MODEL BASED ON VIRTUAL PRIVATE NETWORK: ENHANCING CYBERSECURITY IN THE RWANDAN UNIVERSITY SECTOR

ISSN 2277-7733
Volume 13 Issue 1, June 2024

BANA Philbert
University of Kigali, Kigali, RWANDA

Abstract

The rapid growth of technology and digitalization has revolutionized the way universities operate and conduct their academic activities. However, this progress has also exposed the Rwandan university sector to an ever-increasing range of cyber threats and vulnerabilities. The main objective of this research is to design and implement a robust model based on Virtual Private Network (VPN) technology to enhance cyber security in the Rwandan universities. The problem statement revolves around not only escalating cyber security challenges and loopholes at the Universities, but also issue of using a single security measure of currently using only firewall as a security measures which has some drawbacks, and all these may lead to data breaches, unauthorized access, and potential loss of sensitive information. To achieve the research objectives, a mixed-methods approach has been adopted, qualitative data have been gathered through interviews and focus groups with IT related personnel to gain insights into the existing security vulnerabilities and concerns. Additionally, quantitative data have been collected to assess the frequency and nature of cyber-attacks experienced by the Universities. The study used different tools including Eve-ng, AnyConnect, VMware workstation and Wireshark for network traffic analysis. In this project, a novel and practical model based on Virtual Private Network technology has been designed to reinforce the cyber security infrastructure of the University of Kigali. Secondly, the research findings shed light on the current cyber security landscape in the Rwandan university sector and provide valuable recommendations to other universities in the country to bolster their own security measures.

Keywords: *Virtual Private Network, cybersecurity, Network Access Control, Intrusion Detection System*

Nowadays, the world is rapidly evolving technologically where our society is getting more connected than have never been in the past. The education system is also improved so much as the results of technology.

Worldwide, because of the availability of general connection such as internet, majority of the higher learning institutions are wishing to give their students and staff members an opportunity to access centrally installed servers and database remotely. In specific way, educators or instructors wants to deliver and guide lab activities in distance. But, the utilization of internet augmented network security threats and challenges due to the big amount of data circulating on internet (Roy, Nag, Maitra & Bandyopadhyay, 2013).

The easiest way and quite decision of most organization is to put into practice Virtual Private Network for distant communication. However, there are many challenges that needs to be mitigated before its deployment. It is very necessary to know on how many strategies which can be adopted so that VPNs should be implemented and which one should be taken depending on the requirements. An IPSEC provide everlasting and permanent-on VPN access requirements (Chawla, Gupta & Sawhney, 2014).

Universities and educational institutions have become the main target for cyber-attacks and have already become affected by such problems. Educational institutions keep large quantity of important research, and valuable individual data, which make them an attractive target for cyber-attacks or incident, espionage and hacktivist (Ulven, Wangen 2021). Apart from that is the constant change of internet velocity which negatively impact communication and resources sharing. Often broadband fluctuate as the results of more users on wide home networks. Velocity decline may be caused by factors internal and external to the household. Internal factors consist of bandwidth severe applications choking a connection, old computing materials affecting stalls or majority people utilizing the internet concurrently making bottlenecks. External factors include the access ICT itself (e.g: cable) (chetty et al, 2011).

The Rwandan university sector, faces a growing challenge in effectively safeguarding its digital assets and sensitive information from the increasing cyber threats prevalent in today's interconnected world. Despite the existence of some security measures, the current cyber security infrastructure may not be sufficient to thwart sophisticated attacks, leaving the university's network vulnerable to data breaches, unauthorized access, and potential disruptions to academic and administrative operations.

As our case, currently University of Kigali is using Physical firewall which has many drawbacks such as Hardware firewalls handle egress traffic from the local network as safe, which is sometimes a threat if malware, such as a worm, penetrates your network and attempts to connect to the Internet and also hardware firewalls are more difficult to configure, especially for novices (Scheeres, 2006) and these misconfigurations can cause crucial network failures such as security violations which can lead to data loss or theft.

The lack of a comprehensive and tailored cyber security solution based on Virtual Private Network (VPN) technology further exacerbates the problem, making it imperative to address the inadequacies in cyber security measures to protect the university's digital ecosystem effectively. Therefore, the problem at hand revolves around the need to design and implement a robust model based on VPN technology to bolster cyber security in the Rwandan university sector, focusing on the specific case of the University of Kigali, and provide valuable insights and recommendations for other institutions facing similar threats.

The primary objective of this paper is to apply the Model based on Virtual Private Network as a way of enhancing Cyber Security in the Rwandan University sector; Case of University of Kigali.By implementation of such project there will be an enjoyable environment for Administrative staffs (non-academic staffs) because they will have some secured directories through which they receive order and they report their work with improved paperless system.

Literature review

Cybersecurity refers to the practice of protecting computer systems, networks, and digital information from unauthorized access, attacks, and damage. It involves implementing measures and protocols to ensure the confidentiality, integrity, and availability of data and resources in the digital domain (Jang-Jaccard & Nepal, 2014).

A Virtual Private Network (VPN) utilizes the internet, to enable secure communication where it adds a layer of security by encrypting the data flowing between companies and authenticating users to ensure that only authorized users can access that VPN connection ("MBA Knowledge base," 2018b).

A tunnel could be created by peering two VPN routers together. Alternatively, telecommuters would typically have a VPN client on their PC, and would be dialing into, like, a VPN pool in their business environment VPN router at home. Because household VPN routers are now available, you may dial into your home and utilize the internet to connect to your home network via a secure channel. Then you have access, not only to any machines you have at home, but to the Internet, just as you would at home, out from that router (Ezra et al, 2022).

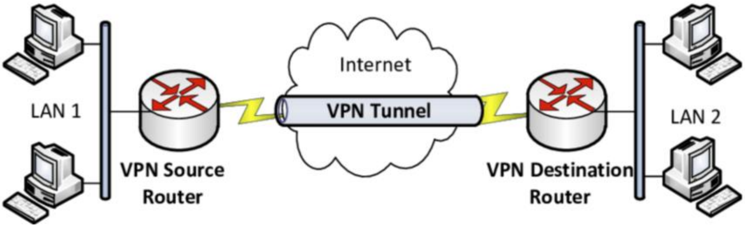


Figure 1 : VPN Tunneling structure (Salman, 2017)

IPSEC is the structure of open standard for a set of internet protocol (IP) in charge of protecting communication. It basically depends on existing algorithms to put into practice the encryption, authentication and main exchange (Singh, Chaba & Rani, 2007). Cisco was the main author in raising an idea of putting into practice IPSEC as a standard (or set of standards and technology) for remote access VPNs (Narayan et al 2016).

