity and software currency custodians.
* This network topology unfurls as a multi-layered digital organism, balancing the trinity of functionality, efficiency, and security. It reflects a deliberate design ethos, encapsulating zones tailored for diverse access levels and service demands. Advanced security integrations manifest a vigilant stance toward safeguarding the network's digital frontier. The comprehensive server farm embodies the network's commitment to sustaining a robust infrastructure that supports the organization's expansive processes and the vast spectrum of data stewardship.

## Network Segmentation

**Description**

Network segmentation is the process of breaking up a large network into more manageable, isolated zones or parts. Stricter access restrictions, reducing the impact of security breaches, and network performance optimization are the main goals of network segmentation. Customizing segmentation strategies to fit unique organizational demands is possible by considering variables such as organizational structure, security requirements, and functional responsibilities within the network. Two methods that are often used in network segmentation are subnetting and zoning.

## Subnetting

**Description**

IP addresses may be allocated more effectively by subnetting, which divides the large IP address space into smaller, easier-to-manage portions. Subnets share the same main network address but have a unique subnet mask that defines the portion dedicated to specific devices within the subnet. This allows for more efficient use of IP addresses and improved control over network traffic. By restricting communication between various network segments and lowering the possibility of unwanted access, subnetting enables organizations to apply access restrictions and security rules at the subnet level.

**Method Of Procedure (MOP)**

* Navigate to the Network section and then Interfaces in the Firewall management interface.
* Locate the physical interfaces connected to your access switches for each VLAN.
* Locate the section for IPv4 Address or similar within the interface configuration. Here, you can assign the subnet for the corresponding VLAN.

VLAN 100: 172.16.1.0/24

VLAN 110: 172.16.2.0/24

VLAN 200: 172.16.3.0/24

VLAN 300: 172.16.4.0/24

VLAN 500: 172.16.5.0/24

VLAN 10: 172.16.6.0/24

VLAN 20: 172.16.7.0/24

VLAN 30: 172.16.8.0/24

VLAN 40: 172.16.9.0/24

VLAN 50: 172.16.10.0/24

VLAN 60: 172.16.11.0/24

VLAN 70: 172.16.12.0/24

* After configuring each interface with the appropriate subnet details, click OK to save the changes.

**Observation**

The implemented subnetting with /24 blocks for each of the 12 VLANs (VLAN 100, VLAN 110, VLAN 200, VLAN 300, VLAN 500, VLAN 10, VLAN 20, VLAN 30, VLAN 40, VLAN 50, VLAN 60, VLAN 70) creates a more efficient and secure network environment. This allows for better IP address allocation, simplifies network management by segmenting devices, and strengthens security by restricting traffic flow between VLANs. The clear separation and ample address space within each subnet also make it easier to manage and scale the network in the future.

## Zones

**Description**

Network resources are grouped into security zones according to their security requirements through zoning, which enables organizations to set strict access restrictions and security standards between various network segments. Zoning protects critical assets from compromise by dividing network resources into distinct zones, which stops threats from moving laterally and restricts security events.

**Method Of Procedure (MOP)**

* **Headquarters (HQ):**
  + Inside Zone (VLAN 10 - Wired, VLAN 20 - Wireless):
    - **Wired Section (VLAN 10):** Computers, printers, and file servers are among the internal equipment of the company located.
    - **Wireless Section (VLAN 20):** Allows employees to use their own devices—such as phones and laptops—for work-related tasks.
  + **DMZ Zone (VLAN 500):** Contains application servers and web servers accessible from the internet.
  + **Server Zone (VLAN 30):** Houses critical backend servers like:
    - Backup and Storage Servers
    - Asset Manager
    - Multi-Factor Authentication (MFA) Server
    - Mobile Device Management (MDM) Server
    - Patch Manager
    - Security Information and Event Management (SIEM) Server
    - Endpoint Detection and Response (EDR) Server
    - Network Monitoring Servers:
    - Database Servers:
    - File Server
  + **Guest Zone (VLAN 40):** Provides internet access for guests in HQ, with restricted access.
* **Branch 1:**
  + **Inside Zone (VLAN 110 - Wired, VLAN 200 - Wireless):**
    - Wired Section (VLAN 110): Contains internal devices like computers and printers in Branch 1.
    - Wireless Section (VLAN 200): Allows employees in Branch 1 to connect personal devices for work purposes.
  + **Guest Zone (VLAN 300):** Provides internet access for guests in Branch 1, with restricted access.
* **Branch 2:**
  + **Inside Zone (VLAN 50 - Wired, VLAN 60 - Wireless):**
    - Wired Section (VLAN 50): Contains internal devices like computers and printers in Branch 2.
    - Wireless Section (VLAN 60): Allows employees in Branch 2 to connect personal devices for work purposes.
  + **Guest Zone (VLAN 70):** Provides internet access for guests in Branch 2, with restricted access.

**Zoning Setup**

* Access the Firewall web interface.
* Navigate to **Network** > **Zones**.
* Create zones for each HQ, Branch 1 and Branch 2 zones (Inside - Wired & Wireless, DMZ, Server for HQ only, Guest).
* Configure zone details and assign member interfaces based on their corresponding VLANs.

**Observation**

The implemented zoning structure, utilizing distinct VLANs (/24 blocks for VLAN 100, 110, 200, 300, 500, 10, 20, 30, 40, 50, 60, 70) and dedicated zones (Inside, DMZ, Server, Guest), creates a more secure and manageable network. This approach optimizes IP allocation, simplifies administration by segmenting devices, enhances security through traffic control between zones, and allows for future scalability due to the clear separation and ample address space within each subnet.

## Router

A router is a traffic director for the network, deciding the best path to send data between devices and potentially connecting our network to the wider internet.

* **Branch 1 Router and Branch 2 Router:** These routers connect the Branch 1 and Branch 2 locations to the HQ (Headquarters) network. They are responsible for routing traffic between the branch locations and the HQ. They also likely connect the branch locations to the internet. They typically use SD-WAN to manage traffic flow across different internet connections, like MPLS and site-to-site links. This redundancy ensures a reliable connection even if one path fails.
* **HQ Router:** The HQ router acts as the central router for the network, routing traffic between the Branch 1 and Branch 2 locations, and likely also connecting the HQ network to the internet. It can also leverage SD-WAN for optimal routing across its connections.

## Switch

A switch is a networking device used to forward data packets between devices connected to a network. Different types of switches, such as distribution switches and core switches, are used in our design to effectively handle network traffic and provide dependable connectivity.

**Distribution Switch**

* Connects multiple access switches, which connect devices like computers and servers, to the core switch.
* Acts as a security barrier by controlling traffic flow between different VLANs.
* VLANs can be created to segment the network based on department, function, or security requirements.
* Provides high-speed connections to the core switch for efficient data transfer between network segments.
* The distribution switch thoroughly controls the flow of data between these VLANs. It acts as a security barrier, preventing unauthorized communication between zones. For example, it ensures the internet zone doesn't exchange data with the sensitive DMZ or the guest zone, enhancing overall network security.

**Core Switch**

* Forms the backbone of the network, providing high-speed connections between all the distribution switches.
* Acts as a central hub for data communication between different network segments.
* Typically has more processing power and higher bandwidth capacity than distribution switches.
* It remains the central nervous system of the HQ network, interconnecting major devices like the distribution switch, firewalls, and servers.
* Branch core switches would connect to the HQ core switch for communication between the HQ and branch offices. This connection could utilize MPLS, site-to-site links, or the internet.
* While the core switch connects to major devices, it likely doesn't directly connect to user devices or individual VLANs. This segregation enhances security and manageability.

