Ilona Pukelyte

The computer network security implementation in an enterprise project

Bachelor's thesis

Engineering

Information Technology

2021

South-Eastern Finland
University of Applied Sciences

Author (authors)	Degree title	Time
Ilona Pukelyte	Bachelor of Engineering	May 2021

Thesis title

The computer network security implementation in an enterprise project

69 pages
14 pages of appendices

Supervisor
Matti Juutilainen

Abstract
The main purpose of this thesis is to investigate existing information security technologies and implement these elements into a computer network. The project has two main parts: research and implementation. Each part has its own objectives.

The objectives in the research part consisted of determining what modern technologies exists to enhance a network security and concluding what kind of technology should be installed in the implementation part. The objectives in the implementation part consisted of creating tables with data that could be used, creating a simulation environment, which would somewhat represent the real world, deciding between using a graphic user interface and a command line interface as well as using commands that could be executed to install the chosen security tool. However, it is important to note that while the chosen commands are used for a specific device, yet the technologies can be implemented anywhere where they meet the hardware and software requirements as their working principle stays the same.

Qualitative methods were used to obtain specific information about technologies and security measures. The data was collected by using books and official documentation. The thesis is formatted to be used as a technology installation guide.

All things considered the thesis could be marked as complete because data transmission with security means were analyzed and implemented in a designed environment with a set of parameters corresponding to created specifications.

Keywords
a virtual private network, information security, user groups, security design, authentication

Table of contents

1 INTRODUCTION

Time has always been significant for people, not only as a part of the lifecycle but also in business. Even one famous 18th century's American scientist, politic and inventor, Benjamin Franklin, said: "Time is money". Within time, a person can collect useful information, which later can be used accordingly— what to buy, where to invest, what and how to create, etc.

For a long period of time, collected information was saved in hand—written (even drawn) sources. Wanting to expose the information to the public it needed to be delivered from person to person through speech or written copies, which were made by hand.

With genius people's help new ways emerged and today a well—known fact is— the appearance of the modern technologies eased the data capturing and sharing activity. As computers and networks appeared, processes, such as information capturing and sharing were alleviated of the old ways burden.

Enterprises were quick to integrate modern technologies into their workplace. As companies were rapidly expanding and new businesses were quickly appearing, additional work features were created. These new characteristics consisted of decreasing the duration spent on the tasks as much as possible and increase of the work quality.

As the collected information's value grew, a new danger was presented. Modern technologies in enterprise not only maximized the quality of work and reduced the duration of it, they also created a new burden of breached security. The violated security created a great probability of unauthorized access to the data that would lead into illegal use, data disclosure, deletion, modification, corruption, or it even being shared with competitors.

Because most of the times the security is being invaded by using modern technologies, few solutions to block the attacks were developed.

One solution to prevent unauthorized access to data would be to create an intra-net— a local communication network. However, that does not solve everything because additional problems arise— what to do if enterprise's departments are geographically scattered around the city or even other countries or continents? How to ensure that the shared information would not be unlawfully accessed? Physical solutions, such as laying internet cables, would require enormous re-sources, which smaller business could not afford.

It is hard to evaluate which modern technologies are going to prevail in the future, and because of that, it is very important to solve this problem with existing solu-tions.

While there are few solutions to this problem, one solution differs from them all. The solution is called a virtual private network technology. A virtual private net-work is local networks or separate nodes conjugated to one by using a global net-work. With this technology secure data transmission tunnels are created, data is encrypted, and authentication of a user is required. One of the biggest strengths of this technology is that it does not require supplementary physical cable lines— virtualization is the key.

A virtual private network function can be declared as a service, which makes it possible to create closed user groups and authorize communication between user belonging to the same group (Perez 2014).

Because of its characteristic to connect separate nodes to single one, creating a virtual local network, this service is very useful to companies, which maintain other companies‘ information technology sector.

The virtual private network installation is required in a company called Pczona. This company co—operates with other companies and contributes to their infor-mation technology (later referred to as IT) infrastructure maintenance. Pczona handles software and hardware of computers and other devices, even maintains

network on a basic level. Because this company usually carries out their activities remotely and has access to other companies' sensitive and confidential information, it is required that the remote access would be secure.

