JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 40, 1093-1114 (2024)
DOI: 10.6688/JISE.202409_40(5).0011

An IKEv2-based Approach for Remote Access VPN on MikroTik Router

WOEI JIUUN TAY, SOOK LING LEW+ AND SHIH YIN OOI
Faculty of Information Science and Technology
Multimedia University
Melaka, 75450 Malaysia
E-mail: sllew@mmu.edu.my+

The university provides massive and regular use of Virtual Private Networks (VPNs) to set up a private connection system using a public network connection. No matter how the setup and cost, many universities continue to use antiquated protocols despite their security vulnerabilities. When the Remote Access Control (RAC) is weak, unauthorized people are permitted to access the university's network. In-depth VPN configuration and performance evaluation are still absent, despite previous research pointing to unmanaged group level access, the widespread use of antiquated protocols, and poor firewall configuration as sources of security issues. With the MikroTik router and IKEv2 VPN as a solution, this study aims to provide an in-depth configuration for improved security, reliability, and performance. This paper presents the performance of VPNs and their step-by-step configuration.

Keywords: IKEv2 VPN, virtual private networks (VPNs), remote access control (RAC), MikroTik, VPN configuration

1. INTRODUCTION

1.1 Overview

For remote teaching and learning (T&L) operations, the universities' infrastructure must uphold and sustain a sizeable volume of network connection. In response to user demand, the public network must enable secure remote access to university resources [1]. A Virtual Private Network (VPN) has emerged as a more effective method of delivering the services across the public network infrastructure. Features of VPN include cheap rate, network capacity use, flexible and dynamic operations, and confidential and safe access. Both the server and client sides must deploy the same tunnelling protocol in to establish a VPN connection. In order to ensure secure communications, it provides a host device that sends and receives data over a public network while encrypting and encapsulating each packet before sending it through a tunnel [2]. Similar features including security, authentication, confidentiality, integrity, and encryption techniques are offered by all VPNs [3]. This study proposes an easy and cost-effective RAC solution for campuses.

1.2 Problem Statement

Previous study has identified unmanaged group level access, the widespread use of outdated protocols, and improper firewall configuration as sources of security problems [4]. Therefore, the following research questions have been formulated in this study to

Received February 17, 2023; revised July 12, 2023; accepted October 18, 2023.
Communicated by Lee Hung Liew.
+ Corresponding author.

provide an additional in-depth configuration for improved security, reliability, and performance:

- How to establish an improved security, reliability VPN for for remote access?
- How well the developed Remote Access VPN performs?

1.3 Research Objectives

- To develop an IKEv2-based Remote Access VPN on MikroTik Router for remote connection.
- To assess the developed IKEv2-based Remote Access VPN.

2. LITERATURE REVIEW

2.1 Introduction

Virtual Private Network (VPN) is widely used nowadays. This is because VPN is a cheaper solution for organizations, providing the same functionality as a leased line. Each VPN type and protocol has its own capabilities, advantages, and disadvantages [5]. The following sections review the VPN protocols.

(A) VPN Protocols

A VPN protocol is a set of guidelines or instructions that specify the precise path that data will take between a client and a server. Depending on how they are specified, these protocols each have advantages and disadvantages [6]. These protocols are used in VPN configuration to support the security or performance priorities that are chosen.

(1) PPTP

Point-to-Point Tunnelling Protocol (PPTP) was invented by Microsoft in 1995 (Fig. 1). It is the oldest type of VPN that is still in use today because it is quick and easy to set up. It also has faster computational speeds.

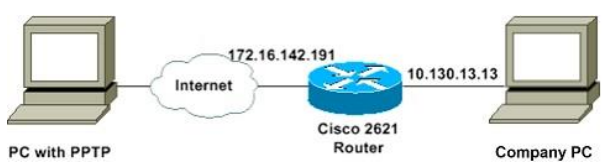

Fig. 1. Examples of PPTP setup.

Several security concerns have been raised about this protocol as security professionals consider PPTP as an outdated protocol. It uses 128-bit encryption that provides handshake authentication provided by Microsoft Challenge Handshake Authentication Protocol (MS-CHAP). This protocol has been successfully compromised by extracting the password from the key exchange [7].

(2) L2TP/IPsec

Fig. 2 shows an example of Layer 2 Tunnelling Protocol (L2TP). L2TP is the replacement of PPTP VPN protocol that is added with Layer Two Forwarding (L2F). It combines two reliable protocols. Microsoft PPTP and Cisco L2F [8].

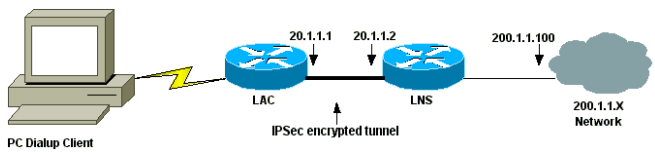

Fig. 2. Examples of L2TP over IPsec setup.

L2TP does not encrypt data by default. It can only do the encryption at the tunnel ends. Therefore, L2TP is often used with IPsec to provide additional layers of protection such as authentication, integrity, and data confidentiality to enhance the security when communicating through the VPN tunnel [1].

(3) IPsec/IKEv2

IKEv2 is the latest protocol that offers several improvements over IKEv1. They are quite similar, but IKEv2 supports more features and is more secure.

Although both IKEv1 and IKEv2 use IPsec, IKEv2 outperforms over IKEv1. IKEv2 uses four messages in total to create an IKE SA and a pair of IPSec SAs between client and server [9], while IKEv1 uses six messages on the main mode and three messages on aggressive mode which contains several vulnerabilities. However, it is fast as it reveals an unencrypted authentication hash while establishing the connection.

(4) OpenVPN

OpenVPN is an open-source SSL VPN which uses SSL/TLS protocol to encrypt data and provide a secure tunnel connection for point-to-point or site-to-site connection over the public network. OpenVPN must be set up on both the server and client sides to work.

OpenVPN uses private keys, certificates, or username and password as authentication while building the connection between server and client using OpenSSL encryption [10]. OpenVPN uses layers 2 and 3 tunnels in Open Systems Interconnection (OSI) layer. It is also easy to set up, and users can modify the script file to adjust the OpenVPN configuration to suit their needs. Besides, OpenVPN has more portability than has been widely deployed in organisations and homes today.