## DDoS Protection

At the network's entry point, just before the protective embrace of the firewall, sits an advanced DDoS protection system, strategically stationed to act as the vanguard against volumetric cyber threats. This system operates with the precision of a digital sieve, meticulously filtering the vast streams of data packets flowing towards the HQ, singling out and discarding the malicious deluge that characterizes DDoS onslaughts.

This DDoS protection not only serves as a bulwark, shielding the firewall and the network's inner sanctum from data floods, but it also functions with surgical efficiency to ensure that the firewall's resources are judiciously reserved for scrutinizing more nuanced traffic patterns. With an array of mitigation tactics at its disposal, from rerouting egregious traffic to throttling down the deluge to a trickle, the system is adept at defusing the potency of an attack right at the network's doorstep.

The integration of this DDoS protection into the network's gateway is both smooth and sophisticated, maintaining a state of constant vigilance while remaining unobtrusive during regular traffic flow. It reacts instinctively to any signs of an attack, with minimal need for human intervention, underscoring its role as an autonomous guardian of the network's gateway.

By situating this layer of defense at the forefront, the network architecture exhibits a multi-tiered defense strategy. It's a deliberate design choice that recognizes the complexity of modern cyber threats and counters them with a diverse array of defense mechanisms, each with its own area of expertise, all working in concert to fortify the network's defenses.

## SD-WAN

**Description**

The network topology indicates a three-site organization, including a main headquarters (HQ) and two branch offices. The design incorporates multiple security layers and network segmentation using VLANs.

**HQ:**

The HQ houses the central network resources, including a core switch that connects to a firewall for external traffic management. An IDS/IPS solution is in place for threat detection and prevention. The network includes a Network Access Control (NAC) system, suggesting a robust security posture with access management. Additional network services such as DDoS protection before the firewall, multi-factor authentication (MFA), endpoint detection and response (EDR) in the server farm, and web application firewall (WAF) are integrated to enhance security. A site-to-site VPN suggests existing secure connectivity to the branch offices. A VLAN structure is evident, segregating traffic into different zones such as DMZ, Guest, and Internal networks.

**Branch Offices:**

Both branches mirror a similar, scaled-down setup with a router connecting to a firewall, which then connects to a core switch. The branches also utilize VLANs to segregate traffic internally.

For SD-WAN implementation, the following steps align with the existing topology:

* Install SD-WAN appliances at each location to connect to the Internet and MPLS circuits for dual transport functionality.
* The SD-WAN appliances will be seamlessly added to the current VLAN configuration, preserving the current traffic segmentation, and adhering to the security policies.
* The SD-WAN will control the site-to-site VPN connections and MPLS, selecting the best path based on application needs, live link performance, and set policies.
* Improved Security: By implementing IDS/IPS at the headquarters, the SD-WAN will collaborate with these security measures to guarantee complete visibility and protection against threats for all network traffic.
* Centralized Management: By utilizing the centralized control plane of the SD-WAN, network administrators can oversee performance, set policies, and control traffic for all three sites from the headquarters.
* The SD-WAN offers automated failover between MPLS and Internet connections to ensure continuous connectivity for essential applications, demonstrating resiliency.
* Application-Aware Routing: Implementing application-aware policies to dynamically direct traffic through the most optimal path, enhancing performance and user satisfaction.
* This network structure enables a robust, safe, and adaptable SD-WAN implementation, utilizing MPLS and Internet connections to enhance connectivity and application performance throughout the organization.

**Method Of Procedure (MOP)**

MOP for Configuring Inter-Site Connections with SD-WAN

**Part 1: Pre-Deployment**

* Inventory Verification and Configuration Backup.
* Equipment Check: Verify that all the hardware in the network topology is accounted for and operational.
* Backup Configuration: Back up the current configurations of all devices that will be modified.
* Documentation Preparation: Prepare a detailed documentation package, including IP schemes, device roles, and login credentials.

**Part 2: MPLS and VPN Provisioning**

**MPLS Setup:**

* Coordinate with the MPLS provider to confirm pertinent information, including the PE-CE routing protocol and any necessary QoS.

**Test MPLS Connectivity.**

**Site-to-Site VPN:**

* Establish VPN Parameters, configure VPN Tunnels, and Test the VPN's connectivity.

**Part 3: SD-WAN Configuration**

**SD-WAN Edge Installation:**

* Deploy SD-WAN appliances at HQ and branches.
* Connect each appliance to the respective MPLS and Internet links.

**SD-WAN Overlay Network Setup:**

* Configure the overlay network to use both MPLS and Internet underlays.
* Validate that each SD-WAN appliance can reach the others across both underlays.

**Traffic Steering and Policies:**

* Define and apply traffic steering rules on the SD-WAN appliances.
* Implement QoS policies, as per organizational needs, to prioritize critical applications.

**Part 4: Integration and Routing**

**Integrate with Existing Network:**

* Ensure that the SD-WAN appliances are integrated with the existing VLAN configurations at each site.
* Update routing protocols to include the SD-WAN appliances in the path selection process.

**Policy Implementation:**

* Update firewall rules at HQ and branches to allow SD-WAN management traffic.
* Coordinate with the NAC and IDS/IPS to align with the new SD-WAN deployment.

**Part 5: Testing**

**Functionality Testing:**

* Perform end-to-end connectivity tests for Internet access and inter-site communications via MPLS and the VPN across the SD-WAN.
* Test application traffic to ensure correct path selection by SD-WAN policies.

**Resiliency Testing:**

* Simulate failures to verify automatic failover and traffic rerouting.
* Ensure that the IDS/IPS correctly detects traffic across the SD-WAN network.

**Part 6: Monitoring and Management**

**Monitoring Tools Configuration:**

* Set up monitoring for the MPLS, VPN, and SD-WAN links.
* Integrate SD-WAN monitoring into the existing network monitoring platform.

**Management and Reporting:**

* Configure centralized management for the SD-WAN to provide visibility into network performance.

**Part 7: Documentation and Handover**

* Final Documentation: Update network diagrams and configurations reflecting the changes made during the SD-WAN implementation.
* Training and Handover: Provide necessary training to the operations team on managing and troubleshooting the SD-WAN setup.

**Part 8: Post-Deployment**

* Operational Handover: Transition of the new SD-WAN setup to the operations team for day-to-day management.
* Review and Compliance: Ensure the new setup meets all organizational and regulatory compliance standards.

**Final remarks**

* Change Management: Every modification must undergo a change management approval process before implementation.
* Plan Outages: Let everyone know when planned breaks are made for testing, implementation, and changes.
* Continuous Improvement: After deployment, get user feedback to help the SD-WAN solution get better over time.

This MOP is a preliminary framework that might need to be modified as the deployment continues. It's critical to constantly communicate with all stakeholders throughout the process and adjust to unforeseen obstacles.

**Low Level Diagram**

A diagram of a computer network

Description automatically generated

## Firewall

**Description:**

Firewalls are software applications or hardware devices used to provide network security for organizations/businesses of all sizes. They are security measures used to control incoming and outgoing traffic of a network. Preconfigured security rules are typically used to monitor and filter traffic against malicious activities, unauthorized access preventing security breach which if unmitigated, could lead to expensive negative repercussions for an organization or entity. As per our topology, the intended Firewall to be used is the Palo Alto Next-Generation Firewall. With the Palo Alto firewall, it offers a simplified, unified, and centralized configuration platform making it easy to set rules, policies and monitor an organization’s network. As per our topology, a total of 6 palo alto firewalls were deployed. Two firewalls were deployed to each site for redundancy purposes if one of the firewalls does fail. This would ensure high availability of the firewall implementation. In addition to the palo-alto firewall, an extra layer of firewall is deployed. The WAF (web application firewall) is deployed to protect the DMZ zone. It filters traffic that comes from the internet. Suspicious traffic trying to have access to the DMZ zone are blocked.