Therefore, the main goal of this project is to conclude why the virtual private network should be considered as having the best data protection, access control and network isolation, characteristics and why it should be chosen for security's assurance. The another aim of this thesis is to practically create a virtual private network in a chosen environment, as in intention to use it for Pczona and other companies.

Other objectives:

1. Determine what technologies and practices are used to connect to another network remotely; what protocols are involved; what safety procedures these technologies are using— authentication and encryption;
2. Come to conclusion of what remote connectivity technology is best for the company;
3. Analyze company's hardware and decide if it is usable for the project or a new hardware is required;
4. Implement the best technology.

2 RESEARCH

In this part objects, such as determined objectives, remote access technologies, encryption and authentication methods, are analyzed. Also, after taking everything into account an overall opinion is formed.

The main network objective could be simplified into data exchange between a sender and a receiver. This can be seen in Figure 1. The sent information must cross from one local area network (later referred to as LAN), where the sender is found, to another LAN, where the receiver is located. Then, sent data needs to travel from one point to another through wide area networks (later referred to as WAN).

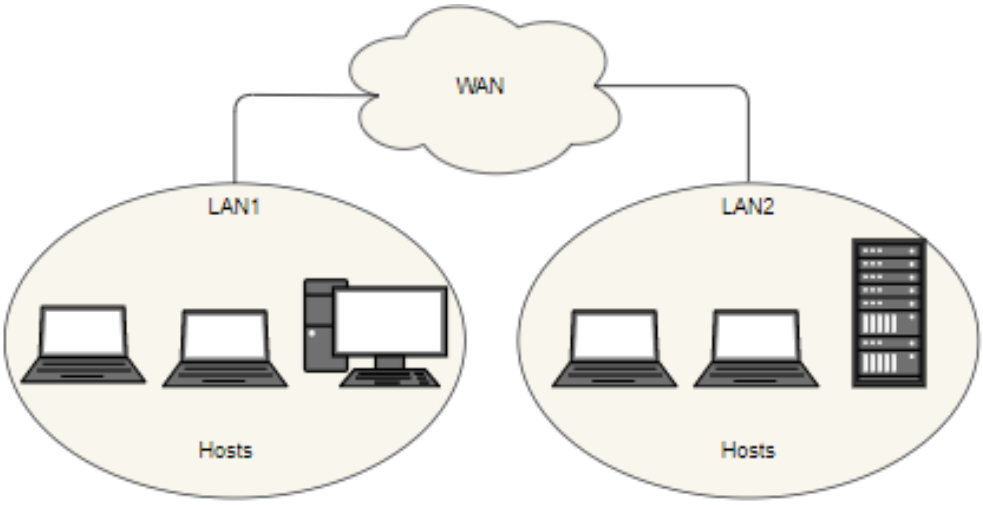

Figure 1 Abstract network model

Often higher—profile enterprises have departments and subdivisions that are geographically distant from the headquarters and other main offices. This leads to all branches of the enterprises to have different LANs. The separate computer network then requires large amounts of resources: separate databases and mail servers, different scanning and network equipment. Also, under those circumstances, the workload of the computer network administrator is increased because a separate network like this is hard to supervise and maintain, especially remotely.

Relevant problems appear when enterprise want to expand— for example, a freshly appeared branch requires additional resources: hardware, software, human resources. In addition to the problems listed above, there are also other areas of concern: confidentiality and data security.

We can see a simple model in the picture below (referring to Figure 2), which shows us the headquarter with geographically remote divisions. Each depicted building has its own LAN, and with the main head office, these units communicate through a global network. In the picture the plain arrows represent not only that the data is being transmitted but, also, that it is being shared without additional security measures. In this context, security measures mean encryption.

This case also raises a question— will the transmitted data reach the destination safely? Or the data will be modified, spoofed, looked over by unauthorized people and machines, while traveling to its destination. What will be the cost of the lost information?

While not all sent information contains confidential data or information that could potentially be harmful to the company, should the data still not be protected to maintain the privacy safe? Especially the private workers lives, their messages and activities, while they reach out to communicate inside the company's network.

