Sapientia Foundation Journal of Education, Sciences and Gender Studies (SFJESGS), Vol.6 No.2 June, 2024; pg.167 – 182
ISSN: 2734-2522 (Print); ISSN: 2734-2514 (Online)

DESIGNING AND IMPLEMENTATION OF SITE-TO-SITE ETHERNET TUNNEL USING INTERNET PROTOCOL SECURITY

UMARU, MODIBBO
Department of Computer Science
Adamawa State Polytechnic Yola, Nigeria
modibbo1@adamawapoly.edu.ng / +2348035870375

MIJINYAWA, MOHAMMED
Department of Operations Research
Modibbo Adama University Yola, Nigeria
M.mijinyawa@mau.edu.ng| / +234031386699
&
UMARU UMARU
Department of Computer Science
Adamawa State Polytechnic Yola, Nigeria
ubabayiumar@gmail.com / +2347068794744

Abstract

Large organizations use Virtual Private Network (VPN) to reduce costs and improve network flexibility via the establishment of secure remote access to the company's network or public network such as the Internet. Organization uses IP/Multiprotocol Label Switching (MPLS) based VPN service as from the country's ISP. Although it is an innovative and excellent service, it costs a lot to the organisation. In response, an in-house IPSec-based VPN service is designed and proposed to the security management. According to the results of simulation of the broadband IPSec VPN connection that is not controlled by any third party is less expensive, more secure and had a high level of latency and jitter. A case study within experimental design approach has been used to study existing VPN solutions. A secured and less expensive IPSec VPN has been successfully set up and implemented to encrypt network traffic from the remote site to the organisation

.

Keywords: Multiprotocol Label Switching (MPLS), Virtual private Network (VPN), Ethernet over internet Protocol (EOIP), Internet Protocol security (IPSEC), Wide Area Network (WAN) and Mikrotik

1. Introduction

Today, organizations are doing their best to stay in control and help protect their corporate networks and data assets from digital threats. Be that as it may, they are very dependent on customers as the main line of defense who are not always consistent in managing security guidelines as ordered. In this way, the industry should ensure network security awareness and, if possible, information security proposals that can be leaked by cyber-attacks such as malware and network outages.

In addition to current approaches and organizational security components and management, IPsec VPN is recommended to industry leaders as the most central security best practice for security and safety frameworks. Ezra et al. (2021) conducted a review that focused on VPN design for IP protection. They are exploring the use of VPNs as a way to bypass services. censorship and access to geo-restricted services. Their work introduced IP protection a VPN

arrangement that used virtual connections to transmit packets securely over a public network. The aim of the research was to ensure secure access for companies and to overcome the access restrictions set by encrypted communication.

Thara (2021) explained the importance of VPNs in creating virtual networks over the Internet that connects intranets of various industries. The author emphasized the importance of VPNs in ensuring the secure transmission of sensitive business data, highlighting the confidentiality, authentication and integrity provided by VPNs. The study covered various VPN protocols such as IPSec, TLS and SSTP and highlighted overlay and peer models for VPN implementation. Some tunneling protocols like IPsec and VPN were also mentioned.

IPSec VPN secures and encrypts the virtual connection between two hubs, that is, using Internet Protocol Security (IPSec) policies from one site to another and Ethernet over Internet Protocol (EOIP) to operate the VPN can help protect against framework weaknesses such as IP- falsification., meeting capture, traffic sniffing. In this regard, the implementation of security measures to ensure confidentiality, respect and accessibility.

Damanik (2021) proposed a security data network configuration for enterprise growth that focuses on using private networks to optimize network services and applications. The study proposed solutions for businesses with limited bandwidth and rapid deployment requirements using VPN architecture and cellular network connections. VPN tunnel protocols such as EOIP and SSTP were investigated, and VLAN bridging was used for WAN virtualization systems. VPN basics require secure and fast remote connectivity to topographically dispersed areas and remote clients. A virtual private network (VPN) replicates broadband coverage between regions using data encryption.

Muc et al. (2020) emphasized the need for modern network technologies that enable secure remote access to corporate IT resources, given the increase in remote work. They highlighted the costs and security issues associated with cloud services and VPS. An encrypted VPN tunnel has emerged as a cost-effective and secure option that allows devices in remote locations to securely connect to a company's local network and access its resources as if they were physically connected. It provides access to manage the organization's assets, ensuring complete data security for internal and remote clients.

Network security contracts to secure data resources. Virtual privacy arrangements are progressing in importance, for example IP Security VPN is now regularly used Esper et al (2022, March)/ Unlike MPLS VPN currently used in the industry, Mikrotik OS, Mikrotik Router Device, Ethernet over Internet Protocol (EOIP) IPSec VPN is widely configured and used for secure data transfer. Use of IP layer data packet inspection and encryption A VPN based on multiprotocol label switching (MPLS) is very expensive and does not provide internal encryption capabilities, but mostly a covered private organization that is theoretical for external organizations. Tunneling is the basic foundation of a VPN system, which aims to create, process and provide point-to-point connections from source to destination, where its private network process is useful to capture all data packets and encapsulate them or wrap them in. other packages before sending them over the web Zhou et al (2020).

Internet Protocol Security (IPSec) contains a set of contracts designed to ensure the triple security, respect and availability of data exchange through a network of network contracts [1]. IP protection can be done in two modes, especially vehicle mode and pass-through mode. Pass-through mode is usually used when establishing a door-to-door VPN connection. In the Passage model, IPSec mixes the entire IP packet with a header and then creates another header that is added to the pre-encoded IP packet. Vehicle mode is like mileage mode; but the first IP header is not modified or a second IP header is created.

1.2 Statement of the Problems

An organization with branches that need to be connected to each other to share data used a VPN based on Multi-Convention Mark Exchange, which is very expensive Bitbit et al (2023). Similarly, the security of the organization is completely shared with the external provider of the country's network connections, which has become a concern. Similarly, VPN-based MPLS should actually be replaced by IPSec VPN and use an Ethernet over Internet Protocol (EOIP) tunnel to ensure secure data encryption and limit costs. Because of this challenge, internal IPSec VPN management was created for the core reasons of the organization and its availability to its regional bases. The purpose of this research was to design and implement a secure, reliable and economically reliable wide area network using IPSec virtual trust organization between the base regions and local areas of the organization..