**Method Of Procedure (MOP)**

This section outlines the Method of Procedure (MOP) which can be used to install and configure the Palo Alto Network Firewall.

* Preparatory Steps:
  + **Information gathering:** All necessary information like IP addresses, default gateway, should be retrieved, subnet masks should be gotten. Note that the network agreed upon by the IT Team lead is 172.16.1.0/24 with CIDR /24. Receive further confirmation and approval from IT-Team lead before proceeding or commencing any configuration.
  + **Spin-up management computer**: Ensure that the management computer is set up on network. It should have necessary connectivity to the firewall.
  + **Install firewall**: Ensure that the firewall physical device is mounted on rack and turned on.
* Configure Web Interface:
  + **Connect interface**: Based on network topology, ensure that the appropriate network cables are connected to the firewall.
  + **Configure Management IP**: A static IP address should be configured on the machine to serve as default web interface. Use 172.16.1.1
  + **Change default login details**: Using the default login details, login to the firewall web interface. Change the default configuration immediately after entry. Document this information and provide it to the necessary personnel.
* Network and Security Policy Configuration:
  + **Configure network interfaces:** In thefirewall’s network interface, assign appropriate configurations (IP addresses, default gateway, subnet masks) based on network design.
  + **Configure Security Zones**: Categorize network trafficto setupnetwork’s security zones.
  + **Configure Security:** Define network traffic that is allowed/blocked to control traffic flow in your network.
* Test Connection:
  + **Verify connectivity and policies:** Verify your network connectivity by pinging resources. Remember to enable ping management ping.

**Observation**

* **Centralized Management**: In Palo Alto, management features like Panorama arise that will allow you to manage, configure, and process reports for NGFWs that are deployed on multiple networks. These centralized implementations drive security processes management that makes it simple to have your infrastructure secured, as well as maintaining coherent security policies.
* **Traffic Inspection**: Palo alto NGFW is way more sophisticated than ordinary firewalls that encounters traffic only via ports and trading protocols; it goes deeper and inspects the traffic content to monitor the data exchange. This helps them spot where the bad guys hide, such as advanced malware, zero-day attacks or application layer threats that can otherwise bypass the regular firewalls.
* **Application Identification & Control**: Through these NGFWs you can establish what specific applications are moving through the network e.g. web browsers, video streaming or social media. This enables that to be considerably detailed through the ability of allowing or denying certain application based on particular security policies. Additionally, you can enable a throttling mode that allows you to prioritize business critical applications like video conferencing and control access to social media and gaming applications.
* **Threat Prevention**: Palo Alto NGFWs use advanced threat intelligence feeds and machine learning scan into non-friendly situation and block known and unknown threats instantly as they happen. Within this paradigm, security providers should identify malware by sandboxing, where malicious files are detonated in a safe virtual environment for behavior analysis.
* **Integration with Security Ecosystem**: Palo Alto NGFWs have capabilities to work with endpoint protection platforms (EPP) too. Efficient integration of multiple security solutions provides a strong security infrastructure. This ensures that any control of integrated security and threat intelligence shared among the units fortifies the security over and above the network.

## Certificate Authority (CA)

**Description:**

Certificate Authority (CA), a digital middleman trusted by other certificates is typically used to verify the identity of websites, servers, important applications and in many cases even network users. CA’s typically issue out digital certificates which are just like your e-passports which contains an entity's verifiable identity and special key to encryption. The purpose of this is to ensure that every certain communication at any given time is safe. This helps to ascertain that one is communicating with one who claims to be who they say they are. Certificates Authority verify information using strong key and sign a certificate that can be used to create a chain of trust. What this does is that it gives guarantee that the data is authentic, personal data is encrypted and that integrity of the data has not been tampered with. As per our topology, the CA would be deployed in the server farm which is situated in the headquarters site.

**Method Of Procedure (MOP)**

**1.Installation and configure of CA Server:**

•Install the CA server software on a dedicated server within your network. Operating system for the server can be any flavor of Linux.

•Configure the CA server with information such as its name, validity period of issued certificates, and cryptographic settings.

**2.Create a Root Certificate:**

•Use CA software to generate the root certificate. This would serve as a basis of trust for all other certificates issued that would be issued by this CA.

•Secure the private key of the root Certificate.

**3.Issue Server and User Certificates:**

•Clients (servers or users) make certificate signing requests (CSRs) containing their public key and identity information.

•This request should be validated by the CA server. After approving, it should issue signed certificates making use of the root certificate’s private key.

•Clients should then be able to install signed certificates in order to establish communication.

**Observation(Expected Security Outcome)**

•With respect to the proposed topology, the implemented certificate authority housed in our server farm would serve as an authentication agent that would verify an entity’s identity within our network.

•A very important feature that a certificate authority has is that it is able to generate a certificate that can be used to represent an entity’s identity within a network. As such, data integrity is assured.

•By using certificate authority, communication is secure since encryption is implemented. The encrypted data can be decrypted only by authorized parties that have the decryption key

When a certificate is compromised, the CA’s are able to invalidate a compromised certificate by using a revocation mechanism. As such, once a compromised certificate is identified, trust is removed from the certificate making it known within the network that the certificate is no longer trustworthy. This can prevent unauthorized access to a network’s resource.

## NAC

**Description**

Network Access Control (NAC) is a security solution implemented at the network entry points to enforce policies and ensure that only authorized devices and users can access the network. In this topology, NAC will be deployed at the headquarters to regulate access to the Inside Zone, where company devices are connected.

**Method Of Procedure (MOP)**

**Step 1: Define NAC Policies:**

Determine the criteria for granting network access, including device type, user identity, health status, etc.

Configure policy rules specifying allowed and denied access based on these criteria.

**Step 2: Install NAC Solution:**

Install and configure the NAC solution on a dedicated server or appliance.

Ensure integration with existing network infrastructure, including switches and firewalls.

**Step 3: Configure Switch Ports:**

Identify switch ports connected to devices in the Inside Zone.

Configure these switch ports to operate in NAC enforcement mode.

**Step 4: Implement Authentication Mechanisms:**

Set up authentication methods such as 802.1X, MAC authentication, or captive portal for user/device authentication.

Integrate with existing authentication servers if applicable (e.g., Active Directory).

**Step 5: Establish Health Assessment:**

Implement mechanisms to assess the health status of connecting devices (e.g., antivirus, OS patches, firewall status).

Define actions for devices failing health checks (e.g., quarantine, remediation).

**Step 6: Monitor and Logging:**

Enable logging and monitoring features to track network access attempts and policy violations.

Configure alerts for suspicious activities or policy breaches.

**Observation**

**Role-Based Access Control (RBAC) Policy:**

* Identify different user roles within the organization based on job responsibilities (e.g., network administrators, regular employees, guests).
* Define access privileges for each role, specifying which resources and zones they can access.
* Configure RBAC rules to enforce these access restrictions at the network entry points (e.g., switch ports, wireless access points).