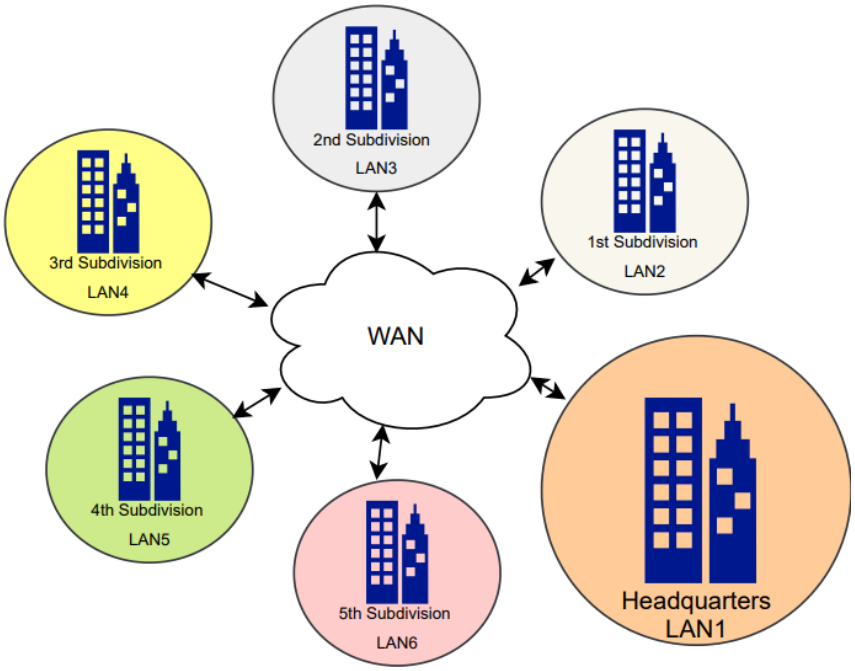

Figure 2 LANs being separated by Internet

While it comes to enterprises' board directors and owners to decide, companies should determine if the data security is their biggest priority because in the shown network an unauthorized third parties could breach the security and see the sent packets' information and modify them.

If companies decide that their business needs security upgrade, one of the methods how to protect their network could be to operate and transmit data only in the same LAN.

There are few technologies, which allows a user, or a group of users, virtually appear in the needed private network(by remotely connecting to another LAN and sending information from there). These technologies can be diverted into two categories: individual remote users accessing another LAN and group of users connecting to another LAN.

Individual remote users connecting to another LAN could be described as a client entering another LAN with one device while using technologies, such as: Telnet, SSH, remote desktop service, virtual private network.

Meanwhile group of users connecting to another LAN could be described as a group of clients (devices) entering another LAN without additional configuration for an individual device. With this method there is no need to configure, for example, ten computers' parameters mechanically for them to access another LAN. This method can work by using virtual private network and laying down cables of peer—to—peer private telecommunication network.

These technologies not only let separate enterprise private network to share a one, common, network, but it also protects data from being leaked, modified and deleted.
However, it is necessary to consider not only the main aspects, such as encryption, third—party intervention and information modification, user identification but also to answer additional questions:

1) Will a user with a low level of computer literacy be able to use the technology;
2) whether the technology will require large amounts of resources (both software and hardware);
3) whether a large amount of money will be spent to introduce the technology to the computer network.

Hence, the main topics of this bachelor's thesis are to find out what measures could be used to connect separate computer networks via Internet, into one organization network and analyze the chosen technology's reliability and security standards.

One of the most important topics— how do those measures assure the network security. How do they protect the sent information inside the packets? How do they authenticate the packets were received by authorized user? How do they work in general?

2.1 Remote Desktop Service

Few tools let users access and handle services over a network, often they have security measures installed to let them operate over an unsecured network. One of these tools is called Remote desktop service (later referred to as RDS). This tool is a platform, which lets clients reach a server and software with remote connection. The principle of it could be described simply as output devices sending graphic transmission signals from a remote server to a client, while the client sends input devices signals to the remote server. This virtualization environment lets users fully control what information the user can reach— desktop or other remote software. (Montoya, et al. 2017)

This technology was implemented by Microsoft[1] and is accessible to any remote client machine, which supports Remote Desktop Protocol (later referred to as RDP). RDP was developed to let users connect to other computers through network connection with provided graphical interface.. It has three client components— Windows Remote Assistance (later referred as WRA), Remote Desktop Connection (later referred as RDC), Fast User Switching. Both WRA and RDC utilities allow users to take control of a remote computer through the internet. While connected, the user has a full access to any of their application, files, and servers.

