Company Network Design

This document outlines a robust network design for a Comany in Egypt's New Administrative Capital, prioritizing scalability, security, and efficiency.

Prepared by

Depians Defenders Team

Students

Ahmed Atef Elbialy Ghanam
Moustafa Magdy Loutfy
Ammar Yasser Gomaa Hussien
Abdelrahman Nagaty Ahmed Ahmed
Said Abdo Elmaghawry Mohammed
Esraa Sherif Soliman

Track

Cisco Cybersecurity Engineer (CCNA and CyberOps)

Supervisor

Mamdouh Al Tahiry

Date

October 2024

Introduction: Objectives and Challenges

1 **Scalability**

The network must accommodate future growth and expansion.

2 **Security**

Protecting sensitive data is paramount.

Considering CIA triad,.. (Confidentiality, Integrity, and Availability)

3 **Realibity**

The network should facilitate smooth operations, ensure the delivery of time-sensitive content to multiple recipients simultaneously

Why you have to choose us?

Expertise in Cybersecurity

- Advanced knowledge in network security, including hands-on experience with industry-standard tools like QRadar and various security tools.

Customized Scalable Solutions

- **Tailored network designs that grow with your business, reducing future costs and ensuring smooth expansion**

Proven Reliability

- **Robust disaster recovery plans and real-time monitoring to ensure maximum uptime and data protection.**

Cost-Effective Approach

- **Efficient use of resources and tools to minimize overhead and operational costs.**

Cutting-Edge Technology

- **Incorporating the latest technologies like VLANs, firewalls, and secure VPNs to keep your business ahead of the curve.**

Market Research

Prior Research & Solutions:

The team studied existing corporate networks focusing on hierarchical designs and robust security measures.

Technology Exploration:

A comprehensive review of technologies was conducted, including Cisco Networking, firewalls, and security tools like SIEM Solutions and other tools.

Benchmarking & Competitor Analysis:

The team analyzed existing company network systems to ensure the proposed design adheres to industry best practices for scalability and security.

Building Layout and System Requirements

Building Layout

The Company has three floors, each dedicated to specific departments:

- The first floor houses management & IT.
- The second floor houses HR and finance departments.
- The third floor houses Marketing and Sales departments.
- IT Floor Houses All Important infrastructure assets, like DMZ And other Network devices.

System Requirements

The network design needs to consider various requirements. VLAN segmentation is essential to ensure performance and security.

Additionally, WEB, DNS,FTP and Email servers are crucial for operations. With advanced security measures, including firewalls, disaster recovery servers, HoneyPot, Backup, NIDS and other security assets.

Building Layout and User Requirements

Floor 1

Management And IT Assets which includes.

1- DMZ Servers (DNS, WEB, MAIL, FTP, Backup and also NIDS).

2- DR Assets (DR Server 1 & 2), Root PC.

3- Network devices (Routers, Switches, Firewalls)

4. HoneyPot.

5. IT PCs & Domain Controller.

Floor 2

2nd Administration departments (HR, Finance & other.)

Floor 3

Marketing and sales departments.

VLAN Structure and IP Subnetting

7VLAN 10 (IT): Subnet 192.168.1.0/27 for IT department.

VLAN 20 (Management): Subnet 192.168.1.32/27 for Management .

VLAN 30 (HR): Subnet 192.168.1.64/27 for Human Resources.

VLAN 40 (Finance): Subnet 192.168.1.96/27 for Finance Department.

VLAN 50 (Sales): Subnet 192.168.1.128/27 for Sales.

VLAN 60 (CS & Marketing): Subnet 192.168.1.160/27 for CS & Marketing.

VLAN 99 (DC): Subnet 192.168.1.192/27 for DC server.

Security Tools and Expertise

Industry-Standard Security Tools

The project team utilizes industry-standard security tools to ensure robust network security.

Cisco Devices

Cisco devices provide a secure and reliable network infrastructure.

Let’s Defend Platform

Let’s Defend is a hands-on cybersecurity training platform offering real-world SOC analyst challenges

QRadar Monitoring

The team leverages QRadar's capabilities to monitor network activity and identify potential security threats.

