Design and Implementing Secured Company Network

This report presents the design and implementation of a secure network for a company, aimed at enhancing the organization's information security posture. The primary objectives were to ensure data integrity, confidentiality, and availability while providing a scalable solution that can accommodate future growth. The network design incorporates a multi-layered security approach, utilizing advanced technologies such as firewalls, and secure wireless access protocols. This report details the methodologies used, the challenges encountered, and the solutions implemented, offering valuable insights for similar projects in the future.

Table of Content:

|  |  |
| --- | --- |
| 1. | Introduction |
| 2. | Ip addressing |
| 3. | design and Implement a Network Architecture |
| 4. | Configure all the devices |
| 5. | Technologies implemented |
| 6. | Conclusion |

Project done by

K. Satyanarayana

[satyanarayanakokkirala18@gmail.com](mailto:satyanarayanakokkirala18@gmail.com)

Introduction:

A secure network is critical for protecting company assets, maintaining customer trust, and ensuring regulatory compliance. The primary objective of this project was to design and implement a secure network for that addresses current and future security challenges. The specific goals included:

* Protecting sensitive data from unauthorized access and breaches.
* Facilitating secure communication across all departments.
* Providing scalability to accommodate future growth and technological advancements.
* Implementing multi-layered security protocols to protect against both internal and external threats.
* Designing a network that supports future growth and maintains optimal performance under varying loads.

The following components have been incorporated:

Internet Services Provider (ISP): The Company has established a subscription with two ISPs to ensure redundant internet connectivity.

Network Security: Two Cisco ASA Firewalls from the 5500-X series have been acquired to enhance network security and redundancy.

Network Routing: Both the firewalls and the core switches will be used instead of a router.

Switching Infrastructure: The network includes two Catalyst 3850 48-Port Switches for each campus, and Catalyst 2960 48-Port Switches to ensure robust local network connectivity.

Server Hardware and Virtualization: Two physical servers will be utilized for virtualization through the hypervisor to achieve multiple virtual machines for various services. For redundancy or failover, we will have two DHCP servers running at the same time..

Wireless Infrastructure: Two Cisco Wireless LAN Controllers (WLC) and various Lightweight Access Points (LAPs) will centralize the management of the wireless network.

VoIP or IP Phones: A Cisco Voice Gateway will be used to enable telephony service in the network.

Cloud computing as an important technology is used to connect clients across the world to the company services and resources thus the proposed network should allow the team access to these resources

IP address :

Management Network: For the management, the IP address range of 192.168.10.0/24 has been allocated.

WLAN: The WLAN network will operate within the IP address range of 10.20.0.0/16.

LAN: For the local area network (LAN), the IP address range of 172.16.0.0/16.

VoIP: For the local area network (LAN), the IP address range of 172.30.0.0/16.

DMZ: The Demilitarized Zone (DMZ) will be assigned IP addresses from the range 10.11.11.0/27.

Public Addresses: Public IP addresses from the range 105.100.50.0/30 and 197.200.100.0/30

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | Network &  Subnet mask | Valid Host  address | Default gateway | Broadcast address |
| Management | 192.168.10.0/24 | 192.168.10.1 – 192.168.10.254 | 192.168.10.1 | 192.168.10.255 |
| WLAN | 10.20.0.0/16 | 10.20.0.1 – 1020.2555.254 | 10.20.0.1 | 10.20.255.254 |
| LAN | 172.168.0.0/16 | 172.16.0.1 – 172.16.255.254 | 172.16.0.1 | 172.16.255.255. |
| VOIP | 172.30.0.0/16 | 172.30.0.1 –  172.30.255.254 | 172.30.0.1 | 172.30.255.255 |
| DMZ | 10.11.11.0/27 | 10.11.11.1 –  10.11.11.30 | 10.11.11.1 | 10.11.11.31 |
| Insiders server | 10.11.11.32/27 | 10.11.11.33 – 10.11.11.62 | 10.11.11.33 | 10.11.11.63 |

.

Ip address Between the Cloud, ISP, Firewall, Routers and Layer3 switches:

|  |  |
| --- | --- |
| CLOUD Area | 8.0.0.0/8 |
| ISP1-Internet | 20.20.20.0/30 |
| ISP2-Internet | 30.30.30.0/30 |
| ISP1-FWL1 | 105.100.50.0/30 |
| ISP1-FWL2 | 105.100.50.4/30 |
| ISP2-FWL2 | 205.200.100.0/30 |
| ISP2-FWL2 | 205.200.100.4/30 |
| FWL1 to-MLSW1 | 10.2.2.0/30 |
| FWL1 to-MLSW2 | 10.2.2.4/30 |
| FWL2 to-MLSW1 | 10.2.2.8/30 |
| FWL2 to-MLSW2 | 10.2.2.12/30 |

VLANS:

Management-10

WLAN-20

LAN-50

VOIP-70

INSIDER SERVER-90

BLACKHOLE(unused ports)-199

Procedure:

1. **Basic Device Configuration:**

* 1. Configure all devices with basic settings including hostname, console, VTY lines, and SSH.