[1] American technology company founded by Bill Gates and Paul Allen

Connecting with RDP can be done by doing RDP Connection Sequence— it lets client and server exchange settings and specify common options. It can be divided into ten phases: connection initiation, basic settings exchange, channel connection, RDP security commencement, secure setting exchange, optional connect—time auto—detection, licensing, optional multitransport bootstrapping[2], capabilities exchange, connection finalization.

Also, it is worth to mention that when enhanced security is chosen, two approaches appear: negotiation—based and direct.

When negotiation—based approach is being used, a client proposes security package it supports, while the server selects them. After a handshake message, security packages are exchanged, and traffic is secured by those packages.

When direct approach is being used, decided security protocol is immediately executed prior to the traffic exchange, resulting in RDP traffic being secure straight away. (Zhang 2021)

2.2 Telnet and Secure Shell

Other remote access tool is called Telnet. Telnet is an old technology, which let users access devices through the network by creating TCP[3] connection, that is used to transmit data with Telnet information. There are three principles of its work process: when connection is established at the first time, each end devices

[2] Bootstrapping is a process that automatically loads and executes commands.

[3] The Transmission Control Protocol is a transport protocol which ensures reliable transmission of packets.

must work on Network Virtual Terminal[4]; an agreement on the negotiation options[5] is made; a symmetric view of the terminal and its process is created[6] (Postel, J.; Reynolds, J.; ISI 1983)

However, this technology does not have any safety mechanisms and the transmitted information is transparent. Because of that, this technology was changed with Secure shell (later referred to as SSH).

An author has stated that SSH has few meanings, such as— a network protocol, where information is encrypted; a command interface; client\ server software (Dwivedi 2004).

While SSH can provide users with access to other devices through the internet, its main purpose is to protect TCP connection. It does that by having three main protocols:

SSH—TRANS transportation protocol, SSH—USERAUTH protocol and SSH—CONNECT protocol. The protocols are usually transmitted through TCP/UDP port 22. (T. Ylonen, SSH Communications Security Corp, C. Lonvick, Ed., Cisco Systems, Inc. 2006a)

SSH—TRANS protocol is used for a server authentication and data protection implementation (that involves compression algorithms and keys). When a client and a server start exchanging messages, this protocol encapsulates the packets and adds its own header, which contains the information of packet length, padding length, padding field, Message Authentication Code (later referred to as MAC) and Sequence Number (later referred to as SN).

---

[4] Network Virtual Terminal makes a telnet program map incoming codes so they could be executed in the needed device.

[5] A request for additional services available within network virtual terminal.

[6] The view lets avoid loops that consists of seeing incoming commands not as acknowledgment but as a request.

To hinder unauthorized third parties, additional information is added in messages' beginning, middle and the end, before the encryption, with the hope that third—party would encounter as much difficulty as possible while trying to guess the data length.

Encryption is applied to the data before the encapsulation, packet length, padding and its length fields.

The SSH—TRANS operating principle can be described as this: usually, after an exchange of an identification message (between the client and the server), follows negotiation of algorithms, and only after deciding which algorithms will be used, the keys are exchanged.

After keys are swapped, the two end points start the generated master key exchange, then the data is encapsulated, encrypted and authenticated. (T. Ylonen SSH Communications Security Corp C. Lonvick, Ed. Cisco Systems, Inc. 2006b)

Meanwhile, SSH—USERAUTH protocol is used to authenticate a client— a client submits their identification to the server, then the server checks the received information— it responds with an error message if the information is not correct, however, it responds with success message if the authentication is successful.