1.3 Objectives of the Study

The objective of this research work is to design and implement a secured, reliable and affordable IPSec point-to-point VPN WAN.

1. Using smart draw tool to draw network design
2. Using winbox tool to access and to configure the Mikrotik operating system or
3. Using Mikrotik routerOS devices

1.4 Scope and justification

This project is intended to help medium-sized business organisation incorporate and carry out higher organization security between various areas subsequently further developing the general organization layer security and decreasing organization weaknesses. The objective of the VPN over Powerful IPsec Passages usefulness is to give an answer that upholds network across covering tends to in client website where a distant client webpage should be progressively distinguished utilizing internet while at the same time protecting web traffic between switches utilizing IPsec. Notwithstanding, because of time and monetary requirements, this exploration will be directed in a virtual climate utilizing the GNS3 test system and MikrotkOS variants transferred on multi-facet changes to copy the Site A and Site B2.

3. Methodology network design

3.1 Research Design

This study employed a developmental research design in which the researchers designed and crafted a network plan for organization. In the past, several studies utilized this research design and produced information technology-based solutions such as network plans, network design, and software applications (Dela Fuente et al., 2023; Reguyal et al., 2023; Amboya et al., 2022; Olipas et al., 2022; Olipas et al., 2021; Olipas, 2020).

This study applied a qualitative case study methodology with an Qualitative research allowed the gathering of information on how to use winbox tool, mikrotik operating system and that would be used for configuring of Mikrotik devices and Ethernet over internet protocol (EOIP and IPSec VPN based on the attributes such as availability, network security, management, These VPN protocol models include Point to Point Tunnel Protocol, Internet Security protocol VPN, Sec VPN, Ethernet over internet protocol (EOIP) and Layer 2 Tunneling Protocol.

In addition, the IPSec based VPN security uses cryptographic algorithms and suites, the IPSec, Ethernet over internet protocol (EOIP) WAN was set up and implemented in the Site A1 as well as the Site 2 The following section describes the network design of this VPN project.

3.2 Smart Draw Tool

Smart draw would be used to Design Network to show or develop diagram and provide users with ready use, smart drawwould be use to Design Network of all sizes manage diagramming processes through predefined templates and create infographics, network designs, mind maps, organizational charts, and documenting information about software-intensive systems and more.

3.3 Winbox Tool

Winbox tool would be used to monitor traffic across all traffic streams in real time and also to upload and download files to/from routers. As a graphical user interface, Winbox would allow you to configure and manage MikroTik RouterOS devices. The program can be run on windows, Linux and macOS using Wine.

3.4 Mikrotik RouterOS Devices

RouterOS would be used as operating system of RouterBOARD would be use and also be installed on a PC and would turn it into a router with all the necessary features - routing, firewall, bandwidth management, wireless access point, backhaul link, hotspot gateway, internet protocol security (IPSec), VPN server and more.

Smart Draw Tool

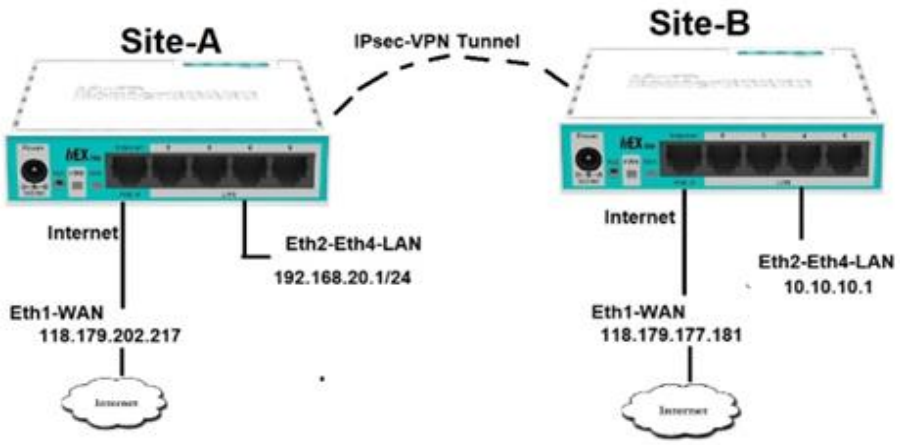
The tool is used to design the entire network how the network would look like showing each router would and how network connected to each other and their place. The user, used the application enough to realign and fix drawings as the user want the network design. The user creates a custom using a pre-built template, or by drawing it from scratch, and utilize tools.
The user diagram indicates each step taken in each site from office1router to Site B router in different location or area and show also the plan internet protocol address for both wide area network (WAN) local area network (LAN) internet protocol.

4. Network design, configuration and implementation

4.1 Network Design

At this stage, the researchers configured the different network equipment deployed by the two designs using MikrotikOS Router Devices (Operating System) using Winbox tool user interface in order to allow for configuration. The purpose of the Winbox used at each stage is provided for better understanding. The winbox have interface that researcher used to configure the router along with an explanation directly below.

To configure a site-to-site EoIP VPN Tunnel (with IPsec) between two MikroTik Routers, I am following a network diagram like below image.



Site to Site EOIP Tunnel with IPsec

In the Design network, Site A Router is connected to internet through ether1 interface having IP address 192.168.70.2/30. In your real network this IP address will be replaced with public IP address provided by your ISP. Office1 Router's ether2 interface is connected to local network having IP network 10.10.11.0/24. After EoIP tunnel configuration, an EoIP tunnel interface will be created in Office 1 Router whose IP address will be assigned 172.22.22.1/30.

Similarly, site A Router is connected to internet through ether1 interface having IP address 118.179.202.217. In your real network this IP address will also be replaced with public IP address. Site B Router's ether2 interface is connected to local network having IP network 192.168.20.1/24. After EoIP tunnel configuration an EoIP tunnel interface will also be created in Office 2 Router whose IP address will be assigned 172.22.22.2/30.

