Open Access Library Journal
2025, Volume 12, e12489
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Enterprise Network Design and Security Optimization

Kelechi Ikpe*, Evans Ashigwuike

Department of Electrical and Electronics Engineering, University of Abuja, Abuja, Nigeria
Email: *k_ikpe@yahoo.com, ecashigwuike@ymail.com

How to cite this paper: Ikpe, K. and Ashigwuike, E. (2025) Enterprise Network Design and Security Optimization. *Open Access Library Journal*, **12**: e12489.
https://doi.org/10.4236/oalib.1112489

Received: October 17, 2024
Accepted: March 22, 2025
Published: March 25, 2025

Abstract

Enterprise networks are the backbone of an organization's ability to communicate and share data. Information Technology Systems (ITS) extends beyond Computers and includes Phone Systems, Fax Machines, Internet of Things (IoT), applications, and other communication and data devices. A large company may have an extensive enterprise network that connects buildings around its headquarters campus with a high-speed network and other prerequisites, thereby making it highly vulnerable to threats and attacks. Enterprise network security is protection and precaution against confidentiality, integrity, availability, and accountability breaches. It entails protecting users and data against intruders by installing at several endpoints, encryption devices to sophisticate identification and authentication processes by cascading on the network, application, and transport layers of the open system interconnect (OSI) model architecture. This design will focus on the security challenges of both wired and wireless networks. Wireless Local Area Networks (WLAN) is more vulnerable to attacks because it transmits and receives data over the air and thus collectively combine data connectivity with ease of mobility [1]. It can be concluded that a properly set network having the right set of services such as Routing Protocols(RP), Access Lists(ACLs), Virtual Local Area Networks(VLANs), Firewalls, Virtual Private Networks (VPNs), Intrusion Detection Systems(IDS) all accurately configured and infused together have high-security performance for protecting and mitigating attacks carried out by both internal users and intruders on a network, providing about 99.9% protection against threats and vulnerabilities [2]. Virtual Private Network (VPN) provides a means by which remote computers communicate securely across a public Wide Area Network (WAN) such as the Internet. Firewalls are the main technology for access control between devices. All these devices are used to develop frameworks and policies which are enforced on the network to make it "airtight". Given the huge relevance of communication and system security in today's IT environment, this finding suggests that enterprise computer security remains an under stud-

ied research topic [3].

Subject Areas

Computer and Network Security

Keywords

Security, Design, Firewalls, VPNs, DMZ

1. Introduction

With the tremendous increase in cyber threats, the security of data traveling over a network has become a significant concern for clients, employers and employees. The importance of network security was never as great a concern as it is now because of the amount of data that is exchanged through it. Unethical hacking has become one of the most common network threats as hackers or malicious users manipulate and attack the loopholes of vulnerable networks and take control of them. Therefore, this project body of work is aimed at designing a safe, powerful, flexible, and highly scalable security-based network for addressing the risks of cyber intrusion, data loss, and malware distribution. Therefore, the goal of this project is to develop one or multiple ways and tools to improve network security within corporate environments. Enterprise network and security optimization is a critical process and focussing on improving the performance, reliability, and security of an organization's network infrastructure should be a top priority for the technology department, if the organization is to remain in business. The entire network optimization process involves conceptualizing a waterproof network flow design, accurate device configurations as described in this project work, analyzing and fine-tuning various network security components, such as routers, switches, firewalls, and security systems, to ensure optimal functionality and protection against cyber threats and attacks.

2. Why Must We Secure Our Enterprise Networks?

Due to the increasing demand for business continuity, commercial environments have tasked themselves with providing technology-enabled solutions that are supposed to be powered by high-capacity networks. With the increasing presence of various kinds of official devices in a corporate network, an organization will certainly be constantly under cyber or network threats and attacks and it will be extremely catastrophic if the data of corporate organizations gets compromised. E.g. Universities, Banks, Tax organizations, etc. Two main threat categories resulting in potential harm are:

i) Data Breaches

Lack of innovative security standards, allows hackers to infiltrate systems and steal confidential data [4]. For a poorly designed and less secure network, data

breaches are a common threat. This can be caused by both insiders and intruders. In situations where enterprises do not implement principle of least privileges properly, internal employees can cause more harm than illegal intruders on corporate networks.

Figure 1 shows the two distinct means used in network infiltration, the Internet and Local Area Network (LAN). Sometimes the attacker is within the environment or works for the organization. A securely designed network can help mitigate the effect of poorly managed internal users and hackers. A breach of internal LAN and wireless networks opens the door to the invading hacker. As soon as they get network access, they then compromise you or your client's data, which can pose a huge risk to privacy and business operations. In some cases, hackers can go as far as locking you out of your system so that you can not access any of the data needed by your business to function. This is called a ransomware attack.

