2024

COMPANY K

Network Infrastructure Proposal for Company D

Prepared by: DK Consults
Date: [26/05/2024]

1. Executive Summary

DK Consults is pleased to submit this proposal for the network infrastructure design and implementation at Company D. This proposal details a comprehensive plan to deploy a scalable, secure, and reliable network that will meet the current and future needs of the organization. Our solution includes network switches, a robust firewall, and a modern CCTV surveillance system, all designed to enhance operational efficiency, security, and monitoring.

2. Project Scope

The network infrastructure project for Company D aims to cover the following areas:

- Installation of network switches to provide efficient connectivity between devices.
- Deployment of a next-generation firewall for advanced network security.
- Implementation of an IP-based CCTV surveillance system for physical security monitoring.
- Provision of ongoing maintenance, support, and monitoring for the installed infrastructure.

3. Objectives

The objectives of this project are:

1. **Scalability:** Design a network that can easily scale as Company D expands, supporting additional users and devices.
2. **Security:** Implement state-of-the-art security systems, including a firewall and secure network segmentation, to protect against internal and external threats.
3. **Reliability:** Ensure the infrastructure is highly available and reliable, minimizing downtime and optimizing network performance.
4. **Surveillance:** Install an IP-based CCTV system that provides high-quality surveillance for monitoring critical areas and improving security measures.

4. Network Design

4.1. Network Topology

The proposed network topology for Company D is designed with a three-layered architecture:

- **Core Layer:** Provides high-speed backbone connectivity between departments.

- **Distribution Layer:** Manages routing between different VLANs (Virtual Local Area Networks).
- **Access Layer:** Connects end-user devices (desktops, printers, etc.) to the network.

The topology ensures redundancy, scalability, and efficient traffic management. Network diagrams will be provided in the final implementation phase to illustrate connectivity between switches, the firewall, and CCTV systems.

4.2. Switches

We propose installing **Layer 2/Layer 3 switches** to ensure robust connectivity within the network. The key components include:

- **Layer 2 Switches**: Cisco Catalyst 2960 series or equivalent, for connecting user devices to the access layer.
- **Layer 3 Switches**: Cisco Catalyst 3850 series or equivalent, for routing and managing traffic between VLANs.

Each switch will support **Power over Ethernet (PoE)** for devices like IP cameras, reducing the need for separate power supplies.

4.3. Firewall

The **next-generation firewall (NGFW)** will be a cornerstone of Company D's network security. We recommend using a firewall solution such as **Fortinet FortiGate** or **Cisco ASA**, which provides:

- Intrusion detection and prevention.
- Deep packet inspection (DPI).
- Virtual Private Network (VPN) capabilities for remote access.
- Application-layer filtering for enhanced security against malware and other threats.

The firewall will ensure that Company D's sensitive data is protected from unauthorized access while allowing legitimate traffic to flow freely.

4.4. CCTV System

We propose the installation of an **IP-based CCTV system** to monitor key areas in and around Company D’s premises. The CCTV system includes:

- **High-definition (HD) cameras** with night vision and motion detection capabilities.
- **Network Video Recorders (NVRs)** for real-time footage storage and remote access.
- A web-based interface for monitoring and managing video feeds from authorized devices.

The CCTV cameras will be positioned in strategic locations, such as entrances, exits, server rooms, and parking areas. The system will be integrated into the network, allowing video data to be securely stored and accessed via the firewall-protected network.

5. Implementation Plan

5.1. Equipment Procurement

The required network hardware will be procured from certified vendors, ensuring top-quality devices that meet Company D's performance needs. The list of required hardware includes:

- Cisco Layer 2 and Layer 3 switches.
- Fortinet FortiGate/Cisco ASA firewall.
- IP-based CCTV cameras and NVR systems.
- Cat6 Ethernet cables and patch panels for connectivity.

5.2. Network Setup

5.2.1. Switch Installation

- Installation of Layer 2 switches in the access layer for end-user connectivity.
- Layer 3 switches will be placed in the distribution layer, ensuring effective routing and network segmentation.
- VLANs will be created to isolate different departments and ensure traffic segmentation.

5.2.2. Firewall Configuration

- Firewall rules will be configured to allow secure communication between internal and external systems.
- VPN configuration for secure remote access by authorized personnel.
- Setup of application control policies to manage bandwidth usage and prevent unauthorized access.

5.2.3. CCTV Deployment

- IP cameras will be installed in strategic locations across the premises.
- Cameras will be connected to the network via PoE-enabled switches.
- NVR systems will be configured to store footage securely, with access restricted to authorized users.

5.3. Timeline

The implementation will follow a phased approach:

1. **Phase 1: Planning and Design**
   Duration: 1 week
   Tasks: Network design, procurement of equipment, and site preparation.
2. **Phase 2: Installation and Configuration**
   Duration: 2-3 weeks
   Tasks: Installation of switches, firewall, and CCTV system, and configuring devices.

3. **Phase 3: Testing and Training**
   Duration: 1 week
   Tasks: System testing, optimization, and training of IT staff for ongoing management.
4. **Phase 4: Go-Live**
   Duration: 1 week
   Tasks: Full deployment, final testing, and handover to Company D's IT team.

6. Security Considerations

6.1. Firewall Security

- **Firewall Rules:** Strict inbound and outbound access control rules will be implemented to prevent unauthorized access.
- **VPN Security:** VPN connections will be encrypted with AES-256, ensuring safe and secure remote access for users working offsite.

6.2. Network Segmentation

- Different VLANs will be created for key areas, such as finance, operations, CCTV, and guest access, reducing the impact of potential attacks.

6.3. Data Encryption

- Sensitive data (such as CCTV footage) will be encrypted during transmission and storage, ensuring that it is protected from unauthorized access.

7. Budget Estimate

Item	**Description**	**Cost (USD)**
Cisco Layer 2 Switches	10 PoE-enabled switches	Ksh20,000
Cisco Layer 3 Switches	3 distribution switches	Ksh12,000
FortiGate Firewall	NGFW with VPN and DPI	Ksh15,000
CCTV Cameras (IP-based)	15 high-definition cameras	Ksh10,000
NVR System	Network Video Recorder	Ksh5,000
Cabling and Accessories	Cat6 cables, patch panels	Ksh3,000
Total Estimated Cost		**Ksh65,000**

---

8. Maintenance and Support

DK Consults will provide ongoing maintenance and support services for the network infrastructure, including:

- **Hardware Maintenance:** Regular checks and replacements of faulty equipment.

- **Software Updates:** Firewall, switch, and CCTV firmware updates to ensure optimal performance.
- **Monitoring Services:** 24/7 monitoring of network health and security.

---

9. Risk Assessment

Potential Risks

- **Hardware Failure:** To mitigate, spare hardware components will be kept on hand for immediate replacement.
- **Cybersecurity Threats:** The firewall will be regularly updated to defend against evolving cyber threats.
- **Delays in Equipment Delivery:** We will work with trusted suppliers to minimize delays in hardware procurement.

---

10. Conclusion

This network infrastructure proposal provides a comprehensive solution to enhance the security, scalability, and performance of Company D's IT systems. By implementing the recommended switches, firewall, and CCTV systems, Company D will enjoy a secure and reliable infrastructure capable of meeting current and future business needs.