

VPN VIRTUAL PRIVATE NETWORK APPLICATIONS IN DATA PREDICTION

Dorjan Zela

University College of Business , Faculty of Engineering and Computer Science, Tirane.

E-mail address: d.zela@kub.edu.al

Besjana Mema

Mediterranean University of Albania ,Faculty of Informatic, Tirane, Albania.

E-mail address: besjana.mema@umsh.edu.al

Katerina Zela

Mediterranean University of Albania ,Faculty of Informatic, Tirane, Albania.

E-mail address: katerina.male@umsh.edu.al

Abstract

The evolution and age of the latest programs and services, along with the expansion of encrypted communications, make it difficult for site visitors within a security enterprise. Virtual private networks (VPNs) are one example of an encrypted communications provider that is becoming popular as a way to bypass censorship in addition to gaining access to geo-blocked offerings. This paper examines the presentation of an IP security, VPN. The Cisco Packet Line Platform is used for simulation, evaluation, and verification. It uses a virtual connection to carry data packets from a non-public network to remote locations.

Network data transmission used on an unsecured public Internet network so that you can access the network from cross-purposes and search for data traffic. One solution that can be done is with Virtual Private Network techniques using OpenVPN on learning networks. The results of the implementation of the Virtual Private Network using OpenVPN are that the effort gives a positive result, this is proven by sniffing the data that cannot detect the username and password sent. Quality of Service measurement results showed a decrease in network quality with latency parameters increasing from 51.4 ms to

463.4 ms, packet loss increased from 7.8% to 20.2%, throughput decreased from 82.8% to 71.6%, and bandwidth decreased from 64786 to 6.6 bits. 55589 bit/s, is due to the time-consuming encryption and encapsulation process. A virtual private network (VPN) can be defined as a way to provide secure communication between members of a group through the use of public telecommunications infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. There are many different VPN solutions out there, and simply deciding which one to choose can be difficult as they all have advantages and disadvantages. VPNs can be categorized as secure or trusted VPNs, client-based or web-based VPNs, client-side or provider-based VPNs, or outsourced or

in-house VPNs. These categories often overlap with each other. To decide which VPN solutions to choose for different parts of the enterprise infrastructure, the chosen solution should be the one that best meets the requirements of the enterprise.

Keywords: *Virtual Private Network, Authentication, Security, Privacy, OpenVPN, Mikrotik, Analytics.*

1. INTRODUCTION

Considering that in today's world of information technology there are "hackers" everywhere, we definitely need something to reassure us again. It is precisely the Virtual Private Network (VPN –) that accomplishes this, in a LAN, WAN and remote access of various remote users. We can say that there are people around the world who use VPN on a WAN and send secure messages using a service provider's network [1].

Also, there are many people who work outside or from home and who use a VPN to securely connect to their company's infrastructure with the help of an ISP (Internet Service Provider). By implementing a VPN from a computer to a Cisco device (eg a Cisco VPN concentrator) using IPSec [2].

We are able to send and receive information securely from both sides of this VPN. In this way, a secure environment is created for remote users who can perform their work on a WAN. So, in this diploma project, the material has been prepared in such a way as to give a clear idea about virtual private networks, describing them from a technical and functional point of view. The architecture and protocols used for the realization of the VPN are also presented in detail. The advantages and disadvantages of using VPN are highlighted, and the protocols on which this technology is based are delved into.

It will give an overview of VPN and IPSec protocol. used in these networks. It then describes and talks about the VPN axioms that determine and influence the construction of almost any VPN design. It presents the remote user construction and the four construction options of this construction together with the component devices.

It once again describes the architecture of the IPSec technology, its structure, the way this technology works, as well as the protocols on which this technology is

based, going into them in more detail. At the end, a glossary is presented which explains the new terms used, so that they are better understood. provides an example of implementing a VPN system between a host and a server on a Linux system, as well as configuration methods and problems that may arise.