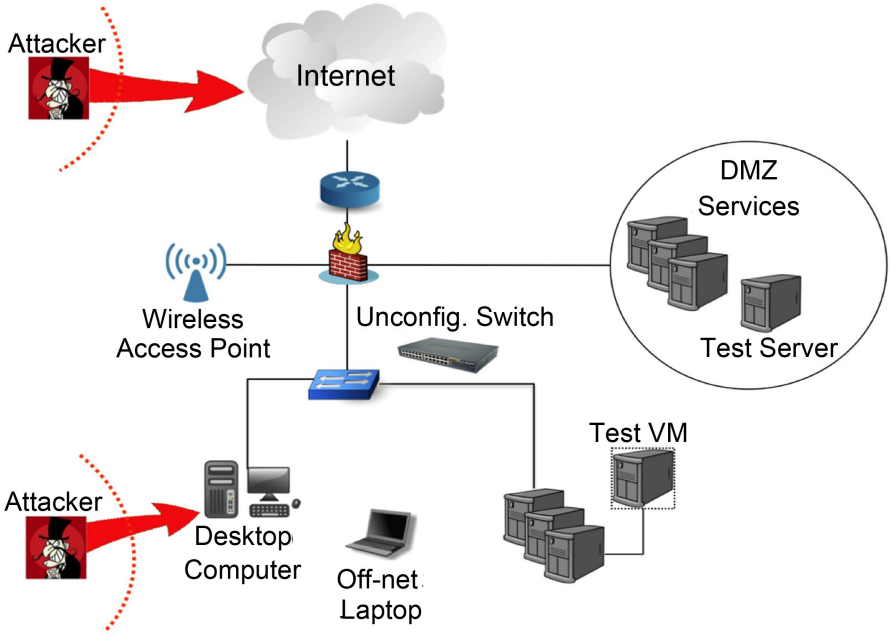


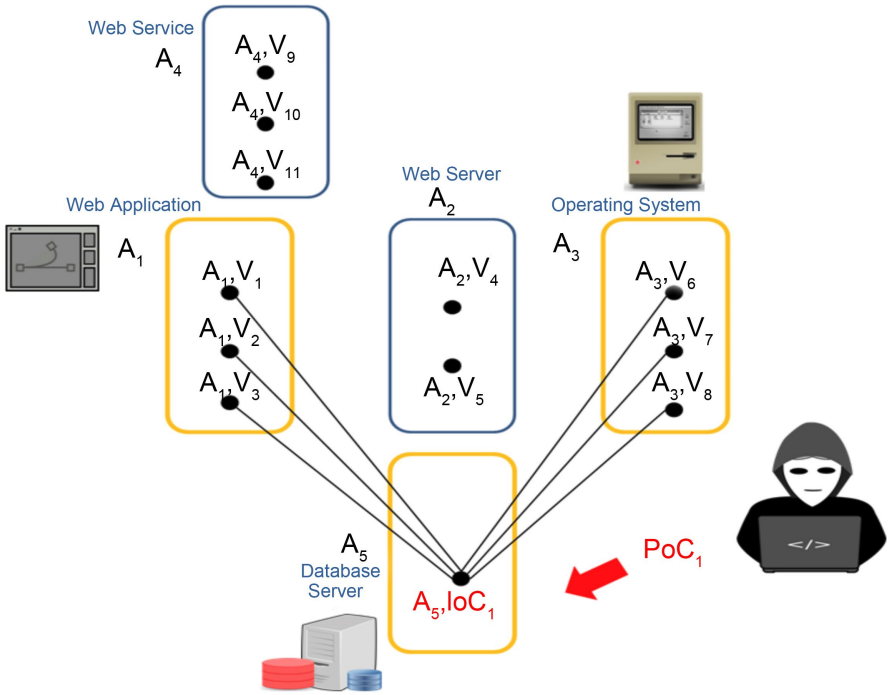
Figure 1. Intruding cyber attack strategy.

Figure 2 explains the logic hackers employ to spot vulnerabilities on the network, identify assets that will provide a back door entry into the systems, and utilize lateral movements through the network until they get to their indicator of compromise. What is worse in these situations is that if a hacker has access to your network and is sending out nefarious software, the business users are not usually aware of what is going on. This can go on for long periods before anything is detected. At a point, the damage is already done and can be catastrophic.

ii) Malware Distribution

Malware is a catch-all term for various malicious software, including viruses, adware, spyware, browser hijacking software, and fake security software. Malware distribution is a considerable risk that can cause maximum damage and lead to

100 percent loss of data when it finds its way to an insecure LAN or when utilizing an insecure Wi-Fi network. Hackers can easily bypass security settings that are enabled on mid or low-end technology. As soon as they gain back door access, hackers can utilize your network to send harmful software to unsuspecting users and perform other notorious activities [5].



A= Asset; V=Vulnerability; IoC=Indicator of Compromise; PoC= Proof of Concept.

Figure 2. Network infiltration strategy.

Key Areas to Consider when Optimizing Enterprise Network and Security

i) Network Architecture: Evaluate the current network architecture and identify any bottlenecks or areas for improvement. This may involve redesigning the network to ensure efficient data flow and minimize latency.

ii) Bandwidth Management: Implement bandwidth management techniques to prioritize critical applications and allocate network resources effectively. This helps optimize network performance and ensure smooth operation for essential business processes.

iii) Network Monitoring: Deploy network monitoring tools to gain real-time visibility into network traffic, performance, and security events. This enables proactive identification and resolution of issues before they impact the network's performance and security.

iv) Security Policies: Review and update security policies to align with industry best practices and compliance requirements. This includes implementing robust access controls, intrusion detection systems, and encryption mechanisms to protect sensitive data and prevent unauthorized access.

v) Endpoint Security: Endpoint security should be handled with care especially wireless devices as they are prone and vulnerable to password attacks. Most of the dictionary password-guessing attacks on WPA2-PSK are based on capturing the four-way handshaking frames between an authorized wireless client and the Access Point (AP) [6]. Regularly update and patch all devices to mitigate vulnerabilities and protect against malware and other cyber threats.

vi) User Authentication: Implement strong user authentication mechanisms, such as multi-factor authentication, to ensure that only authorized personnel can access the network resources. This helps prevent unauthorized access and enhances network security.

vii) Incident Response: Develop and regularly test an incident response plan to effectively handle security incidents. This includes defining roles and responsibilities, establishing communication channels, and conducting post-incident analysis to learn from any security breaches.

viii) Employee Awareness and Training: Employees' adherence to Information Security Policy (ISP) established in the organization is crucial in reducing security risks [6].

Educate employees about best practices for network and security management, including password hygiene, phishing awareness, and safe browsing habits. Regular training sessions can help reduce the risk of human error leading to security breaches.

By focusing on these areas, organizations can optimize their network infrastructure and enhance security posture, leading to improved performance, reduced downtime, and better protection against cyber threats.