PPTP should be avoided as it has major security vulnerabilities. Since IKEv2 offers superior security, reliability, and speed compared to other VPN protocols, it is chosen to configure the remote VPN in the MikroTik router [4]. In comparison to WireGuard, it also offers improved user and certificate management for trusted and guest groups in the router configuration.

3. METHODOLOGY

3.1 Introduction

The network was designed using the Prepare, Plan, Design, Implementing, Operate

and Optimize (PPDIOO) network cycle. For this study, various applications and tools have been proposed.

3.2 PPDIOO

Fig. 3 displays the six phases of the PPDIOO. These phases demonstrate a continuous life cycle of services required for an organisational network [12, 13].

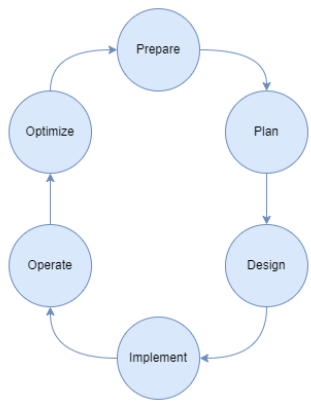

Fig. 3. PPDIOO network cycles.

(A) Prepare Phase

This phase involves establishing organizational requirements in a campus environment [13-15]. This study aims to develop an easy and cost-effective RAC for the campus. While the requirements are acknowledged, proposing a high-level conceptual architecture can be done in this phase, then identifying which technologies can support this architecture. The proposed architecture should be validated through proof-of-concept testing [12, 13, 15].

This study highlighted the need of setting up a VPN connection between the server and client when configuring the network. To access server resources, the server side must accept numerous clients.

(B) Plan Phase

This phase involves establishing organisational requirements in a university or campus environment [13-15]. There will be project plans since this study was done to set up the RAC and will implement the proper tasks, resources, and responsibilities required to implement the network so it will align with the correct scope of an organizational requirements [12, 13, 15].

This study planned to set up a common RAC solution enabling two or more devices or networks to connect remotely. This VPN protocol has been chosen based on the comparison done above. The MikroTik hEX RB750Gr3 router was used since it integrates IKEv2 with firewall and IPSec. It was employed in this study to set up the VPN.

(C) Design Phase

The organizations will start developing the network design based on the planned phase [12, 13, 15]. The common solution for RAC setup of network design will be implemented based on current RAC setup research conducted. Low-Level Design (LLD) was shown while designing the network to have more detailed information on which component of the network and other information will be used in the design. This design provided the basis for implementation activities in the next phase.

The end users were allowed to access specific devices in the local area network (LAN) after establishing an IKEv2 VPN connection to the MikroTik router. A mobile app for Android was adopted to test the connection between the end user's smartphone device and Windows device.

(D) Implement Phase

Implementation will begin after the design has been done and verified. This study was set up using a MikroTik router because it supports multiple VPN protocol setups and provides other features that consumer routers do not have, such as a custom firewall and Quality-of-Service (QoS) setup for different network conditions.

Several implementations need to be done for different operating systems, such as Android, iOS, and Windows, because different IPsec authentication algorithms, encryption algorithms, and certificate types are needed. These can give the optimum speed and stability of VPN connection on different OSes.

(E) Operate Phase

In this phase, it will be a final test of the network design implemented, which is also the longest phase in PPDIDO. The network should be operating day-by-day and monitored through it [12, 13, 15]. Due to the implementation being done in the home network, this study's operation phase was carried out on a smaller scale. To ensure that the setup is functioning properly for end devices, the router is linked to a number of devices across the house. Additionally, the IKEv2 VPN connectivity test was performed to guarantee that there would be no connection drops after the VPN tunnel connection has been created. Additionally, a network test with latency and performance in the IKEv2 VPN was conducted between the MikroTik router and end devices. The RouterOS graphing tool is used to track the average CPU and memory utilization while the router is running.

Upon testing, there was several RouterOS update performed automatically. After the update has been applied, VPN connectivity is also tested to ensure that the connection can still be established. Other network configurations were also checked and continue to operate to ensure no other error occurred.

(F) Optimize Phase

This phase will be happened at any time based on how the network will be operated in future days. Since the MikroTik router was used for this study, real assessment on the mobile app that connects external to the system to validate accessibility will be conducted. There will have check-ups periodically while the network design and configuration has done. Any minor fault needs to be troubleshoot immediately to prevent sudden failures such as internet connection outages, VPN connection drops, and internal network cannot access that might happen in the entire networking [12, 13, 15].

3.3 Software & Tools

MikroTik hEX RB750Gr3 router was used in this study to implement the proposed remote VPN (Fig. 4). It is a five port Gigabit Ethernet router that equipped with RouterOS. It comes with a dual-core 880MHz CPU and 256MB RAM, capable of all the advanced configurations that RouterOS supports. IPsec hardware encryption and The Dude server package are supported.

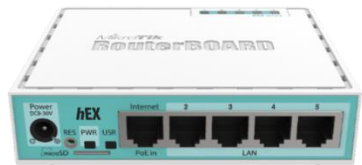

Fig. 4. MikroTik hEX RB750Gr3 router.

Fig. 5. Physical network setup for remote VPN.

Fig. 5 shows the actual setup for the current study. There are four network devices (1) modem provided by ISP; (2) MikroTik router; (3) TP-Link router in Access Point (AP) mode and (4) D-Link router in AP mode.

The MikroTik router is the primary device that manages the traffic flow between the routers and the public network. The MikroTik router uses four ports for the network setup. The first port count from the left is connected to the modem that the Internet traffic comes from ISP. The second port connects to the TP-Link router, letting WiFi users connect to this AP. The third port connects to the D-Link router mainly for the smart home devices, which act as the guest devices, and the fourth port connects to the PC server.

MikroTik provides a WinBox application for Windows, a small tool that allows the administration of MikroTik RouterOS using a quick and easy GUI. It can only run in Windows. Linux and macOS (OSX) users can run the application using Wine, the utility that runs Windows programs in the Linux system.

3.4 Conclusion

This study relies on the actual environment using the MikroTik device to set up a network for the proposed RAC. PPDIDO network cycles are proposed to ensure a good network is implemented.

The MikroTik device is used in the actual context of the study to establish a network for the proposed RAC. To ensure the implementation of a good network, PPDIDO network cycle is suggested.

4. SETUP AND RESULTS

4.1 Introduction

This section shows the setup to establish the IKEv2 VPN connection from the router to the client using the MikroTik router. Limitations and problems faced are also discussed.