According to Huang, Smith and Sun (2015) indicated AH is also known as IP protocol 51 and is put into practice when privacy is not asked or accepted. It gives authentication for as many of the IP header as possible, as well as for high level protocol data. However, some IP header field can deviate in the transit and the value of these field cannot be expected by the sender. Those values of the fields might by AH. Thus, the defense brought by AH is not partial in many situations.

Unlike AH, ESP not only ensures integrity of the data but also protects against malicious users from examining the contents by encrypting the IP datagrams with a key to cipher it in a way only peers can decipher ("MBA Knowledge base," 2018b).

Internet security association and main management protocol (ISAKMP), protocol refers the process for authenticating a communicating group, starting and control of security association (SAs), main production techniques, and threats mitigation. It demonstrates the process and packets format to start, deal. Change and erase security association. It also explains payloads for exchanging main generation and authentication data. These formats give a consistent framework for changing main and authentication mechanism. ISAKMP typically uses internet main exchange for exchanging.

Focusing on the nowadays, situation at worldwide, regional and in our country context aboutVirtual Private Network as a way of enhancing Cyber Security in the Rwandan University sector; as It has clarified and debated by many researchers depending on statistics and statement. There is a gap on how it can affect learning outcome in higher institutions of learning. Because inadequate writing and researchers on this learning outcomes is facing many challenges which should be mitigated.In University of Kigali particularly, referring to the discussions the researcher had with the lab attendants, IT managers, Network administrators and other expert in virtual network. There is a gap on how prevent data attacks in institutions. According to these, since 2015-2020 Cyber Security in the Rwandan University sector can plays impact. After analyzing the literature review of other writers, scholars, authors and researchers from various part of the world, regional and at local level there is limited researches about Virtual Private Network and Cyber Security in the Rwandan University sector. Basing on above highlighted indicators few research were conducted about that. This is discovered as gap since information on the relevance on this. That is the reason why researcher was interested in investigating further this in higher institutions of learning.

Methodology

Descriptive research design was used to study significance effect of Model based on Virtual Private Network as a way of enhancing Cyber Security in the Rwandan University sector.

This research targeted 9 Lab attendants, 1 network administrator, 1 IT manager (Kigali campus), 5 HoDs, 3 from HR Department and 10 from Finance, means total study population was 29 respondents in this research.

Data has been collected using questionnaire and documentary review.

After gathering data from the field, the answer from questionnaire has been coded, edited, tabulated then after those data was entered in computer for analysis. Data was summarized, arranged according to the research objectives and questions. The data was processed and analyzed in frequencies, percentages, averages and standards deviations. The data was edited to prove the reliability. The numerical codes assigned to questionnaire responses allowed for a quantitative exploration of connections between different factors. Additionally, the study investigated the correlation between simulated network configurations and identified security vulnerabilities, providing valuable insights into the effectiveness of the implemented Virtual Private Network (VPN) model at the University of Kigali.

Results and Discussions

Table 1 : Techniques and technology used for Cyber Security at University of Kigali

Question	Frequency	Percentage
Have you experienced a cyber-attack or data leakage?		
a) Yes	10	34.48%
b) No	19	65.52%
What are the techniques used for Cyber Security at University of Kigali?		
a) Virtual Private Network	0	0.00%
b) Antivirus	25	86.21%
c) Access Control List	12	41.38%
d) Intrusion detection system	15	51.72%
e) Intrusion prevention system	11	37.93%
f) Firewall	23	79.31%
Do you have Virtual Private Network configured in your network environment?		
a) Yes	0	0.00%
b) No	29	100.00%

Source: Primary data, 2023

The findings reveal that 34.48% of respondents have experienced a cyber-attack or data leakage, while the majority (65.52%) have not encountered such incidents. This indicates that a significant portion of the respondents have had first-hand experience with cybersecurity threats.

The survey indicates that a substantial proportion of respondents are utilizing various cybersecurity techniques at the University of Kigali. Antivirus software is the most widely used technique (86.21%), followed by firewalls (79.31%). None of the respondents highlighted the use of virtual private networks as a security measure adopted at UoK. The relatively lower adoption rates of intrusion prevention systems (37.93%) and access control lists (41.38%) suggest potential areas for improvement in these specific security measures.

Interestingly, none of the respondents indicated having a Virtual Private Network (VPN) configured on their routers. This could potentially reflect a gap in awareness or understanding of VPN technology among the respondents, highlighting an area that may require further attention and education.

Interpretation and discussion

The analysis of the responses regarding the techniques and technology used for cyber security at the University of Kigali provides valuable insights into the current state of the university's cybersecurity practices.

Usage of Various Techniques: The findings indicate that the University of Kigali employs a diverse range of techniques to safeguard its digital infrastructure. Notably, antivirus software (86.21%) and firewalls (79.31%) are the most widely adopted measures. This suggests that traditional security tools are prevalent and form the foundation of the university's defense against cyber threats.

Opportunities for Improvement: While techniques such as antivirus and firewalls are widely embraced, the adoption rates for other measures such as intrusion prevention systems (37.93%) and access control lists (41.38%) are comparatively lower. This highlights potential areas for improvement and indicates that there might be untapped potential in enhancing these specific cybersecurity aspects.

Potential Impact of VPN: The presence of virtual private networks (VPNs) within the university's cybersecurity strategy (58.62%) suggests an understanding of the need to secure communication and data transmission. However, it's worth noting that none of the respondents had VPNs configured on their routers. This signals an opportunity for education and implementation, as VPNs can significantly contribute to data encryption and secure remote access.

