**Design of a Secure Network for a Small Accounting Firm**

# Introduction

This project presents the design of a secure network infrastructure for a hypothetical small accounting firm. The goal is to create a network that supports internal operations, remote access, secure data sharing, and protection from common cybersecurity threats. The design leverages layered security and scalable architecture to meet both current and future business needs.

# Goals and Objectives

# Ensure secure and reliable connectivity for internal staff and remote workers.

* Facilitate secure communication and data exchange within the organization.
* Implement a layered security model to defend against common cyber threats.
* Separate guest and internal networks to minimize exposure.
* Design with scalability and adaptability for future growth.

# Organizational Needs

The accounting firm consists of 15 employees, including administrators, accountants, and customer service representatives.

The organization requires:

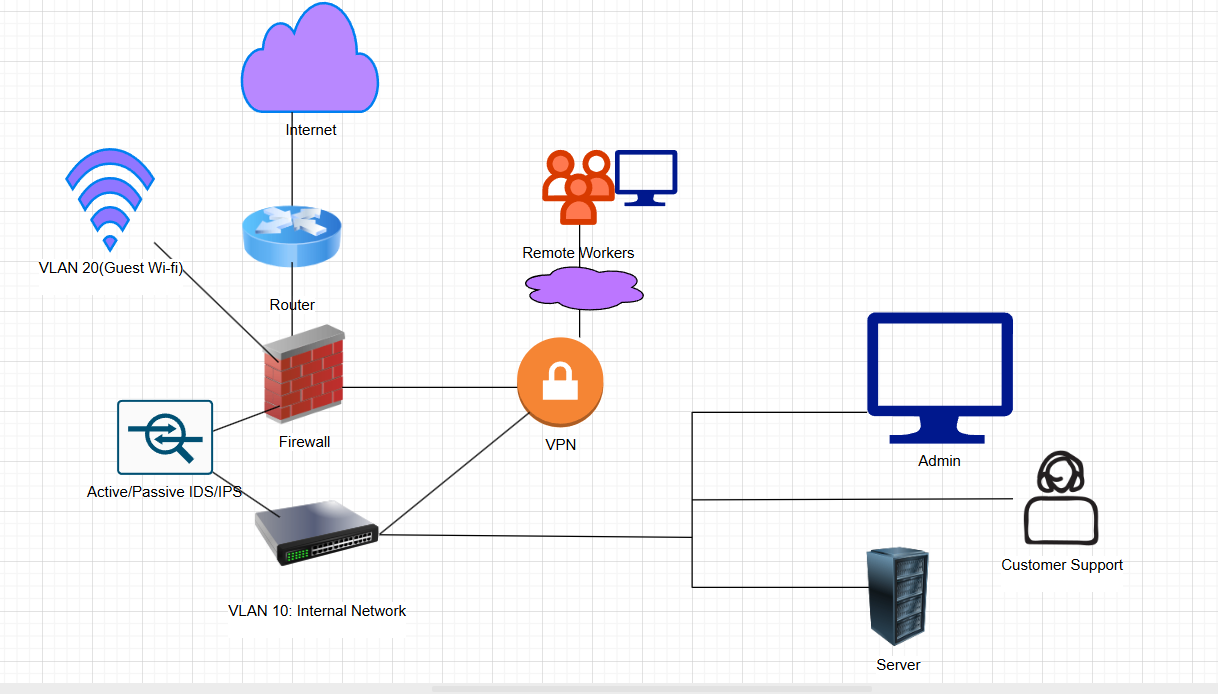
* Secure internal access to shared files and applications.
* Remote access for offsite employees.
* Internet connectivity with restricted access to potentially harmful sites.
* Wireless access for staff and guests.
* High availability and data protection.

# Threats and Vulnerabilities

* Unauthorized access to internal resources.
* Malware, ransomware, and phishing attacks.
* Unsecured wireless access.
* Data interception during remote communication.
* Insider threats due to weak access controls.

# Network Schematic

A detailed network diagram has been created and attached, showcasing physical and logical components of the proposed network.



**Detailed Schematic of the Proposed Network Design**

The updated diagram illustrates a secure network architecture designed for an organization that requires internal segmentation, guest access, remote connectivity, and intrusion monitoring.

It includes:

* Internet cloud connected to a core router
* A firewall protecting the internal network
* Active/Passive IDS/IPS device between the firewall and internal Layer 3 switch
* A Layer 3 switch that routes internal VLANs
* A VPN gateway for remote worker access
* VLAN segmentation for Internal (VLAN 10) and Guest Wi-Fi (VLAN 20)
* Devices connected under VLAN 10 including Admin, Customer Support, and Server roles

**Key Components of the Network**

* Internet: The external gateway for all network communication.
* Router: Connects to the ISP and segregates guest traffic from internal traffic.
* Firewall: Enforces traffic filtering, NAT, and segmentation policies.
* IDS/IPS: Monitors traffic between the firewall and internal network to detect and/or prevent suspicious activity.
* VPN Gateway: Secures remote access using encrypted tunnels.
* Layer 3 Switch: Manages inter-VLAN routing for internal devices.
* Admin, Customer Support, Server: Represent internal business roles with access controlled by VLAN policies.

