



**Site to site VPN between Company Branches**

A graduation project submitted within the cybersecurity engineering track of the Pioneers of Digital Egypt initiative

Under Supervision of:

**Eng. Khalid Abd\_rabo**

Prepared by:

**Yomna Adel**

**Hour Ahmed**

**Maram Ahmed**

**Nourhan Abdel-Mawla**

Oct 2024

# **Acknowledgment**

The project team wishes to express his gratitude and sincere thanks to Dr. Khalid Abd\_rabo for her supervision, encouragement.

Contents

[**Acknowledgment** 4](#_Toc180228317)

[**Chapter 1: Introduction** 5](#_Toc180228318)

[**Chapter 2: Network Design** 6](#_Toc180228319)

[2.1 Network Topology: 6](#_Toc180228320)

[2.2 Network Segmentation: 7](#_Toc180228321)

[2.3 IP Addressing Scheme: 7](#_Toc180228322)

[**Chapter 3: Security Measures** 9](#_Toc180228323)

[3.1 Firewall Rules: 9](#_Toc180228324)

[3.2 Intrusion Prevention System (IPS): 9](#_Toc180228325)

[3.3 Secure Remote Access (VPN): 9](#_Toc180228326)

[3.4 Access Control Lists (ACLs): 10](#_Toc180228327)

[**Chapter 4: Configuration and Implementation** 10](#_Toc180228328)

[4.1 Device Configuration 10](#_Toc180228329)

[4.1 Firewall and Security Configurations 10](#_Toc180228330)

[4.1 Secure Remote Access 11](#_Toc180228331)

[**Chapter 5: Security Implementation and Testing** 11](#_Toc180228332)

[5.1 Security Hardening: 11](#_Toc180228333)

[5.2 Vulnerability Assessment: 11](#_Toc180228334)

[5.3 Security Monitoring: 12](#_Toc180228335)

[**Conclusion** 12](#_Toc180228336)

# **Chapter 1: Introduction**

* Purpose**:** This document outlines the design, implementation, and security procedures for securing the small business network consisting of 30 employees. The network supports employee workstations, printers, a small server, and guest Wi-Fi, with a focus on securing access to sensitive data and protecting the business from cyber threats.
* Scope**:** The project includes designing a network topology, implementing network segmentation, providing site of site VPN; the employees in site A can communicate with employees from site B .

# **Chapter 2: Network Design**

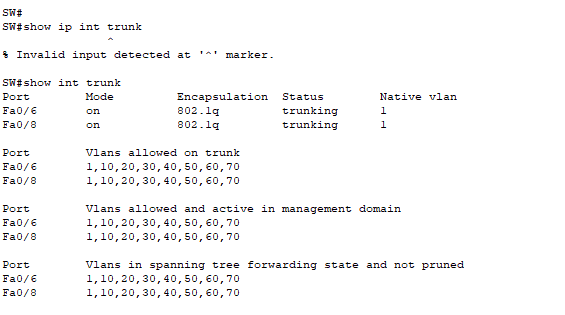
## 2.1 Network Topology:

* **Overview:** The network consists of routers, switches, wireless access points (APs), and a firewall. The design includes segmented networks (VLANs) for employee workstations, servers, and guest access to ensure proper security and isolation.
* **Diagram:** Include a detailed network diagram with labeled components, connections, and segments. For example:
  + **Router 1**: Connects the business to the internet.
  + **Router 2**: For configurations and IPs addresses
  + **Router 3**: For vpn and site to site communication
  + **Switch 1**: Core switch handling connections between employee workstations and the server.
  + **Switch 2**: Connects servers of employee and guest.
  + **Firewall**: Positioned between the router and internal network to control traffic and protect against threats.
* **Components:**
  + **Router**: Manages external connectivity and routing between internal VLANs and the internet.
  + **Switches**: Allow the segmentation of the network using VLANs.
  + **Access Points (APs)**: Provide wireless connectivity to employee and guest devices.
  + **Firewall**: Protects the internal network from external threats.

## 2.2 Network Segmentation:

* **Employee Network (VLAN 10):** 10.1.10.1/24
* Contains workstations for a department 1 (employees)
* **Employee Network (VLAN 20):** 10.1.20.1/24
  + Contains workstations for a department 2 (employees)
* **Employee Network (VLAN 30):** 10.1.30.1/24
  + Contains workstations for a department 3 (employees)
* **Guest Network (VLAN 40):** 10.1.40.1/24
  + Provides isolated internet access for guests, separate from the internal business network to reduce security risks.
* **Printer Network (VLAN 50):** 10.1.50.1/24
* Contains workstations for all printers.
* **Server\_Employee Network (VLAN 60):** 10.1.60.1/24
  + Dedicated to the small server for sensitive data storage and internal applications.
* **Server\_Guest Network (VLAN 70):** 10.1.70.1/24
  + Dedicated to the small server for guests.