Description of the proposed system

The increasing reliance on digital infrastructure in educational institutions, coupled with the growing threat landscape of cyberattacks, has underscored the need for robust cybersecurity measures. Recognizing these challenges, our research aims to develop a holistic VPN-based model that addresses the specific needs of the University of Kigali's network infrastructure. By implementing secure site-to-site communication and controlled remote access, we intend to fortify the university's network against potential breaches, while ensuring authorized personnel can access resources efficiently.

System Requirements Analysis: In this section, the researcher conducted a thorough analysis of the requirements for the proposed VPN-based cybersecurity model within the University of Kigali context. The successful implementation of secure site-to-site communication and controlled remote access hinges on a comprehensive understanding of the technical, functional, and non-functional requirements.

Technical Requirements: The technical requirements outline the specifications and technical aspects necessary to ensure the successful deployment and functioning of the VPN framework.

Network Infrastructure: The existing network infrastructure of the University of Kigali must be assessed to determine its compatibility with the VPN solutions. This includes evaluating the networking equipment/ devices, bandwidth availability, and network topology.

VPN Protocols: Selection of appropriate VPN protocols, such as WebVPN, IPsec, or SSL/TLS, must be based on factors like security, compatibility, and performance.

Encryption and Authentication: The encryption algorithms and authentication mechanisms employed must adhere to industry standards for ensuring data confidentiality and user access control.

Functional Requirements: The functional requirements define the specific functionalities that the VPN solutions must offer to meet the objectives of the research.

Site-to-Site Communication: The site-to-site VPN should enable seamless and secure communication between different campuses of the University of Kigali. It must ensure data integrity, encryption, and minimal latency.

Remote Access: The remote access VPN should provide authorized personnel with the ability to connect to the university's network from remote locations. This requires user authentication, role-based access control, and secure connectivity.

Non-Functional Requirements: The non-functional requirements encompass the qualities and characteristics that define the performance and usability of the VPN solutions.

Security: The VPN solutions must offer a high level of security, safeguarding data against unauthorized access, eavesdropping, and other cyber threats.

Scalability: The architecture should be designed to accommodate potential growth in the number of users, devices, and campuses over time.

Performance: The VPN framework should minimize latency and provide satisfactory network performance, even during peak usage periods.

Usability: The solutions should be user-friendly, allowing authorized users to establish connections with ease and efficiency.

Compatibility: The VPN solutions should be compatible with a variety of devices, operating systems, and networking technologies.

This analysis of the technical, functional, and non-functional requirements forms the foundation for the subsequent phases of system design and implementation. A clear understanding of these requirements ensures that the developed VPN solutions align closely with the intended goals of enhancing cybersecurity and network accessibility within the University of Kigali's context.

System Design

In this section, the researcher presents the detailed designs of the site-to-site and remote access VPN solutions. Visual aids, including diagrams and flowcharts, are incorporated to enhance the understanding of the architectural concepts and processes involved.

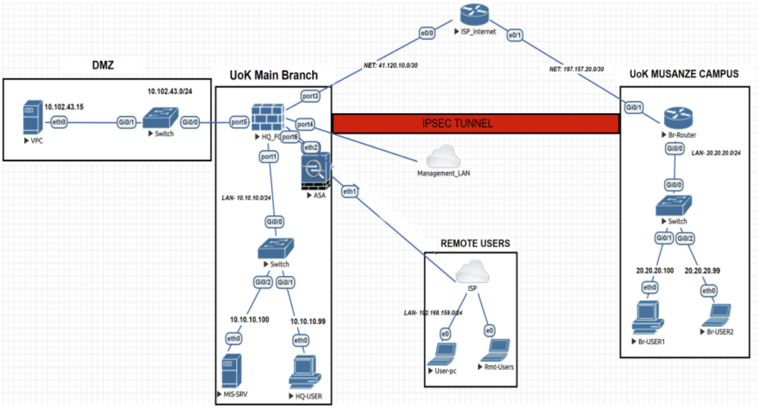
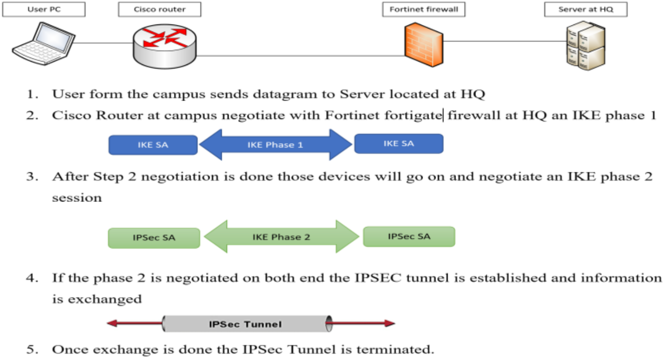


Figure 2: VPN-Based model Network Architecture Diagram

Site-to-Site VPN Design: The site-to-site VPN design focuses on establishing secure communication tunnel between University of Kigali campuses, ensuring confidentiality and data integrity throughout the exchange. The following components are integral to this design:



1. User form the campus sends datagram to Server located at HQ
2. Cisco Router at campus negotiate with Fortinet fortigate firewall at HQ an IKE phase 1
3. After Step 2 negotiation is done those devices will go on and negotiate an IKE phase 2 session
4. If the phase 2 is negotiated on both end the IPSEC tunnel is established and information is exchanged
5. Once exchange is done the IPSec Tunnel is terminated.

Figure 3: UoK's Site to Site VPN architecture (Source: Own drawing)

Remote Access VPN Design: The remote access VPN design focuses on providing authorized personnel with secure remote connectivity to peripheral network devices. Key design elements are as follows:

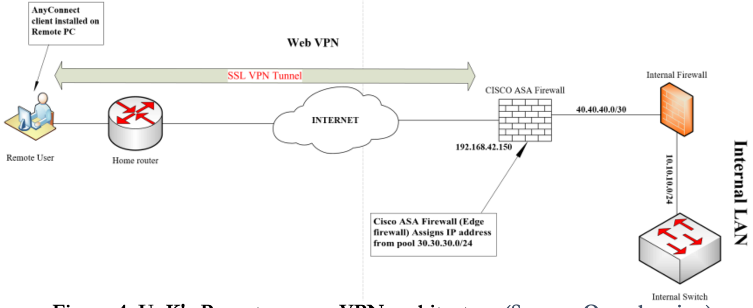


Figure 4: UoK's Remote access VPN architecture (Source: Own drawing)

System Implementation

In this section, the researcher delves into the practical implementation of the designed VPN solutions: the site-to-site VPN for secure inter-campus communication and the remote access VPN for authorized personnel. The researcher provides step-by-step details of the implementation process, tools used, and challenges encountered.