3. Implementation of a Secured and Optimized Network

Designing and implementing a secured network entails breaking the entire network into component networks and securely implementing them separately, implementing the entire workload in phases and integrating them as a single unit. i.e. Adequate load balancing and segmentation, planning for the risk of failure by factoring fault tolerance, creating an independent Demilitarised Zone (DMZ), designing a Virtual Private Network (VPN), securing the Local Area Network (LAN) voice and data with proper firewall configuration, etc.

Figure 3 details a secure enterprise network design. The security architecture of this design is very dynamic as it is built to accommodate little alterations arising from environment uniqueness. This design relies on the effectiveness of the layers of the OSI architecture, as all communication within the enterprise and outside the Internet is encrypted and secured. This is enforced by the functional design and location of the firewall and other network devices. For instance, at layer 7, all data are encrypted with various encryption standards such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), etc. to protect the data at rest and in motion. For layers 3 and 4 we have the Internet Security and Key Management Protocol (ISAKMP) service running

which helps in securing Virtual Private Network (VPN) sessions. At layer 1 and layer 2, there are encryption protocols such as 802.1x, Wireless Access Protocol (WAP), Wireless Access Protocol 2 (WPA2), Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) etc., which will provide authentication, authorization and encryption for all enterprise data. On layer 3, Virtual Local Area Network (VLAN) and Port Security division are implemented to ensure that only clients' registered Media Access Control (MAC) address and VLAN in the switch can be connected to the network or the Internet [2].

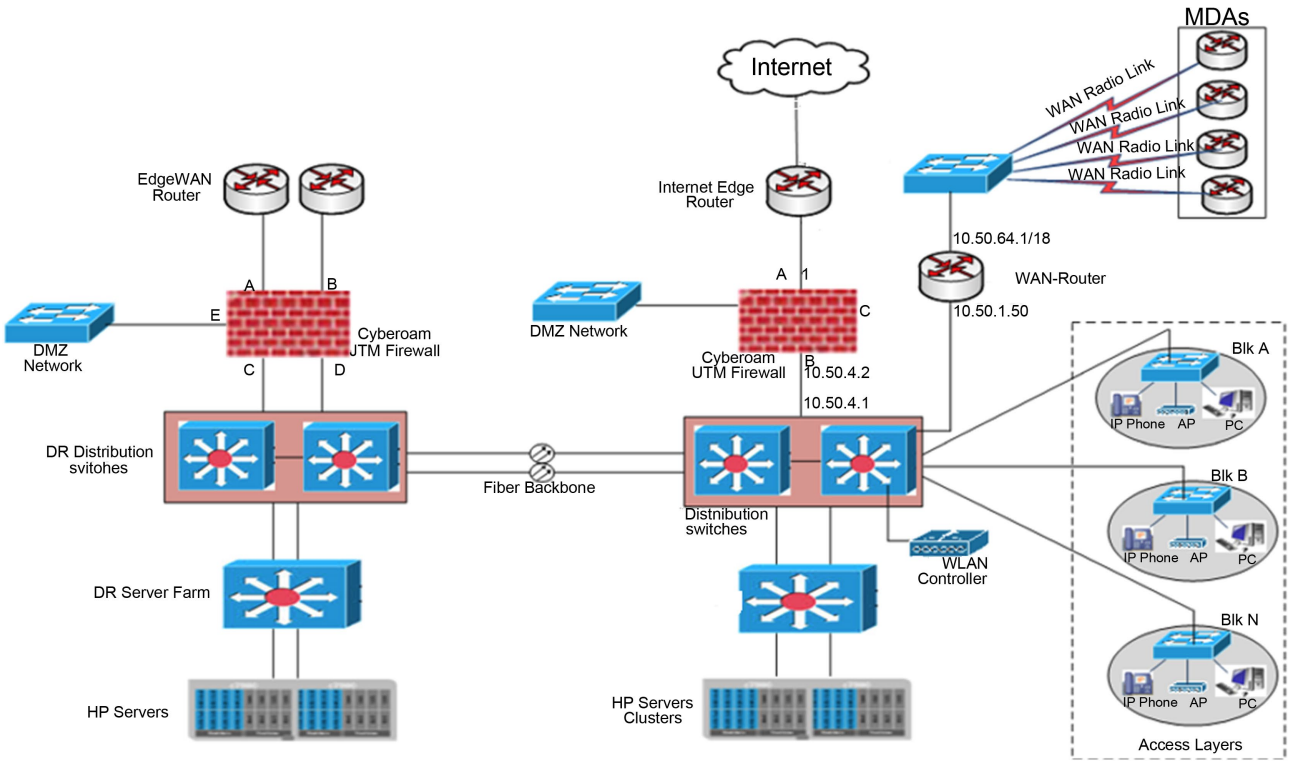


Figure 3. Secured network design.

The security devices and components deployed in this design are:

i) LAN/WAN Router: Helps you connect multiple devices to the Internet, and a gateway between multiple networks.

ii) Firewall Router: For Network LAN security, DMZ and VPN Connection.

iii) Radio Links: To simulate WAN Network source. This mostly connects multiple geographically dispersed sites to a single note.

iv) Core Switch: Regarded as a network backbone switch. It is used for routing and data switching at the core layer of the network.

v) Cisco LAN Switch: It connects devices on a computer network by using packet switching to receive data from the source and forward it to the destination. It connects clients, servers, and network devices.

vi) Servers: Used to host services and test security settings and configurations.

vii) Cisco Wireless Router: A device that acts as a wireless local area network (WLAN) controller.

viii) Cisco Access Points: Access points are used to extend the wireless coverage of an existing local area network, thereby increasing with ease the number of users allowed for connection by wirelessly assigning IP addresses to all approved devices.

ix) VOIP Telephones: Voice over IP (VoIP) technology supports your phone system to use ethernet or the Internet to make and receive calls, also used for communication within the enterprise.

