رواد مصر الرقمية

وزارة الاتصالات
وتكنولوجيا المعلومات

Secure Network Architecture project

Under super vision

Eng. Amr Adel Kamal

project participants

Karim Mohamed Ali Farghaly

Mina Gamal Ezzat Fahmy

Mohamed Kamal Kawashti

Abanoub Eshak Azmy

Secure Network Architecture,

This document outlines the design and implementation of a secure network architecture for CloudNexus, a progressive cloud solutions provider. The plan covers various aspects of the network infrastructure, including internet connectivity, security measures, routing, switching, servers, and wireless capabilities, to ensure optimal performance, redundancy, scalability, and availability. The network architecture will be designed to meet the specific needs of CloudNexus and will be tailored to their current and future business requirements. It will be built on a robust and scalable foundation, ensuring that it can handle the increasing demands of their business. The architecture will also be designed to be highly secure, protecting CloudNexus's data and systems from unauthorized access.

Case Study and Requirements

Proplem

CloudNexus, a dynamic and progressive cloud solutions provider, specializes in offering cutting-edge cloud services to customers worldwide. The company, which employs 600 people, is growing and preparing to relocate to a larger facility. The new three-story building will house a server room, administrative and public relations ICT, finance and accounts, human resources and logistics, sales and marketing, and finance and accounts departments. The ICT department includes project managers, business analysts, software developers, cloud engineers, cybersecurity engineers, network engineers, system administrators, and IT support specialists.

Solutions provided

Before the relocation, a new network service must be developed and implemented in the new building. CloudNexus will put in place several security measures to protect the network against both external and internal threats, ensuring strong security. The firewall will be divided into three security zones: inside, outside, and DMZ. Critical servers will be placed inside the secured area, and servers for Active Directory (AD), DHCP, DNS, and Radius will be on the inside zone, while servers for FTP, WEB, email, applications, and network storage will be in the DMZ.

Network Infrastructure

1

Internet Services Provider (ISP)

To ensure redundant internet connectivity, the company has set up subscriptions with two ISPs.

2

Network Security

Two Cisco ASA Firewalls from the 5500-X series have been purchased to improve redundancy and network security.

3

Network Routing

Both firewalls and core switches will be utilized instead of a router.

4

Switching Infrastructure

The network includes two Catalyst 3850 48-Port Switches per campus and two Catalyst 2960 48-Port Switches to ensure strong local network connectivity.

Server and Virtualization Infrastructure

The ICT infrastructure consists of physical hardware, including servers and virtualization technology. Two physical servers will be virtualized using a hypervisor, allowing multiple virtual machines (VMs) to be created. These VMs will host various services, optimizing resource usage and flexibility. To ensure high availability and continuity, two DHCP servers will be configured to run in parallel, providing redundancy or failover capabilities. This setup enhances reliability, ensuring that network services remain operational even if one server experiences downtime.

Wireless and VoIP Infrastructure

Wireless Infrastructure

The wireless network will be centrally managed using a number of Lightweight Access Points (LAPs) and two Cisco Wireless LAN Controllers (WLC).

VoIP or IP Phones

A Cisco Voice Gateway will be utilized to enable phone service in the network.

IP Address Ranges

Management Network	192.168.20.0/24
VoIP	10.10.10.0/24
DMZ	10.11.11.0/27
Public Addresses	105.100.50.0/30 (ISP1), 197.200.100.0/30 (ISP2)

Network Design and Implementation

1

Hierarchical Design

A hierarchical approach with redundancy will be used to improve network resilience.

2

VLAN and Inter-VLAN Routing

VLANs will be implemented with the following IDs: 199 for Blackhole, 20 for LAN, 50 for WLAN, and 70 for VoIP. Inter-VLAN routing will be set up using a multilayer switch.

3

Routing and High Availability

Open Shortest Path First (OSPF) will be used as the routing protocol, and HSRP will be configured for load balancing, redundancy, and failover.

Network Security and Testing

Firewall Configuration

The Cisco ASA Firewall will be configured with default static routes, basic settings, security levels, zones, and policies to specify access control and resource usage within the network.

Access Control List (ACL)

A basic VTY line Access Control List (ACL) will be created to allow remote administration operations via SSH for the Senior Network Security Engineer PC only.

Final Testing

The entire network setup will be thoroughly tested to ensure all components are working as intended and communication is correct.