**Placement of Security Measures**

* Firewall: Sits between router and Layer 3 switch, handling inbound and outbound traffic.
* IDS/IPS (Active/Passive): Positioned inline between the firewall and switch, inspecting all traffic entering the internal LAN.
* VPN: Connected to the firewall, providing secure tunnel access for remote workers.

**Wireless Network Considerations**

* Guest Wi-Fi (VLAN 20) is separated from VLAN 10.
* Routed directly through the router and not the internal switch.
* Ensures guests cannot access internal systems or devices.

**Description of Security Measures**

Firewall Rules:

* Allow only specific inbound VPN ports (UDP 500, 4500, ESP)
* Block VLAN 20 (Guest Wi-Fi) from accessing VLAN 10 (Internal)
* Allow HTTP, HTTPS, and DNS traffic for internal devices

IDS/IPS Settings:

* Signature-based detection enabled
* Alerts configured for port scans, brute force, unusual outbound traffic
* Passive mode for logging; active mode for critical threats

VPN Setup:

* Uses IKEv2/IPSec
* MFA required for login
* Split tunneling disabled to enforce all traffic through VPN tunnel

**Threat Mitigation via Security Measures**

* Firewall: Blocks unauthorized access, protects against external threats
* IDS/IPS: Detects and optionally prevents attacks such as scans, DDoS, malware C2 traffic
* VPN: Protects data in transit from remote users
* VLANs: Isolate traffic to prevent unauthorized lateral movement
* MFA: Stops password-only login vulnerabilities

**Wireless Security Strategies**

* Separate SSIDs for internal and guest users
* WPA3 Encryption enabled on access points
* Guest VLAN 20 blocked from internal VLAN 10
* MAC Filtering on internal wireless SSID

**Justification**

* Reduces risk of internal compromise via guest devices
* Ensures only authorized devices access business-sensitive systems

**Implementation Steps**

* Configure ISP router for VLAN support
* Deploy firewall with NAT, ACLs, and VPN support
* Install and configure IDS/IPS inline between firewall and Layer 3 switch
* Set up Layer 3 switch for inter-VLAN routing
* Assign devices to VLAN 10 (Admin, Server, Customer Support)
* Configure Guest Wi-Fi on VLAN 20 via access point
* Apply firewall rules for inter-VLAN control
* Deploy and test VPN setup with MFA

**Appendix – Configuration Snippets**

# VLAN Configuration

vlan 10

name Internal

vlan 20

name Guest

interface g0/1

switchport mode access

switchport access vlan 10

interface g0/2

switchport mode access

switchport access vlan 20

# Firewall ACL

access-list 101 deny ip guest\_net subnet\_mask internal\_net subnet\_mask

access-list 101 permit ip internal\_net subnet\_mask any

**Testing Network Security**

* Run scans with Nessus/OpenVAS to test firewall and IDS/IPS detection
* Use Kali Linux tools (Nmap, Hydra) to simulate attacks
* Test VLAN isolation by trying cross-VLAN pings/access
* Monitor VPN logs for unauthorized access attempts

**Success Indicators:**

* Alerts generated by IDS/IPS on abnormal activity
* Firewall blocks unauthorized access between VLANs
* VPN enforces secure, logged, and encrypted connections
* Internal network remains isolated from guest users

**Key Takeaways from the Project**

This project was a great learning experience. It gave me the chance to design and implement a secure, scalable network for a small accounting firm, keeping both internal and remote users in mind. One of the biggest wins was applying a layered security model that included firewalls, VPN, VLANs, and an IDS/IPS system. Separating the guest Wi-Fi from the internal network helped tighten security, and I was proud to see how the system could support both onsite and remote operations without compromising on safety.

**Challenges Faced and How They Were Addressed**

Understanding Real-World Behavior: Without devices to test on, I had to mentally walk through how things like ACLs, VLANs, and VPN traffic would behave. I really had to lean into the logic of networking.

Keeping It Realistic: I had to find a balance between what would look impressive and what would actually make sense in a real organization. Simplicity and clarity won out in the end.

Heavy Dependence on Research: Since we weren’t doing hands-on work, I had to spend time diving into documentation and configuration guides to make sure what I designed was actually feasible.

**Scalability and Adaptability**

* The design allows for straightforward scaling:
* Additional VLANs can be created on the Layer 3 switch.
* More users and endpoints can be added with minimal reconfiguration.
* Cloud integration can be introduced by modifying routing rules.
* Remote branch sites could connect via site-to-site VPN.
* Security components like IDS/IPS and firewall can be upgraded modularly as needs grow.

**References:**

*Mersch, A. (2021, October 4). What is layered security & how does it defend your network? Prosource.* [*https://blog.totalprosource.com/what-is-layered-security-how-does-it-defend-your-network*](https://blog.totalprosource.com/what-is-layered-security-how-does-it-defend-your-network)

*Basan, M. (2024, October 22). What is a VLAN? Ultimate guide to how VLANs work. Avatar.* [*https://avataracloud.com/blog/what-is-a-vlan*](https://avataracloud.com/blog/what-is-a-vlan)

*Netwrix. (n.d.). Remote Access Security Best Practices. Retrieved from* [*https://www.netwrix.com/remote-access-security-best-practices.html*](https://www.netwrix.com/remote-access-security-best-practices.html)

*Meter. (2024, September 6). 15 essential strategies for secure network design.* [*https://www.meter.com/resources/secure-network-design*](https://www.meter.com/resources/secure-network-design)