This material includes detailed graphical representations that complete the idea about VPN networks. These schemes start with the presentation of a general VPN network to the most detailed structures that present in detail the structure and the way the technology works, as well as the protocol frames used. Based on the purpose of this diploma topic, a general description of VPNs is first given, and then it goes deeper into its basic structures and the protocols used. Another objective of this degree project is to present remote user design and design options. The work of this diploma topic is based on three books entitled "Cisco-Safe VPN-IPSec in depth", "VPN-How to", "Cisco Network Security" as well as on materials obtained from the Internet.

1. AN OVERVIEW OF VPN AND IPSEC TECHNOLOGY

1.1 *What is a VPN?*

Theoretically and perhaps even abstractly, a VPN is a Virtual Private Network [3].

Remote users, mobile users and remote offices of companies different can be connected to the company headquarters via VPN.

The VPN uses encryption and tunneling within an otherwise insecure network as it is Internet to realize communication and connection.

Cisco devices can be configured and work as active VPN devices only by configure IOS "features". There are many concentrators, but also a PIX or a base router are activated as active VPN devices by configuring their IOS [3].

1.2 *Other elements in building a VPN*

Since security is the main problem, it is up to us to take care of it and protect it through encryption by configuring it according to our purposes. It should be noted that a VPN does not offer the required flexibility if critical services are encountered during its operation,even when it consists of dial-up connections which are not very fast. The standards of tunneling used by Cisco VPNs are:

IPSec., L2TP and GRE, while in the technologies of encryption may include DES and 3DES.

A VPN consists of a private and secure tunnel between a remote point and a gateway. The nature of "sensitive" and somewhat problematic of some communications makes it possible to use IPSec.

To ensure: 1) Integrity 2) Confidentiality 3) Authentication.

Here's what these services do:

Confidentiality

If something is sent, then the desired person can read it, while other members can they can grasp it but they cannot read it. This is accomplished by encryption algorithms such as

DEC.

Integrity

It is concerned with ensuring that the data transmitted from the source reaches the desired destination

without errors and deformations. This is ensured by hashing algorithms such as MD5.

Authentication

It is about recognizing that the data received is the same as the data sent and that the sender

who claims to have sent them is actually the real sender. This is accomplished by mechanisms such as

is the exchange of digital certificates.

1.3 A general description of the VPN

The Necessity of VPNs

Virtual Private Networks operate on a distributed infrastructure. So, companies can extend their corporate network at a reasonable cost to places where before

the cost of expansion was high. In most international applications and those home VPNs are a more cost-efficient solution to WAN connections. VPNs allow also that a large part of the traffic is concentrated on a single particular connection which necessarily requires potentially large bandwidth. This brings cost savings because many independent circuits and connections that end up in the central corporation are eliminated.

In this context VPNs provide an alternative to building a virtual private network for site-to-site communications or dial-in access. Another relief of these types of private networks it is because they have no maintenance costs. We can also say that VPNs enable increasing productivity within the company.

So instead of using slow dial-in connections, users can communicate with the office their from home using the advantages of the VPN "elevated" over the digital DSL connection (Digital Subscriber Line), or made with a cable modem. Mobile workers can also take advantage of the high-speed Ethernet connections available today many hotels to access corporate resources while traveling. Only cost savings,since you will not have to pay telephone bills for long distance communications,can justify the use of VPNs in these cases.

Finally, companies can use VPN technologies to enable new applications and business process[6]. For example, new business models of Internet commerce and management supply chain have been implemented through the automotive industry through the use of Automated Network Exchanges (ANX), which are based on VPN technology.Summing up, we can cite that the reasons for using a VPN are presented by points e the following:

- ✚ Its cost is very effective because the service provider offers personal support for new hardware and connections used in the WAN.

- ✚ It can be used to expand the existing infrastructure, finding application in the case of the existence of mobile users, remote offices or branches, etc.

