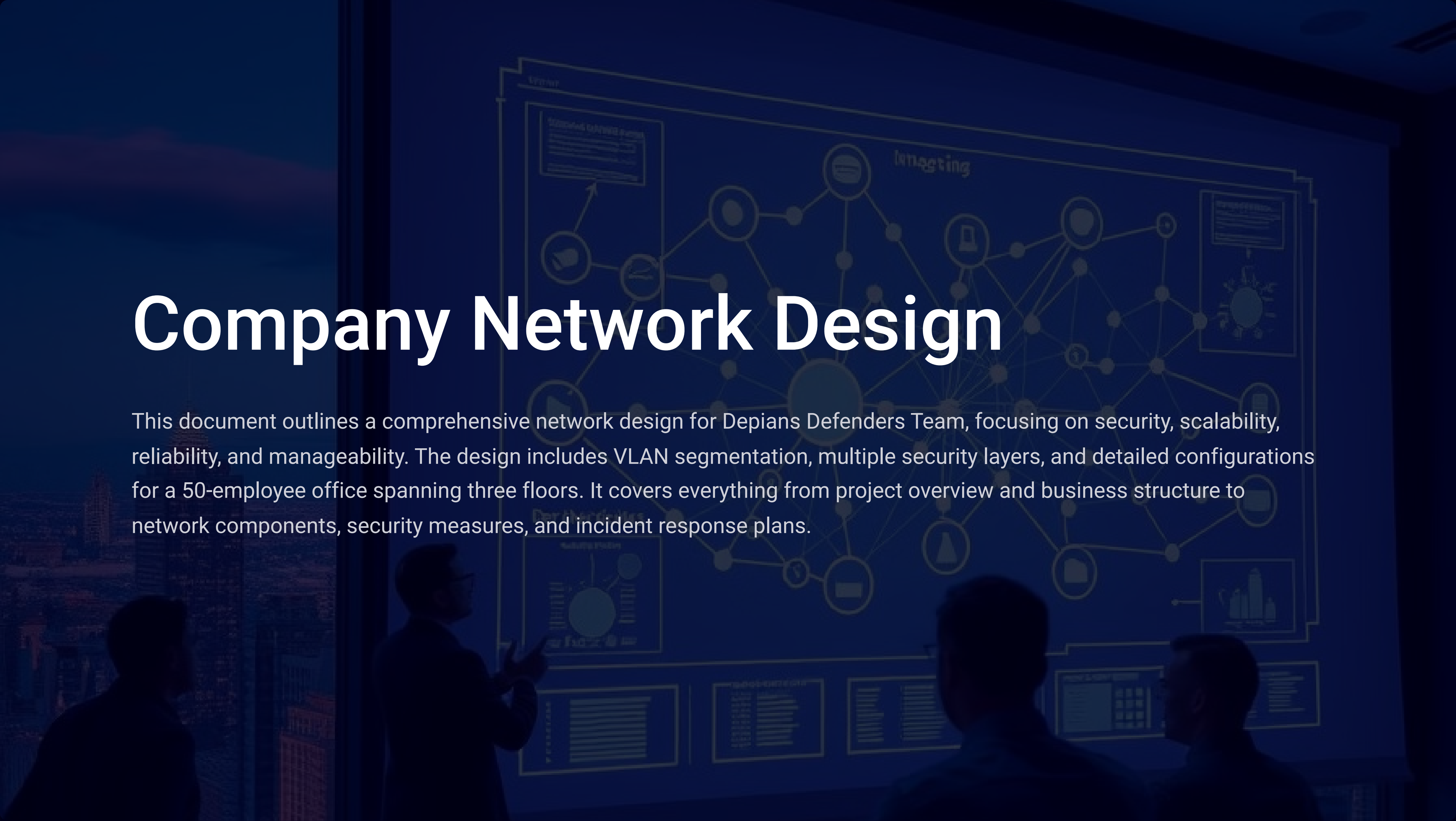

Company Network Design

This document outlines a comprehensive network design for Depians Defenders Team, focusing on security, scalability, reliability, and manageability. The design includes VLAN segmentation, multiple security layers, and detailed configurations for a 50-employee office spanning three floors. It covers everything from project overview and business structure to network components, security measures, and incident response plans.

Project Overview and Business Structure

The purpose of this project is to design a secure, segmented, and efficient network infrastructure for an IT consulting firm. This infrastructure facilitates secure communication within departments, protects sensitive data, and enables robust defense mechanisms against potential cyber threats.

The scope of this documentation details the network topology, security mechanisms, component configuration, and best practices. It is meant to guide network administrators, IT personnel, and security analysts in understanding the design, configuration, and operational aspects of the network.

Objectives

- Security: Implement multiple layers of security to prevent unauthorized access and protect sensitive data.
- Scalability: Ensure the network design can support future expansion, such as additional departments or new security layers.
- Reliability: Design redundant features, including a backup server, to maintain data integrity and business continuity.
- Manageability: Enable ease of monitoring, logging, and control through centralized management and VLAN segmentation.

Business Overview

- Industry: IT Consulting
- Location: Single office building (3 floors)
- Number of Employees: 50

Departmental Structure

The network is segmented by floors and departments to support data access and operational security.