2.3 Multiprotocol Label Switching

Multiprotocol label switching (later referred to as MPLS) is a protocol that uses encapsulation and label methods to transmit the information. This technology functions by forwarding first time sent packets to specific equivalence class, which puts labels on the packets. (Rosen and Rekhter 1999)Later, the packet goes from one node to another. This technique is used to avoid complex inspection and speed up information transfer flow. (Ghein 2007)

Nevertheless, MPLS itself does not provide any encryption method because of that one way for it to provide any protection is to use virtual private network characteristics This combination is called MPLS virtual private network. It uses virtual private network's encrypted tunnels to ensure that the packets are being forwarded to correct VPN sites. However, this technology is dangerous because users lose the visibility of core networks and this could lead into additional routers being inserted by malicious servers. (Behringer and Morrow 2005)

2.4 Virtual private network

The picture below (referring to Figure 3) abstractly portrays information transmission without additional safety measures. It works well if we imagine a situation—a worker, from a company called "X", must travel aboard for a conference. The worker wants to spend their free time working on the remain parts of their work project. The transport, the worker is using, provides free access to Wi—Fi[7].

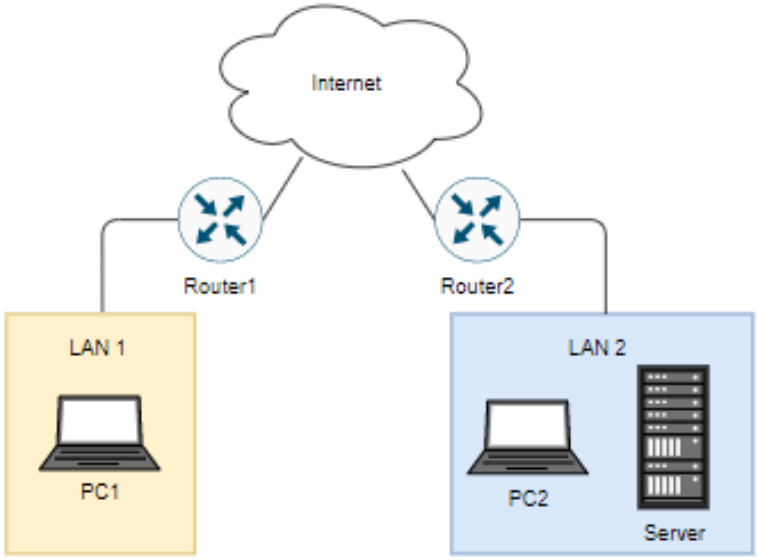

Figure 3 Abstract data transmission without safety precocious

[7] Wi—Fi— wireless network protocol, which is based on the IEEE 802.11 family standards.

The documents, the worker needs, are stored in organization's server. The worker can easily access the server while providing their authentication and continue to work. The employee has used provided wireless network and downloaded the needed documents to their laptop with file transfer protocol[9]

In the same transportation vehicle a hacker was scanning the packets of the free access wireless network and with whatever purpose the hacker decided to sniff the workers packets. Because the worker was not provided enough knowledge of safety and downloaded a confidential document without any security measures, suspicious intends having experienced hacker could have obtained the packet's information and found the location from where it was sent. The hacker also could have injected the packet with their own malicious information and masked it as responding packet.

We can imagine the same situation happening again, however, this time, the company was worried with their network security and installed an additional safety technology— a virtual private network (later referred to as VPN). The worker accessed the public Wi—Fi but, also, they have used the VPN. With a VPN they easily accessed the encrypted tunnel and their computer became a part of company's domain— all security existing in the company's zone was applied to the worker's Internet connection.

The unauthorized person, who was trying to see the exchanging data between the server and the client, could not access the packet's information because, as we can see in the picture below (referring to Figure 4), an encrypted tunnel, through which data travelled, was created.

Now, the worker could securely download the needed documents into their device and continue their work without any problems regardless of IT safety(Dale Liu; Syngress; Stephanie Millers; Mark Lucas; Abhishek Singh; Jennifer Davis 2006)

[9] File Transfer Protocol is a network protocol, which lets transfer files from a server to a client.