VPN also affects the improvement of:

a) Productivity

- b) Communication flexibility
- c) Network management

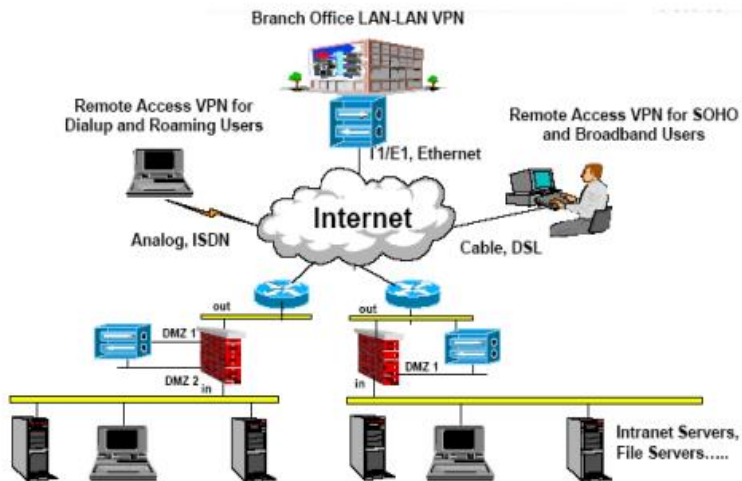


Figure 1. A simple typical VPN model

2. THE BASIC PRINCIPLES ON WHICH VPN IS BASED

The following principles influence almost every VPN design.

2.1 IP Addressing Method

In any large IP network, to realize a VPN as efficient and successful as possible choose the most suitable IP address because it can be considered critical.

It is recommended that remote sites use a large network subnet to allow summarizing so that manageability, scalability and performance also increase.

If local networks are themselves comprehensible then cryptographic ACLs of used will have a single line for each local network and preferably a single entry.

For example, a remote site network 10.1.1.0/24 is resumable to the network of big 10.0.0.0/8. If any host on the 10.1.1.0/24 subnet needs to connect to any subnet other on the 10.0.0.0 network through the hub a single ACL entry is sufficient.

If the remote network cannot be aggregated into a larger network, then the on-site is required remote An ACL entry for each local network connected to the remote network. Increase ACL entries it slows down performance, increases problems, and makes scalability difficult as a result of ACL exchanges of remote sites constantly for their adaptation to the new networks located in the central part. Each ACL entry builds a split tunnel (two SAs of IPSec). A convenient subnet makes for simplified core configurations spoke-to-spoke communication is enabled and a smaller number of tunnels are used in all devices to classify traffic flows[7]. This type of addressing also significantly affects many features of VPNs including remote management connectivity of nested networks.

2.2 Intrusion detection, network access control, trust, and VPNs

When considering the deployment of VPN technology, it should be remembered that doing so such a thing expands the security perimeter of the network to include some areas that are not considered with high security. This includes:

- ✚ Employees' houses
- ✚ Airports
- ✚ Hotels
- ✚ Internet cafes

One of the first questions an organization must answer is who the trust level is

about the VPN technology itself and the surrounding applications and hardware that will use it. The best way to reach a conclusion is by answering this question: Do you want to organization to trust a remote individual or site accessing a VPN as much as you would local employees and sites connected via a WAN link? If you answer this question with "yes", then you should distribute the VPN technology in the same way as the connections are distributed WAN and modems today. However due to the position of Cisco and most of the its customers, VPN links should be trusted less. For this reason, IPSec VPNs often are created with access control and intrusion detection layers around them [5].

Although IPSec with 3DES is very secure, the human potential to store keys in the unsafe way and misconfigure equipment creates enough uncertainty to warrant additional security; not to mention old laptops or trojans.