We will configure a site-to-site EoIP Tunnel between these two MikroTik Routers so that local network of these routers can communicate with each other through this VPN tunnel across public network.

4.1 Using Mikrotik routerOS devices
MikroTik RouterOSCore Devices and IP Information
To configure a site-to-site EoIP VPN between two Routers, I am using two **MikroTik RouterOSv6.38.1**. IP information that I am using for this network configuration are given below.

- Site A Router WAN IP: 118.179.202.217, LAN IP Block 192.168.20.1/24 and Tunnel interface IP 172.22.22.1/30
- Site B Router WAN IP: 179.177.181, LAN IP Block 10.10.10.1 and Tunnel interface IP 172.22.22.2/30

This IP information is just for researcher purpose. Change this information according to your network requirements.

4.2 Winbox tool

The researcher used winbox tool to Site-to-Site EoIP Tunnel Configuration with IPsec We will now start our site-to-site EoIP VPN configuration according to the above network diagram. Complete configuration can be divided into four parts.

- MikroTik RouterOS basic configuration
- EoIP tunnel configuration with IPsec
- Assigning IP address on tunnel interface
- Static route configuration

4.3 MikroTik RouterOS Basic Configuration

Basic RouterOS configuration includes assigning WAN IP, LAN IP, DNS IP and Route, NAT configuration. According to our network diagram, we will now complete these topics in our two MikroTik RouterOS (Site A Router and Site B Router).

4.1.1 Site A Router Basic Configuration

The following steps will guide you how to perform basic configuration in your Site A RouterOS.

- Login to Site A RouterOS using winbox and go to IP > Addresses. In Address List window, click on PLUS SIGN (+). In New Address window, put WAN IP address (118.179.202.217) in Address input field and choose WAN interface (ether1) from Interface dropdown menu and click on Apply and OK button. Click on PLUS SIGN again and put LAN IP (10.10.11.1/24) in Address input field and choose LAN interface (ether2) from Interface dropdown menu and click on Apply and OK button.
- Go to IP > DNS and put DNS servers IP (8.8.8.8 or 8.8.4.4) in Servers input field and click on Apply and OK button.
- Go to IP > Firewall and click on NAT tab and then click on PLUS SIGN (+). Under General tab, choose srcnat from Chain dropdown menu and click on Action tab and then choose *masquerade* from Action dropdown menu. Click on Apply and OK button.
- Go to IP > Routes and click on PLUS SIGN (+). In New Route window, click on Gateway input field and put WAN Gateway address (192.168.70.1) in Gateway input field and click on Apply and OK button.

Basic RouterOS configuration has been completed in Site A Router. Now we will do similar steps in Site B RouterOS.

4.1.2 Site B Router Basic Configuration

The following steps will guide you how to perform basic configuration in your Site B RouterOS.

- Login to Site B RouterOS using winbox and go to IP > Addresses. In Address List window, click on PLUS SIGN (+). In New Address window, put WAN IP address (118.179.202.217) in Address input field and choose WAN interface (ether1) from Interface dropdown menu and click on Apply and OK button. Click on PLUS SIGN again and put LAN IP (10.10.12.1/24) in Address input field and choose LAN interface (ether2) from Interface dropdown menu and click on Apply and OK button.
- Go to IP > DNS and put DNS servers IP (8.8.8.8 or 8.8.4.4) in Server's input field and click on Apply and OK button.

- Go to IP > Firewall and click on NAT tab and then click on PLUS SIGN (+). Under General tab, choose srcnat from Chain dropdown menu and click on Action tab and then choose *masquerade* from Action dropdown menu. Click on Apply and OK button.
- Go to IP > Routes and click on PLUS SIGN (+). In New Route window, click on Gateway input field and put WAN Gateway address (118.179.177.181) in Gateway input field and click on Apply and OK button.

Basic RouterOS configuration has been completed in Site B Router. Now we are going to start EoIP tunnel configuration.

4.1.2 EoIP Tunnel Configuration with IPsec

After MikroTik Router basic configuration, we will now configure EoIP tunnel with IPsec in both MikroTik RouterOS. In EoIP tunnel configuration, we will specify local and remote IP address as well as shared secret for IPsec and Tunnel ID.

4.1.3 EoIP Tunnel Configuration in Office 1 Router

The following steps will show how to configure EoIP tunnel in your Office 1 Router.

- Click on Interfaces menu item from Winbox and click on EoIP Tunnel tab and then click on PLUS SIGN (+). New Interface window will appear.
- Put a meaningful EoIP tunnel interface name (eoip-tunnel-r1) in Name input field.
- Put Site A Router's WAN IP address (192.168.70.2) in Local Address input field.
- Put Site B Router's WAN IP address (192.168.80.2) in Remote Address input field.
- Put a unique ID (for example: 10) in Tunnel ID input field. This ID must be same in both routers.
- Put IPsec shared secret in IPsec Secret input field if your router supports IPsec and you wish to enable IPsec authentication and encryption. You should remember that this IPsec Secret must be same in both routers.
- Also uncheck Allow Fast Path checkbox if it is checked and you want to enable IPsec.
- Click Apply and OK button.
- You will find a new EoIP tunnel interface followed by your given name (eoip-tunnel-r1) has been created in Interface List window.

EoIP tunnel configuration in Site A Router has been completed. Now we will do the similar steps in our Site B Router to create EoIP tunnel interface.

4.1.4 EoIP Tunnel Configuration in Site B Router

The following steps will show how to configure EoIP tunnel in your Site B Router.

- Click on Interfaces menu item from Winbox and click on EoIP Tunnel tab and then click on PLUS SIGN (+). New Interface window will appear.
- Put a meaningful EoIP tunnel interface name (eoip-tunnel-r2) in Name input field.
- Put Office 2 Router's WAN IP address (118.179.202.217) in Local Address input field.
- Put Office 1 Routers WAN IP address (118.179.177.181) in Remote Address input field.
- Put a unique ID (for example: 10) in Tunnel ID input field. This ID must be same in both routers.
- Put IPsec shared secret in IPsec Secret input field if your router supports IPsec and you wish to enable IPsec authentication and encryption. You should remember that this IPsec Secret must be same in both routers.

