# 

A logo for a college

Description automatically generated

**Capstone Assignment- Project Report**

**Access Control**

**Prof. Kristen Macdonald**

**Group 4**

Contents

[Overview 3](#_Toc141889884)

[Introduction: 3](#_Toc141889885)

[What is a VPN (Virtual Private Network)? 3](#_Toc141889886)

[Some important VPN Components: 3](#_Toc141889887)

[The Advantages of Using a VPN in the company: 3](#_Toc141889888)

[Best practices for VPN implementation 3](#_Toc141889889)

[The potential drawbacks and considerations made when implementing VPN. 4](#_Toc141889890)

[Drawbacks while implementing VPN in MOJO Inc.: 4](#_Toc141889891)

[Considerations for a Smooth Implementation: 5](#_Toc141889892)

[Conclusion 7](#_Toc141889893)

[Reference 8](#_Toc141889894)

## Overview

### Introduction:

In today's linked world, enterprises must prioritize safe communication and data security. Virtual Private Network (VPN) technology enables an organization to create encrypted and secure internet connections, allowing distant users and branch offices to safely access corporate resources. This paper describes the establishment of a VPN inside the organization MOJO Inc., which is a product-based firm that specializes in providing cybersecurity solutions to defend organizations against cyber-attacks. The organization’s existing assets comprise a range of digital resources, including servers, databases, cloud infrastructure, and repositories for sensitive data. These resources are essential to the company's daily operations, including product development, customer service, and operational procedures emphasizing the advantages of the VPN and how it fulfills the organization's requirement for secure remote access.

### What is a VPN (Virtual Private Network)?

A VPN is a private and encrypted communication channel that establishes a secure connection between users and devices situated outside the organization's physical network (Moskowitz, R.). It will enable users to access internal resources like files, apps, and databases while maintaining data confidentiality and protecting against illegal access.

### Some important VPN Components:

* MOJO Inc. can protect data privacy during transmission by using tunneling methods to encapsulate data in encrypted packets (Akter, H.,2022). To provide secure connections between distant users and the corporate network, the VPN makes use of dependable tunneling technologies including Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), and Internet Protocol Security (IPsec).
* Encryption: Strong encryption methods, such as AES (Advanced Encryption Standard), secure data while it travels over the internet, rendering it unreadable by malevolent actors.
* Authentication: To increase security, MOJO Inc.'s VPN uses a variety of authentication techniques to verify users' identities before giving access (Chandramouli, R. 2022). These procedures may offer an additional layer of security against unwanted access, such as username/password authentication, digital certificates, and multi-factor authentication (MFA).
* Access Control rules: MOJO Inc. establishes stringent access control policies to outline who or what equipment is permitted to connect to what resources on the company's network. The VPN reduces the danger of unwanted access by applying access control rules and making sure that only authorized users have access to critical information and resources (Santoso, 2021).

### The Advantages of Using a VPN in the company:

* Enhanced Security: MOJO Inc. uses a VPN to make sure that data connections are secured. Sensitive information is kept private thanks to the VPN's robust authentication and encryption measures, which lower the possibility of data breaches and illegal access.
* Remote access and productivity: With the help of VPNs, staff members and authorized users may safely access company resources from anywhere (Einler Larsson, L., & Qollakaj, K. 2023). Employees can operate effectively while on the road thanks to the increased productivity and made-easy flexible work arrangements made possible by this.
* Data Security: MOJO Inc. uses a VPN to make sure that private and encrypted sensitive data is sent. This maintains the integrity and confidentiality of the organization's data by preventing eavesdropping and data interception by malicious parties.
* Cost-Effectiveness: VPNs are a cost-effective option for secure remote access since they make use of the existing internet infrastructure. Implementing a VPN may be more cost-effective than other choices since it makes use of the company's existing resources.
* Network Segmentation: With the use of VPNs, MOJO Inc. can control access depending on user roles and responsibilities. This minimizes the danger of unauthorized access to sensitive information by ensuring that users only have access to the resources they need for their responsibilities (Sirisukha, S. 2003).
* Scalability: Because VPNs scale, they are appropriate for MOJO Inc.'s growing workforce and remote access needs. The VPN can support rising demand as the business expands without the need for expensive infrastructure improvements.
* Compliance: VPNs help MOJO Inc. adhere to legal requirements, particularly in sectors that deal with sensitive customer data. The VPN aids the firm in adhering to relevant data protection and privacy standards by safeguarding data transfer and access.