3. REMOTE USER DESIGNS

There are four options for securing remote users' VPN connections to sites

corporation. Remote connections apply to both mobile and mobile workers

home-office workers. The main purpose of this design is to provide links from the site to distance to corporate headquarters through any means such as the Internet. Four are valid following options:

- ✚ Option with software access – remote user with a software VPN client and personal firewall software on PC.
- ✚ Remote-site firewall option – remote site protected with a dedicated firewall that provides firewalling and IPSec VPN connections to corporate headquarters. WAN connection provided through an ISP, if you own broadband access equipment (ie DSL or cable modem)
- ✚ Hardware VPN client option – remote sites that use hardware VPN client dedicated, which provides IPSec VPN connections to corporate headquarters; WAN connection provided through an ISP, if you have broadband access equipment.
- ✚ Remote-site router option – the remote site uses a router that provides firewalling and IPSec VPN connections to corporate headquarters. The router can provide access broadband directly or go through an ISP, if you own access equipment broadband.

3.1 Main VPN Equipment

- ✚ Broadband access equipment – provides access to the broadband network (DSL, cable, etc.)[8]
- ✚ VPN firewall – provides secure end-to-end encrypted tunnels between remote sites and corporate headquarters; provides protection at the resource network layer remote site and full traffic filtering.
- ✚ Personal firewall software – provides device-level protection for individual PCs.
- ✚ VPN router option with firewall – provides secure end-to-end encrypted tunnels between individual PCs and corporate headquarters.
- ✚ VPN hardware client – provides secure end-to-end encrypted tunnels.

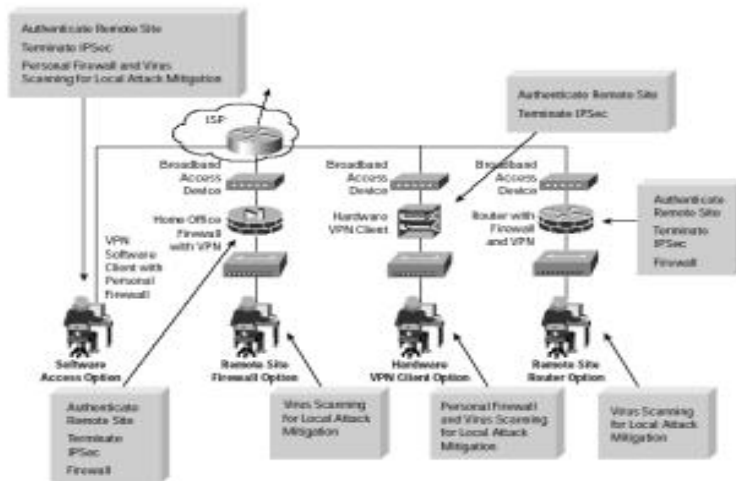


Figure 2. Main VPN devices

4. HOW IPSEC WORKS AND ITS ARCHITECTURE

4.1 PRESENTATION

The term IPsec (IP Security Protocol) refers to a set of mechanisms designed for it protect traffic at the IP level (IPv4 or IPv6). The security services provided by IPsec are integrity, verification of data origin, confidentiality and protection against packet replay. These services are provided at the network layer, thus providing protection for IP and for all protocols of the above layers. In IPv4 IPsec is optional while in IPv6 it is mandatory for every implementation. When IPv6 becomes widespread I used, it will be possible for any user who wants to use the security functions of use IPsec. Meanwhile we have to rely on IPsec implementations under IPv4.

4.1.1 Structure of IPsec

Exchanges on TCP networks can be secured in many ways. Routes vary depending on layer to which they belong, for example: application layer (e.g. encrypted mail), layer e transport (TLS/SSL, SSH...) or in the physical layer (black boxes encrypt all data that pass through a link). IPsec aims to secure exchanges at the network layer

AH and ESP mechanisms.

These objectives are achieved through the use of two security mechanisms. AH and ESP protocols which are added to the traditional processing IP.

Authentication Header (AH) is designed to ensure the integrity and authenticity of IP datagrams, without data encryption (ie no confidentiality)

The principle of AH is to add an additional field to the traditional IP datagram; this field does enable the receiver to check the authenticity of the data contained in the datagram.

✚ Encapsulating Security Payload (ESP) is primarily designed to provide confidentiality, but can also ensure data authenticity.

The principle of ESP is to generate, from a traditional IP datagram, a new datagram in which the original data and hash are encrypted.

