Computer Networks Project Proposal

Virtual Office Network Design using VPN

MARCH 15, 2024

INSTRUCTOR'S NAME:
Sir Ubaidullah

TEAM MEMBERS:
Muhammad Tahir (21K-4503)
Insha Javed (21K-3279)
Sabika Shameel (21K-4606)

Introduction:

In today's digital age, businesses are increasingly reliant on remote work capabilities to ensure operational continuity and accommodate flexible work arrangements. However, ensuring the security and efficiency of remote connections is paramount. This project proposes the design and implementation of a Virtual Office Network using Virtual Private Network (VPN) technology, aimed at securely connecting remote employees to the company's network resources.

Objectives:

The following objectives & requirements apply to this Proposal:

- ➢ Design a secure and scalable network infrastructure using Cisco Packet Tracer.
- ➢ Implement VPN technology to facilitate secure remote access for employees.
- ➢ Ensure high availability and reliability of network services.
- ➢ Provide centralised management and monitoring capabilities.
- ➢ Mitigate security risks associated with remote access.

Proposed Solution:

The proposed solution involves the creation of a Virtual Office Network using VPN technology. This network will comprise multiple components:

- ☐ **VPN Server**: A dedicated VPN server will be deployed within the company's premises to handle incoming VPN connections securely. Cisco Packet Tracer supports various VPN protocols such as IPsec, SSL VPN, and AnyConnect, which will be utilised based on the project requirements.

- ☐ **Firewall and Security Appliances:** Firewall appliances will be implemented to enforce security policies and inspect traffic entering and leaving the network. Intrusion Detection/Prevention Systems (IDS/IPS) may also be incorporated to detect and mitigate potential threats.

- ☐ **Router and Switch Infrastructure**: Core routers and switches will form the backbone of the network, facilitating interconnection between various network segments and ensuring efficient data routing.

- ☐ **Remote Access Clients**: Remote employees will utilise VPN client software installed on their devices to establish secure connections

to the company's network. Various authentication methods such as username/password, digital certificates, or two-factor authentication will be employed to enhance security.

- ☐ **Network Topology:** The network will be designed with a hierarchical topology comprising core, distribution, and access layers. VPN connections will terminate at the core layer, providing access to internal resources. Redundancy and fault tolerance mechanisms such as redundant links, load balancing, and failover will be implemented to ensure high availability.

Implementation Plan:

- ➔ **Network Design**: Design the network topology, considering factors such as scalability, security, and performance.
- ➔ **Configuration of Devices**: Configure routers, switches, VPN servers, and security appliances based on the designed topology.
- ➔ **VPN Setup**: Configure VPN settings on the VPN server and client devices, ensuring compatibility and security.
- ➔ **Security Policies**: Define and enforce security policies on firewall and security appliances to safeguard the network from unauthorised access and threats.
- ➔ **Testing and Optimization**: Conduct thorough testing to ensure the functionality, performance, and security of the network.

Optimise configurations as necessary to enhance efficiency and reliability.

Conclusion

The proposed Virtual Office Network design using VPN technology offers a robust solution for securely connecting remote employees to the company's network resources. By implementing industry-standard security measures and leveraging Cisco Packet Tracer's simulation capabilities, this project aims to deliver a reliable and scalable network infrastructure that meets the demands of modern businesses.