4.2 Setup Results

The network setup was correctly done from scratch. The preloaded setup given was ignored. The network interfaces such as PPPoE WAN connection setup and LAN setup were manually set up, including firewall configuration and access port management, DHCP server, certificate management, and IPsec with IKEv2 VPN setup. The setup configurations mainly show the commands configured using the MikroTik device. For further explanation, graphical screenshots with WinBox GUI or configuration details are provided.

(A) Interface Setup

This section is where the devices connect to the LAN connection. Each interface will be labelled to make it administrator easier to recognize the usage of each ethernet connection.

Fig. 6 shows the properties of each interface available on this router. There are five ports available and enabled specified advertised speed on each port. The first port, whose default name is ether1, was used as a WAN connection connected to the modem provided by ISP. The rest of the ports act as regular LAN connections, such as the ether2 port con-

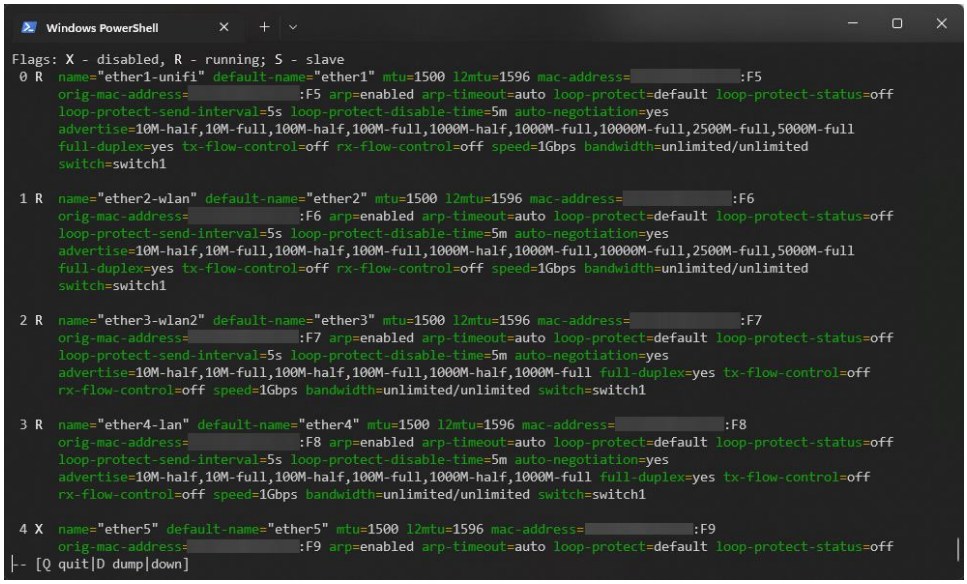

Fig. 6. Interface details.

nected to the TP-Link router that acts as access point (AP) mode and the ether3 port connected to the D-Link router AP mode. The ether4 port connects to the PC server, and ether5 is disabled from the router side as it did not connect to any device, and that port is not allowed for the non-trusted user's to use it.

(B) PPPoE Setup

This section is where the Point to Point over Ethernet (PPPoE) setup was going. PPPoE encapsulates PPP packets into Ethernet frames [16]. Administrators need to configure the PPPoE client on the router side to establish the internet connection. Internet service providers (ISP) will give users a PPPoE username and password to provide them with access to their service.

The configuration below shows the VLAN ID setup. A new VLAN is added into the ether1 port with VLAN ID 500. A sample of setup result:

```
/interface vlan
add interface=ether1-unifi name=vlan500-pppoe vlan-id=500
```

The configuration below shows while adding client configuration for the PPPoE client after the VLAN setup is done. Replace the username and password given by the ISP. Firewall also need to setup the masquerade rule for WAN port to establish the Internet connection. A detailed output of PPPoE client setup result:

```
/interface pppoe-client
add add-default-route=yes disabled=no interface=vlan500-pppoe name=\
    pppoe-unifi use-peer-dns=yes user=<username> password=<password>


/ip firewall nat
add action=masquerade chain=srcnat comment=internet out-interface=pppoe-
unifi \
    src-address-list=""
```

(C) Certificate Setup

This section shows the IPsec setup, which is the main implementation done in this study. Before IPsec was configured, router and client-side certificates were needed to verify the valid identity to establish the VPN connection.

In this study, a certificate for Android, iOS and Windows devices needs to generate separately. The certificate properties of both Android and iOS clients are identical, while Windows has a slightly different setup compared to other devices.

Certificates were generated for Certificate Authority (CA), server, and clients. Certificates' names will use the user-friendly naming scheme to let end users distinguish clearly while installing certificates on their devices. Some sample naming scheme such as "MikroTik CA" is for CA SSL certificate, and "MikroTik Client (Android)" is the certificate for clients that use Android devices.

The configuration below generates the CA SSL certificate before generating server and client certificates. It is a trusted entity that issues Secure Socket Layer (SSL) certifi-

cates [17]. This will sign certificates for servers and clients that will create later. This CA certificate is applicable for Android and iOS device. The certificate will install on these devices.

```
/certificate
add name="MikroTik Guest CA" common-name="MikroTik Guest CA" subject-alt-
name=DNS:ca days-valid=3650 key-usage=digital-signature,key-encipher-
ment,data-encipherment,key-cert-sign,crl-sign,tls-client,tls-server
```

The configuration below generates a server SSL certificate. This was used to let client attempts to connect to this server. The server will present a certificate in handshake process with client device. The client will check the certificate and verify that it has been signed by a trusted CA generated.

```
/certificate
add name="MikroTik Guest Server" common-name= "MikroTik Guest Server" sub-
ject-alt-name=DNS:server days-valid=3650 key-usage=digital-signature,tls-
server
```

The configuration below generates client SSL certificate for Android and iOS. This certificate will install on client devices to authenticate the client device connecting to the server. All certificates were set valid to 3650 days from the day created. Certificate name, common name, and subject alternative name can be any since client devices will not check domain name while establishing the VPN connection.

```
/certificate
add name="MikroTik Guest Client (Android)" common-name=="MikroTik Client"
subject-alt-name=DNS:android days-valid=3650 key-usage=digital-signa-
ture,tls-client
/certificate
add name=="MikroTik Guest Client (iOS)" common-name=="MikroTik Client" sub-
ject-alt-name=DNS:ios days-valid=3650 key-usage=digital-signature,tls-client
```