## Best practices for VPN implementation

To provide a safe and effective remote access solution, deploying a Virtual Private Network (VPN) inside MOJO Inc. requires careful planning, adherence to security standards, and the execution of best practices. The best practices outlined below will explain critical aspects for effectively adopting a VPN inside MOJO Inc.:

1. Approach to Security First: Security should be prioritized in VPN deployment. The following security measures should be prioritized by MOJO Inc.:

* Strong Encryption: To safeguard data transferred over the VPN, the company can use industry-standard encryption techniques such as AES (Advanced Encryption Standard). Strong encryption guarantees that important information is protected even if it is intercepted.
* Strong Authentication: MOJO Inc. can use multi-factor authentication (MFA) to improve user verification. This offers another layer of security beyond the standard username and password, lowering the danger of illegal access.
* Regular Security upgrades: MOJO Inc. maintains VPN software, firmware, and security appliances with the most recent patches and upgrades. This reduces the likelihood of security flaws being exploited.
* Secure Certificate Management: MOJO Inc. can authenticate using digital certificates to secure the integrity of VPN connections and avoid certificate-related threats.
* Centralized Management: Implementation of a centralized management system to monitor and govern VPN connections, allowing for rapid detection and response to possible security problems.

1. Network Segmentation and Access Control: Network segmentation and access control are critical for restricting access to approved users and resources:

* Role-Based Access Control (RBAC): The use of RBAC to give users appropriate access levels based on their employment positions and responsibilities lowers the possibility of illegal access to crucial resources.
* Least Privilege Principle: MOJO Inc. can use the least privilege principle to ensure that users only have access to the resources needed to complete their respective job. Access restrictions reduce the effect of possible security breaches.
* Network Segmentation: To isolate sensitive data and resources, the network into distinct segments or VLANs can be divided. This method offers an additional layer of security by stopping possible intruders from moving laterally.

1. Endpoint Security: It is also critical to secure the devices that connect to the VPN:

* Secure Device Configuration: Enforcing security rules on user devices can ensure they satisfy the security requirements of the enterprise. Disk encryption, secure boot, and deactivating superfluous services are examples of such measures.
* VPN Client Security: Using VPN clients that provide endpoint security features such as host integrity checks and posture assessments before connecting to the VPN can verify the endpoints fulfill security requirements.
* Remote Wipe capabilities: Implementation of remote wipe capabilities for remote access devices to secure sensitive data in the event of loss or theft.

1. Employee Education and Consciousness: It is critical to educate staff about VPN use and associated security risks:

* VPN Usage Policy: MOJO Inc. can create a clear and thorough VPN usage policy including authorized use, security requirements, and policy breaches.
* Security Awareness Training: Frequent security awareness training to workers can be provided to educate them on VPN best practices, password hygiene, and recognizing and reporting any phishing attempts.
* Incident Response Training: Incident response training can be provided as well for the staff so they can react effectively to possible security events.

1. Regular Security Audits and Monitoring: Periodic security audits and constant monitoring are required to keep a VPN infrastructure secure in MOJO Inc.:
   * Security Audits: Conducting frequent security audits can help in discovering vulnerabilities, evaluating the efficacy of security measures, and ensuring policy compliance.
   * Log Analysis: MOJO Inc. can examine VPN records and network traffic for strange patterns, suspicious activity, and possible security breaches.
   * Intrusion Detection and Prevention: MOJO Inc. can install intrusion detection and prevention systems to identify and prevent unauthorized access and possible threats.

## The potential drawbacks and considerations made when implementing VPN.

### Drawbacks while implementing VPN in MOJO Inc.:

1. **Performance Impact:**

* Overhead for VPN Encryption: VPN encryption adds extra overhead, which might result in somewhat worse network performance. Encryption and decryption procedures may slow down data transfer, particularly on low-bandwidth connections.
* Latency: VPNs may cause increased latency, which might interfere with real-time applications such as video conferencing or VoIP conversations (Muhammad et al., 2022).
* Limitations in Bandwidth: The VPN depends on internet bandwidth, which may become a bottleneck if not properly handled, resulting in congestion and lower performance.

1. **Compatibility Problems:**

* Legacy apps: Some legacy apps or protocols may not function properly over VPN connections. To minimize any interruptions, compatibility testing is required by MOJO Inc. prior to transferring crucial services to the VPN.

1. **Endpoint Protection:**

* Employees who use personal devices for VPN connection under the company may expose themselves to security threats such as unprotected equipment or outdated software. To address these dangers, strong endpoint security measures must be implemented.
* Remote Device Management: Ensuring that devices connecting to the VPN follow security requirements such as encryption and security updates may be difficult, especially for a large remote workforce like MOJO Inc.