- Also uncheck Allow Fast Path checkbox if it is checked and you want to enable IPsec.
- Click Apply and OK button.
- You will find a new EoIP tunnel interface followed by your given name (eoip-tunnel-r2) has been created in Interface List window.

EoIP tunnel configuration in Site 2 Router has been completed. Now we will assign IP address in our newly created EoIP tunnel interface in our both RouterOS so that both router can communicate with each other through this VPN tunnel interface.

4.1.5 Assigning IP Address in EoIP Tunnel Interface

After EoIP tunnel configuration, a new EoIP tunnel interface has been created in both routers. So, if we assign same block IP in both interfaces, the both router will be able to communicate with each other through this EoIP tunnel. In this part, we will now assign IP address in our newly created tunnel interface.

4.1.6 Assigning IP Address on Site A Router's EoIP Tunnel Interface

The following steps will show how to assign IP address on Site A Router's tunnel interface.

- Go to IP > Address menu item and click on PLUS SIGN (+).
- Put a new private IP Block IP (172.22.22.1/30) in Address input field.
- Choose newly created tunnel interface (eoip-tunnel-r1) from Interface drop down menu.
- Click Apply and OK button.

Assigning IP address on Site A Router's tunnel interface has been completed. Similarly, we will now assign IP address on Site B Router's tunnel interface.

4.1.6 Assigning IP Address on Site B Router's EoIP Tunnel Interface

The following steps will show how to assign IP address in Site B Router's tunnel interface.

- Go to IP > Address menu item and click on PLUS SIGN (+).
- Put a new private IP Block IP (172.22.22.2/30) in Address input field.
- Choose newly created tunnel interface (eoip-tunnel-r2) from Interface drop down menu.
- Click Apply and OK button.

Assigning IP address on Site B Router's tunnel interface has been completed. In this stage both routers are now able to communicate with each other. But both routers' LAN cannot communicate with each other without configuring static routing. So, in the next part we will configure static routing in our both Site Router.

4.1.7 Static Route Configuration

We will now configure static route in our both Office Router so that each router's LAN can communicate with each other through EoIP tunnel.

4.1.8 Static Route Configuration in Site B Router

The following steps will show how to configure static route in Site A Router.

- Go to IP > Routes and click on PLUS SIGN (+). New Route window will appear.
- In New Route window, put destination IP Block (10.10.12.1/24) in Dst. Address input field.

- Put the Gateway address (172.22.22.2) in Gateway input field.
- Click Apply and OK button.

Static route configuration in Site A Router has been completed. Now we will configure static route in Site B Router.

4.1.9 Static Route Configuration in Site B Router
The following steps will show how to configure static route in Site B Router.

- Go to IP > Routes and click on PLUS SIGN (+). New Route window will appear.
- In New Route window, put destination IP Block (10.10.11.1/24) in Dst. Address input field.
- Put the Gateway address (172.22.22.1) in Gateway input field.
- Click Apply and OK button.

Static route configuration in Site B Router has been completed. Now both router as well as its LAN can communicate with each other through EoIP tunnel across public network.

To check your configuration, do a ping request from any router or any local network machine to other local network machine. If everything is OK, your ping request will be success.

4.1.10 EoIP VPN Tunnel Configuration with IPsec has been explained in this article. I hope you will be able to configure EoIP tunnel with IPsec between your two Site routers. However, if you face any confusion to configure EoIP tunnel in your MikroTik Router, feel free to discuss in comment or contact me from Contact page. I will try my best to stay with you.

Simulation results showed that the system can provide a secured, reliable and cost-effective transmission system over the Internet for organizations. As such, VPNs form an integral part of remote business communications across the internet due to the inherent risks that exist when sending private information over a public network.

5. Results
Simulation results showed that the system can provide a secured, reliable and cost-effective transmission system over the Internet for organizations. As such, VPNs form an integral part of remote business communications across the internet due to the inherent risks that exist when sending private information over a public network.

The goal of this researcher is to design an EoIP VPN tunnel with IPsec. So, in this researcher would show how to create an EoIP tunnel with IPsec to establish a secure site to site VPN tunnel between two MikroTik Routers.

VPN (**V**irtual **P**rivate **N**etwork) is a technology that provides a secure tunnel across a public network. A private network user can send and receive data to any remote private network using VPN Tunnel as if his/her network device was directly connected to that private network. At this stage, the researchers configured the different network equipment deployed by the two designs using MikrotikOS Router Devices (Operating System) using Winbox tool user interface in order to allow for configuration. The purpose of the Winbox used at each stage is

provided for better understanding. The winbox have interface that researcher used to configure the router along with an explanation directly below.

MikroTik provides EoIP (Ethernet over IP) tunnel that is used to create a site-to-site VPN. EoIP tunneling is a MikroTik RouterOS protocol that creates an Ethernet tunnel between two MikroTik Routers on top of an IP connection. EoIP adds an outer header mentioning the entry point of the tunnel (SourceIP) and the exit point of the tunnel (Destination IP) but the inner packet is kept unmodified
IPIP Encapsulation

EoIP tunnel only encapsulates IP packets but does not provide authentication and encryption. EoIP tunnel with IPsec ensures IP packet encapsulation as well as authentication and encryption. IPsec usage makes your packets secure but it works slowly because of having extra authentication and encryption process. So, my opinion is that if data security is your concern, use EoIP tunnel with IPsec but if data security is not so headache, use only MikroTik EoIP tunnel because it works so faster.

6. Recommendations

Designing and implementing a secure site-to-site Ethernet tunnel using Internet Protocol Security (IPsec) involves key steps. Begin with assessing requirements and network topology, then define security policies including encryption, integrity, and authentication methods. Choose a key management strategy like IKEv2 and select compatible VPN gateway hardware/software. Configure IPsec settings, address NAT traversal if needed, and implement Quality of Service for optimal performance. Thorough testing, monitoring, and logging ensure proper functionality. Redundancy, failover mechanisms, and disaster recovery planning guarantee continuous connectivity. Document the setup comprehensively, conduct security audits, and stay updated with patches. Compliance with regulations is essential. Engage experts for a successful implementation.