2. **VLAN Assignment and Trunking:**

* 1. Assign VLANs to appropriate interfaces on L2 and L3 switches.
  2. Configure access ports and trunk ports accordingly.

3. **STP Portfast and BPDU Guard:**

* 1. Enable Portfast and BPDU Guard on all access ports to enhance network stability and security.

4. **EtherChannel Configuration:**

* 1. Implement EtherChannel for aggregated links between switches for improved bandwidth and redundancy.

5. **Subnetting and IP Addressing:**

5.1Plan and implement IP addressing scheme for all network segments.

6. **HSRP and Inter-VLAN Routing:**

* 1. Configure HSRP on L3 switches for redundancy.
  2. Implement inter-VLAN routing and configure IP DHCP helper address for VLANs.

7. **Static IP Addressing for DMZ/Server Farm:**

* 1. Assign static IP addresses to DMZ or server farm devices for security and stability.

8. **DHCP Server Configuration:**

* 1. Configure DHCP servers to provide IP addresses dynamically to network devices.

9. **OSPF Configuration:**

* 1. Implement OSPF routing protocol on routers, L3 switches, and firewall.
  2. Configure network statements and router IDs for OSPF.

10. **Firewall Configuration:**

* 1. Define firewall interface security zones and set appropriate security levels.
  2. Configure firewall routing with OSPF and static routes as required.

11. **Firewall Inspection Policy:**

* 1. Establish and configure firewall inspection policies for traffic filtering and security enforcement.

12. **Wireless Network Configuration:**

* 1. Configure wireless network settings including SSID, security protocols, and access points.

13. **VoIP Configuration:**

* 1. Implement VoIP configurations including QoS settings for voice traffic prioritization.

14. **Verification and Testing:**

* 1. Validate configurations through testing and verification procedures.
  2. Document test results and ensure all configurations meet project requirements.

Technologies Implemented:

Design Tool: Utilize Cisco Packet Tracer for designing and implementing the network solution.

Hierarchical Design: Implement a hierarchical model that incorporates redundancy for enhanced network resilience.

ISPs: Establish connectivity to an ISP Router within the network infrastructure.

WLC: Ensure that each department is equipped with a Wireless Access Point (WAP) to provide WiFi access to employees, corporate users, external auditors, and guests, all centrally managed by a Wireless LAN Controller (WLC).

VoIP: Deploy IP phones in each department to support Voice over IP (VoIP) communication.

VLAN: Maintain VLANs with the following IDs: 10 for Management, 20 for LAN, 50 for WLAN, 70 for VoIP, and finally, 199 for Blackhole in which all unused ports are placed.

EtherChannel: Implement the Link Aggregation Control Protocol (LACP) for EtherChannel configuration, enhancing link aggregation efficiency.

STP PortFast and BPDUguard: Configure Spanning Tree Protocol (STP) PortFast and BPDUguard to expedite port transitions from blocking to forwarding states.

Subnetting: Utilize subnetting techniques to allocate the appropriate number of IP addresses to each network group.

Basic Settings: Configure fundamental device settings, including hostnames, and console passwords, enable passwords, banner messages, password encryption, and disable IP domain lookup.

Inter-VLAN Routing: Enable devices in all departments to communicate with one another by configuring the respective multilayer switch for inter-VLAN routing.

Core Switch: Assign IP addresses to Multilayer switches to enable both routing and switching functionalities.

DHCP Server: Ensure that all devices in the network obtain IP addresses dynamically from the servers located at the server farm site.

HSRP: Implement high-availability router protocols such as HSRP to achieve redundancy, load balancing, and failover capabilities.

Static Addressing: Allocate static IP addresses to devices located in the server room.