Multi-layered Security Architecture

Firewalls & WAF

Cisco ASA Firewall filter traffic and secure communication, with WAF added to secure more the web server traffic.

HoneyPot

HoneyPot to make a trap for any expected threats.

NIDS

Network Intrusion Detection System that monitor the operating systems of network devices and servers to detect any security vulnerabilities or malicious activity.

DR Assets

(Disaster Recovery isolated servers synchronized continuously with Backup server.

VLAN ACLs

VLAN Access Control Lists restrict access to sensitive departments.

Backup and Disaster Recovery

1

Regular Backups

Data is backed up regularly.

2

Offsite Storage

Backups stored securely offsite.

3

Disaster Recovery Plan

Ensures business continuity in case of emergencies.

Monitoring and Troubleshooting

Network monitoring tools will provide real-time insights. This ensures efficient troubleshooting and proactive maintenance.

Key Benefits for your Business

Strong Data Security
Protects sensitive information
Shields against cyberattacks and breaches

Disaster Recovery Plan
Minimizes downtime
Protects the business from unexpected failures

Scalable for Future Growth
Easily adapts to company expansion
Reduces future upgrade costs

Enhanced Performance
Optimizes network speed and efficiency
Reduces congestion with VLAN segmentation

Cost Efficiency
Lowers operational and maintenance costs
Reduces the need for additional hardware

Continuous Monitoring
Proactive threat detection
Real-time troubleshooting reduces potential disruptions

Compliance and Risk Management
Meets industry standards
Reduces financial risks associated with data loss and downtime