The configuration below shows the configuration for the Windows IKEv2 configuration. There was a slightly different configuration for Windows. The CA, server, and client SSL certificates are generated separately from other certificates for Windows to distinguish the Windows certificates from other devices easily. The server SSL certificates are required to specify a real domain name under “common-name” and “subject-alt-name” by replacing “domainname.net” with the real domain name. Dynamic DNS (DDNS) can also be used as the domain name, provided the address can be pinged.

```
/certificate
add name="MikroTik CA (Windows)" common-name="MikroTik CA" subject-alt-
name=DNS:ca days-valid=3650 key-usage=digital-signature,key-encipher-
ment,data-encipherment,key-cert-sign,crl-sign,tls-client,tls-server
add name="MikroTik Server (Windows)" common-name=domainname.net subject-alt-
name=DNS:domainname.net days-valid=3650 key-usage=digital-signature,tls-
server
```

```
add name="MikroTik Client (Windows)" common-name=="MikroTik Client" days-
valid=3650 key-usage=digital-signature,tls-client
```

The configuration below shows that each certificate was signed after relevant certificates were generated. CA SSL certificates are exported using Privacy-Enhanced Mail (PEM) by default, while the client SSL certificates were exported with the passphrase and using Public-Key Cryptography Standards #12 (PKCS12) cryptography standards.

```
/certificate

sign "MikroTik Guest CA"

sign "MikroTik Guest Server" ca="MikroTik CA"

sign "MikroTik Guest CA (Windows)" sign "MikroTik Guest CA (Windows)" ca-
crl-host=domain.net

sign "MikroTik Guest Client (Android)" ca="MikroTik CA"

sign "MikroTik Guest Client (iOS)" ca="MikroTik CA"

sign "MikroTik Guest Client (iOS)" ca="MikroTik CA (Windows)"

export-certificate "MikroTik Guest CA"

export-certificate "MikroTik Guest Client (Android)" export-pass-
phrase=12345678 type=pkcs12

export-certificate "MikroTik Guest Client (iOS)" export-passphrase=12345678
type=pkcs12
```

```
export-certificate "MikroTik Guest Client (Windows)" export-passphrase=12345678
type=pkcs12
```

Certificates that are certificates generated and signed are exported to the router storage with the correct type of CA and client certificate.

(D) IPsec Setup

After the SSL certificate setup has been done, IPsec can be set up as shown in the configuration below. Certificates are needed while configuring the IPsec VPN connection.

The configuration below shows the created IP pool for IKEv2 VPN. There were two IP pool which will give trusted and guest users respectively. Bigger IP pool for guest was bigger so that more IP address can be allocated for users.

```
/ip pool

add comment=trusted name=ikev2-vpn-pool1 ranges=192.168.88.2-192.168.88.6

add comment=guest name=ikev2-vpn-pool2 ranges=192.168.89.2-192.168.89.254
/certificate
```

The configuration below shows the IPsec configuration mode attributes configured. There were two configurations for two address pools. Netmask for the first configuration was set to 29 while the next one remains the default, 24. Matching the netmask to the IP address pool specified to prevent policy errors while establishing the connection is suggested. System DNS is selected by default on this configuration that the addresses will be taken from the router defined in DNS menu section.

```
/ip ipsec mode-config
add address-pool=ikev2-vpn-pool1 address-prefix-length=29 name=ikev2-cfg1
add address-pool=ikev2-vpn-pool2 name=ikev2-cfg2
```

The configuration below shows the IPsec policy group created to separate trusted and guest user groups. The group was created respectively.

```
/ip ipsec policy group
add name=ikev2-trusted-group
add name=ikev2-guest-group
```

The configuration below shows the parameters specified in the IPsec profile configuration to be used for the first phase of the IKE negotiation. AES-128 and AES-256 encryption algorithm was selected to be used in this IKEv2 profile. Others have remained the default.

```
/ip ipsec profile
add enc-algorithm=aes-256,aes-128 name=ikev2-profile1
```

The configuration below shows the IPsec peer configuration. The exchange mode for IPsec peer was chosen as IKE2 to enable IKEv2 for the phase 1 exchange modes [18]. It is possible to use passive mode to wait for the remote peer to start an IKE connection. The option for sending INITIAL_CONTACT is disabled because this setup initiator is for road warrior's clients, meaning remote end users need secure access to the company's infrastructure.

```
/ip ipsec peer
add exchange-mode=ike2 name=ikev2-peer passive=yes profile=ikev2-profile1 \
    send-initial-contact=no
```

The configuration below shows the configuration for the proposal information of IPsec. It will be sent by IKE daemons that establishes Security Associations (SA) for certain policies [18]. The authentication algorithm was set by default which is SHA1. SHA256 was also supported but will lead to a decrease in network speed on Android device while establishing an IKEv2 VPN connection. Lifetime was set to one day, which means the duration of using SA before nuking it. The perfect Forward Secrecy (PFS) group is an IPsec attribute that ensures the exported session key will not be compromised if one of the private keys is compromised [19]. The default option was chosen is modp1024, which is balanced in security and speed.

```
/ip ipsec proposal
add enc-algorithms=aes-128-cbc lifetime=1d name=ikev2-proposal1
```

The configuration below shows the IPsec identities configuration was set up for remote peers based on their devices. Identity configuration's primary function is to manage authentication and confirm the integrity of the peer [18]. Identities were created based on the user base and devices. The identity options were chosen based on the authentication

method created, and the appropriate certificate was chosen to match the type of users and devices required.

For example, the configuration below shows to create an identity for Android guest users. In this configuration, the digital signature was chosen for the authentication method. "MikroTik Guest Server" certificate and "MikroTik Guest Client (Android)" remote certificate are selected. These two certificates are signed by the "MikroTik Guest CA" CA SSL certificate. For configuration mode, "ikev2-cfg2" was chosen, which gives IP address pool in 192.168.89.0/29 for guest users. My ID type is set to a fully qualified domain name (fqdn), and My ID is set to Subject Alternative Name in the certificate "server". Identity peer is set to "ikev2-peer" while for policy template group is set to "ikev2-guest-group" because the user wants to add is guest user.

```
/ip ipsec identity
add auth-method=digital-signature certificate="MikroTik Guest Server" com-
ment=\
    "android guest" generate-policy=port-strict match-by=certificate \
    mode-config=ikev2-cfg2 my-id=fqdn:server peer=ikev2-peer \
    policy-template-group=ikev2-guest-group remote-certificate=\
    "MikroTik Guest Client (Android)"
```

The configuration below shows the IPsec policies to determine whether to apply the security settings to the packet sent out or received. The template option was enabled to assign it to a specified policy group that was created before. The group is set based on the user base, and a proper proposal template was selected. The IKE daemon will send that to establish SAs for this policy. The source address is set to 0.0.0.0/0, which matches any packet in any network to apply transformations specified in each policy and its SA to the destination address specified [17].

```
/ip ipsec policy
add dst-address=192.168.88.0/29 group=ikev2-trusted-group proposal=\
    ikev2-proposal1 src-address=0.0.0.0/0 template=yes
add dst-address=192.168.89.0/24 group=ikev2-guest-group proposal=\
    ikev2-proposal1 src-address=0.0.0.0/0 template=yes
```

(E) Firewall Setup

This section will show how firewall is setup on this network. Firewall is playing an important role on whole network to protect internal or external attacks from end user devices.