1 Site-to-Site VPN Implementation: The implementation of the site-to-site VPN involves several technical steps to ensure secure communication between University of Kigali campuses. The process can be broken down as follows:

Step 1: Hardware and Software Setup: For the hardware and software setup of the site-to-site VPN, we utilized VMWare workstation pro and EVE-NG to allow us to install network devices and other peripheries. Fortinet fortigate firewall used as VPN gateways for each campus. was chosen for its compatibility with IPsec protocol and robust security features. The following steps were taken: Provisioned fortigate firewall at Main campus and cisco router at Musanze campus, each with sufficient resources, on-campus networks, and Internet connectivity; Configured network interfaces and firewall rules to allow incoming and outgoing VPN traffic.

Step 2: VPN Configuration and Authentication Setup: The configuration of the site-to-site VPN involved setting up the IPsec tunnel between the two campuses. The configuration files for CISCO AnyConnect were edited to define the tunnel parameters: Created IPsec configuration files on both VPN gateways, specifying encryption algorithms, authentication methods, and phase 1 and phase 2 settings.

Step 3: Testing and Verification: Testing was essential to ensure the site-to-site VPN was functional and secure: Initiated the VPN connection from both campuses and monitored the logs for successful establishment.

Sent test traffic between campuses and verified its encryption using Wireshark tool; Addressed any connectivity issues or misconfigurations to ensure seamless communication.

Remote Access VPN Implementation

Implementing the remote access VPN solution requires careful configuration to allow authorized personnel secure access to network devices. The implementation process can be outlined as follows:

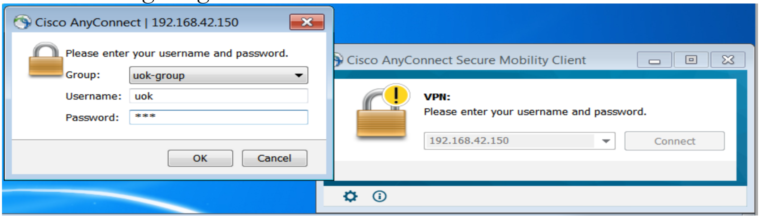
Step 1: VPN Setup: Setting up the remote access VPN server required configuring a WebVPN on edge firewall: Installed Cisco ASA firewall at the edge of main campus as the gateway for remote VPN users; Configured WebVPN on ASA Firewall and allow Anyconnect to enable remote users to connect to the VPN using their AnyConnect; Configure an IPSec tunnel and a pool of IPs that will be assigned to the remote users once they are connect to our network

Step 2: User Authentication Configuration: Configuring user authentication involved creating user accounts and configuring Firewall to authenticate them: Created user accounts for authorized personnel in the CISCO ASA firewall as authentication database; Configured Web VPN to use username and password authentication for remote access.

Step 3: Access Control Policies: Defining access control policies ensured that users had appropriate access to network resources: Defined access control policies based on user roles, allowing different levels of access to network segments and devices; Configured Anyconnect to push routes and DNS settings to connected clients based on their access rights.

Step 4: Client Configuration: Configuring the VPN client software for authorized users was critical for successful remote access: Provided authorized users with AnyConnect client software and configuration files and their credentials; Instructed users on how to initiate the VPN connection.

Step 5: Testing and Validation: Thorough testing was conducted to ensure the remote access VPN solution met the desired security and accessibility goals: Authenticated users tested the remote access connection from various external networks; Verified that they are Connected to remote VPN and being assigned with new IP address.



Cisco AnyConnect | 192.168.42.150

Please enter your username and password.

Group: uok-group

Username: uok

Password: ***

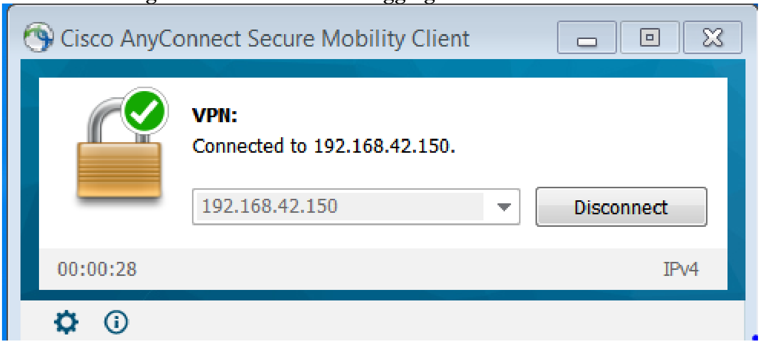
Cisco AnyConnect Secure Mobility Client

VPN:

Please enter your username and password.

192.168.42.150

Figure 5: Authorized User logging in with his credentials



Cisco AnyConnect Secure Mobility Client

VPN:

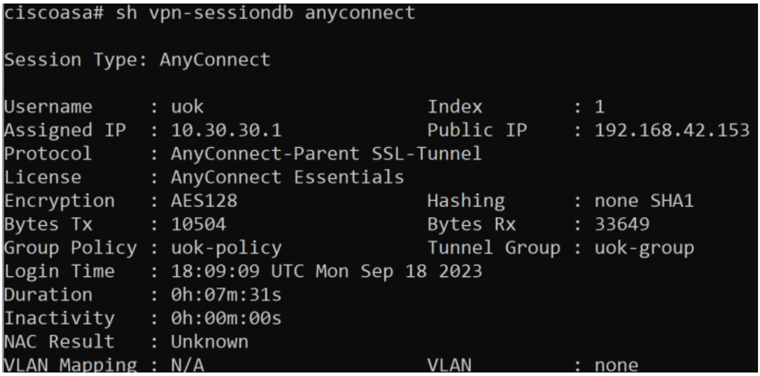
Connected to 192.168.42.150.