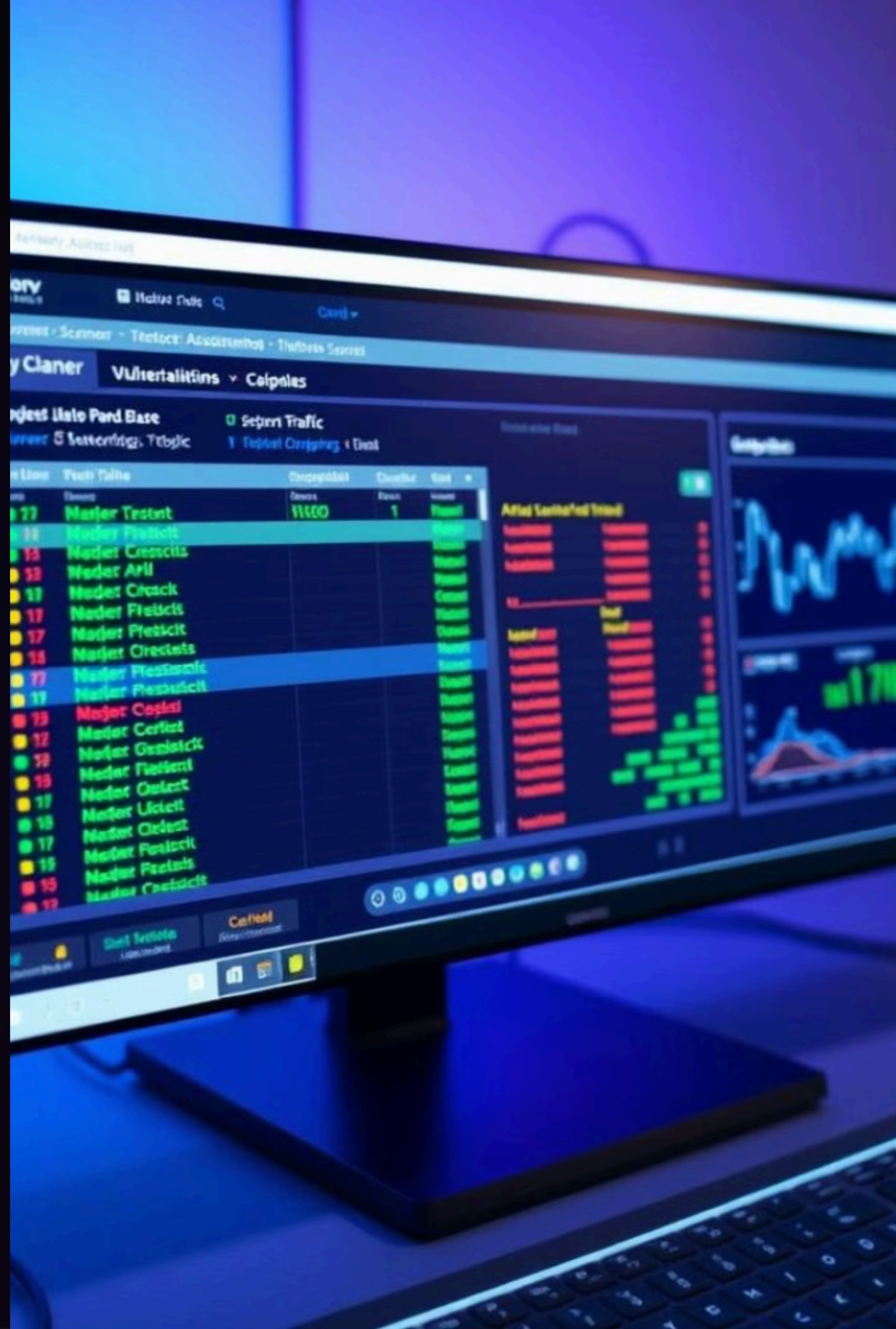
Project Outcome

The Depians Defender team successfully implemented a secure, scalable network for the Business Company needs.

The project achieved all key objectives, including VLAN segmentation, firewall protection, and robust network monitoring & securing.

Future Work/Improvements

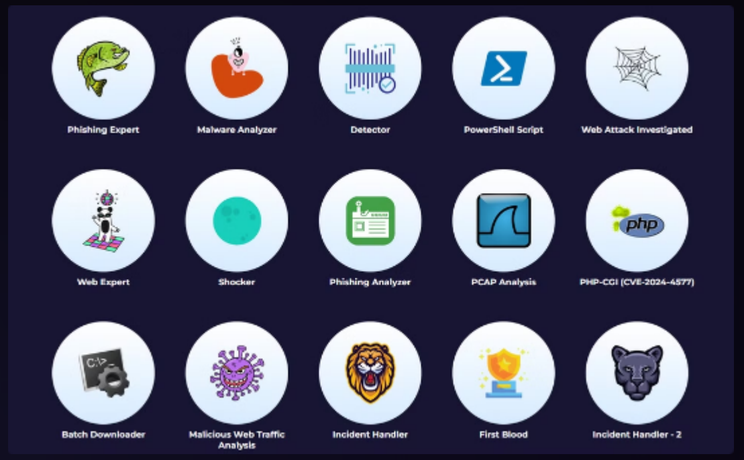
- Enhanced redundancy and disaster recovery plans for critical data and operations
- Expanding the use of cloud services to enhance scalability and operational flexibility
- Integration of additional security measures to counter emerging cyber threats such as advanced phishing attacks and malware
- Implementation of a robust security awareness training program for all employees
- Regular network security audits and vulnerability assessments to identify and address potential weaknesses



Conclusion

Secure and Scalable Solution

The Depians Defender team successfully delivered a highly secure, scalable, and operational network solution for the facility.



Technical Expertise

The project reflects the team's technical skills in network design and cybersecurity, ensuring the highest level of protection for the institution's sensitive data.

Enriched Project Outcomes

Hands-on experience with platforms like Let's Defend and QRadar allowed for anticipation of potential vulnerabilities, enhancing the overall security of the network.

Acknowledgments

Team members

We greatly appreciate your hard work and dedication to this project.

Supervisors

Thank you for your invaluable guidance and support throughout the development process.

Cisco Cybersecurity program

We are grateful for the exceptional knowledge and resources provided by the Cisco Cybersecurity program.

All contributors

We extend our sincere thanks to all contributors for their expertise and valuable contributions to this project.

Questions and Answers

We invite you to ask questions about our project.

Let's discuss your specific concerns and answer your questions.