6. Conclusion

Virtual Private Networks (VPNs) are integral for secure remote business communications over the Internet, countering risks associated with transmitting private data on public networks. In the face of rising online identity theft and data breaches, VPNs offer effective protection, preserving the reputation of organizations. Not only do VPNs prevent unauthorized access to sensitive business information, they also contribute to environmental sustainability by reducing the need for extensive business travel. This is achieved by enabling secure access to company resources from home, curbing office trips, and facilitating remote attendance at meetings through secure video conferencing. Consequently, VPNs not only enhance security but also provide cost-effective alternatives to long-distance leased lines, DSL, and fiber optics networks. Their deployment is especially pertinent in the context of the Covid-19 pandemic, enabling remote participation in meetings and conferences. In the contemporary business landscape, an organization's efficacy and productivity hinge on its IT infrastructure, with VPNs offering an efficient means to reduce costs and establish secure data communication links between geographically dispersed offices, partners, and customers. This presents an opportunity for Cameroonian businesses to leverage connectivity, facilitated by local ISPs like MTN, Airtel, and Glo, to achieve ambitious business objectives, even

considering outsourced VPN services for streamlined router management and further cost reduction.

References

Aung, S. T., & Thein, T. (2020, February). Comparative analysis of site-to-site layer 2 virtual private networks. In *2020 IEEE Conference on Computer Applications (ICCA)* (pp. 1-5). IEEE.

Bitbit, E. D., Gampoy, M. A. B., Ricafort, T. S., Tinio, R. D., Pula, R. L., Leona, R. F., & Olipas, C. N. P. (2023). Crafting a Network Plan for a Microfinancing Establishment and Its Branch Network through Virtual Private Network (VPN) Implementation. *European Journal of Theoretical and Applied Sciences*, *1*(3), 441-448.

Damanik, H.A. (2021). Securing data network for growing business VPN architectures. *Acta Informatica Malaysia (AIM), Zibeline International Publishing, 6*(1), 01-06. https://doi.org/10.26480/aim.01.2022.01.06

Ezra, P. J., Misra, S., Agrawal, A., Oluranti, J., Maskeliunas, R., & Damaševicius, R. (2021). Secured Communication Using Virtual Private Network (VPN). In *Lecture notes on data engineering and communications technologies*. Springer International Publishing. https://doi.org/10.1007/978-981-16-39616_27

Esper, D. A., Datta, S., & Roy, M. (2022, March). Implementing Protection on Internal Networks using IPSec Protocol. In *2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS)* (Vol. 1, pp. 378-383). IEEE.

Febrianti, R., & Ryansyah, M. (2022). Implementation of virtual private network using point to point tunneling protocol mikrotik router at state fighter vocational school haurgeulis indramayu. *Jurnal Mantik*, *6*(3), 3350-3357.

Haris, A. I., Ferianda, R. A., & Basuki, A. I. (2022, November). QoS Analysis of Site-to-Site VPN and Its Integration Potential for Securing Communication on Electric Vehicles. In *Proceedings of the 2022 International Conference on Computer, Control, Informatics and Its Applications* (pp. 25-28).

Kaklauskas, L., & Pugačius, D. (2023). Secure remote client connection to higher education institution internal computer network through VPN. *Applied Scientific Research*, *2*(1), 74-81.

Ma, X., Qu, J., Chen, F., Liu, W., Li, J., Tao, J., ... & Zhang, Z. L. (2021). One Host with So Many IPs! On The Security Implications of Dynamic Virtual Private Servers. *IEEE Communications Magazine*, *59*(2), 64-69

Muc, A., Muchowski, T., Murawski, L., Szelenzinski A. (2020). Providing the ability of working remotely on local company server via VPN. *Multidisciplinary Aspects of Production Engineering*, *3*, 195-205. https://doi.org/10.2478/mape-2020-0017

Olipas, C.N.P. (2020). The developmental and assessment of an online student affairs system with short message service. *International Journal of Scientific and Technology Research*, 8(12), 1674-1681. https://www.doi.org/10.5281/zenodo.7817465

Olipas, C.N.P., Sawit, R.C.M., & Esperon, R.M. (2021). The design and assessment of a church records and information management system. *International Journal of Research and Innovation in Applied Science*, *6*(1), 48-52. https://doi.org/10.5281/zenodo.8024706

Olipas, C.N.P., Villoria, J.P., Mateo, S.M., Sta Maria, S.A.P., Bisnar, E.P., & Vallecera, M.L.M. (2022). MediCord: A web-based healthcare management system. *Journal Healthcare Tretment Development*, *2*(5), 35-35. https://doi.org/10.55529/jhtd25.35.45

Reguyal, J.M.T., Agno, A.M.S., Martinez, M.C., Castro, J.T., Cariazo, B.V.C., Olipas, C.N.P. & Alegado, R.T. (2023). Ob-Gyn Clinic OnlineScheduling System. *Formosa Journal of Computer and Information Science* , *2*(1), 25-36, https://doi.org/10.55927/fjcis.v2i1.4076

Siadi, I. W., Fitri, I., & Nuraini, R. (2020). Tunneling Design with Point to Point Protocol over Ethernet (PPPoE) using Mikrotik RB-941 (Case Study of SMK Taruna Bhakti): Tunneling Design with Point to Point Protocol over Ethernet (PPPoE) using Mikrotik RB-941 (Case Study of SMK Taruna Bhakti). *Jurnal Mantik*, *4*(1), 238-247.