These mechanisms can be applied separately or in combination with each other provided the desired security services.

Security Association (SA) concept[9].

The mechanisms mentioned above use cryptography, and therefore require some parameters (encryption algorithms used, keys, mechanisms chosen...) with which members who communicate must agree. In order to manage these parameters, IPsec uses the Security Association (SA) concept. A security association is a one-way "link" that provides security services the traffic it carries. We can also refer to it as a set of parameters that describe how a communication will be provided. Since an SA is unidirectional, to protect a typical two-way communication requires two SAs, one for each direction. Security services are available through the use of AH or ESP. If both are used in traffic, then two or more.

SAs are created to protect traffic; they are called an SA bundle.

Each SA is uniquely identified by the following triplet:

- ✚ Destination address of the packet
- ✚ Security protocol identifier (AH or ESP)
- ✚ Safety Parameter Index (SPI)

An SPI is a block of 32 bits which is transmitted in the clear in the header of each packet exchanged; the receiver chooses it. IPsec stores all active SAs in a database called Security Association Database (SAD). It contains all the parameters associated with each SA and is consulted to know how to handle a sent or received packet.

Management of keys and SAs

Key management for IPsec is linked to various mechanisms through SAs. How to can be configured manually when the situation is simple, but the general rule is to a specific protocol is used, which allows a dynamic negotiation of SAs and in particular session key exchange. In addition, IPv6 is not intended to support the management of in-band keys, where data related to key management would be transported by use a separate IPv6 header. Instead, an out-of-band key management system is used, where data related to key management is transported by a protocol of layers above such as UDP or TCP.

This allows a clear distinction of the key management mechanism from other key management mechanisms safety. The protocol to negotiate SAs developed for IPsec is the Internet Security Association and Key Management Protocol" (ISAKMP). Actually ISAKMP is not used alone: it is one general structure which allows the use of different protocols for the exchange of keys. Within the IPsec standardization framework, ISAKMP is associated with a part of the

SKEME and Oakley protocols resulting in a protocol called IKE (Internet Key exchange)

Security policies

The protections provided by IPsec are based on the choice of line of action determined by SPD. This database is set up and maintained by a system administrator or an application installed by the user. This makes it possible to determine, for each package, whether they will be given to you IPsec security services, will be dropped or allowed to pass IPsec.

The SPD contains an ordered list of rules, where each rule is identified by one or several selectors which define the set of IP traffic affected by this rule.

The potential selectors are the amount of information available in the network and transport layer header.

5. EXAMPLE VPN IMPLEMENTATION ON LINUX

In this section we will explain step by step how to set up a VPN system. At first you will let's talk about the server, then we'll move on to the client.

5.1 Planning

Let's imagine we have a company named mycompany.com. In the central offices, yes we use the reserved network 192.168.0.0, dividing class B into 256 class C networks to allowed routing. We have also built two remote offices, and we want to add them on our network. We also want to allow employees who work from home to be able to use their DSL and cable modem instead of dialup connections. Before we start we will have to plan things a little [10].

We decide to give each remote office a Class C address to allow them to expand later if they wish. So we reserve the networks 192.168.10.0 and 192.168.11.0. also for users from home we have enough numbers and we won't have to mask them VPN server side. Each client gets its own internal IP. So we need to reserve one another class C, say 192.168.40.0. What we need now is to add these addresses to our router.

Let's imagine that our company owns a small Cisco 192.168.254.254 that holds all traffic through OC1. We simply define the routes in Cisco so that the traffic directed to these reserved networks goes to the VPN server (192.168.40.254). We place the VPN server on the network of home users for reasons that will become clear later. The server's external interface we'll call it vpn.mycompany.com and the internal interface vpn-internal.mycompany.com.

As for external numbers, we will not have to recognize them explicitly.