3.1. Network-Load Segmentation

The first network security technique employed in this project is load segmentation. This was achieved by separating the network into multiple networks, namely LAN, Wireless, Voice, VPN, DMZ, etc., using Virtual Local Area Networks (VLANs), Software Defined Networking. All these are done to create service independence. With this approach, attackers and threats can be spotted easily and contained effectively while isolating other parts of the network thereby making them safe. As described in the design, this project's network architecture was segmented on service. That way, users of one service do not have access to another unless given rights and permissions. Whenever a threat exists in any segment, the other segments are isolated automatically as the incidence response commences.

3.2. Network High Availability—Fault Tolerance

The second technique employed in the design is network high availability techniques. Modern secured enterprise networks should come with some level of fault tolerance otherwise the data that we preserve will be lost to intruders due to negligence. The design employed a network fault tolerance configuration by having two distinct sites. i.e. Production and Disaster Recovery (DR) sites are linked with a WAN source using fibre backbone or microwave radio. The high availability technique deployed here is on the port level through the use of Link Aggregation Configuration Protocol (LACP) or on the switch and router by stacking via the Virtual Switching System (VSS) or stack-wise technology. While the LACP port configurations provide tolerance for the network in port failures the VSS provides tolerance in the event of a total switch or router failure. Stacking switches together can improve network reliability and flexibility, increase bandwidth, and simplify networking. Stacking saves users from managing multiple devices at the same time, especially in medium Data Centres or IT rooms. Benefits of the high availability setups include:

i) Providing redundancy to the active devices and tolerance during failure.

ii) It allows the addition or removal of switches at any time without disrupting the running network or affecting its performance.

iii) The Master switch provides all switching-related features and functions such as Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), Virtual Local Area Networking (VLAN), Spanning Tree Protocol (STP), etc.

3.3. Demilitarized Zone (DMZ)

The third security technique employed in the design to provide robust network security is the creation of a Demilitarized Zone (DMZ). This DMZ segment is necessary and was used to separate the LAN services from the Internet facing services. Most hacking scans and incidents always come from the Internet and enter your network. So, there is a core need for the Internet application servers to be resident in the DMZ network, protected by stringent firewall rules, and also segmented out from the other LAN to avoid lateral movements of attack. This should be a fundamental part of enterprise networks. A demilitarized zone or DMZ allows your servers to respond to public IP addresses. DMZs could be a physical or logical network (subnet) and are also known as perimeter networks or screened subnetworks.

Figure 4 explains a Demilitarized Zone (DMZ) functionality. The project's secured DMZ network was created using the following configuration details.

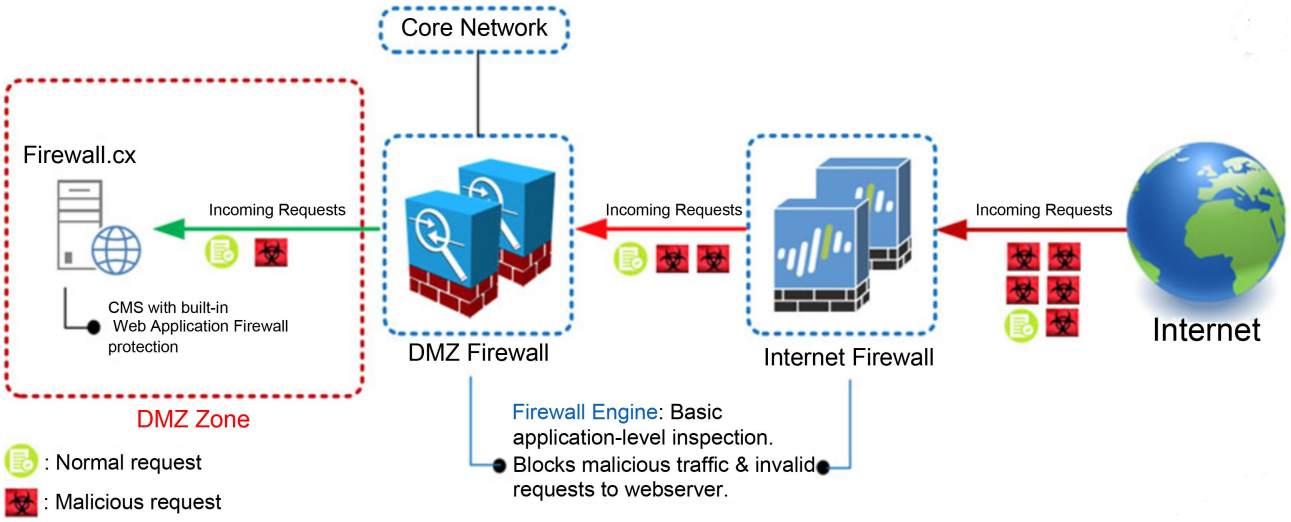


Figure 4. The DMZ setup.

DMZ Configuration (Steps)

i) Configure NAT to allow LAN users to access the Internet

In this setup, the AutoNAT service of ASA 5506-X firewall is used to create the NAT rules that permit hosts on the LAN segments Internet access. Network Address Translation, often abbreviated as NAT is used because hosts on the LAN network use private IP addresses and can not be routed on the Internet. Network Address Translation makes the addresses appear like the firewall outside interface IP address.

AutoNAT configuration for the LAN subnet is configured by creating a network to represent the available LAN subnets. In each of these objects, a dynamic nat rule is configured to conduct Port Address Translation (PAT) on these clients as they pass from the inside to the outside interface.

Each interface is configured with name if as below:

nat (inside, outside) dynamic interface

object network LAN

subnet **10.0.0.0** 255.0.0.0

nat (inside, outside) dynamic interface

ii) Configure NAT to permit DMZ servers Internet access.