**Device Authentication Policy:**

* Require all devices connecting to the network to authenticate before gaining access.
* Implement 802.1X authentication protocol for wired connections and WPA2-Enterprise for wireless connections.
* Integrate with authentication servers (e.g., RADIUS) to validate user credentials and device identity.

**Health Check Policy:**

* Define health assessment criteria to ensure connecting devices meet security standards before granting access.
* Require devices to have up-to-date antivirus software, operating system patches, and firewall enabled.
* Configure NAC to conduct health checks upon device connection and periodically thereafter.

**Guest Access Policy:**

* Establish policies for granting temporary access to guests and visitors.
* Limit guest access to specific zones (e.g., Guest Zone) and resources, while restricting access to internal networks.
* Implement captive portal authentication for guest users, requiring them to accept terms of use before accessing the network.

**Quarantine Policy:**

* Define actions to be taken for devices failing health checks or violating access policies.
* Quarantine non-compliant devices in a separate network segment (e.g., Quarantine Zone) with limited access to remediation resources.
* Notify administrators and users of quarantine actions and provide instructions for remediation.

**Policy Enforcement:**

* Specify enforcement mechanisms for implementing NAC policies at network entry points.
* Configure access control lists (ACLs) on switches and firewalls to enforce role-based access restrictions.
* Implement VLAN segmentation to isolate different user groups and zones based on their access policies.

## IPS/IDS

**Description:**  
IDS and IPS are essential safeguards in network security, aiming to identify and block malicious activities in a network setting. Let's delve into the specifics of each:

**Intrusion Detection Systems**

**Objective:** IDS monitors network and system flows and pinpoints suspicious activities or contradicting security norms. It's designed to catalogue such incidents, maintain logs, and notify the network's overseer or a central management framework.

**Variants:**

* Network-centric IDS (NIDS): This variant monitors the entire network's traffic.
* Host-centric IDS (HIDS): Focuses on monitoring the data flow to and from a singular computer or host.

**Detection Techniques:**

* Pattern-based detection matches the network's data flow against known threat patterns or signatures repository.
* Deviation-based detection: Sets a standard for regular activity and marks any divergence from this norm as a potential threat.
* Reaction: Typically, IDS's role ends at detection and notification, leaving the response to the potential threat to be manually managed or addressed by other mechanisms.

**Intrusion Prevention Systems**

**Objective:** IPS carries a mantle similar to IDS, scrutinizing network or system activities. However, it stands out with the authority to undertake automatic actions to thwart or alleviate detected threats. It integrates into the network's data flow, analyzing and implementing real-time preventive actions.

**Variants:**

* Network-centric IPS (NIPS): Ensures the protection of the network by scrutinizing both incoming and outgoing traffic.
* Host-centric IPS (HIPS): Installed on individual hosts, it aims to detect and counteract threats directed at those specific hosts.

**Detection and Prevention Techniques:**

* It employs detection techniques similar to those of IDS, using pattern-based and deviation-based methods.
* Capable of implementing measures like traffic blocking, connection resets, and network device reconfiguration to counter threats.

**Reaction:** Unlike IDS, IPS can autonomously respond to threats, eliminating the need for manual intervention.

**Distinctive Aspects**

* Intervention: The core distinction lies in their mode of operation; IDS is about detection and notification, whereas IPS extends its functionality to prevent and mitigate threats.
* Network Positioning: While IPS is usually positioned in line with the network traffic for active monitoring and immediate response, IDS is placed externally, monitoring a duplicate of the network traffic.

In essence, IDS and IPS are critical to bolstering network security. IDS is dedicated to detecting and alerting threats, and IPS provides the enhanced functionality of actively preventing and mitigating potential security breaches.

**Method Of Procedure (MOP)**

**Part 1 – Installation of Essential Packages and SNORT**

Install the necessary packages:

Update the package repository: yum install epel-release

Install the DNF package manager: yum install dnf

Install SNORT: dnf install https://www.snort.org/downloads/snort/snort-2.9.20-1.centos.x86\_64.rpm

**Part 2 – Configuring SNORT for IDS**

**Basic configuration:**

Refresh shared library cache: ldconfig

Verify SNORT installation: snort -v

If there's an error, link libraries: ln -s /usr/lib64/libdnet.so.1.0.1 /usr/lib64/libdnet.1

**Create necessary directories and set permissions:**

mkdir -p /etc/snort/rules

mkdir /var/log/snort

mkdir /usr/local/lib/snort\_dynamicrules

Apply permissions: chmod -R 5775 /etc/snort, /var/log/snort, /usr/local/lib/snort\_dynamicrules

**Initialize rule files:**

touch /etc/snort/rules/{white\_list.rules,black\_list.rules,local.rules}

**Setting up Pulledpork (a tool for managing SNORT rules):**

Install Perl modules: dnf install perl-libwww-perl perl-core perl-LWP-Protocol-https

**Clone and set up Pulledpork:** git clone https://github.com/shirkdog/pulledpork.git

cd pulledpork/

**Move and make the script executable:** cp pulledpork.pl /usr/local/bin && chmod +x /usr/local/bin/pulledpork.pl

**Copy configuration files:** cp etc/\*.conf /etc/snort

**Prepare IP lists:** mkdir /etc/snort/rules/iplists && touch /etc/snort/rules/iplists/default.blocklist

**Validate Pulledpork setup:** pulledpork.pl -V

**Integrate Pulledpork with SNORT:**

Modify snort.conf to include rules: Append rule paths to snort.conf.

Obtain an Oinkcode by registering at SNORT and configure it in pulledpork.conf.

Execute Pulledpork to update the rules: pulledpork.pl -c /etc/snort/pulledpork.conf

Configuring Network and Rules in SNORT:

**Define network settings and paths in snort.conf.**

Test SNORT's configuration: snort -T -c /etc/snort/snort.conf

If there are issues, adjust the snort.conf file accordingly.

**Deploying and Testing SNORT:**

Add test rules to local.rules and set SELinux to Permissive: sudo setenforce 0.

Run SNORT in console mode to monitor traffic: snort -c /etc/snort/snort.conf -A console -i ens192.

Test the setup by generating ICMP traffic and observing alerts.

By following these steps, you will have a functional IDS using SNORT to monitor network traffic for suspicious activities.

## Site-to-Site VPN

**Description**

Setting up a site-to-site VPN (Virtual Private Network) between a data center and its branches is a standard method for ensuring safe internet communication and data exchange. This enables branch offices to securely access data center-hosted resources such as programs, databases, and shared files as if they were directly connected to the local network.

**Method Of Procedure**

Setting up a site-to-site VPN (Virtual Private Network) in Palo Alto Networks firewall involves several steps. Here's a general overview of how to configure a site-to-site VPN between two Palo Alto Networks firewalls:

**Prechecks:**

* Ensure that Palo Alto Networks firewalls have valid licenses for VPN functionality. This includes Global Protect and Threat prevention.
* Determine each firewall's public IP address. This IP address will be used to establish a VPN connection and must be reachable over the Internet.
* Determine pre-shared keys (PSKs) to authenticate the VPN connection between the client device or VPN server or between two VPN gateways. It's essential to choose a strong and unique PSK to ensure the security of the VPN connection.
* Plan the local and remote networks that are accessible over the VPN tunnel. We should use the subnets and IP ranges that are in the Organization’s network.