Top Floor

- Executive: 5 employees (restricted access to critical resources)
- Finance: 10 employees (sensitive financial data access)
- HR: 5 employees (employee data management)

Middle Floor

- IT: 10 employees (network and systems management)
- Sales: 10 employees (sales and CRM)

Ground Floor

- Customer Support & Marketing: 10 employees (client interactions and marketing data)

Network Design and Components

3.1 VLAN Segmentation

Objective: Segregate traffic to enhance security and minimize broadcast domains.

Internal VLANs:

- VLAN10 (IT Department): 192.168.1.0/27
- VLAN20 (Executive Management): 192.168.1.32/27
- VLAN30 (HR): 192.168.1.64/27
- VLAN40 (Finance): 192.168.1.96/27
- VLAN50 (Sales): 192.168.1.128/27
- VLAN60 (Customer Support & Marketing): 192.168.1.160/27
- VLAN99 (Data Center Servers): 192.168.1.192/27

3.2 IP Addressing Scheme

Each VLAN is allocated a specific subnet with enough IPs for scalability. Subnetting minimizes IP wastage and controls access between VLANs.

3.3 Routing & Access Control

- Inter-VLAN Routing: Performed by a Layer 3 switch, allowing controlled communication between VLANs.
- Access Control Lists (ACLs): Enforced on the Layer 3 switch to permit or deny traffic based on VLAN requirements, enhancing security.

4. Network Components and Security Layers

1

Firewalls

External Firewall: Acts as the primary barrier between the internal network and the internet, blocking unauthorized access and filtering harmful traffic. DMZ Firewall: Protects DMZ servers from direct exposure to the internet and separates them from internal network resources, adding a layer of defense in depth. Internal Firewall: Protects internal departments from DMZ breaches and prevents lateral movement in case of a security compromise.

2

Network Intrusion Detection System (NIDS)

Located in the DMZ, the NIDS monitors inbound and outbound traffic, detecting anomalies and flagging potential intrusions. It provides real-time alerts to administrators, enabling rapid response.

3

Web Application Firewall (WAF)

The WAF shields the public-facing web server from threats like SQL injection and cross-site scripting (XSS), protecting sensitive applications from common vulnerabilities.

4

Honeypot

The honeypot is a decoy system that lures attackers, gathering data on their methods and tactics. Positioned in the DMZ, it isolates and logs malicious activity, aiding forensic analysis.

5

Backup Server with Dedicated Firewall

A backup server is installed to store essential data and configurations, ensuring data integrity in the event of an attack or failure. Its dedicated firewall isolates it from other segments, allowing secure backups without exposing sensitive data.

Security Measures and Monitoring

5. Logical Security Measures

- Host Intrusion Detection System (HIDS): Monitors critical hosts, alerting administrators to unauthorized changes.
- Log Management: A centralized log server collects logs from all devices. Analysis tools like Splunk or the ELK Stack parse logs for security incidents.
- Password Policies: Enforces password complexity and periodic changes to reduce vulnerability to brute-force attacks.
- Security Awareness Training: Regular training for employees on phishing, social engineering, and best security practices.
- Multi-Factor Authentication (MFA): For remote access to critical systems.

6. Physical Security Measures

- CCTV: Security cameras monitor key areas, ensuring 24/7 surveillance.
- Biometric Access: Restricts access to sensitive areas, such as the server room, to authorized personnel only.
- Fire Protection: Fire alarms and suppression systems installed to safeguard equipment.
- UPS: Ensures continuous power to critical systems during power outages.
- On-Site Security: Security personnel regularly patrol and monitor the building.

7. Monitoring and Maintenance

Regular Monitoring

- NIDS: Regularly monitor alerts for any signs of intrusion.
- Log Analysis: Review logs weekly, looking for suspicious patterns or potential threats.
- Backup Server: Verify backup integrity and functionality monthly.

Maintenance Schedule

- Patch Management: Apply security patches to all devices and systems quarterly.
- Firewall Rules Review: Update firewall rules bi-annually to accommodate any changes in network requirements.
- Training Refreshers: Conduct security training for employees bi-annually.

8. Incident Response

Incident Response Plan

1. Detection: Identify and document the incident using NIDS and HIDS alerts.
2. Containment: Isolate affected systems or VLANs to prevent lateral movement.
3. Eradication: Remove malware or close exploited vulnerabilities.
4. Recovery: Restore data from backup and bring systems back online.
5. Post-Incident Review: Analyze logs and honeypot data to improve future response.

Case Study: Simulating a Cybersecurity Incident

If an attacker bypasses the external firewall, they encounter the DMZ firewall, which blocks lateral movement to the internal network. Attempting to access sensitive systems triggers the NIDS, and if they interact with the honeypot, their activity is logged for analysis. The backup server ensures data recovery in case of a severe breach, providing resilience.

Backup Configuration and Future Improvements

9. Backup Server Configuration

Purpose

The backup server securely stores regular copies of critical data, configurations, and logs, supporting disaster recovery.

Setup

- Location: Segregated in a separate VLAN with a dedicated firewall.
- Firewall Configuration: Restricts access to the backup server, only allowing traffic from internal servers for backup purposes.
- Schedule: Automated backups occur daily, with a full backup performed weekly.

10. Potential Future Improvements

1. VPN Access: Implement VPN for secure remote access, especially for executives and IT staff.
2. RADIUS Server: Add a RADIUS server for centralized authentication and improved access control.
3. Enhanced DDoS Protection: Deploy additional DDoS prevention measures to safeguard against large-scale attacks.