## 



## 2.3 IP Addressing Scheme:

* **Internal IP Subnets:**
  + **Employee Network: 10.1.10.1/24 -> 10.1.30.1/24**
  + **Guest Network: 10.1.40.1/24**
  + **Printer Network: 10.1.50.1/24**
  + **Server Network: 10.1.60.1/24 and 10.1.70.1/24**
* **Static IP Assignments: Servers and network devices are assigned static IPs for management and configuration.**
  + **Router 1: 203.0.113.1/24**
  + **Router 2: 100.1.1.1/24**
  + **Router 3: 100.1.2.1/24**
  + **Core Switch: 10.1.1.1**
* **Dynamic IPs: Employee and guest devices receive IPs via DHCP within their respective VLANs.**

## 2.4 OSPF Routing:

|  |  |  |
| --- | --- | --- |
| Devices | Ips neighbours | |
| Router 1 | 203.0.113.1/24 | 203.0.114.1/24 |
| Firewall 1 | 203.0.113.2/24 | 10.1.1.2/24 |
| Router 2 | 100.1.1.1/24 | 10.1.1.1 |
| Firewall 2 | 203.0.114.2/24 | 100.1.2.2/24 |
| Router 3 | 100.1.2.1/24 | 10.100.1.1/24 |

# **Chapter 3: Security Measures**

## 3.1 Firewall Rules:

**Purpose:** The firewall protects the network by controlling traffic between internal VLANs and the internet. Key firewall rules are implemented for:

* **Denying inbound traffic** unless explicitly allowed (default deny policy).
* **Allowing outbound traffic** from the employee and server networks.
* **Blocking communication between VLAN 40 (Guest) and VLANs 10 ,20,30 and 50** to ensure guest devices do not access internal resources.
* **Specific Rules:**
  + Allow HTTP/HTTPS outbound traffic from all VLANs.
  + Allow VPN traffic (port 1194 for OpenVPN).
  + Block all inbound traffic except for VPN access.

## 3.2 Site to site (VPN):

 **Purpose:** To securely connect multiple office locations over the internet, allowing them to function as a single network.

 **Technology Used:** IPsec VPN or OpenVPN for site-to-site connectivity.

 **Network Integration:**

* **Inter-Site Connectivity:** Employees at remote locations can securely access internal resources (e.g., servers, applications) as if they were in the main office.
* **Site-to-Site Traffic:** All traffic between the two sites is encrypted using IPsec (or OpenVPN), ensuring data security.

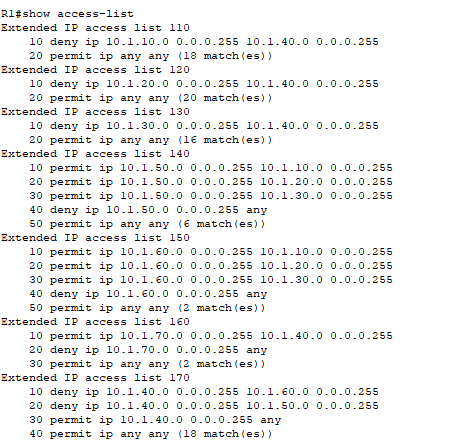


## 3.3 Access Control Lists (ACLs):

 **Purpose:** ACLs limit access to specific network segments based on IP address or protocol.

 **Implementation:**

* ACLs are applied to switches and routers to prevent unauthorized access between VLANs.
* Only employees have access to the server VLAN; guest VLAN access is restricted to the internet.



# **Chapter 4: Configuration and Implementation**

## 4.1 Device Configuration

 **Router:** Configured to support inter-VLAN routing, VPN services, and firewall rules.

 **Switches:** VLANs are implemented on Layer 2 switches, with trunk ports allowing communication between switches and the router.

 **Access Points:** Configured with two SSIDs, one for employee access (with WPA2-Enterprise) and one for guest access (WPA2-Personal).

## 4.2 Firewall and Security Configurations

 **Firewall:** Configured with the rules mentioned in Section 3.1

## 4.3 Configure Site to Site VPN

Configure site to site IPsec VPN on the ASA FWL

* Create crypto ikevl policy
* Tunnel group to specify pre\_shared key
* Create IPsec Transform set
* ACL to identify traffic of interest
* Create crypto map
* Enable ikevl and apply crypto map on the interface

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

# **Conclusion**

 **Summary:** The network is designed to ensure secure access to resources while protecting against cyber threats through segmentation, firewall rules, VPN access, and active monitoring.

 **Future Recommendations:** Suggestions for periodic vulnerability assessments, employee security training, and ongoing patch management to ensure long-term security.