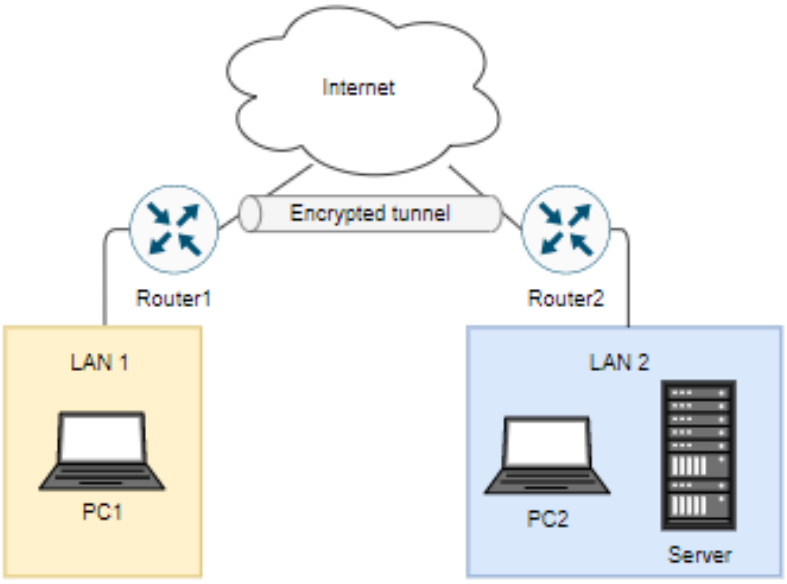

Figure 4 Created encrypted tunnel between Router1 and Router2

Delving deeper into a VPN technology clarifies why it ensures the safety so perfectly. First, a VPN is a technology that creates a private network from separate local area networks over a public network by using virtual connections instead of dedicated physical connections. Before the data is sent, from a VPN client to a VPN server[10], through the tunnel, it goes over encapsulation and encryption processes. Even though the data is modified it still can be confirmed as valid and can be normally routed— the packet's destination is hidden, yet the VPN server's address comes up to receive the packet. When the packet is delivered to the VPN server, only the server can use a symmetrical key to decrypt contents of the packet and deliver it to the final destination.

This provides a conclusion that what makes a VPN technology safe is two points: tunnel protocol (through which data travels) and cryptographic authentication.

The general VPN categories could be divided into four parts (Andrea 2014):

1) A Policy—Based VPN;
2) a Route—Based VPN;
3) a Secure Socket Layer—Based VPN;
4) a Dynamic Multiport VPN.

[10] A VPN client is an VPN connection initiator, while a VPN server is connection acceptor.

The Policy—Based VPN could be defined as a VPN type which uses defined policies, such as Access Control List. The flowing traffic is encapsulated and encrypted accordingly to the defined polices. This type can be divided into two categories, one category being: Site—to—Site VPN and Hub and Spoke VPN; another category being: Client Remote Access VPN. One of the advantages of this type is that it has strong security and it is supported by most network devices.

Secondly, there is a Route—Based VPN type which does not need policies to dictate what traffic enters the VPN server. It relies on tunnel interfaces and static, and dynamic, routes. It is based on a virtual tunnel interface (known as VTI) and Generic Routing Encapsulation (later referred to as GRE). Nevertheless, this VPN type is only supported by Cisco[11] routers. Another minus of this type is that VTI and GRE cannot provide security on their own and must be combined with Internet Protocol Security.

Then, there is a Secure Socket Layer (later referred to as SSL)—Based VPN which lets remote users connect to another network through Web Browser while using SSL encryption. The clientless type has limited functions as the client can only access internal Web applications, Email servers, etc. Despite that, if users want to have full access, the user needs to download a client application and install it into their computer. The main drawbacks of this type are that it leads to poor performance under high load and that when a user needs full control, they need to manually download Java[12] or ActiveX[13] file and install it, this could be problem if a firewall is blocking them.

[11] Cisco Systems is United States company that bases their activity on IT services and products, especially network hardware. All their products are better known by Cisco.

[12] Java is object—oriented programming language.

[13] ActiveX is a software framework from Microsoft (MSFT)

Lastly, there is a Dynamic Multiport VPN type that does not require traffic to pass through a VPN server or a router and it uses Multipoint GRE[14] and Internet Protocol Security protection. One of the main disadvantages of this technology is that it is only supported on Cisco Routers.