192.168.42.150

00:00:28

IPv4

Figure 6: User connected to University's VPN



```
ciscoasa# sh vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : uok                    Index        : 1
Assigned IP  : 10.30.30.1             Public IP    : 192.168.42.153
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Essentials
Encryption   : AES128                 Hashing      : none SHA1
Bytes Tx     : 10504                  Bytes Rx     : 33649
Group Policy : uok-policy             Tunnel Group : uok-group
Login Time   : 18:09:09 UTC Mon Sep 18 2023
Duration     : 0h:07m:31s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Figure 7:New IP address is assigned to the connected user

Testing: With both the site-to-site and remote access VPN solutions successfully implemented, the next crucial step involved their seamless integration into the existing network architecture of the University of Kigali. This integration ensured that the VPN solutions functioned harmoniously with the pre-existing infrastructure, promoting efficient data flow and maintaining network security.

The integration process encompassed the following key aspects: Network Segmentation: We designed the network architecture to create distinct segments for campus-to-campus communication, remote access connections, and the DMZ. This ensured that traffic destined for specific purposes was efficiently routed.

Access Control Policies: Access control policies were extended to encompass the newly implemented VPN solutions. These policies defined which users had access to different network segments and resources, ensuring that security measures remained consistent across the entire network.

Traffic Routing: Routing tables were updated to include routes to the remote campuses through the site-to-site VPN tunnel. This allowed seamless and encrypted communication between different campus networks.

Network Configuration: Adjusted the routing tables and firewall settings to accommodate the VPN tunnels while maintaining the overall network security posture.

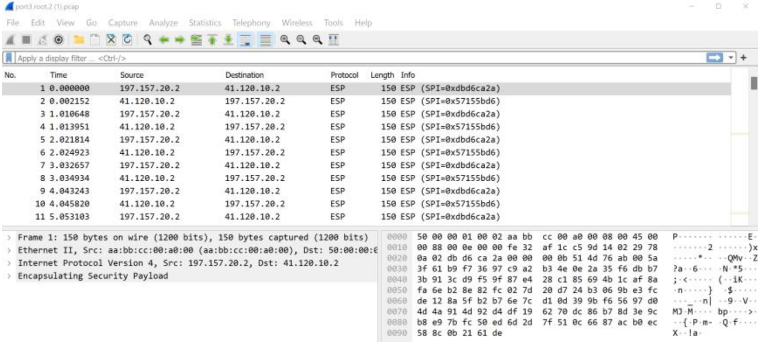
DMZ Setup: Resources that are needed by the users from outside was placed in DMZ apart from internal LAN as an extra layer of security for mitigating potential security risks.

Segmentation and Zones: Segregated network segments based on security zones, with clear demarcation between internal campus networks and the external-facing DMZ. This aided in enforcing access control policies.

Comprehensive Testing: Comprehensive testing was a crucial phase to ascertain the effectiveness, security, and reliability of the integrated VPN solutions. Rigorous testing scenarios were designed and executed to evaluate various aspects of the VPN framework:

Security Testing: Rigorous penetration testing was conducted to identify vulnerabilities and potential attack vectors. The results were analyzed, and necessary security enhancements were implemented to fortify the network against potential threats.

Results of packet captured by Wireshark showed that information being sent and the protocol that is being used is ESP (Encapsulation security Payload) which means that in case of Man in the middle attack, the attacker can have a clue of what is being done.

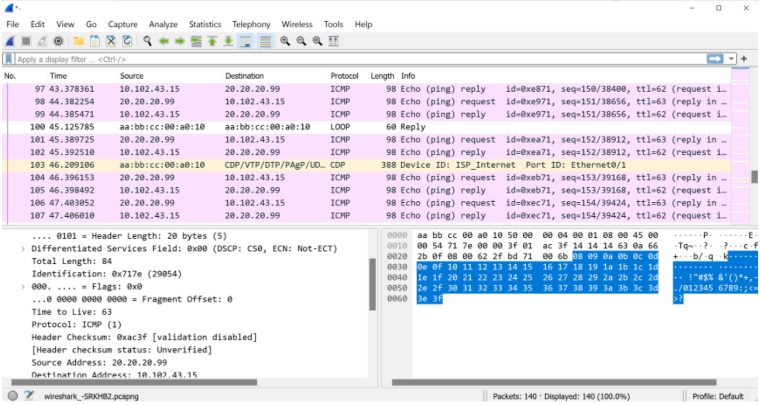

port3.root.2 (1).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time      Source        Destination   Protocol Length Info
   1 0.000000  197.157.20.2  41.120.10.2   ESP      150 ESP (SPI=0xdbd6ca2a)
   2 0.002152  41.120.10.2   197.157.20.2  ESP      150 ESP (SPI=0x57155bd6)
   3 1.010648  197.157.20.2  41.120.10.2   ESP      150 ESP (SPI=0xdbd6ca2a)
   4 1.013951  41.120.10.2   197.157.20.2  ESP      150 ESP (SPI=0x57155bd6)
   5 2.021814  197.157.20.2  41.120.10.2   ESP      150 ESP (SPI=0xdbd6ca2a)
   6 2.024923  41.120.10.2   197.157.20.2  ESP      150 ESP (SPI=0x57155bd6)
   7 3.032657  197.157.20.2  41.120.10.2   ESP      150 ESP (SPI=0xdbd6ca2a)
   8 3.034934  41.120.10.2   197.157.20.2  ESP      150 ESP (SPI=0x57155bd6)
   9 4.043243  197.157.20.2  41.120.10.2   ESP      150 ESP (SPI=0xdbd6ca2a)
  10 4.045820  41.120.10.2   197.157.20.2  ESP      150 ESP (SPI=0x57155bd6)
  11 5.053103  197.157.20.2  41.120.10.2   ESP      150 ESP (SPI=0xdbd6ca2a)
```

```
> Frame 1: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits)
> Ethernet II, Src: aa:bb:cc:00:a0:00 (aa:bb:cc:00:a0:00), Dst: 50:00:00:6
> Internet Protocol Version 4, Src: 197.157.20.2, Dst: 41.120.10.2
> Encapsulating Security Payload
```

```
0000  50 00 00 01 00 02 aa bb  cc 00 a0 00 08 00 45 00   P······· ······E·
0010  00 88 00 0e 00 00 fe 32  af 1c c5 9d 14 02 29 78   ·······2 ······)x
0020  0a 02 db d6 ca 2a 00 00  00 0b 51 4d 76 ab 00 5a   ·····*·· ··QMv··Z
0030  3f 61 b9 f7 36 97 c9 a2  b3 4e 0e 2a 35 f6 db b7   ?a··6··· ·N·*5···
0040  3b 91 3c d9 f5 9f 87 e4  28 c1 85 69 4b 1c af 8a   ;·<····· (··iK···
0050  fa 6e b2 8e 82 fc 02 7d  20 d7 24 b3 06 9b e3 fc   ·n·····}  ·$·····
0060  de 12 8a 5f b2 b7 6e 7c  d1 0d 39 9b f6 56 97 d0   ···_··n| ··9··V··
0070  4d 4a 91 4d 92 d4 df 19  62 70 dc 86 b7 8d 3e 9c   MJ·M···· bp····>·
0080  b8 e9 7b fc 50 ed 6d 2d  7f 51 0c 66 87 ac b0 ec   ··{·P·m- ·Q·f····
0090  58 8c 0b 21 61 de                                  X··!a·
```