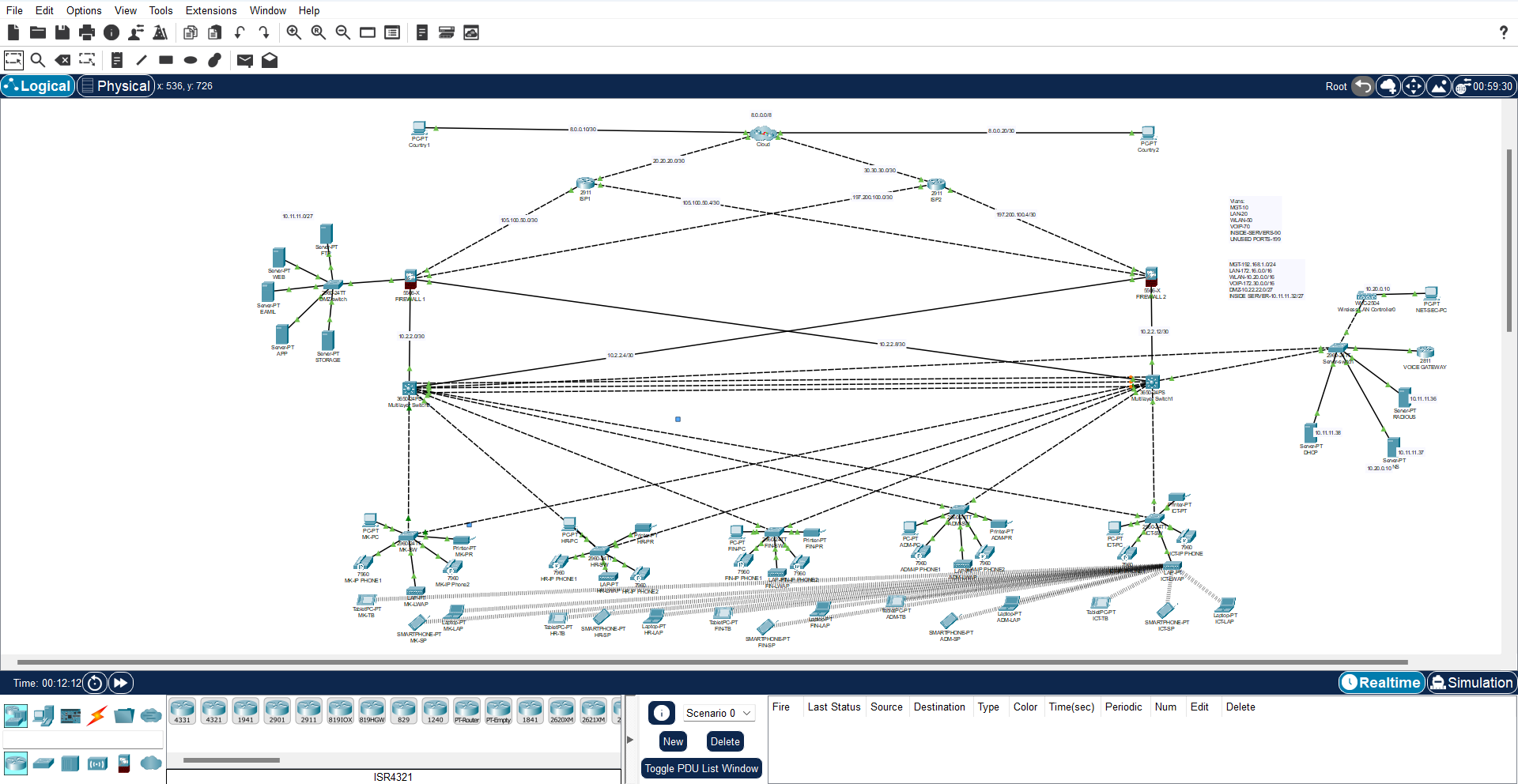
Routing Protocol: Utilize Open Shortest Path First (OSPF) as the routing protocol to advertise routes on the firewall, routers, and multilayer switches.

Standard ACL for SSH: Establish a simple standard Access Control List (ACL) on the VTY line to permit remote administrative tasks via SSH only for the Senior Network Security Engineer PC.

Cisco ASA Firewall: Configure default static routes, basic settings, security levels, zones, and policies on the Cisco ASA Firewall to define access control and resource utilization within the network.

Final Testing: Conduct thorough testing to verify proper communication and ensure that all configured elements function as intended.

The final network architecture:



Conclusion:

The design and implementation of a secure company network have been meticulously executed to address the growing demands for robust cybersecurity measures in today's digital landscape. This project has successfully achieved its primary objectives of enhancing network security, ensuring data integrity, and providing a scalable infrastructure capable of supporting future growth.

The introduction of a multi-layered security architecture, incorporating advanced technologies such as firewalls and AAA has significantly fortified the network against both internal and external threats. By segmenting the network into distinct zones and implementing strict access controls, the risk of unauthorized access and potential data breaches has been minimized.

The project also underscores the importance of adhering to industry best practices and standards, ensuring compliance with relevant regulations. Through careful planning, execution, and continuous improvement, has established a secure network environment that safeguards its critical assets and supports its business objectives.

Furthermore, the implementation ensures end-to-end connectivity throughout the world, facilitating seamless global communication and collaboration. This global connectivity is crucial , enabling it to operate efficiently across different geographical locations while maintaining a high level of security and performance. The secure network design allows employees, partners, and clients to connect and share information securely, regardless of their location, fostering a more dynamic and interconnected business environment.

In conclusion, the project has laid a solid foundation and providing a resilient network infrastructure that can adapt to evolving threats. The lessons learned and methodologies applied during this project offer valuable insights for future endeavors, emphasizing the critical role of security in modern network design and implementation. The success of this project not only enhances the company's security posture but also reinforces its commitment to protecting the privacy and integrity of its data, fostering trust among clients and stakeholders. Additionally, the established end-to-end global connectivity ensures that can continue to grow and thrive in an increasingly interconnected world.