In essence, a Policy—Based VPN type is best to use when there is a need to create VPNs between devices that have different vendors; a Route—Based VPN types should be used when there is a need for a VPN to support Internet protocol (later referred to as IP) unicast, multicast and non—IP protocols; a SSL based VPN is best to use with few users and low—medium network activity; a Dynamic Multiport VPN is best to use with huge VPN topologies.

The VPN has three interesting connection types for individual users and group of users (Battu 2014). Illustrations below will help to describe these types. The VPN could be parted into three types: *Remote, Intranet, Extranet*

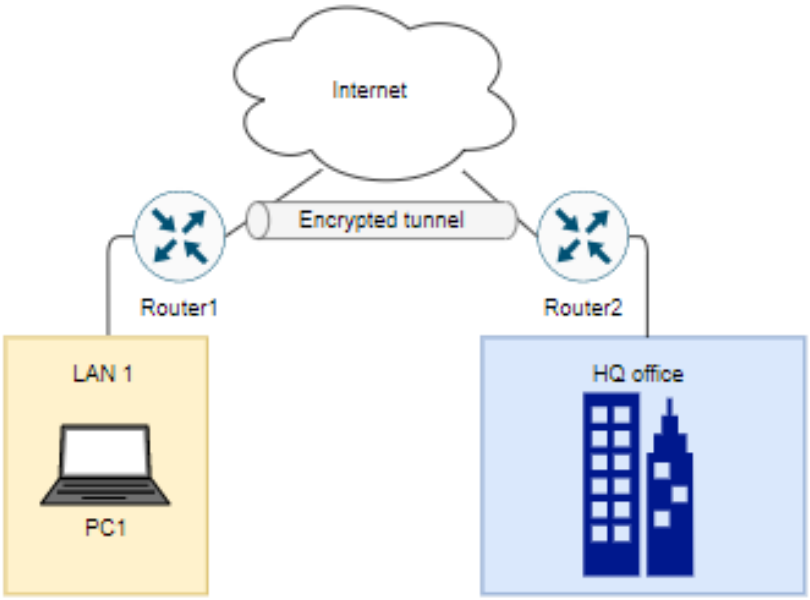

Figure 5 Remote VPN

The Figure 5 portrays a remote VPN type which lets an individual user reach a private network by providing a password (there is a possibility for device ID to be recognized too).

[14] This protocol allows one node to communicate with many nodes.

The Figure 6 depicts an intranet VPN type that lets connect company's branches and subsidiary companies while they are geographically detached. This type allows not only one user to use a VPN technology, but it also lets a group of users, who exists in the same LAN, to connect. Also, it is worth to mention that this type does not require individual configurations for all devices.