The configuration below shows the example filter list that is configured in the firewall. Each firewall rule adds its respective comment to label clearly which rules are for what purposes. There are three predefined chains: forward, input and output need to select correctly to specify where the traffic should accept and drop its connection.

Input is used to process packets entering the router through an interface where the destination IP address is one of the router's addresses. Output is used to process packets

from the router and leave through one interface. Packets passing through the router are not processed through the input and output chain rule but using the forward rule to process it. The forward rule was used frequently to accept or drop packets within the local network and public network.

The example of firewall configuration for IPsec will be explained as it is the main implementation in this study. It specifies the VPN IP range to allow connection to specify an IP address and port number, which is 192.168.1.2:8384 using a TCP connection to ether2 interface and drops all connections under 192.168.0.0/16 that blocks VPN users from accessing the local network devices. UDP connection is allowed. ICMP ping drops when disallowed packages go in the router, where VPN users cannot access to router page after the connection is established.

```
/ip firewall filter
    "WAN: drop www, www-ssl web interface from public network" dst-port=\
    80,443 protocol=tcp src-address=192.168.0.0/16
add action=drop chain=input dst-port=80,443 in-interface-list=!LAN proto-
col=\
    tcp
add action=accept chain=forward comment=\
    "IPSEC: only allow specific LAN access, blocks router access" \
    dst-address=192.168.1.2 dst-port=8384 out-interface=ether2-wlan proto-
col=\
    tcp src-address=192.168.89.1-192.168.89.6
add action=drop chain=forward dst-address=192.168.0.0/16 src-address=\
    192.168.89.1-192.168.89.6
add action=accept chain=input dst-port=53 protocol=udp src-address=\
    192.168.89.1-192.168.89.6
add action=drop chain=input protocol=!icmp src-address=\
    192.168.89.1-192.168.89.6
add action=accept chain=forward comment="IPSEC: accept in ipsec policy" \
    ipsec-policy=in,ipsec

add action=accept chain=forward comment="IPSEC: accept out ipsec policy" \
    ipsec-policy=out,ipsec
```

Fig. 7 shows the firewall filter rules in WinBox to have a better view in Graphical User Interface (GUI) mode. In this interface, administrators can move the order of firewall rules because it will run them in sequence from the top. For example, the firewall needs to accept which connection can be passed through the router, then drop all connections after the accept rule action. Besides, the firewall only works if the traffic goes through the router,

which means if the IP address under 192.168.1.0/24 is connected to the Wireless AP, the traffic of that IP range will not route through the router's firewall. They can access each other if the firewall rules do not apply to Wireless AP.

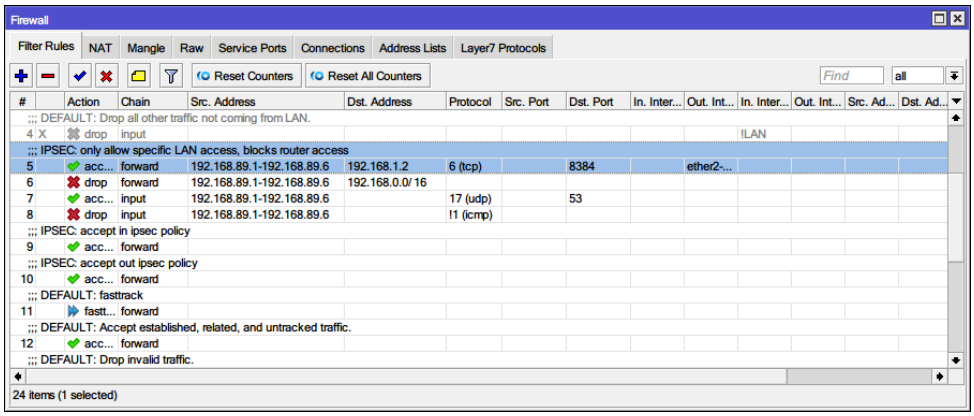

Fig. 7. Firewall filter rules.

The configuration below shows the firewall mangle feature that marks the packets for future processing with special marks [20, 21]. IKEv2 connection needs this to solve some connectivity problems that might occur in VPN connection, such as connection drop and sometimes unable to establish the VPN connection. These problems occurred as a result of IP packet fragmentation brought on by the payload size exceeding the IP maximum transmission unit (MTU) of the network channel between the client and server during IKEv2 connection formation. However, it happens frequently that intermediary devices like firewalls, NAT devices, and routers restrict IP fragmentation [22]. The fragmentation issue can be resolved by setting a custom MSS value. It can reduce packet loss and make the network more stable while the user establishes the VPN connection.

```
/ip firewall mangle
add action=change-mss chain=forward new-mss=clamp-to-pmtu passthrough=yes \
    protocol=tcp tcp-flags=syn
add action=change-mss chain=output new-mss=clamp-to-pmtu passthrough=yes \
    protocol=tcp tcp-flags=syn
```

The configuration below shows the firewall Network Address Translation (NAT) rules. NAT allows hosts in LAN to employ two different sets of IP addresses for internal and external communication. IPsec is set to accept source NAT (srcnat) chain rule to accept IPsec policy matched. This rule is useful while setting up policy-based IPsec VPNs in future. In the next rule, firewall NAT action masquerade was used for the PPPoE interface to adjust to the specific usage in circumstances where public IP can fluctuate. The router will remove all entries for masqueraded connections of the disconnected interface or IP changes and improves system recovery time if public IP changes [23].

```
/ip firewall nat
add action=accept chain=srcnat comment=\
"accept all that matches IPSec policy" ipsec-policy=out,ipsec
```

(F) Queue Setup

This section will show how the queue feature is implemented for IKEv2 VPN users. Traffic is constrained and prioritised via the queue feature. The queue tree feature is used to limit VPN users' traffic as only this feature can parse the IPsec traffic to achieve bandwidth limitations.