Thiara, V.B.S. (2021). Enterprise Based VPN. *Education and Research Archive*. https://doi.org/10.7939/r3-ax5r-h012

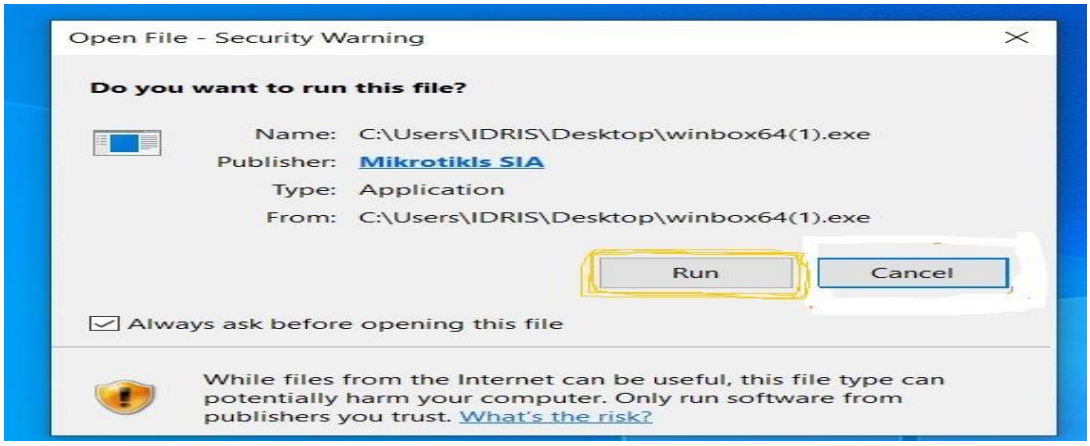
Thiede, A., & Samen, J. (2023). A Cross-Platform Always On VPN Solution for Ensuring Online Security.

Zhou, Y., & Zhang, K. (2020, June). DoS vulnerability verification of IPSec PN. In 2020 IEEE International Conference on Artificial Intelligence and omputer Applications (ICAICA) (pp. 698-702). IEEE

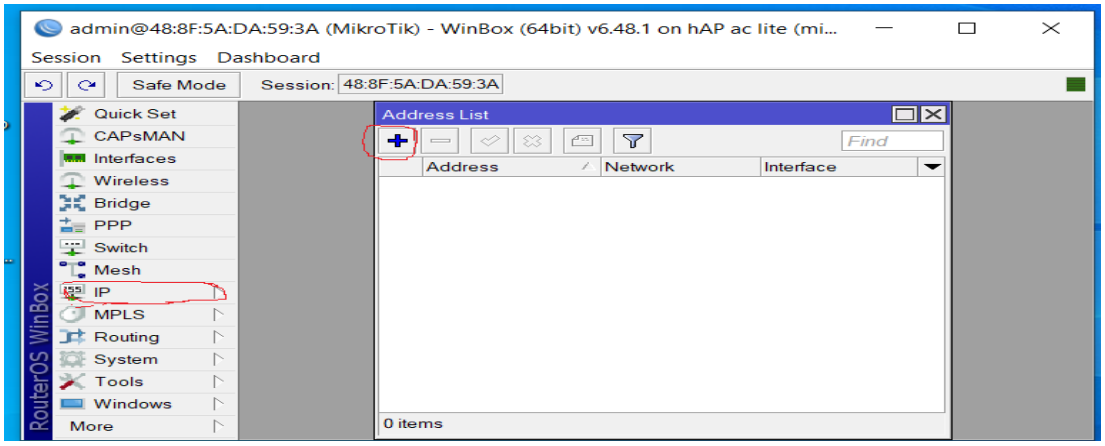
APPENDICES

Site A Router Basic Configuration

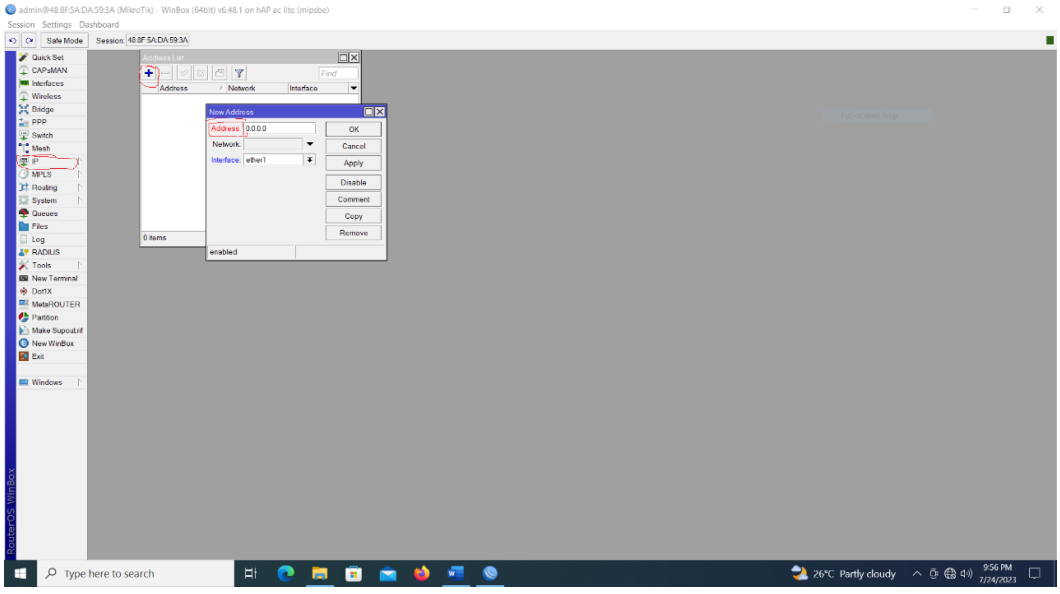
The following steps will guide you how to perform basic configuration in your Site A RouterOS.