**Firewall Setup:**

* Log in to the Palo Alto Networks firewall web interface.
* Assign Interfaces to the firewall. Go to Network > Interfaces to access the interface configuration page. Configure basic settings for each interface, including IP address, subnet mask, MTU (Maximum Transmission Unit), and interface mode (e.g., Layer 3, Layer 2, virtual wire).
* Add a virtual router. Go to Network >Virtual Routers
* Create a static route. Specify the destination network or IP address and subnet mask for the static route. It defines the network or destination that you want to reach. Enter the next hop IP address or gateway for the route. This is the IP address of the next-hop router or interface through which traffic will be forwarded to reach the destination network.

**Configure IKE Gateway**:

* Navigate to Network > Network Profiles > IKE Gateways.
* Create a new IKE Gateway profile.
* Specify the public IP address of the remote firewall and configure IKE (Internet Key Exchange) parameters such as encryption algorithms, authentication methods, and Diffie-Hellman (DH) groups.

**Configure IPSec Crypto Profile**:

* Navigate to Network > Network Profiles > IPSec Crypto.
* Create a new IPSec Crypto profile.
* Define the encryption and authentication algorithms for IPSec VPN tunnels.

**Configure IPSec Tunnel**:

* Navigate to Network > IPSec Tunnels.
* Create a new IPSec tunnel.
* Associate the previously configured IKE Gateway and IPSec Crypto profiles with the tunnel.
* Specify the local and remote endpoints for the VPN tunnel and the local and remote networks that will be accessible over the tunnel.

**Configure Proxy IDs**:

* Define Proxy IDs to specify which local and remote networks can communicate over the VPN tunnel.
* Navigate to Network > IPSec Tunnels > Proxy IDs.
* Create Proxy IDs for each pair of local and remote networks that need communication.

**Configure Security Policies**:

* Define security policies allowing traffic flow between the local and remote networks over the VPN tunnel.
* Navigate to Policies > Security.
* Create security policies allowing traffic from the local zone to the VPN tunnel interface and vice versa.

Review the configuration settings for the virtual router to ensure accuracy and completeness. Once satisfied, commit the changes to apply the new virtual router configuration to the firewall.

**Testing and Validation**:

* Test the VPN connection by initiating traffic between the local and remote networks.
* Ensure the tunnel is established successfully and traffic flows as expected.

**Documentation and Backup**:

* Document the VPN configuration, including IKE and IPSec parameters, Proxy IDs, and security policies.
* Regularly back up the firewall configuration to ensure that VPN settings are preserved in case of hardware failure or configuration changes.

**Observation**

Site-to-site VPNs are useful for **companies prioritizing private, protected traffic** and particularly helpful for organizations with more than one office spread out over prominent geographical locations. By establishing encrypted tunnels over the internet, site-to-site VPNs ensure that data transmitted between locations remains confidential and protected from unauthorized access. This encrypted communication, coupled with authentication mechanisms, safeguards against eavesdropping, data tampering, and unauthorized intrusions. Moreover, VPNs enable secure remote access to network resources, facilitating seamless connectivity for authorized users while enforcing access controls to prevent unauthorized entry. With centralized management and monitoring capabilities, administrators can efficiently configure security policies, monitor VPN connections, and detect potential threats across all connected sites. Additionally, VPNs aid in compliance with regulatory requirements by safeguarding sensitive data in transit and ensuring adherence to data protection and privacy standards. Overall, site-to-site VPNs serve as a cornerstone of network security architecture, offering a robust framework for protecting organizational assets and maintaining secure connectivity across distributed network environments.

* **IPsec (CIA)**

IPSec is a layer3 protocol suite that secures data in transit across VPN.

IPSEC VPN peers establish a **Security Association (SA),**a “connection” or “policy” between the two endpoints of the VPN tunnel. An SA is a **one-way**virtual tunnel between the VPN peers; Thus, for full communication between peers to occur, *two*SA’s must be established, one for each [direction. To](https://direction.to/) have an established SA, several parameters should be negotiated between two peers, and here is the role of the I**nternet Key Exchange (IKE**) protocol. Before anything, we need here to have a defined IKE Policy at each peer to be negotiated by IKE protocol with the far-end peer and make sure they are matched.**IKE Policy Sets**several parameters, including:

* The **encryption algorithm**(such as DES, 3DES, or AES).
* The **hashing algorithm**(such as MD5 or SHA-1).
* The **authentication method**(such as shared keys or RSA signatures).
* The **Diffie-Hellman (D-H) group**for creating and sharing keys.
* The **SA Lifetime**is measured in seconds or kilobytes sent.

That step is called “**IKE Phase 1**,” which is responsible for negotiating parameters for the tunnel.

Now we can go to “**IKE Phase 2**” to establish the IPSEC SA which details the AH or ESP parameters and we can perform is by defining the “**IPSEC Transform Set**”.

**Target**

All the traffic between the HQ & Branch will pass through the GRE tunnel, which is encrypted by IPSEC.

**Configuration**

Define the ISAKMP policy on both peers (HQ & Branch), which states using AES as an Encryption algorithm, Pre-Share Authentication & Diffie-Hellman Group 2.

#crypto isakmp policy 10

   authentication pre-share

   encryption aes

   group 2

   exit

Create an IPSEC transform-set named “GRETEST” on both peers, specifying using the ESP and AES algorithms with 128 bits running in transport mode.

#crypto ipsec transform-set GRETEST esp-aes 128

   mode transport

   exit

Create IPSEC profile name “GREPROFILE” on both peers to apply the transform-set “GRETEST”

#crypto ipsec profile GREPROFILE

   set transform-set GRETEST

   exit

Protect the GRE Tunnel on both peers by the IPSEC profile.

#interface tunnel 0

   tunnel protection ipsec profile GREPROFILE

All these steps is applicable also to protect DMVPN Tunnels

## Remote Access VPN

**Description**

* Remote Access Clientless VPN enables safe access to an organization's private network from any place.
* Regardless of where they are physically located, users may create a secure connection to their network.
* It eliminates the requirement for users' devices to have certain client software installed.
* Users can access the network using common web browsers like Chrome, Firefox, or Safari.
* We ensure encrypted communication between users' devices and our network.
* Data transmitted over the internet is safeguarded for confidentiality and integrity using SSL/TLS protocols.

**Method Of Purpose (MOP)**

* Establish user accounts for VPN access, ensuring users have appropriate credentials.
* Configure GlobalProtect to facilitate Remote Access VPN functionality.
* Create an authentication profile using the local database, ensuring secure user authentication.
* Generate and certify digital certificates (GP-cert, portal-cert, gateway-cert) for secure communication.
* Configure SSL/TLS service profiles (portal-cert, gateway-cert) using the certified certificates.
* Establish a tunnel interface (e.g., tunnel.1) and allocate it to a Layer3 zone for network segmentation.
* Set up the GlobalProtect Portal to manage VPN connections.
* Configure the GlobalProtect Gateway to enable secure access to the network.

**Observation**

* By establishing Remote Access Clientless VPN rather than installing and configuring specialized VPN client software, users may now safely access our organizations network resources straight from their web browsers. Users' remote access is simplified, and IT teams' administrative burden is decreased.
* Data transfer between user devices and the organization's network is protected by encrypted communication using SSL/TLS protocols. This protects sensitive data from illegal access or interception and guarantees its confidentiality and integrity.
* Remote Access Clientless VPN allows a more adaptable work environment by providing safe and simple remote access via web browsers. No matter where they are physically located, users may continue to be productive, which increases organizational efficiency overall.