The configuration below shows the mangle rules that must be defined prior to the implementation of the queue tree. All connections' traffic that goes via the router is marked. By turning on the IPsec policy in and out for each incoming and outgoing rule, the IPsec traffic forward chain is designated for incoming and outgoing connections from end-user devices.

```
/ip firewall mangle
    "GLOBAL: travelling via the router of traffic " new-connection-mark=all-
mark
add action=mark-packet chain=forward comment=\
    "IPSEC: traffic coming in for guest" connection-mark=all-mark \
    dst-address=192.168.89.0/24 ipsec-policy=out,ipsec new-packet-mark=\
    guest-incoming passthrough=no
add action=mark-packet chain=forward comment=\
    "IPSEC: traffic going out for guest" connection-mark=all-mark ipsec-pol-
icy=\
    in,ipsec new-packet-mark=guest-outgoing passthrough=no src-address=\
    192.168.89.0/24
```

The configuration below shows the queue functionality was added after the mangle rule was configured for the IPsec connection. For both incoming and outgoing connections, the queue type is made. Per Connection Queue (PCQ), which functions as a queuing discipline rule that may be utilised to dynamically equalise or shape traffic for various users while requiring minimum administrative effort, is the queue kind currently selected. The PCQ rate for each connected user is set at 10Mbit/s.

The global parent is chosen when creating the queue tree parent, after which a second tree is created beneath it with the appropriate queue type and packet markings for incoming and outgoing connections. The maximum limit for an IKEv2 connection has been specified for both connections.

```
/queue type
add kind=pcq name=pcq-download-ikev2-guest pcq-classifier=dst-address \
    pcq-rate=10M
add kind=pcq name=pcq-upload-ikev2-guest pcq-classifier=src-address pcq-
rate=\
    10M
```

```
/queue tree
add name=queue-tree1 parent=global queue=default
add comment="IPSEC: limit per user bandwidth" max-limit=30M name=\
    ikev2-guest-down packet-mark=guest-incoming parent=queue-tree1 queue=\
    pcq-download-ikev2-guest
add max-limit=70M name=ikev2-guest-up packet-mark=guest-outgoing parent=\
    queue-tree1 queue=pcq-upload-ikev2-guest
```

4.2 Device Configuration

This section shows the VPN connectivity on each OS device, respectively. The setup procedures and network tests were done on these devices. PEM format for CA SSL certificate and PKCS12 with a passphrase for client SSL certificate should be used. These formats support all devices, which will be shown below.

(A) Android

Android adds IKEv2 support since Android 11. The StrongSwan app was chosen to set up the IKEv2 VPN client side for Android devices so that users on different Android versions can connect to the IKEv2 VPN service. It can be found in Google Play Store. The setup was done in Android 12L running on a Xiaomi POCO F1 device.

There were two methods to import the certificate. The first method is using the StrongSwan app to import the CA certificate into the application. Users can navigate to 3 dot settings – CA certificates menu, then go to 3 dot settings again, select “Import certificate”, and follow the instructions to add the CA certificate into the StrongSwan app.

The second method might be complicated for users because each vendor device has its customized Android interface. Some popular Android interfaces in the market include Samsung OneUI, Xiaomi MIUI, Oppo ColorOS, and Pixel stock Android experience. Each vendor’s certificate location might differ but usually falls under the “Security” category. The certificate installation method will use Pixel stock Android experience to show the steps to install it into the Android system.

Starting from Android 11, CA SSL certificates only can install manually from the device settings menu. For older Android versions, users can directly tap the CA certificate and install it directly from any application.

Users can now import the CA certificate in Settings – Security – Encryption & credentials – Install a certificate – CA certificate menu and follow the instruction to install it. Next, the user can install client certificates directly under the VPN & app user certificate menu. After installing both certificates, users can navigate to trusted and user credentials to check the certificate information. Certificates can be uninstalled by tapping the certificate and choosing the “Uninstall” option.

Users can continue to add VPN profiles after the CA certificate has been imported. The server IP address only was supported by StrongSwan. It does not allow DDNS because it will fail to resolve the address. Users need to install the appropriate user certificate and select it if not installed in Android settings. CA certificate was chosen by the user that installed in StrongSwan or Android settings. Server identity must match Subject Alt. Name

specified in the server's certificate. Client identity follows the same procedure as server identity but follows the specified client's certificate.

(B) iOS

iOS device has native support of IKEv2 since iOS 9 [24]. The setup was done through the inbuilt VPN setup provided by Apple. The operating system version is iOS 15.5, and the device is the iPhone 6S Plus. Certificates need to save on the device before installing it. Users need to open these files from the Files app and follow the instructions to install them into the device.

VPN configuration can be done in Settings – General – VPN & Device Management – VPN menu. Users can now add the VPN configuration. Description can be any name the user likes. The server can use an IP address or DDNS. Remote ID must match Subject Alt. Name specified in the server's certificate. Local ID follows the same procedure as remote ID but follows the specified client's certificate. There was no user authentication in the authentication part, but the user needed to enable the "Use Certificate" option and select the appropriate client certificate file installed. The user should be able to establish the VPN connection after the setup has been completed.

(C) Windows

Windows has native support for the IKEv2 connection. Windows 11 Enterprise with version 22H2 and OS build version 22622.290 will be used to set up a sample IKEv2 VPN. Certificates must be stored in local storage. It can be installed either by double clicking the certificate file or using "Manage computer certificates" under "Microsoft Management Console" on the local computer.

Certificates were imported under Personal and Trusted Root Certification using the import feature. Users will follow the instructions to import CA and client certificates under Personal and Trusted Root Certification.

After installation, the certificates were shown in both Personal and Trusted Root Certification. Users can add the VPN connection under Windows Settings – Network & Internet – VPN – Add VPN. The domain name is needed for the server name or address section. The domain name can refer to the CA certificate signed with CA CRL Host in the MikroTik certificates list. IKEv2 was chosen for VPN type and left username and password blank since the certificate only was used to establish a VPN connection.