5.2 Collection of tools



We will need some pieces of software which we will then install

For Server:

- pppd (version 2.3 or greater)

- ssh (version 1.2.26 or higher)

For the customer:

-  Pppd (same version as server)
-  Ex

5.3 Server: Building the kernel

Before we begin we will need to rebuild the kernel for the server. We have to make sure that

the options below are enabled in connection with our networking and anything else that may us

is needed.

For 2.0 kernels:

- CONFIG_FIREWALL
- CONFIG_IP_FORWARD
- CONFIG_IP_FIREWALL
- CONFIG_IP_ROUTER
- CONFIG_PPP

For 2.2 kernels:

- CONFIG_FIREWALL
- CONFIG_IP_ADVANCED_ROUTER
- CONFIG_IP_FIREWALL
- CONFIG_IP_ROUTER
- CONFIG_PPP

5.4 Server: Networking Configuration

If the server has only one network card, it is good to install another one and be done network reconnection. The best way to keep the network private is by having its own connections.

So if we have two network cards we will need to know how to configure both of them. Will use eth0 for the external interface and eth1 for the internal interface.

Configuring interfaces

The internal interface of the server is 192.168.40.454 and we need to configure this interface.

For 2.0 kernels we use:

```
# /sbin/ifconfig eth1 192.168.40.254 netmask 255.255.255.0 broadcast 192.168.40.255
```

```
# /sbin/route add -net 192.168.40.0 netmask 255.255.255.0 dev eth1
```

For 2.2 kernels we use:

```
# /sbin/ifconfig eth1 192.168.40.254 netmask 255.255.255.0 broadcast 192.168.40.255
```

This fixes both interfaces. Now we can communicate with devices on both local networks that are

connected to the server.

Determination of roads

Although we can communicate with devices on both local networks, we cannot communicate with the rest of the internal network. For this we need a few more lines of code. In the way that to reach devices on other subnets, we need to have a path that tells traffic to go to

Cisco router. This line is:

```
# /sbin/route add -net 192.168.0.0 gw 192.168.254.254 netmask 255.255.0.0 dev eth1
```

This line tells the kernel that all traffic directed to the 192.168.0.0 network must come from eth1. Traffic for our local network goes where it is supposed to because the routing tables are sorted according to the size of the mask. If we had other internal networks in our network, for everyone network, we would have a line like the one above.

6. CONCLUSION

Basically a VPN is a private network that uses a public network (generally the Internet) for connect remote sites or users to each other. Instead of using a real connection of dedicated, a VPN uses "virtual" connections routed to the Internet from the company's private network to site or remote worker.

A well-built VPN brings many benefits to the company. For example, it can:

- ✚ To increase the geographical distance of connections
- ✚ Improves security
- ✚ Reduces operating cost compared to traditional WANs
- ✚ Reduces transportation time and cost for remote users
- ✚ Productivity improves
- ✚ Network topology is simplified
- ✚ Provides global networking opportunities
- ✚ Provides telecommuting opportunities
- ✚ It offers the possibility to adapt to the broadband connection of the networks

A well-designed VPN should include:

- ✚ Security
- ✚ Reliability
- ✚ Scalability
- ✚ Network management
- ✚ Management of security policies

There are two general types of VPNs.

1) Remote access VPNs, otherwise called virtual private dial-up networks (VPDN), is a user-LAN connection used by a company that has employees who need to connect to the corporate private network from remote locations.

A corporation that wants to create a large remote access VPN network will use an enterprise service provider (ESP).

2) ESP frames a network access server (Network Access Server (NAS)) and equips it

remote users with client software for their computers.

3) The telecommuters then dial a toll-free phone number to reach the NAS and use VPN client software to access the corporate network. Access VPNs to distance provide secure encrypted connections between a company's private network and remote users through a service provider[11].

4) Site-to-site VPNs. Using dedicated hardware and large-scale encryption, a companies can connect multiple sites over a public network such as the Internet. VPNs site-to-site can be of one of two types:

- ✚ Intranet VPN – if a company has one or several locations which they wish to connect

on a private network, they can create an intranet VPN to connect LAN to LAN.

