Documentation for the Network Diagram of a Small Office

**Project:** Network Solution for a Small Office with 15-20 Employees

Table of Contents:

1. Network Design Overview
2. VLAN Structure
3. Security Measures
4. Intranet Server Plan
5. Setup Guide
6. Security Policies
7. Troubleshooting Guidelines

**1. Network Design Overview**

**Network Topology**

**[Internet] --- [Router] --- [Firewall] --- [Switch 1 - Management/Server VLAN]**  
 **| |**  
 **| +-- [File Server]**  
 **| +-- [Intranet Server]**  
 **|**  
 **+-- [Switch 2 - Employee VLAN]**  
 **| |**  
 **| +-- [Employee Workstations]**  
 **| +-- [Printers]**  
 **|**  
 **+-- [Switch 3 - Guest VLAN]**  
 **|**  
 **+-- [Guest Wi-Fi Access Points]**

**Components:**

* **Router:** Cisco RV340
* **Firewall:** Cisco ASA 5506-X
* **Switches:** Cisco SG350-28 (3 units)
* **Access** Points: Cisco Aironet 1832i
* **Servers:** Dell PowerEdge T40 (File Server, Intranet Server)

Description: This network design incorporates a router connected to the internet, a firewall for security, and three switches to segment the network into management, employee, and guest areas. Wireless access points provide Wi-Fi connectivity for employees and guests.

**2. VLAN Structure**

**VLAN 10 - Management:**

* Devices: Network management devices (router, firewall, switches).
* Users: Network administrators.

**VLAN 20 - Servers:**

* Devices: File Server, Intranet Server.
* Users: Employees with access to server resources.

**VLAN 30 - Employees:**

* Devices: Employee workstations, printers.
* Users: Office staff.

**VLAN 40 - Guests:**

* Devices: Guest Wi-Fi access points.
* Users: Office visitors.

Purpose: The VLAN structure segments the network to improve security, performance, and management.

**3. Security Measures**

**Firewall Rules:**

* Block all incoming traffic by default.
* Allow HTTP/HTTPS traffic for web browsing.
* Allow VPN connections for remote access.
* Restrict access to management VLAN (VLAN 10) to specific IP addresses.

**Wireless Security:**

* Employees: WPA3 encryption, SSID: Office-WiFi.
* Guests: WPA3 encryption, SSID: Guest-WiFi, isolated from the internal network.

**Additional Measures:**

* Enable network monitoring and logging.
* Regularly update firmware and software.
* Implement an Intrusion Detection/Prevention System (IDS/IPS).

**4. Intranet Server Plan**

Server Configuration:

* OS: Ubuntu Server 20.04
* Web Server: Apache HTTP Server
* Platform: Drupal CMS
* Database: MySQL

Functions:

* Document storage and sharing.
* Internal news and announcements.
* Employee resources and links to other internal systems.
* Forums and feedback forms.

Access Control:

* Restrict access to employees only.
* Use LDAP or Active Directory for user authentication.

**5. Setup Guide**

1. Router Configuration:

* Connect the router to the ISP.
* Configure WAN settings as provided by the ISP.
* Set up basic LAN settings (IP range, DHCP).

2. Firewall Configuration:

* Connect the firewall to the router.
* Configure firewall rules as specified.
* Set up VPN for remote access.

3. Switch Configuration:

* Connect switches to the firewall.
* Configure VLANs on each switch.
* Assign ports to appropriate VLANs.

4. Access Points Configuration:

* Connect APs to the employee and guest VLANs.
* Configure SSIDs and wireless security settings.

5. Server Setup:

* Install the operating system on servers.
* Set up the web server and CMS on the intranet server.
* Configure file sharing services on the file server.

**6. Security Policies**

Password Policy:

* Use strong, unique passwords for all devices and accounts.
* Change default passwords immediately after setup.
* Implement multi-factor authentication (MFA) where possible.

Network Access Control:

* Limit access to management VLAN to network administrators only.
* Use firewall rules to control traffic between VLANs.
* Regularly review and update access controls.

Data Backup:

* Schedule regular backups of all critical data.
* Store backups in a secure, off-site location.
* Test backup and restore procedures periodically.

**7. Troubleshooting Guidelines**

Common Issues and Solutions:

* No Internet Connectivity:
* Check router and firewall configurations.
* Verify ISP connection and settings.

Slow Network Performance:

* Ensure VLANs are correctly configured to reduce broadcast traffic.
* Check for hardware issues (e.g., faulty cables or ports).

Unable to Access Intranet Server:

* Verify server is powered on and connected to the network.
* Check web server and CMS configurations.
* Ensure firewall rules allow access to the intranet server.

Wireless Connectivity Problems:

* Ensure APs are properly configured and connected.
* Check wireless security settings (SSID, encryption).
* Verify VLAN assignments for APs.