Users will get an IKE authentication error or be unable to connect if they tap connect button now. Further settings are required. Navigate to Windows Settings – Network & Internet – Advanced network settings – More network adapter options, right-click the VPN connection created. Navigate to the "Security" tab and choose "Use machine certificates" to use the certificate imported. IPv6 option also need to be disabled since we do not use an IPv6 VPN connection to prevent any connection issue while browsing the Internet through VPN.

4.4 Connectivity Tests

This section performs web access testing and speed tests to show the established VPN network's access and stability. An application "iCully" for Android was tested that allows the application connects through the specific ports defined by the Windows application to perform remote access control.

(A) Web Access

Web access testing was done on each device to ensure users could access the Internet and self-hosted services on the local server. Windows devices were used as a testing bed to access websites and services through VPN using guest user credentials.

Fig. 8 shows the sample of IPsec firewall rules configured. The rules show it accepts connection to port 6464 for IP address 192.168.0.2 for guest VPN users and drops connection under 192.168.0.0/16, which guest users cannot access to all local devices. Guest users cannot access to the web interface of router.

```
7   ;;; IPSEC: only allow specific LAN access for guest, blocks router access
    chain=forward action=accept protocol=tcp src-address=192.168.89.1-192.168.89.254 dst-address=192.168.0.2
    out-interface=ether4-lan dst-port=6464 log=no log-prefix=""

8   chain=forward action=drop src-address=192.168.89.1-192.168.89.254 dst-address=192.168.0.0/16 log=no log-prefix="">

9   chain=input action=accept protocol=udp src-address=192.168.89.1-192.168.89.254 dst-port=53 log=no log-prefix=""

10  chain=input action=drop protocol=!icmp src-address=192.168.89.1-192.168.89.254 log=no log-prefix=""
```

Fig. 8. IPsec firewall rules.

Guest users cannot access to 192.168.0.2:9000, while users can access port 6464 but denied access to 192.168.0.1.

(B) Speed Test

Speed tests were done on each device to test how much throughput they can achieve while connected through a VPN. The speedtest application was used in Android and iOS devices, while the speedtest.net website was used on Windows. The maximum speed provided by ISP is 111.70Mbps download and 55.93Mbps upload.

(C) iCully

The application “iCully” is a remote access application that provides various remote-control features, as shown in Fig. 9 that Android device successfully connected to the iControl server.

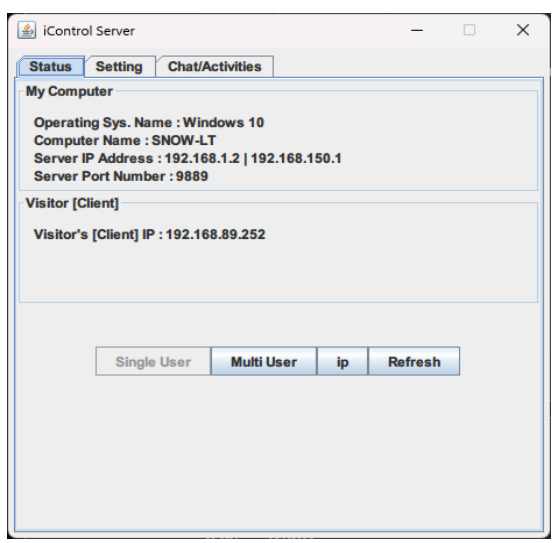

Fig. 9. iControl Server for iCully.

The configuration below shows the firewall rules were modified to match the current usage for iCully. The destination address was changed to 192.168.1.2, which iControl server was running on this device. The destination port was modified to let the guest user access port 9889, which is for single user access, and 5005 for multiple user access for iCully to the iControl server.

```
/ip firewall filter
add action=accept chain=forward comment="IPSEC: only allow specific LAN ac-
cess\
    \_for guest, blocks router access \
    dst-address=192.168.1.2 dst-port=9889,5005 out-interface=ether2-wlan \
    protocol=tcp src-address=192.168.89.1-192.168.89.254
```

The iControl server chat/activities tab will monitor the activities and chats sent from client devices. Fig 10 shows two users connected to the server, and activities are logged while users enter the chat room. Both users from client devices send text messages.

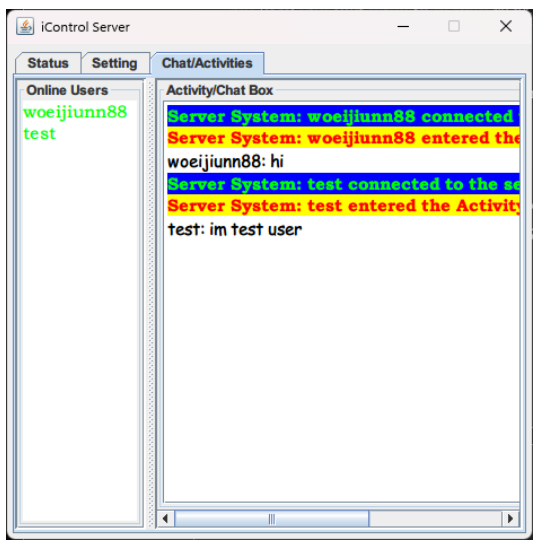

Fig. 10. iControl server chat for multiple devices.

(D) Bandwidth Limits

Queue tree setup has done for guest VPN users. Fig. 13 shows the result of two devices connected to the guest VPN and running the speed test simultaneously. Both do not receive and send the connection over 10Mbps.

4.5 Limitations & Problems

Although the setup has been done without any errors, some limitations and problems were found while setting up the network for this study.

Windows cannot specify certificates installed directly on Windows settings. Windows will select the latest client certificate installed that was created by the MikroTik router while connecting the VPN.

StrongSwan Android client might have a bug in speed in the cellular data network. After several tests, the Android client might face an issue with upload speed that slows down below 1Mbps. The root cause was still unknown because this bug is rarely triggered. The speed test result is 45.51Mbps download and 0.42Mbps upload, while maintains a good ping at 54ms. It can be solved temporarily by force-stopping the StrongSwan application and reopening and reconnecting the VPN. Aeroplane mode is also recommended to toggle off and on to change the IP address given by the mobile ISP.

5. CONCLUSIONS

This study proposes a cost-effective solution for remote access control for universities. Specifically, an IKEv2-based approach for Remote Access VPN on MikroTik router was configured, implemented and well tested in this study. The small scale configuration setup is able to scale up to a company level even though this study was carried out using a MikroTik router, a non-consumer-grade router, because the router offers features that consumer-grade routers do not, such as a fully customised firewall, certificates management, routing, and various VPN protocols like L2TP, PPTP, IPsec, and WireGuard. If the RouterOS configuration setup is the same on several routers, the configuration can be rebuilt and transferred.