Figure 8: Ping sent to Devices that are internal at HQ


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source             Destination          Protocol Length Info
  97 43.378361  10.102.43.15       20.20.20.99          ICMP     98 Echo (ping) reply    id=0xe871, seq=150/38400, ttl=62 (request i…
  98 44.382254  20.20.20.99        10.102.43.15         ICMP     98 Echo (ping) request  id=0xe971, seq=151/38656, ttl=63 (reply in …
  99 44.385471  10.102.43.15       20.20.20.99          ICMP     98 Echo (ping) reply    id=0xe971, seq=151/38656, ttl=62 (request i…
 100 45.125785  aa:bb:cc:00:a0:10  aa:bb:cc:00:a0:10    LOOP     60 Reply
 101 45.389725  20.20.20.99        10.102.43.15         ICMP     98 Echo (ping) request  id=0xea71, seq=152/38912, ttl=63 (reply in …
 102 45.392510  10.102.43.15       20.20.20.99          ICMP     98 Echo (ping) reply    id=0xea71, seq=152/38912, ttl=62 (request i…
 103 46.209106  aa:bb:cc:00:a0:10  CDP/VTP/DTP/PAgP/UD… CDP     388 Device ID: ISP_Internet  Port ID: Ethernet0/1
 104 46.396153  20.20.20.99        10.102.43.15         ICMP     98 Echo (ping) request  id=0xeb71, seq=153/39168, ttl=63 (reply in …
 105 46.398492  10.102.43.15       20.20.20.99          ICMP     98 Echo (ping) reply    id=0xeb71, seq=153/39168, ttl=62 (request i…
 106 47.403052  20.20.20.99        10.102.43.15         ICMP     98 Echo (ping) request  id=0xec71, seq=154/39424, ttl=63 (reply in …
 107 47.406010  10.102.43.15       20.20.20.99          ICMP     98 Echo (ping) reply    id=0xec71, seq=154/39424, ttl=62 (request i…
```

```
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x717e (29054)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 63
    Protocol: ICMP (1)
    Header Checksum: 0xac3f [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 20.20.20.99
    Destination Address: 10.102.43.15
```

```
0000  aa bb cc 00 a0 10 50 00  00 04 00 01 08 00 45 00   ······P· ······E·
0010  00 54 71 7e 00 00 3f 01  ac 3f 14 14 14 63 0a 66   ·Tq~··?· ·?···c·f
0020  2b 0f 08 00 62 2f bd 71  00 6b 08 09 0a 0b 0c 0d   +···b/·q ·k······
0030  0e 0f 10 11 12 13 14 15  16 17 18 19 1a 1b 1c 1d   ········ ········
0040  1e 1f 20 21 22 23 24 25  26 27 28 29 2a 2b 2c 2d   ·· !"#$% &'()*+,-
0050  2e 2f 30 31 32 33 34 35  36 37 38 39 3a 3b 3c 3d   ./012345 6789:;<=
0060  3e 3f                                              >?
```