## Access Points

Wireless access points (APs) are networking devices that are typically used to extend available wireless Local Area Networks (WLANs) in a location. They’re usually used to connect wired and wireless networks. What this implies is that they make Wi-Fi enabled devices, including laptops, smartphones, and tablets, to be able to connect to the network and take the internet or shared resources. As per our network topology, a total of 6 access points is deployed. Employees and non-employees alike were considered during the network design in each site.

## Servers In Server Farm

In the heart of this network, there’s a hub where data, applications, and security converge – the server repository. It’s a bustling digital warehouse where all the critical information and operational tools are securely stored and meticulously organized.

Here’s where everything comes together: The safeguarding vault, which we call the Backup and Storage Server, pairs up with the Database Server. Think of them as the keepers of information, where nothing gets lost – every bite of data is accounted for, duplicated for safekeeping, and locked away for safe retrieval.

There's a sentinel at the gateway to this digital repository – the Multi-Factor Authentication system. It's like a series of complex locks that only the right keys can open, ensuring that only those with verified access can enter. It’s backed by the Certificate Authority server, the digital notary that vouches for the identity of each keyholder.

On the watchtower, there’s the EDR solution, scanning the horizon for signs of trouble, ready to act if a threat looms. It works in concert with the SIEM system, a keen-eyed observer constantly analyzing patterns, spotting anomalies, and keeping the guards informed.

Managing the assets and patches is like keeping the hub’s gears well-oiled and tuned. The Asset Manager catalogues the tools and resources, while the Patch Manager constantly updates them, fortifying the walls against vulnerabilities.

The Network Monitoring Tools act as the hub's senses – they keep a pulse on the data flow, ensuring everything runs smoothly and efficiently. They ensure that the File Server, the central library of the hub, is consistently orderly and accessible.

And let’s not forget the MDM, the overseer of all the digital messengers that come and go. It ensures that every device that connects to the hub is trusted, secured, and follows the rules.

All these parts are encased within a digital fortress, guarded by a firewall and scrutinized by the IDS/IPS systems to fend off unwanted visitors. A web of dedicated pathways – the VLANs – interconnects them and guides data flow securely and swiftly.

Finally, with SD-WAN in the mix, this hub doesn’t just stand on its own – it reaches out, connecting with clouds and remote outposts. It's like a network of highways that can adapt to traffic, find the best routes, and keep communication swift and steady.

This is not merely a server repository; it's a carefully woven tapestry where each thread supports the others, creating a picture of security, efficiency, and readiness for whatever the future might bring to the organization. It's a testament to thoughtful design, with each piece playing its role, ready to grow and adapt with time.

The server farm is a meticulously orchestrated digital ecosystem in our network topology where various servers and services interlock to form the organization's operational backbone.

**Components:**

The server farm is a constellation of specialized servers and services. It houses the Backup and Storage Server, ensuring data resilience and accessibility. The MFA fortifies access control, while the EDR system vigilantly monitors for threats.

Asset management is streamlined through the Asset Manager, and the Patch Manager is pivotal in maintaining system integrity. The Network Monitoring Tools provide a panoramic view of the farm's health and performance.

The File Server organizes and provides access to shared data, while the Mobile Device Management (MDM) system secures and governs mobile endpoints. The Security Information and Event Management (SIEM) system offers comprehensive visibility into security events and data patterns.

Essential databases reside on the Database Server, central to the farm's functions, and the Certificate Authority (CA) server underpins network security by managing digital certificates.

**Functionality:**

This farm isn't just a storage space; it's the core of our digital operations, hosting and managing crucial applications and services. Its architecture ensures high availability and redundancy, which is critical to uninterrupted business continuity.

**Security:**

Security is a fundamental component of the farm, not merely an add-on. Our farm has advanced security protocols to protect against potential threats and unauthorized access, in addition to the vigilant NIDS systems, thus guaranteeing a secure data environment.

**Maintenance and Management:**

Maintenance is proactive, with regular updates via the Patch Manager and continuous health checks through our Network Monitoring Tools. This diligence keeps the farm not just running but optimized.

**Integration with SD-WAN:**

The farm is future-ready, thanks to its integration with SD-WAN. This setup doesn't just streamline traffic—it smartly routes it, ensuring performance and reliability while paving the way for efficient cloud access and interconnectivity across the network.

**Future Scalability:**

The design anticipates growth and is ready to scale up with additional servers or expand storage as needed, ensuring the farm remains at the forefront of the organization's digital evolution.

This server farm is a dynamic, secure, resilient digital hub integral to our network's architecture. It's not just about the servers and software; it's about how they work in unison to support and propel the organization's objectives, ready to adapt and expand in the ever-evolving tech landscape.

**High Availability:**  
The architecture of the network topology is thoughtfully devised, emphasizing continuous uptime and reliable network service delivery. This reliability is underpinned by a series of strategic and technological enhancements embedded within the network's framework.

The integration of redundant mechanisms and infrastructures is at the core of the topology's resilience. Notably, the server farm is fortified with backup and storage servers, establishing a robust framework for data preservation and swift retrieval in hardware glitches or data loss scenarios. The foundational network infrastructure is equipped with dual routing and switching capabilities, augmented by the advanced functionalities of SD-WAN technology. These elements are critical for ensuring that traffic flow is seamlessly redirected along alternate routes if the primary channel is compromised, thereby avoiding service interruptions and maintaining seamless user interactions.

The network's robustness is further enhanced by the incorporation of SD-WAN into the server farm. This integration facilitates intelligent traffic allocation across diverse connections, including MPLS and broadband internet, optimizing bandwidth utilization and guaranteeing uninterrupted service through instant transitions to backup connections when needed. The network's operational efficiency and reliability are significantly elevated by SD-WAN's capability to adapt traffic routing in alignment with real-time network conditions.

Sophisticated monitoring tools and protocols reinforce proactive support for the network's stability. These systems continuously scrutinize the network's operational state, swiftly pinpointing and mitigating anomalies or potential failure points. This vigilant monitoring is instrumental in preempting disruptions and bolstering the network's enduring availability.

Ultimately, the network topology design transcends mere reactive measures, adopting a forward-looking approach to foresee and counteract potential challenges. This ensures that the network stands resilient, agile, and consistently available, aligning with the organization's ongoing operational needs.

## Wireless Network

This section of the document is a guide on best practice on how to go about establishing and continuously ensuring a secure wireless network in the organization which aligns with organization’s security strategy.

* Hardware Installation:
* Mount access point in strategic location as earlier discussed.
* Initial configuration:
  + Login to access point management interface. Consult user manual.
  + Configure network name for WIFI-Network.
  + Use WPA3 security to enable robust data encryption.
  + Ensure to choose non-overlapping channel based on existing WIFI-Networks to minimize interference. A WI-FI analyzer should help you here
* Regular Maintenance:
  + Regularly check for firmware updates for the access points.
  + On interval basis, ensure to carry out wireless security assessments using tools as recommended by IT department in order to identify any vulnerability in network,
  + Ensure to update WIFI-password periodically.
  + Use strong password. A combination of mix case, numbers and symbols would help here.

## High Availability

The architecture of the network topology is thoughtfully devised, emphasizing continuous uptime and reliable network service delivery. This reliability is underpinned by a series of strategic and technological enhancements embedded within the network's framework.

The integration of redundant mechanisms and infrastructures is at the core of the topology's resilience. Notably, the server farm is fortified with backup and storage servers, establishing a robust framework for data preservation and swift retrieval in hardware glitches or data loss scenarios. The foundational network infrastructure is equipped with dual routing and switching capabilities, augmented by the advanced functionalities of SD-WAN technology. These elements are critical for ensuring that traffic flow is seamlessly redirected along alternate routes if the primary channel is compromised, thereby avoiding service interruptions and maintaining seamless user interactions.