Several evaluations were made to guarantee proper access for trusted and non-trusted users while the VPN connection was being established. While guest users can only access a limited number of the devices and ports that are included in the firewall filter rules, trusted users will have complete access to the local network. Additionally, the local network device is subject to the firewall rules in order to restrict local device access to server resources across various subnets. In accordance with the encryption mechanism used in IPsec proposals and profiles, the speed test was also performed to ensure that user end devices would operate at an appropriate speed. An application's ability to have effective remote access control across the established VPN connection was examined.

After a few weeks of operation and numerous inspections, it was discovered that there were some limitations, such as a Windows certificate issue and an Android speed issue, which was eagerly anticipated to be fixed so that customers could have a more flawless VPN experience.

REFERENCES

1. S. Jing, Q. Qi, R. Sun, and Q. Li, "Study on VPN solution based on multi-campus network," in *Proceedings of the 8th International Conference on Information Technology in Medicine and Education*, 2016, pp. 777-780.
2. F. A. Salman, "Implementation of IPsec-VPN tunneling using GNS3," *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 7, 2017, pp. 855-860.

3. S. T. Aung and T. Thein, "Comparative analysis of site-to-site layer 2 virtual private networks," in *Proceedings of IEEE Conference on Computer Applications*, 2020, pp. 1-5.
4. W. J. Tay, S. L. Lew, and S. Y. Ooi, "Remote access VPN using Mikrotik router," in *Proceedings of International Conference on Computer and Drone Applications*, 2022, pp. 119-124.
5. P. Paganini, "The strengths and weaknesses of different VPN protocols," https://securityaffairs.co/wordpress/84506/digital-id/strengths-weaknesses-vpn-protocols.html, 2019.
6. M. Calvello, "VPN Protocols: Are you using the right one?," https://www.g2.com/articles/vpn-protocols, 2020.
7. VPN University, "PPTP VPN: What it is, When to use it, and better alternatives," http://www.vpnuniversity.com/learn/pptp-vpn-protocol, 2020.
8. B. Santoso, A. Sani, T. Husain, and N. Hendri, "VPN site to site implementation using protocol L2TP and IPSEC," *Teknokom*, Vol. 4, 2021, pp. 30-36.
9. L. Yu, S. Jia, C. Xu, J. Guan, and D. Gao, "An IPsec seamless switching mechanism with high availability and scalability by extending IKEv2 protocol," in *Proceedings of International Conference on Advanced Intelligence and Awareness Internet*, 2011, pp. 25-29.
10. B. Mustapha, H. Abdelhakim, and B. Abderrahim, "High accuracy localization method using AOA in sensor networks," *Computer Networks*, Vol. 53, 2009, pp. 3076-3088.
11. M. Iqbal and I. Riadi, "Analysis of security virtual private network (VPN) using open-VPN," *International Journal of Cyber-Security and Digital Forensics*, 2019, pp. 58-65.
12. Cisco Press, "Cisco's PPDIOO network cycle," https://www.ciscopress.com/articles/article.asp?p=1697888, 2011.
13. T. Slattery, "Computer network design using PPDIOO method with case study of SMA Negeri 1 Kunir," https://www.techtarget.com/searchnetworking/tip/A-guide-to-network-lifecycle-management, 2021.
14. Cisco Press, "Analyzing the Cisco enterprise campus architecture," https://www.ciscopress.com/articles/article.asp?p=1608131, 2010.
15. A. Elrashdi, S. E. Khiralla, and S. S. Albaseer, "Development PPDIOO methodology to be compatible with technical projects for computer networks," *International Science and Technology Journal*, Vol. 15, 2018, pp. 1-19.
16. C. Artūrs, "PPPoE – RouterOS," https://help.mikrotik.com/docs/display/ROS/PPPoE, 2019.
17. R. Awati, "What is a certificate authority (CA)?" https://www.techtarget.com/searchsecurity/definition/certificate-authority. 2021.
18. C. Artūrs, "IPsec – RouterOS," https://help.mikrotik.com/docs/display/ROS/IPsec.
19. "Perfect forward secrecy," https://www.ibm.com/docs/en/sss/3.1.1?topic=reference-perfect-forward-secrecy, 2021.
20. C. Artūrs, "Mangle – RouterOS," https://help.mikrotik.com/docs/display/ROS/Mangle, 2020.
21. Electric Sheep Fencing LLC and Rubicon Communications LLC., "pfSense® software Configuration Recipes – Configuring IPsec IKEv2 Remote Access VPN Clients

– Configuring IPsec IKEv2 Remote Access VPN Clients on iOS," http://docs./netgate.com/pfsense/en/latest/recipes/ipsec-mobile-ikev2-client-ios.html, 2022.
22. R. M. Hicks, "Troubleshooting always on VPN Error Code 809," https://directaccess.richardhicks.com/tag/ikev2-fragmentation, 2019.
23. C. Artūrs, "NAT – RouterOS," https://help.mikrotik.com/docs/display/ROS/NAT, 2019.
24. "Configuring IPsec IKEv2 Remote Access VPN Clients on iOS," https://docs.netgate.com/pfsense/en/latest/recipes/ipsec-mobile-ikev2-client-ios.html, 2022.

Woei Jiunn Tay received the Bachelor of Information Technology (Hons.) Data Communications and Networking from Multimedia University, Malaysia. His research interests include communication networks and network configurations. He is working as part of IT management for small business in Sin Soon Hup Auto.

Sook Ling Lew received her Ph.D. from Multimedia University (MMU), Malaysia in 2013. She has been a Lecturer (now Associate Professor) in Multimedia University, Faculty of Information Science and Technology since 2001. Her research interests include educational technology, business analytics, Internet marketing, knowledge management (KM), image processing and recreational studies.

Shih Yin Ooi received the Bachelor of Information Technology (Hons), Master of Science (Information Technology), and Ph.D. (Information Technology) from the Multimedia University, Malaysia, in 2017. She is currently served as a Deputy Director of Technology Transfer Office (TTO) at Multimedia University, Malaysia. Her research interests include temporal classification, tree-based algorithms, and machine learning applications in the field of biometrics and cybersecurity.