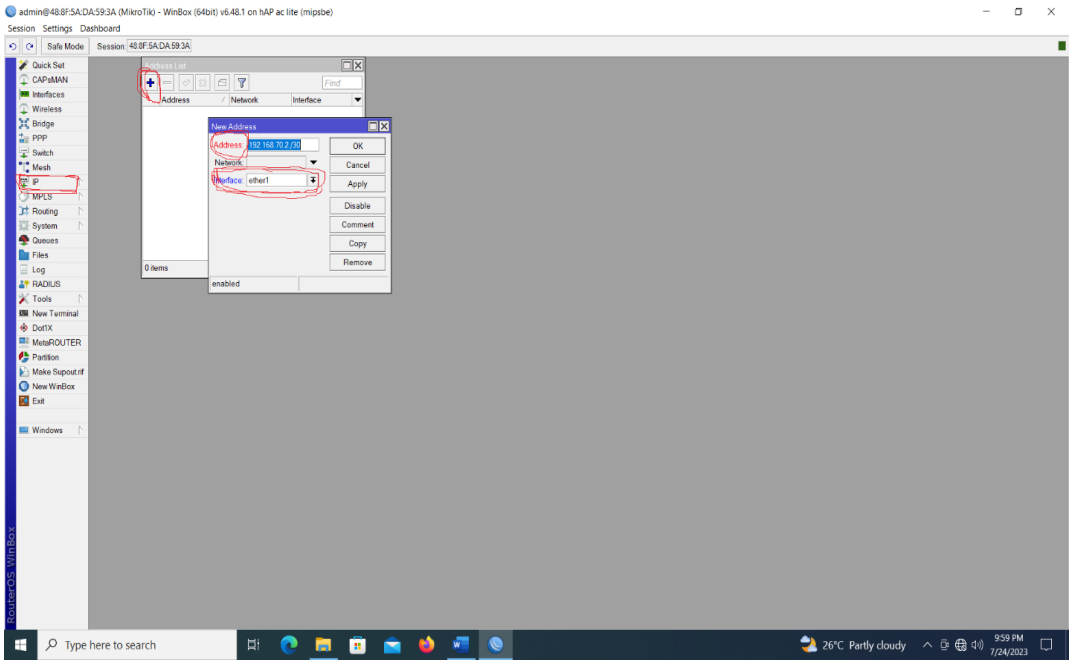


Open winbox click run

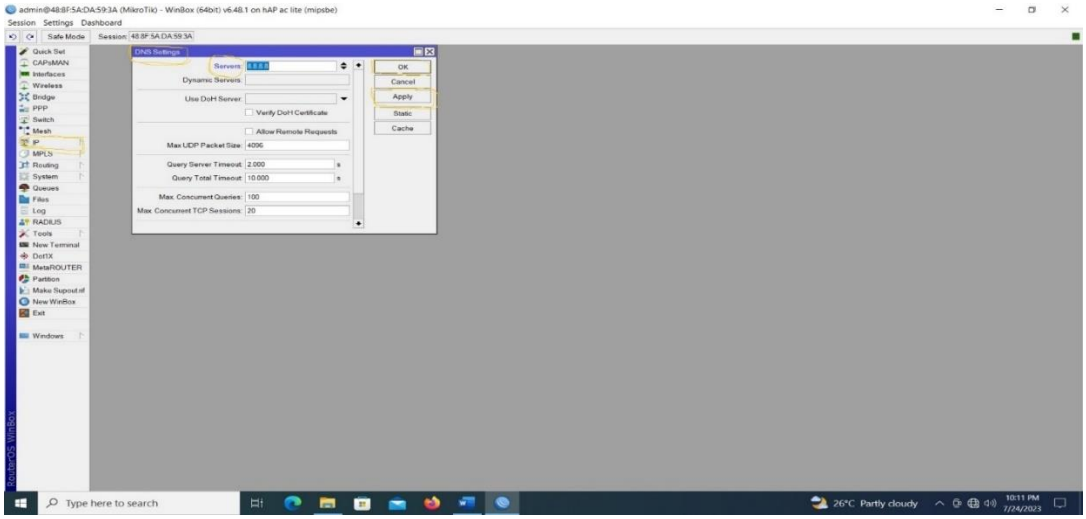


Login to Site A RouterOS using winbox and go to IP > Addresses. In Address List window, click on PLUS SIGN (+).