The network's robustness is further enhanced by the incorporation of SD-WAN into the server farm. This integration facilitates intelligent traffic allocation across diverse connections, including MPLS and broadband internet, optimizing bandwidth utilization and guaranteeing uninterrupted service through instant transitions to backup connections when needed. The network's operational efficiency and reliability are significantly elevated by SD-WAN's capability to adapt traffic routing in alignment with real-time network conditions.

Sophisticated monitoring tools and protocols reinforce proactive support for the network's stability. These systems continuously scrutinize the network's operational state, swiftly pinpointing and mitigating anomalies or potential failure points. This vigilant monitoring is instrumental in preempting disruptions and bolstering the network's enduring availability.

Ultimately, the network topology design transcends mere reactive measures, adopting a forward-looking approach to foresee and counteract potential challenges. This ensures that the network stands resilient, agile, and consistently available, aligning with the organization's ongoing operational needs.

## Threat Assessments

* **Threat Intelligence Analysis**

1. Gather threat intelligence data from reputable sources such as industry reports, security bulletins, threat feeds, and information sharing platforms.
2. Utilize automated tools and subscriptions to continuously collect and update threat intelligence data.
3. Analyze the collected data to identify potential threats and vulnerabilities relevant to the network topology.
4. Categorize and prioritize threats based on their severity, relevance, and potential impact on the organization's infrastructure.
5. Correlate threat intelligence data with the organization's network topology, infrastructure, and security policies.
6. Understand how each identified threat could exploit vulnerabilities within the network and impact critical assets and operations.
7. Tailor the threat intelligence analysis to focus on threats and vulnerabilities specific to the organization's network topology and operational environment.
8. Establish mechanisms for continuous monitoring and updating of threat intelligence analysis.
9. Stay abreast of evolving threats and emerging attack vectors by regularly reviewing and refining analysis methodologies
10. Ensure that threat intelligence analysis remains current and relevant to the organization's security posture.

* **Play Book Flow chart**

A diagram of a process

Description automatically generated

## Security Audits & Penetrating testing

**Security Audits**

To evaluate and strengthen an organization's cybersecurity defences, regular security audits are essential. To identify vulnerabilities and ensure compliance with regulatory standards, these audits entail methodical assessments of policies, processes, and controls. Through the implementation of both planned audits and spontaneous spot checks, establishments may embrace a proactive stance towards security evaluations, detecting vulnerabilities prior to their use by criminal forces.

**Identify Threats and Vulnerabilities:**

Enumerate all potential threats, including malware, data breaches, and power outages, along with vulnerabilities, such unpatched systems, and weak passwords. Consider industry trends and your specific network configuration.

**Analyse Risks:**

Estimate the likelihood of each threat occurring (high, medium, low). Assess the potential impact of each threat if it materializes (financial loss, reputational damage, data exposure). Combine likelihood and impact to determine the overall risk level (high, medium, low).

**Evaluate and Prioritize:**

Review the identified risks and their assigned levels. Focus on mitigating high-risk threats first.

**Develop Mitigation Strategies:**

Define actions to address each risk. This may involve implementing security controls, patching systems, or raising employee awareness.

**Implement and Monitor:**

Implement your mitigating tactics. Maintain a regular eye out for fresh dangers and weaknesses on your network.

**Who carries out the risk analysis?**

For a risk assessment, a cross-functional team with a variety of specialties is ideal:

* **IT security**: Offers technical expertise on dangers and weaknesses.
* **Business Operations**: Understands the impact of risks on business processes.
* **Risk Management**: Offers experience in risk assessment methodologies.
* **Senior Management**: Provides support and resources for mitigation strategies.

**Risk Levels:**

Risks are typically categorized into three levels:

* **High**: These threats have a high chance of occurring and could have a significant negative impact. They require immediate attention.
* **Medium**: These threats have a moderate chance of occurring and could have a moderate negative impact. They need to be addressed but may not be as urgent.
* **Low:** These threats have a low chance of occurring and would likely have a minimal negative impact. They can be monitored but may not require immediate action.

**Policy and Compliance:**

Review and update your security policies often to take into account the newest dangers and legal requirements.Assure adherence to pertinent industry standards and data security laws (e.g., PCI DSS, HIPAA).

**Training on Employee Awareness:**

Provide regular cybersecurity training to staff members, including topics like phishing awareness, password hygiene, and avoiding social engineering techniques. Train them on reporting suspicious activity.

**Physical Security:**

Put in place access restrictions to limit physical access to locations that are sensitive (like server rooms). Think about installing security cameras, alarms, and security personnel. Protect the building's entryways and prevent unwanted access.

**USB Lockers:**

Consider installing USB lockers to restrict unauthorized data transfer through USB devices. Provide authorized access only for legitimate use cases.

**Playbook and SOAR:**

Make a cybersecurity playbook with action items to follow in the event of specific cyberattacks. Installing a Security Orchestration, Automation, and Response (SOAR) platform may boost output and automate incident response procedures.

**Updating Procedures:**

Plan to have your risk assessment, policies, training materials, and other security procedures reviewed on a regular basis (at least once a year). Update them to consider emerging vulnerabilities, shifting compliance requirements, and shifts in the threat landscape.

**Recommendations:**

Seek the assistance of outside security professionals to ensure a thorough and impartial evaluation. To expedite the process, make use of risk assessment frameworks and instruments. To increase awareness, share the risk assessment's findings with all relevant parties.

**Penetration Test**

This strategy document provides a comprehensive approach to executing penetration tests within the organization's network framework. Its primary goal is to identify and remediate vulnerabilities effectively, bolstering the network's defense mechanisms.

Coverage: This strategy encompasses all digital infrastructures within the organization's network, including server farms, data backup systems, authentication processes, and network segmentation.

**Types of Penetration Tests:**

**Black Box Analysis:** Testers, without prior network knowledge, mimic an external attacker's perspective. This method is pivotal for discovering vulnerabilities that an external adversary could exploit.

**Application:** This is particularly relevant for assessing the fortitude of the network's external defences, such as perimeter security and intrusion detection systems.

**Gray Box Analysis:** With partial network knowledge, testers simulate a threat from an insider or an external entity with limited insider insights. This approach is vital for identifying potential internal security weaknesses.

**Application:** Optimal for examining crucial network components' internal workings and security protocols like the server farm's Database Server and MFA mechanisms.

**White Box Analysis**: Here, testers are equipped with full knowledge of the network, including architecture diagrams, code, and credentials. This exhaustive approach is aimed at uncovering deep-rooted vulnerabilities.

**Application:** Ideal for a thorough examination of system components, network protocols, and application layers, providing a comprehensive security overview.

**Testing Exercises:**

**Scenario-Based Workshops:** These theoretical sessions involve dissecting various cyber-attack scenarios to critique the organization's response efficacy and pinpointing any strategic or communicational gaps.

**Frequency:** Biannually or following significant modifications in network design or response strategies.

Practical Penetration Exercises: Direct testing activities, executed as black, gray, or white box tests, tailored to specific targets and security objectives.

**Frequency:** Annually or more often based on the network's criticality and compliance mandates.

**Execution Guidelines:**

**Pre-test Planning:** Comprehensive planning is essential, including defining precise objectives, scope, and methodologies. Obtaining requisite approvals from relevant authorities is mandatory.