The same configuration as for the LAN subnet is replicated to the DMZ servers subnet. The source interface name is replaced by the DMZ named interface.

object network DMZ

subnet **172.16.0.0** 255.255.0.0

nat (DMZ, outside) dynamic interface

iii) Configure inbound NAT rule for 172.16.0.5 DMZ webserver access

The following NAT rule statically maps the DMZ 172.16.0.5 webserver address to the 143.15.20.3 public address.

object network webserver

host **172.16.0.5**

nat (DMZ, outside) static 143.15.20.3

vi) Configure ICMP rules

Configure an extended access-list with the required rules to accept incoming echo replies.

access-list OUTSIDE extended permit icmp any any echo-reply

access-list OUTSIDE extended permit icmp any any unreachable

v) Configure Access list to permit incoming traffic to the DMZ web server

Complete the previous access-list with the rules to allow inbound HTTP traffic and apply the ACL to the outside interface.

object network webserver-external-ip

host 143.15.20.3

access-list OUTSIDE extended permit tcp any object webserver eq www

access-list OUTSIDE extended permit tcp any host 143.15.20.3 eq www

access-group ICMP-REPLY in interface outside

vi) Test HTTP connectivity Internet to the DMZ web server

Open a web browser on the "Public LAPTOP" located on the right of the network diagram.

The connection to http://143.15.20.2 should display the following welcome page.

Change 10.0.0.0 to **10.10.0.0**

Change 172.16.1.0 to **172.16.10.0**

3.4. Firewall and Virtual Private Network (VPN)

Virtual Private Network (VPN) service is the fourth security technique deployed in this project design. VPNs provide secure encrypted communication between remote networks worldwide using Internet Protocol (IP) tunnels and a shared medium like the Internet. End-to-end connectivity is established by tunneling [7]. The method used here is regarded as site-to-site Internet Protocol Security (IP-

SEC) VPN. In fact, with the general operation of a VPN, all traffic between the two endpoints of the VPN is encapsulated into pre-established tunnels that can be on different levels of the Open System Interconnection (OSI) model, (IPSEC or IKEv2 IPSEC at layer three, Point to Point Tunnelling Protocol (PPTP) at layer five, Layer 2 Tunnelling Protocol (L2TP) at layer two and OpenVPN or Virtual Tunnel Daemon at layer four) [8]. IPSEC is a VPN protocol based on different authentication methods to ensure security, e.g., Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) v2. By changing MS-CHAP-v2 with Protected Extensible Authentication Protocol (PEAP), the security level of PPTP increases, although it is recommended to use L2TP/IPsec [9] or Secure Socket Tunneling Protocol (SSTP) [10]. PPTP offers an integrated client for almost all platforms, including smartphones [11]. The VPN tunneling implemented here is done using the ASA 5505 firewall. It is often used as an alternative to expensive leased lines. In traditional setups, VPN endpoints are set up in hardware appliances, such as firewalls or routers [10]. By default, the Cisco ASA 5505 firewall denies the traffic entering the outside interface if no explicit access list (ACL) has been defined to allow the traffic. All malicious URLs and suspicious traffic were also blocked from both the inward and outward interfaces of the firewall service. These firewalls can inspect traffic in layers 2, 3, 4 and 7 of the OSI Model [7]. Other firewall incorporated technologies setup with the VPN include packet filtering, network address translation, circuit-level gateways, proxy services, application proxies and application level gateways [4].

Figure 5 highlights a VPN setup and working operation. The VPN service is able to protect users and data in transport because IPsec encrypts the entire IP traffic before the packets are transferred from the source node to the destination. To date, the IPSEC VPN remains the most robust and agile solution for interconnecting remote sites or networks [12]. IPSec can be configured in two modes, transport and tunnel. Tunnel mode is used for both VTI and classic IPSec (crypto maps). In tunnel mode, IPSec encrypts or authenticates the entire packet. After encryption, the packet is then encapsulated to form a new IP packet that has different header information. VPN Firewall or Cisco 2811 security routers use the Internet Security and Key Management Protocol (ISAKMP) and IPsec tunnelling standards to create and manage tunnels. IPsec provides authentication and encryption services to prevent unauthorized user and data access or modification. ISAKMP is the negotiation protocol that makes peers negotiate on how to build the IPsec security association. VPNs can be used with or without firewalls, but they are not recommended to be implemented without firewalls as their primary purpose is to secure network traffic [13].

In this design, an offsite located in a different geographic region will be securely connected to the HQ enterprise network through the Internet pipe using VPN technology. No dynamic routing protocol will be configured between the two sites.

Based on the secured network design a secured VPN Network was created with the following configuration details.

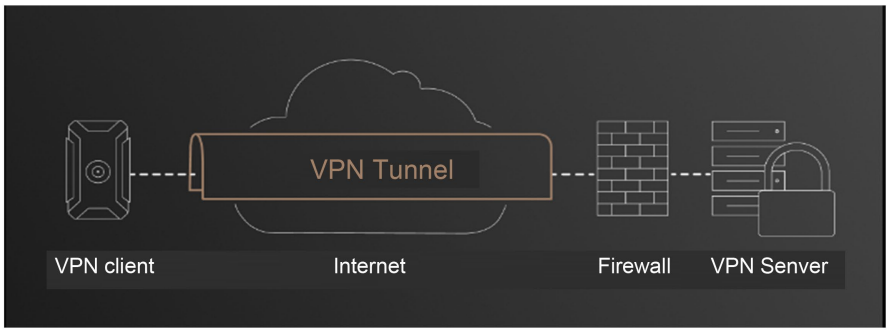


Figure 5. VPN tunnelling.