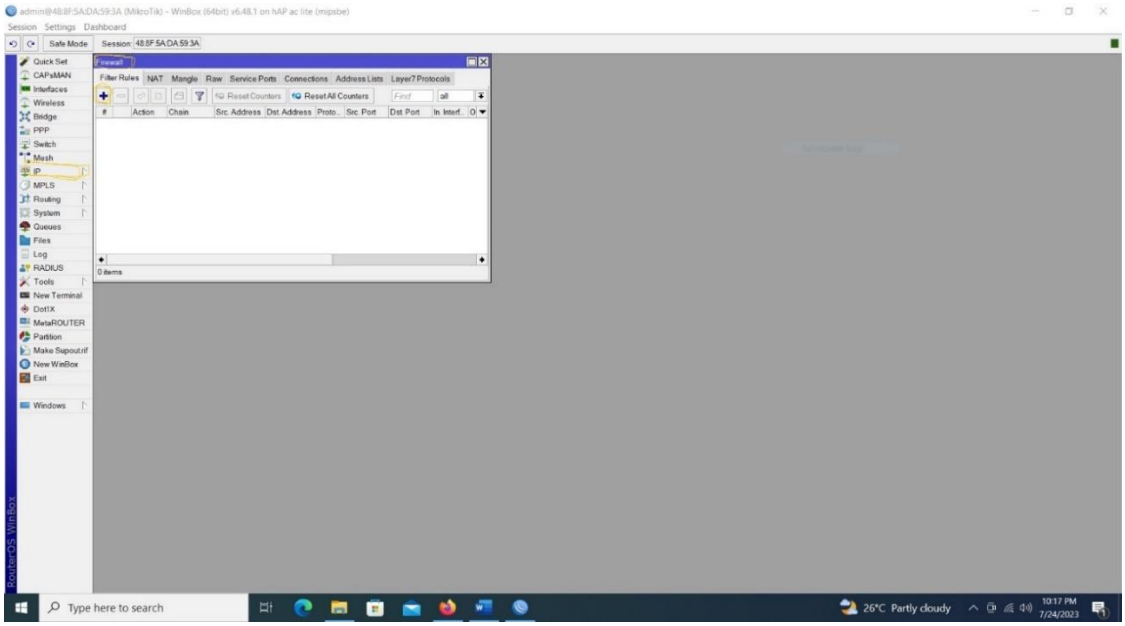




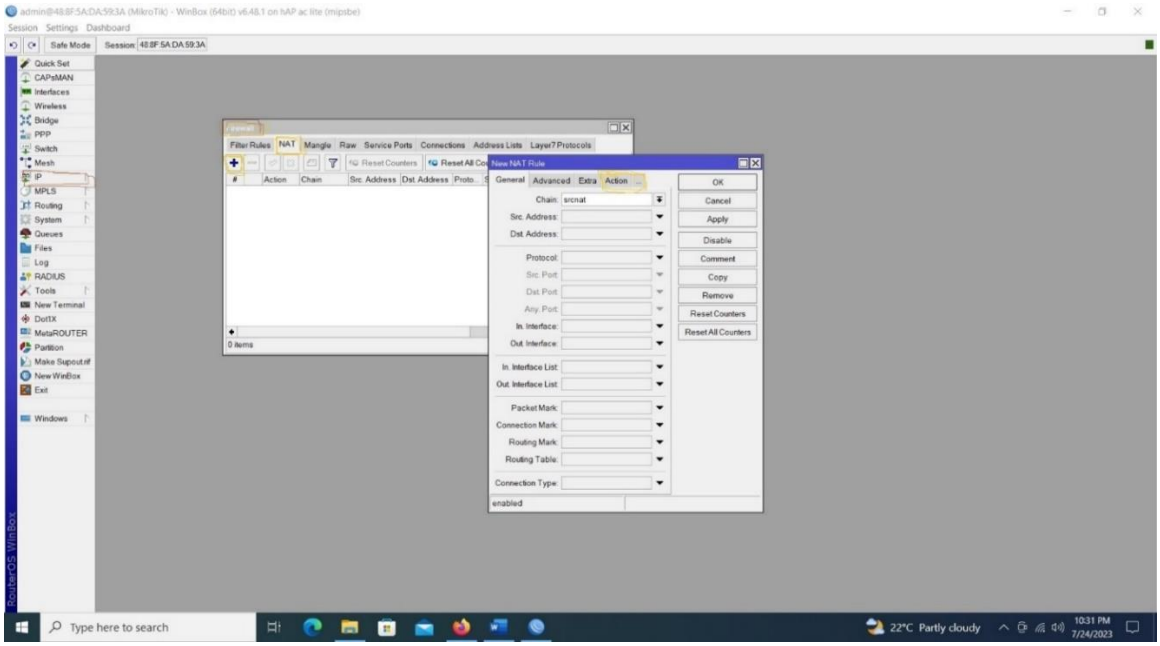
In New Address window, put WAN IP address (192.168.70.2/30) in Address input field and choose WAN interface (ether1) from Interface dropdown menu and click on Apply and OK button.

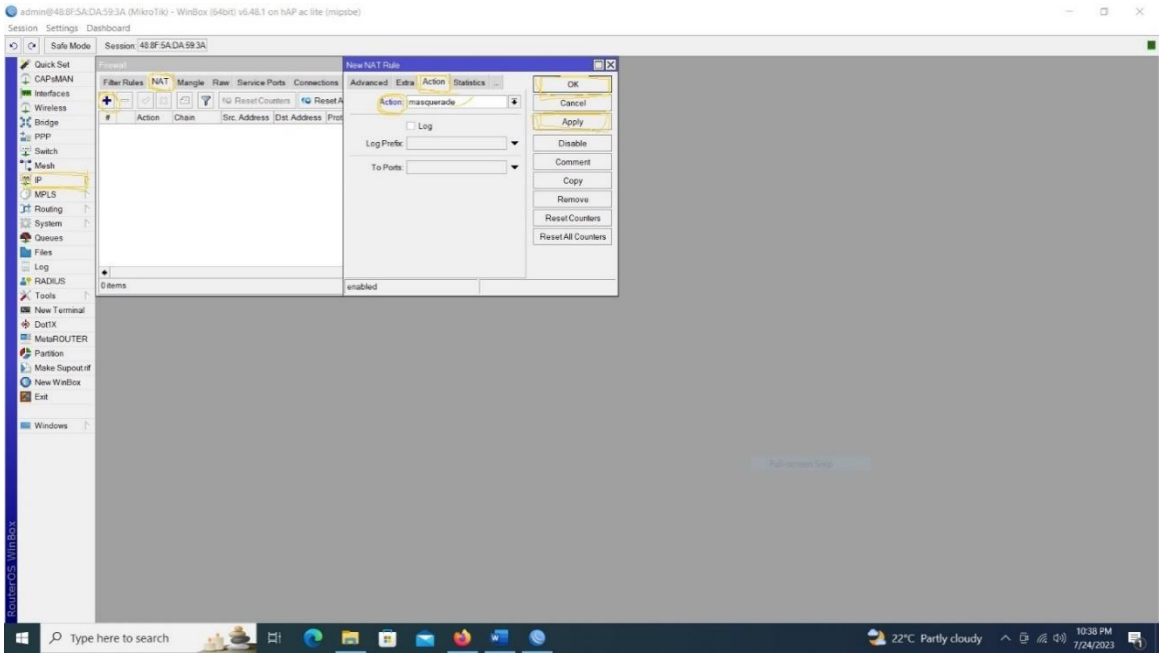


Go to IP > DNS and put DNS servers IP (8.8.8.8 or 8.8.4.4) in Servers input field and click on Apply and OK button.



Go to IP > Routes and click on PLUS SIGN (+). In New Route window, click on Gateway input field and put WAN Gateway address (192.168.70.1) in Gateway input field and click on Apply and OK button.





Go to IP > Firewall and click on NAT tab and then click on PLUS SIGN (+). Under General tab, choose srcnat from Chain dropdown menu and click on Action tab and then choose *masquerade* from Action dropdown menu. Click on Apply and OK button.