**Test Implementation:** Ensure that the testing aligns with agreed strategies and remains within the authorized boundaries.

**Immediate Incident Reporting:** Any anomalies or unexpected outcomes during the test must be promptly reported to the designated coordinator.

**Post-test Review:** A detailed report of the test findings, methodologies employed, and mitigation suggestions should be compiled. It is essential to have further conversations with stakeholders to discuss the results and devise corrective measures.

**Remediation and Reassessment:** It's critical to address vulnerabilities found promptly and verify the efficacy of the remedial actions with verification tests.

**Sustainability and Adherence:**

Regularly revisiting this strategy ensures its relevance with the evolving network environment and organizational dynamics.

## Security Policies

* **Access Control Policy:**
* Define user roles and privileges based on job responsibilities.
* Implement role-based access control (RBAC) to restrict unauthorized access to sensitive resources.
* Enforce strong authentication methods such as multi-factor authentication (MFA) for accessing critical systems.
* Regularly review and update access rights based on personnel changes and job roles.
* **Incident Response Policy:**
* Establish a clear incident response plan outlining roles, responsibilities, and escalation procedures.
* Define criteria for identifying security incidents and the severity levels.
* Implement automated alerting and monitoring systems to detect anomalies and potential security breaches.
* Conduct regular drills and simulations to test the effectiveness of the incident response plan.
* Document post-incident analysis and lessons learned to improve response procedures.
* **Security Awareness and Training Policy:**
* Mandate security awareness training for all employees, contractors, and vendors.
* Cover topics such as phishing, social engineering, and password best practices.
* Provide regular updates and refresher courses to reinforce security awareness.
* Encourage reporting of suspicious activities and incidents through a designated channel.
* Recognize and reward employees for demonstrating good security practices.
* **Data Backup and Recovery Policy:**
* Define backup schedules and retention periods for critical data and systems.
* Implement automated backup solutions with off-site storage for redundancy.
* Regularly test backup and recovery procedures to ensure data integrity and availability.
* Assign responsibility for managing backups and conducting regular audits.
* Establish procedures for restoring data in the event of a data loss incident.
* **Password Policy:**
* Enforce strong password complexity requirements, including length, complexity, and expiration.
* Implement password hashing and encryption techniques to protect stored passwords.
* Enforce password lockout mechanisms after a certain number of failed attempts.
* Prohibit password sharing and reuse across multiple accounts.
* Encourage the use of password managers to securely store and manage passwords.

## ZTNA

**Description**

* ZTNA enforces strict access restrictions, making sure that devices and users need to authenticate in order to access network resources.
* Before being allowed access, users and devices must authenticate themselves, which improves security by lowering the possibility of unwanted access.
* ZTNA enables secure connections for both internal and distant users, irrespective of their location.
* Organizations can enforce least privilege access and segregate network resources by defining access policies based on Zero Trust concepts.
* Traffic is constantly watched over in order to improve overall security posture by quickly identifying and addressing possible threats.

**Method of Preparation:**

We have implemented Zero Trust Network Access (ZTNA) in our project through:

* Verifying user identities and establishing policies for context-based access.
* Micro-segmentation is being put into practice for least-privilege access.
* Setting up ACLs and assigning roles with the lowest privilege.
* Using anomaly detection and ID/IPS for ongoing monitoring.
* Utilizing VPNs, ADC, and SDP to secure application access.

**Observation**

Strict access limits and verification procedures are enforced by Zero Trust Network Access (ZTNA), which improves security. Organizations may reduce the risk of unwanted access and data breaches by requiring users and devices to authenticate before accessing network resources. ZTNA enables secure connections for both internal and distant users, irrespective of their location. Moreover, ongoing network traffic audits and monitoring assist enterprises in immediately identifying and countering such attacks, therefore fortifying their security stance.

## NIST Framework

Our network topology aligns with the NIST Cybersecurity Framework, which comprises five key functions: Identify, Protect, Detect, Respond, and Recover. This framework provides a strategic view of the lifecycle of an organization’s management of cybersecurity risk. Here’s how the components of the network topology correspond to each of these functions:

**Identify**

* Asset Management: The inclusion of Asset Managers and databases in the server farm enables the organization to identify and manage data, devices, and systems as part of the cybersecurity risk management strategy.
* Network Segmentation: VLANs help identify and categorize network traffic, which is crucial for risk management and organizational understanding of its resources and network architecture.

**Protect**

* Access Control (NAC): By ensuring that only authorized devices can access the network, the NAC aligns with the 'Protect' function, enforcing the principle of least privilege.
* Firewalls and WAF: These serve as barriers that protect the network from unauthorized access and potential threats, implementing safeguards like security policies and perimeter defense.
* MFA (Multi-Factor Authentication): MFA adds a layer of protection by requiring multiple forms of verification to reduce the likelihood of unauthorized network access.

**Detect**

* IDS/IPS: These systems actively monitor network traffic and user behaviors to detect potential cybersecurity events in real-time.
* Network Monitoring Tools: Continuous monitoring for the detection of anomalies and events, and the verification of the effectiveness of protective measures, is in line with the NIST framework.

**Respond**

* Incident Response: The network topology does not detail specific incident response mechanisms, but the presence of IDS/IPS, network monitoring, and server management tools suggests an infrastructure that can support a swift response to detected incidents.

**Recover**

* Backup and Storage Servers: These components enable the organization to restore any lost data in the aftermath of an incident, which is key to the recovery process.
* Planning: While not depicted in the topology, recovery planning would be an intrinsic part of the organization's policies and procedures, ensuring resilience and the restoration of any capabilities or services impaired due to a cybersecurity incident.

## Conclusion

This project has successfully established a secure network framework across a corporate headquarters and its branch offices, emphasizing strategic security measures and advanced technological integrations. By incorporating sophisticated systems like IDS/IPS, NAC, and SD-WAN, we have developed a security infrastructure that protects critical information and maintains high operational standards across multiple locations.

Our network design utilizes technologies such as VPNs and security zones, which are crucial for maintaining continuous network performance and security. Enhanced authentication protocols are enforced through the strategic deployment of certificate authorities, aligning with our commitment to rigorous security compliance.

The approach to cybersecurity in this project is proactive, with continuous evaluations through security audits, threat assessments, and penetration testing. These activities are essential for detecting vulnerabilities and adhering to security standards. Moreover, the adoption of the NIST cybersecurity framework guides our risk management practices, boosting our network’s resilience.

This initiative not only meets current security demands but also provides a scalable and flexible network architecture, ready to adapt to future technological advances and challenges. It exemplifies a comprehensive strategy to network security, ensuring not just defense against potential threats but also supporting the organization’s ongoing and future operational requirements.

In summary, the network security project has significantly strengthened our security framework, serving as a model for future security initiatives and reinforcing our organization’s capability to support secure, efficient operations.

## References

* 1. *Cisco Learning Network*. (n.d.). Learningnetwork.cisco.com. <https://learningnetwork.cisco.com/>
  2. *Introduction | SD-WAN Architecture for Enterprise*. (2024). Fortinet.com. <https://docs.fortinet.com/document/fortigate/7.2.0/sd-wan-architecture-for-enterprise/342022/introduction>
  3. *HPE Aruba Networking*. (2023). HPE Aruba Networking. <https://www.arubanetworks.com/en-ca/faq/what-is-network-access-control/>
  4. *Global Cybersecurity Leader - Palo Alto Networks*. (n.d.). Www.paloaltonetworks.com. <https://www.paloaltonetworks.com/>

‌