VPN CONFIGURATION (Setup)
hostname HQ-CAMPUS-VPN
interface Ethernet0/0
switchport access vlan 2
interface Ethernet0/1
interface Ethernet0/2
interface Ethernet0/3
interface Ethernet0/4
interface Ethernet0/5
interface Ethernet0/6
interface Ethernet0/7
interface Vlan1
nameif inside
security-level 100
ip address 10.50.4.2 255.0.0.0
interface Vlan2
nameif outside
security-level 0
ip address 134.95.56.17 255.255.255.240
object network BRANCH01_NETWORK
subnet 10.50.0.0 255.0.0.0
object network BRANCH_NETWORK
subnet 172.16.0.0 255.255.0.0
object network CAMPUS_NETWORK
subnet 10.0.0.0 255.0.0.0
object network PRIVATE_NETWORK
subnet 10.0.0.0 255.255.0.0
route outside 172.16.0.0 255.255.0.0 134.95.56.18 1
route inside 10.50.4.0 255.0.0.0 10.50.4.3 1
access-list BRANCH01_TRAFFIC extended permit tcp object CAMPUS_NETWORK object BRANCH01_NETWORK
access-list BRANCH01_TRAFFIC extended permit icmp object CAMPUS_NET-

WORK object BRANCH01_NETWORK
access-list ENTERPRISE_PRIVATE-TRAFFIC extended permit tcp object PRIVATE_NETWORK object PRIVATE_NETWORK
access-list ENTERPRISE_PRIVATE-TRAFFIC extended permit icmp object BRANCH_NETWORK object CAMPUS_NETWORK
access-group ENTERPRISE_PRIVATE-TRAFFIC out interface inside
telnet timeout 5
ssh timeout 5
dhcpd auto_config outside
dhcpd enable inside
crypto map BRANCH1 1 match address BRANCH01_TRAFFIC
crypto map BRANCH1 1 set peer 134.95.56.18
crypto map BRANCH1 1 set security-association lifetime seconds 86400
crypto map BRANCH1 interface outside
crypto ikev1 enable outside
crypto ikev1 policy 1
encr aes
authentication pre-share
group 2
tunnel-group 134.95.56.18 type ipsec-l2l
tunnel-group 134.95.56.18 ipsec-attributes
ikev1 pre-shared-key ALLPASSENGINEERING [14]

Figure 6 shows web filtering, port block and other embedded security controls in a firewall device. Some of the firewall configurations can be done with the graphic user interface as seen in the figure and others through the command line interface.

3.5. Confirmation Test of the Working VPN Ipsec Security Tunnel

As a vital area of the security architecture, the VPN is expected to encrypt data as user connections from the Internet move into the enterprise network and vice versa. To show the functionality of the security tunnel created on this project and how it handles encrypted user traffic and connections, the "crypto isakmp sa command" is used [15]. It shows the Internet Security Association Management Protocol (ISAKMP) security associations which have been negotiated between the two interface firewalls and the show crypto IPsec sa command is used to check IPSEC security associations and monitor encrypted traffic statistics. There are also one or more lines containing an src value or peer address for the remote gateway we specified in the tunnels. The state should be QM_IDLE and status should be active. The absence of an entry, or any in a different state, indicates that the Internet Key Exchange (IKE) is not configured properly but ours was okay, as seen in the results below. You should also see encapsulation and decapsulation hits on the firewall interfaces as encrypted traffic moves through the VPN tunnel.

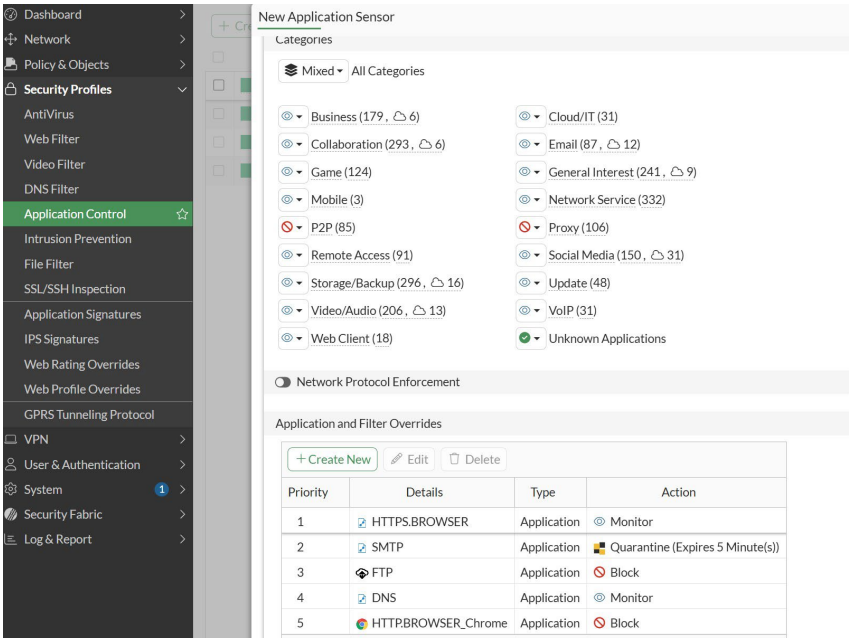


Figure 6. Firewall web filtering and port block sample.