```
wireshark_-SRKHB2.pcapng    Packets: 140 · Displayed: 140 (100.0%)    Profile: Default
```

Figure 9: Ping sent to Devices that are in DMz which is less secured

Performance Benchmarking: Network performance metrics, such as latency, throughput, and packet loss, were measured under varying loads and usage patterns. The VPN solutions were evaluated against predefined performance benchmarks to ensure that they met the desired standards.

User Acceptance Testing: A subset of authorized users participated in user acceptance testing to validate the ease of use and functionality of the remote access VPN. Feedback was gathered to fine-tune the user experience.

Failover and Redundancy Testing: Failover scenarios were simulated to evaluate the resiliency of the VPN solutions. This included testing the automatic re-establishment of VPN tunnels in case of connectivity disruptions.

Compatibility Testing: Compatibility with various devices and operating systems was tested to ensure that users could connect using different devices.

System Analysis and Evaluation

In this section, the researcher analyzes and evaluates the implemented VPN solutions in terms of their effectiveness, impact on cybersecurity, and alignment with the research objectives. The findings from this analysis shed light on the relevance and significance of the VPN framework in bolstering cybersecurity within the University of Kigali.

Security Analysis

Site-to-Site VPN Security: The site-to-site VPN implementation showcased a high level of security through the use of strong encryption and authentication mechanisms. The SHA certificate and PSK ensured mutual authentication between campuses, preventing unauthorized access to the VPN tunnels. Comprehensive security testing confirmed the resistance of the solution to common cyber threats, making it an effective shield against data breaches.

Remote Access VPN Security: The remote access VPN demonstrated a robust security posture by enforcing user authentication and role-based access control. User credentials were transmitted securely, and the VPN client maintained a high level of security while establishing connections from external networks. Vulnerability assessments and penetration tests confirmed the solution's resilience against potential attacks.

Accessibility and Usability Evaluation

Seamless Site-to-Site Communication: The site-to-site VPN facilitated seamless and encrypted communication between University of Kigali campuses. Users experienced minimal latency when accessing resources hosted on different campuses, enhancing collaboration and resource sharing.

Efficient Remote Access: Authorized personnel reported efficient and secure remote access to network devices within the university's perimeter. The user-friendly Anyconnect client interface streamlined the connection process, enabling users to establish connections with ease.

Performance Assessment

Site-to-Site VPN Performance: Performance benchmarks revealed that the site-to-site VPN maintained consistent throughput and low latency, even during peak usage hours. This indicated that the encrypted communication between campuses did not significantly impact network performance.

Remote Access VPN Performance: The remote access VPN exhibited excellent performance, providing rapid connectivity to authorized users. Load testing validated the solution's ability to handle multiple simultaneous connections without compromising performance.

Relevance and Significance

The VPN framework's relevance and significance were evaluated based on its alignment with the research objectives and its potential to enhance cybersecurity within the University of Kigali.

Addressing Research Objectives: The site-to-site VPN successfully established secured inter-campus communication, fostering collaboration and resource sharing. The remote access VPN granted authorized personnel controlled access to network devices, strengthening access control measures.

Contribution to Cybersecurity: The implemented VPN solutions significantly fortified the university's cybersecurity posture. Secure data transmission, user authentication, and access control collectively reduced the risk of unauthorized access and data breaches.

Alignment with University Needs: The VPN framework's alignment with the specific needs of the University of Kigali was evident through its seamless integration into the existing network infrastructure. The solutions catered to the university's objectives of enhancing network security and accessibility.

The analysis and evaluation of the implemented VPN solutions affirm their effectiveness in enhancing cybersecurity within the University of Kigali. The robust security measures, efficient communication channels, and successful integration validate the model's relevance and potential for broader implementation within the Rwandan university sector.

Conclusion

The journey undertaken in this research project has illuminated the paramount importance of cybersecurity within the Rwandan university sector, with a particular focus on the University of Kigali. As the digital landscape continues to evolve, educational institutions must remain vigilant in safeguarding their sensitive data and network resources against an increasingly sophisticated array of cyber threats. Through the lens of a VPN-based model, this study has ventured into the heart of this challenge, weaving together a tapestry of analysis, design, implementation, and evaluation.

The implementation of site-to-site and remote access VPN solutions has yielded tangible achievements. The establishment of secure communication channels between campuses has fostered collaboration, resource sharing, and efficient data exchange. Simultaneously, the controlled remote access framework has empowered authorized personnel with the ability to connect to critical network devices without compromising security. These accomplishments transcend the confines of technology; they lay the foundation for an environment where innovation and education can thrive, unencumbered by the specter of cyber threats.

This research has stood steadfastly aligned with its objectives. The development of a VPN framework has not only addressed the needs of the University of Kigali but has also laid the groundwork for a model that can be extrapolated to other Rwandan higher education institutions. Through meticulous analysis, it is evident that the VPN model has addressed security concerns, enhanced network accessibility, and exhibited a symbiotic relationship with the existing infrastructure.

Recommendations

In light of the comprehensive research undertaken in this study, certain recommendations emerge to guide future endeavors and enhance the cybersecurity landscape within the Rwandan university sector:

Continuous Monitoring and Security Updates: As technology and cyber threats evolve, it is imperative for the University of Kigali and other educational institutions to adopt a proactive stance in cybersecurity. Regular monitoring of network traffic, vulnerability assessments, and timely security updates should become integral to the operational processes. This practice will ensure that security measures remain current and effective in mitigating emerging threats.

Employee Training and Awareness: A strong cybersecurity posture is fortified not only by technological solutions but also by a well-informed human element. Investing in cybersecurity training and awareness programs for faculty, staff, and students is paramount. Educating users about best practices, recognizing phishing attempts, and fostering a culture of cybersecurity consciousness can significantly reduce the risk of social engineering attacks.

Adoption of Multi-Factor Authentication (MFA): To enhance user authentication mechanisms and reduce the risk of unauthorized access, the adoption of multi-factor authentication (MFA) is recommended. Implementing MFA for remote access and critical systems adds an extra layer of security by requiring users to provide multiple forms of verification before gaining access. This approach considerably strengthens access control and prevents unauthorized entry even if credentials are compromised.