- ✚ VPN extranet – when a company has close relationships with another company (eg.

a partner, supplier or customer), they can build a VPN extranet that connects the two LANs, and that allows different companies to work in a common environment.

More about this source textSource text required for additional translation information VPNs rely on creating a tunnel to create a private network that spans the Internet.

In general, tunneling is the process of placing a packet inside another another packet and sending it to the network. The external packet protocol is understood by the network and by the two endpoints, called tunnel interfaces, where packets enter and exit the network.

Tunneling requires three different protocols:

- ✚ Transport protocol – the protocol used by the network over which information travels

- ✚ Encapsulation protocol – protocols (GRE, IPSec, PPTP, L2TP) which encapsulate the the original data.

- ✚ Traveler protocol – the original data (IPX, NetBeui, IP) that is carried.

Tunneling is of great use in VPNs For example, a packet that uses

a protocol that is not supported on the Internet, (such as NetBeui), inside an IP packet and send it safely online. Or you can deploy a package that uses a private IP address (non-routable), inside a packet that uses a unique IP address to extend a private network on the Internet.

In remote access VPNs, tunneling is performed using PPP. As part of the TCP/IP suite, PPP is the carrier for other IP protocols when a host computer and a distant system. L2F, PPTP, L2TP protocols are built using the basic structure of PPP and are used by remote access VPNs.

L2TP can be used as a tunneling protocol for site-to-site and access VPNs

distance. Depending on the type of VPN (remote access or site-to-site) we will need several parts components to build a VPN. These can be:

- ✚ Client software for each remote user
- ✚ Dedicated hardware such as a VPN concentrator or dedicated PIX firewall
- ✚ Dedicated VPN server for dial-up services
- ✚ NAS (network access server) used by the service provider for user access to distance
- ✚ VPN network and security policy management center.

7. LITERATURE

[1] Drapergil, G., Lashkari, A.H., Saiful, M., Mamun, I., Ghorbani, A. A Characterization of encrypted and VPN traffic using time-related features. In: Proceedings of the 2nd International Conference on Information Systems Security And Privacy (ICISSP), pp. 407–414, 2016.

[2] Halpern J., Convery S., Saville R., Safe VPN - IPsec Virtual Private Network in Depth, Cisco Systems, 2001 [3] Liyanage, M., GurtoV, A.: Secured VPN models for LTE backhaul networks. In: 2012 IEEE Vehicular Technology Conference (VTC Fall), 2015, pp. 1–5.

[4] Xiaomei B., Fuli Z., Dan W., The application of VPN technology in the university's library IEEE Xplore, 27-29 May 2011.

[5] Jaha, A.A., Ben Shatwan, F., Ashibani, M. Proper virtual private network (VPN) solution. In: Proceedings of 2nd International Conference on Next Generation Mobile Applications, Services, and Technologies, NGMAST 2008, pp. 309–314, 2008.

- [6] Nawej, M.C., Technologiae, M.: Evaluation of virtual private network impact on network performance, 2016.
- [7] Azhar, M.A., Saudi, M.M., Ahmad, A., Bakar, A.A.: Detection of social media exploitation via SMS and Camera. *IJIM* 13(4), 61–78, 2019.
- [8] Busschbach, P.B. Toward QoS-capable virtual private networks. *Bell Labs Tech. J.* 3(4), 161–175, 1998. [9] Manvi, S.S., Tangade, S. A survey on authentication schemes in VANETs for secured communication. *Veh. Commun.*, 2017.
- [10] Odusami, M., Misra, S., Adetiba, E., Abayomi-Alli, O., Damasevicius, R., Ahuja, R.: An improved model for alleviating layer seven distributed denial of service intrusion on webserver. *J. Phys.: Conf. Ser.* 1235(1), 012020, 2019.
- [11] Deshmukh, D., Iyer, B.: Design of IPSec virtual private network for remote access. In: 2017 International Conference on Computing, Communication and Automation (ICCCA), pp. 716–719. IEEE, 2017.