HQ-CAMPUS-VPN -SHOW RESULT

 # show crypto isakmp sa

IKEv1 SAs:

Active SA: 1

Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)

Total IKE SA: 1

1 IKE Peer: 134.95.56.18

Type: L2L Role: Initiator

Rekey: no State: QM_IDLE

There are no IKEv2 SAs

HQ-CAMPUS-VPN -SHOW RESULT

 # show crypto ipsec sa

interface: outside

Crypto map tag: BRANCH1, seq num: 1, local addr 134.95.56.17

permit tcp object CAMPUS_NETWORK object BRANCH01_NETWORK

local ident (addr/mask/prot/port): (172.16.0.0/255.255.128.0/6/0)

remote ident (addr/mask/prot/port): (172.16.129.0/255.255.255.0/6/0)

current_peer 134.95.56.18

#pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0

#pkts decaps: 6, #pkts decrypt: 6, #pkts verify: 0

#pkts compressed: 0, #pkts decompressed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 134.95.56.17/0, remote crypto endpt.:134.95.56.18/0

path mtu 1500, ip mtu, ipsec overhead 78, media mtu 1500

current outbound spi: 0 × 6386132D (1669731117)

3.6. Penetration Test

Penetration test is a planned attack on a network or computer with aim to uncover vulnerabilities and assessing the effectiveness of the embedded network and infrastructure security controls. Different tools modeled around common attack methods are used for penetration testing, but in this project design, we utilised the Nessus tool. Nessus is a comprehensive vulnerability scanning tool that is predominantly used for compliance checks. The simulation attack test can either be a black box, white box, or grey box testing. Black box testing was utilised on this project, which involves attacking the network from the outside using only a target IP address. The Nessus tool was plugged into the environment after that we simulated a black box attack, and it delivered a vulnerability scan, recording all attack hits and categorizing them using the risk severity levels. i.e. low, medium, high, critical. It must be stated that penetration testing tools like Nessus should be used ethically. Additional security rules were created on the firewall devices to act as Network Intrusion Detection System (NIDS) and Network Intrusion Prevention System (NIPS) providing an efficient way to detect threats and enforce policies [16]. Third-party applications or solutions can also provide the NIDS and NIPS services.

Figure 7 shows several scanning services that can be initiated using the Nessus scanning tool. As the Nessus scans the network target systems for weakness, it keeps probing for various tests to identify potential entry points for attackers. As a network security provider, you have to identify the vulnerabilities identified in the Nessus scan and remediate them before they get exploited by hackers. However, some vulnerabilities don't provide an exploit for the service. The vulnerability assessment report after the scan can be seen in the table below. The result returned only vulnerabilities of low and medium risk that can easily be remediated.

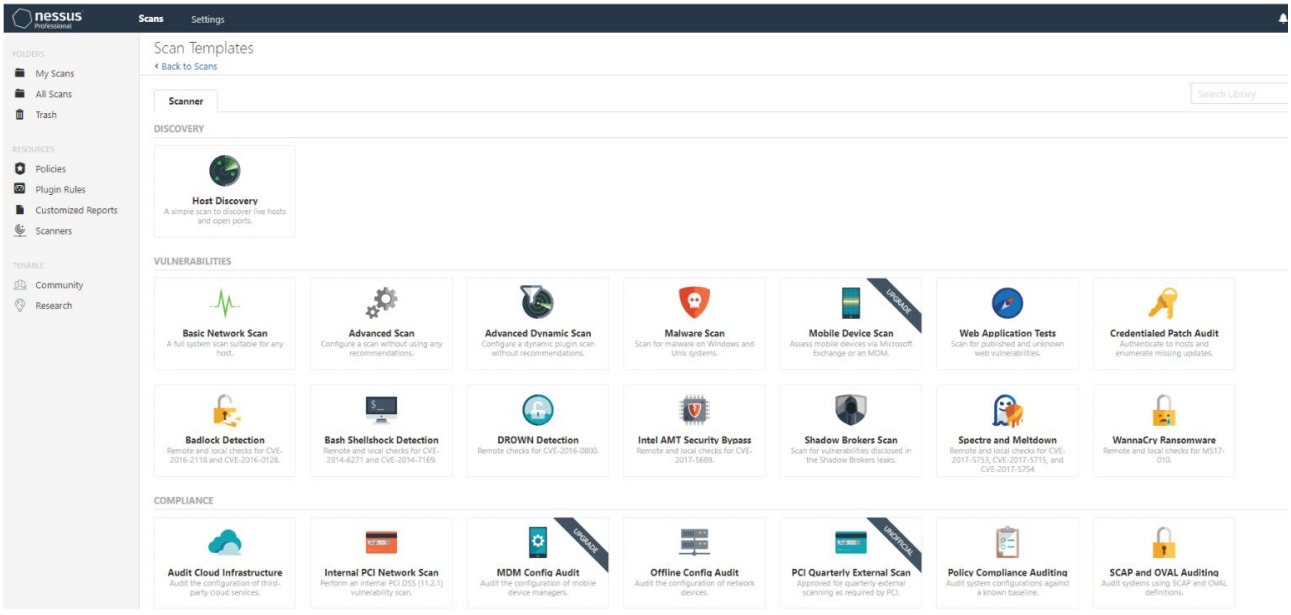


Figure 7. Nessus tool showing several attack scanning services.

The nessus scan report on the designed network can be seen in Table 1 highlighting the operating system type of the scanned systems on the network, the scan plugin ID, Common Vulnerability Exposure (CVE) ID which is a unique alphanumeric identifier assigned by the CVE program, Common Vulnerability Scoring System (CVSS), risk level, identified host, protocol and port number of the running service and the plugin or service name.

Table 1. Nessus network scan report.