Future Directions for Research and Practice: Moving forward, there are several future directions for research and practice in evidence-based teacher management: To further advance the field, future research could explore the integration of advanced intrusion detection systems with the VPN framework to enhance threat detection and incident response capabilities. Additionally, investigating the impact of VPN solutions on network performance under varying load conditions could yield valuable insights.

While the current research focused on the University of Kigali, there are opportunities for broader implementation and exploration. Future studies could delve into scaling the VPN framework to accommodate larger university networks and evaluating its performance in diverse academic environments.

References

Academy, C. N. (2014). CCNA Security Course Booklet Version 1.2-Course Booklets.

Carmouche, J. H. (2007). *IPsec virtual private network fundamentals*. Pearson Education India.

Chawla, B. K., Gupta, O. P., & Sawhney, B. K. (2014). A review on IPsec and SSL VPN. *International Journal of Scientific & Engineering Research*, *5*(11), 21-24.

Chetty, M., Haslem, D., Baird, A., Ofoha, U., Sumner, B., & Grinter, R. (2011, May). Why is my Internet slow? Making network speeds visible. In *Proceedings of the SIGCHI conference on human factors in computing systems* (pp. 1889-1898).

Cocks, K., Cohen, D., Wisløff, F., Sezer, O., Lee, S., Hippe, E., ... & EORTC Quality of Life Group. (2007). An international field study of the reliability and validity of a disease-specific questionnaire module (the QLQ-MY20) in assessing the quality of life of patients with multiple myeloma. *European Journal of Cancer*, *43*(11), 1670-1678.

Cui, J., Xiong, N., Park, J. H., Jia, K., & Wu, L. (2013). A novel and efficient source-path discovery and maintenance method for application layer multicast. *Computers & Electrical Engineering*, *39*(1), 67-75.

Froom, R., Sivasubramanian, B., &Frahim, E. (2010). *Implementing Cisco IP Switched Networks (SWITCH) Foundation Learning Guide: Foundation learning for SWITCH 642-813*. Cisco press.

Huang, C., Smith, P., & Sun, Z. (2015). Secure Network Solutions for Enterprise Cloud Services. In *Cloud Technology: Concepts, Methodologies, Tools, and Applications* (pp. 1464-1486). IGI Global.

Hunt, T. (2016). Cyber Security Awareness in Higher Education. Washington: Central Washington University.

Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., &Damasevicius, R. (2022). Secured communication using virtual private network (VPN). *Cyber Security and Digital Forensics*, 309-319.

Kayombo, K. M. (2017). Competitive positioning of a higher education institution in Zambia: the case of ZCAS.

McLaren, W., Gil, L., Hunt, S. E., Riat, H. S., Ritchie, G. R., Thormann, A., ... & Cunningham, F. (2016). The ensembl variant effect predictor. *Genome biology*, *17*(1), 1-14.

Métivier, R., Gallais, R., Tiffoche, C., Le Péron, C., Jurkowska, R., Carmouche, R., ... &Salbert, G. (2007, March). Dynamics of ERa-mediated transcriptional activation of responsive genes ex vivo. In *Annual meeting of the French society of Endocrinology*.

Mugenda, O. (2003). &Mugenda A. (2003). *Research methods: quantitative and qualitative approaches.*

Narayan, S., Ishrar, S., Kumar, A., Gupta, R., & Khan, Z. (2016, July). Performance analysis of 4to6 and 6to4 transition mechanisms over point to point and IPSec VPN protocols. In *2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)* (pp. 1-7). IEEE.

Abdullah, G., & Hassan, Z. A. H. (2020, November). Using of Genetic Algorithm to Evaluate Reliability Allocation and Optimization of Complex Network. In *IOP Conference Series: Materials Science and Engineering* (Vol. 928, No. 4, p. 042033). IOP Publishing.

Oso, J., & Onen, T. (2005). Employing research tactics: Reliability and validity in research and methodology.

Paul, E. (2020, June 1). */2020/06/01/nigerian-kenyan-universities-hacked/*. Retrieved from https://techpoint.africa: https://techpoint.africa/2020/06/01/nigerian-kenyan-universities-hacked/

Powell, J. M. (2010). The Impact of Virtual Private Network (VPN) on a Company's Network.

Ravikumar, D., Prasath, M., Kumar, N. U., Devi, V., & Vijayalakshmi, P. (2022, May). Internet security protocol for secure data transmission using OSPF and BGP. In *AIP Conference Proceedings* (Vol. 2463, No. 1, p. 020011). AIP Publishing LLC.

Rehman, M. H. (2013). Design and implementation of mobility for virtual private network users. *Global Journal of Computer Science and Technology. Research. Pretoria: Van Schaik Publishers.*

What Is a Remote Access VPN? (n.d.-b). Palo Alto Networks. Retrieved October 1, 2022, from https://www.paloaltonetworks.com/cyberpedia/what-is-a-remote-access-vpn

Roy, S., Nag, S., Maitra, I. K., & Bandyopadhyay, S. K. (2013). International journal of advanced research in computer science and software engineering. *International Journal*, *3*(6).

Scott, C., Wolfe, P., & Erwin, M. (1999). *Virtual private networks.* " O'Reilly Media, Inc.".

Sharma, G. (2021). Secure Remote Access IPSEC Virtual Private Network to University Network System. *Journal of Computer Science Research*, *3*(1).

Singh, K. K. V., & Gupta, H. (2016, March). A New Approach for the Security of VPN. In *Proceedings of the Second International conference on Information and Communication Technology for Competitive Strategies* (pp. 1-5).

Singh, Y., Chaba, Y., & Rani, P. (2007). Integrating–VPN and IDS–An approach to Networks Security. *International Journal of Computer Science and Security*, *1*(3), 1.

Stankard, A., Conlon, B., & O'Brien, H. (2021). 252 Expansion of the Orthogeriatric Service: Early Experiences. *Age and*

Ageing, *50*(Supplement_3), afab219-252. Relay technology. *International Research Journal of Computer Science (IRJCS)* .

Ulven, J. B., & Wangen, G. (2021). A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), 39.

Westbrook, A. (2021). A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets, and Defending National Security. *New York University Journal of Law and Business, Forthcoming.*

Jang-Jaccard, J., & Nepal, S. (2014). A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences, 80(5), 973-993. doi:10.1016/j.jcss.2014.02.003

Ade, P. A. R., Ahmed, Z., Amiri, M., Barkats, D., Thakur, R. B., Bischoff, C. A., ... & BICEP/Keck Collaboration. (2021). Improved constraints on primordial gravitational waves using Planck, WMAP, and BICEP/Keck observations through the 2018 observing season. *Physical review letters*, *127*(15), 151301.

Bertram, C., & Christiansen, I. (2014). Understanding research. *An introduction to reading*

Martin, M. (2022). Prototyping Model in Software Engineering: Methodology, Process, Approach. *Guru99*. Retrieved December 12, 2022, from https://www.guru99.com/software-engineering-prototyping-model.html#2.

Alabady, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. *International Arab Journal of e-Technology*, 26.

Alabady, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. *International Arab Journal of e-Technology*, 28.

Britannica, T. E. (2016, March 3). *Higher education. Encyclopedia Britannica. https://www.britannica.com/topic/higher-education.* Retrieved from https://www.britannica.com: https://www.britannica.com/topic/higher-education

Dan Craigen, Nadia Diakun-Thibault, and Randy Purse. (2014). Defining Cybersecurity. *Technology Innovation Management Review*, 2.

Villanueva, J. (2022, July 14). IPSec: A Comprehensive Guide. *TechGenix*. Retrieved September 30, 2022, from https://techgenix.com/what-is-ipsec-internet-protocol-security/

Salman, F. A. (2017, September 1). Implementation of IPsec-VPN Tunneling using GNS3. *Indonesian Journal of Electrical Engineering and Computer Science*, *7*(3), 855. https://doi.org/10.11591/ijeecs.v7.i3.pp855-860

Sharma*, D. Y. K., & Kaur, C. (2020, March 30). The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World. *International Journal of Recent Technology and Engineering (IJRTE)*, *8*(6), 2336–2339. https://doi.org/10.35940/ijrte.f8335.038620