1. **Flexibility:**

* Overload on the network: As the business expands and more users connect to the VPN at the same time, the VPN infrastructure may suffer scalability concerns, resulting in lower performance and probable connection issues.
* VPN Server Capacity: Increasing the capacity of a VPN server may require extra resources and infrastructure expenditures for the company.

1. **Human Aspect:**

* Employee Education: To avoid typical security hazards such as disclosing passwords or falling prey to phishing efforts, employees must be taught about VPN use and security best practices.

### Considerations for a Smooth Implementation:

1. **Choosing a VPN Solution:**

* Evaluating and choosing a VPN solution that meets the demands, security requirements, scalability, and price limits of MOJO Inc. is very important.
* MOJO Inc. will be considering VPN solutions to handle remote access as well as site-to-site connectivity for its two branch offices.

VPN architecture representation in MOJO Inc.

A computer network diagram with icons

Description automatically generated

The connection between the branch office and head office will be managed by Site-to-Site VPN and the for the remote users for people working from home, the remote access VPN will be put in place.

1. **Performance and Network Infrastructure:**

* Examining the current network infrastructure to verify it can manage the increased VPN traffic and bandwidth demands is crucial.
* MOJO Inc. can consider using QoS methods to prioritize VPN traffic for key applications and services.

1. **Encryption and security:**

* To safeguard sensitive data during transmission, robust encryption techniques and authentication procedures can be used by the company.
* Multi-factor authentication (MFA) should be used to improve user verification and prevent illegal access.

1. **Endpoint Security and Device Administration:**

* MOJO Inc. needs to create and enforce security standards for VPN user devices, such as encryption, firewall settings, and automated updates.
* MOJO Inc. can consider deploying Mobile Device Management (MDM) solutions to guarantee mobile device compliance with security standards.

1. **Employee Education and Awareness:**

* Conducting in-depth training sessions to teach staff about VPN use, security best practices, and how to identify and report any security risks is highly suggested.

1. **Performance Evaluation and Improvement:**

* MOJO Inc. can use monitoring VPN performance and network traffic on an ongoing basis to discover possible bottlenecks and optimize network resources as required.
* The company needs to load test the VPN to verify it can manage peak traffic flows.

1. **Incident Response and Preparedness:**

* Creating explicit incident response processes can handle potential security problems or breaches inside the organization as soon as possible.
* Creating backup procedures can prevent any interruptions in the event of a VPN failure.

## Conclusion

In MOJO Inc., using a VPN will offer a safe and dependable option for remote access and communication. The organization may build a strong VPN infrastructure that protects sensitive data and enables secure remote access for its customers by following best practices, prioritizing security, and resolving any downsides. VPN technology, with appropriate planning, training, and monitoring, may improve the organization's network security while also enabling seamless and secure remote connection for its workforce, therefore complementing the organization's aims and objectives.

## Reference

Moskowitz, R. (1997). What is a Virtual Private Network?. Network Computing Online.

Santoso, B., Sani, A., Husain, T., & Hendri, N. (2021). VPN Site To Site Implementation Using Protocol L2TP And IPSec. TEKNOKOM, 4(1), 30-36.

Einler Larsson, L., & Qollakaj, K. (2023). Cybersecurity of remote work migration: A study on the VPN security landscape post covid-19 outbreak.

Sirisukha, S. (2003). The Advantages A Virtual Private Network For Computer Security. Proceedings of the 16th Annual NACCQ. Palmerston North New Zeland, 397-402.

Chandramouli, R. (2022). Guide to a Secure Enterprise Network Landscape (No. NIST Special Publication (SP) 800-215 (Draft)). National Institute of Standards and Technology.

Akter, H., Jahan, S., Saha, S., Faisal, R. H., & Islam, S. (2022, February). Evaluating performances of VPN tunneling protocols based on application service requirements. In Proceedings of the Third International Conference on Trends in Computational and Cognitive Engineering: TCCE 2021 (pp. 433-444). Singapore: Springer Nature Singapore.

Muhammad, Z. B., Bello, A. B., Bello, A. B., & Maniru, M. U. (2022). Secure and Optimize VoIP Communication Using QoS Technologies and VPN.

Dutkowska-Zuk, A., Hounsel, A., Morrill, A., Xiong, A., Chetty, M., & Feamster, N. (2022). How and why people use virtual private networks. In 31st USENIX Security Symposium (USENIX Security 22) (pp. 3451-3465).