Plugin Family	Plugin ID	CVE	CVSS	Risk	Host	Protocol	Port	Plugin Name
Windows	58751	CVE-2024-3389	3	Low	10.50.4.50	tcp	443	SSL/TLS Protocol initialization Vector Implementation Information Disclosure Vulnerabillity
Windows	57608	CVE-2016-2115	3.5	Low	10.50.4.53	smb	445	SMB Signing Not Required
Windows	57582	CVE-2018-5466	5.6	Medium	10.50.4.60	tcp	443	SSL Self Signed Certificate
Windows	51192	CVE-2023-5422	5.3	Medium	10.50.4.60	tcp	443	Certificate Can Note Be Trusted.
Windows	205451	CVE-2024-38167	4.2	Low	10.50.4.61	http	8080	Security Update for Microsoft.Net Core
Windows	205451	CVE-2024-38168	6.1	Medium	10.50.4.61	http	8080	Net And Visual Studio Denial of Service Vulnerability
Windows	132101	CVE-2018-12130	5.5	Medium	10.50.4.62	N/A	N/A	Windows Speculative Execution Configuration Check
Windows	79834	CVE-2020-1562	4.5	Low	10.50.4.63	N/A	N/A	Vulnerability In Microsoft Graphic Components Could Allow Information Disclosure
Windows	81743	CVE-2016-3216	4.9	Low	10.50.4.65	N/A	N/A	Vulnerability In Windows Photo Decoder Component.
Redhat Linux	175468	CVE-2022-35252	4.4	Medium	10.50.4.66	FTP, HTTP	21	Incorrect handling of control code characters in cookie

4. Summary

As a result of this thesis, we have seen that the cyber security industry will always be under attack and, therefore, needs more inputs and awareness to keep network risks, threats, and vulnerabilities low. The exponential growth of security risks and dangers outside of a network in the present times can strictly confirm the necessity for people to be extremely conscious of their organization's security posture to avoid breaches, attacks or even data loss. As different network threats continue to exist and evolve, there will also be technological advancement to combat them. The security devices used in the implementation of this work are not foolproof yet however, we emphasized accurate design, device arrangement and configurations as the bedrock of a secured network. In addition to the infrastructure, the security of the enterprise can be further enhanced by embedding security-aware services such as monitoring solutions, intrusion detection systems, enterprise vulnerability scanners, etc. These services can support the firewall functionalities and provide real time notification of threats and potential attacks and keep network intrusion to a bare minimum. The purpose of enterprise network and security optimization is to create a secure, reliable, and efficient network infrastructure that supports the organization's operations, protects sensitive data, and enables seamless communication and integrations. Based on the findings from this project, environmental consideration is critical to network and system security designs, as in most situations technical designs are required to fit purpose and in most cases consoli-

date on existing infrastructure. Overall, we hope that our work can be used as a reference by organizations and individuals when planning and designing their networks for optimum security and performance.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Prastavana, M. and Praveen, S. (2016) Wireless Security Using Wi-Fi Protected Access 2 (WPA2). *International Journal of Scientific Engineering and Applied Science*, **2**, 374-382.

[2] Alhasan, A.J. and Surantha, N. (2021) Evaluation of Data Center Network Security Based on Next-Generation Firewall. *International Journal of Advanced Computer Science and Applications*, **12**, 518-525. https://doi.org/10.14569/ijacsa.2021.0120958

[3] Acuna, D. (2016) Enterprise Computer Security: A Literature Review. *Journal of the Midwest Association for Information Systems*, **2016**, 37-53. https://doi.org/10.17705/3jmwa.00016

[4] Tharaka, S.C., Silva, R.L.C., Sharmila, S., Silva, S.U.I., *et al.* (2016) High Security Firewall: Prevent Unauthorized Access Using Firewall Technologies. *International Journal of Scientific and Research Publications*, **6**, 504-508.

[5] Yasar, K. and Lutkevich, B. (2023) Malware Prevention, Detection and How Attacks. https://www.techtarget.com/searchsecurity/definition/malware

[6] Nasir, A., Arshah, R.A. and Ab Hamid, M.R. (2017) Information Security Policy Compliance Behavior Based on Comprehensive Dimensions of Information Security Culture. *Proceedings of the* 2017 *International Conference on Information System and Data Mining*, Charleston, 1-3 April 2017, 56-60. https://doi.org/10.1145/3077584.3077593

[7] Panchakarla, B.P. (2019) Design and Implementation of Firewall to inspect Traffic in Encrypted VPN Tunnels**.** University Of Missouri-Kansas City.

[8] Semwal, P. and Sharma, M.K. (2017) Comparative Study of Different Cryptographic Algorithms for Data Security in Cloud Computing. 2017 3*rd International Conference on Advances in Computing*, *Communication & Automation* (*ICACCA*) (*Fall*), Dehradun, 15-16 September 2017, 1-7. https://doi.org/10.1109/icaccaf.2017.8344738

[9] Coonjah, I., Catherine, P.C. and Soyjaudah, K.M.S. (2015) Performance Evaluation and Analysis of Layer 3 Tunneling between OpenSSH and OpenVPN in a Wide Area Network Environment. 2015 *International Conference on Computing*, *Communication and Security* (*ICCCS*), Pointe aux Piments, 4-5 December 2015. https://doi.org/10.1109/cccs.2015.7374130

[10] Lackovic, D. and Tomic, M. (2017) Performance Analysis of Virtualized VPN Endpoints. 2017 40*th International Convention on Information and Communication Technology*, *Electronics and Microelectronics* (*MIPRO*), Opatija, 22-26 May 2017, 466-471. https://doi.org/10.23919/mipro.2017.7973470

[11] Luo, J. and Ji, Q. (2020) Password Acquisition and Traffic Decryption Based on L2TP/IPSec. 2020 *IEEE* 20*th International Conference on Communication Technology* (*ICCT*), Nanning, 28-31 October 2020, 1567-1571. https://doi.org/10.1109/icct50939.2020.9295700

[12] St-Hilaire, W.A. (2021) Digital Risk Governance. University of Ottawa Canada.

[13] Chandel, S. (2020) Securing a Network: How Effective Using Firewalls and VPNs Are? New York Institute of Technology.

[14] Packettracer, N. (2023) Site to Site IPSEC VPN with ASA 5505. https://www.packettracernetwork.com/labs/lab17-asa-ipsec-vpn.html

[15] Cisco Technology Support (2023) https://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec-debug-00.html

[16] Erlacher, F. and Dressler, F. (2020) On High-Speed Flow-Based Intrusion Detection using Snort-Compatible Signatures.