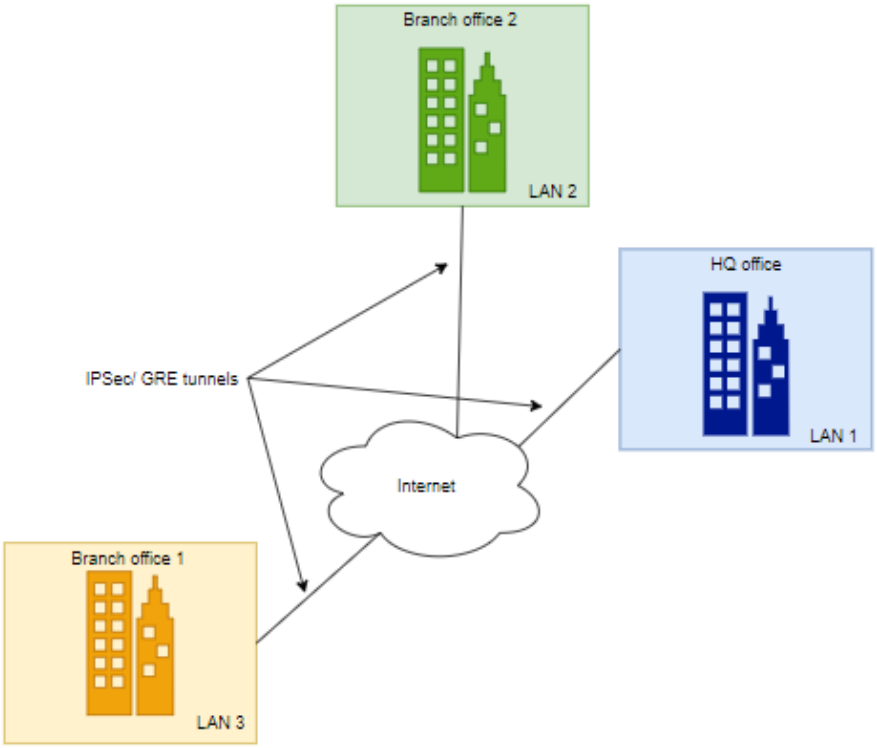

Figure 6 Intranet VPN

The Figure 7 represents an extranet VPN type. This type is very similar to the intranet type, the only difference is that it is made with LANs that only need the secure tunnel. This means that with this type neither of LANs can access each other intranets because it is prohibited.

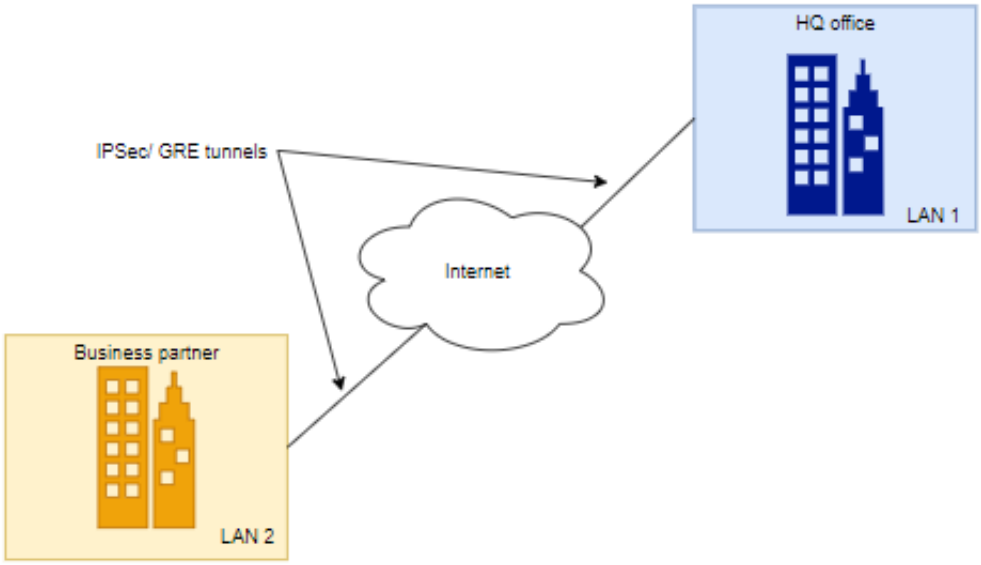

Figure 7 Extranet VPN

Additionally, to the VPN types there are different protocols devoted to different instances. In 1994 Cisco Systems introduced a new protocol called Generic Routing Encapsulation The GRE protocol encapsulates the packets, while adding extra IP addresses and a GRE header, and sends them over the Internet. This protocol provides a tunnel, however, it does not provide any security measures.

Then, there is the Internet Protocol Security (later referred to as IPSec) which is suite of protocols used to enable secure and encrypted communication by providing data confidentiality, integrity, and authentication. It can operate in two modes: transport mode (only the headers are authenticated, and the information is encrypted) and tunnel mode (all IP packets are encapsulated with authentication header and encapsulating security payload).

The IPSec consists of encapsulating security payload (used to encrypt IP packets' data payload), authentication header, internet key exchange (used for encryption keys, IPSec peers and security parameters trading), encryption algorithms (DES, 3DES, AES, etc.), Diffie—Hellman Group (public—key cryptography

protocol to establish session keys), hash algorithms (MD[15], SHA[16]), security association (peer identification storing). (Bollapragada, Khalid and Wainner 2005)

Authentication header is perfect for the IPSec because it counts TCP/ IP headers' control sums. If the control sums are not identical— the packet is dopped. The only problem is that if the network address translation (later referred to as NAT) changes headers' information, it can also be dropped. (Prasad and Prasad 2005)

In the IPSec the working principle consists of few steps— phase 1, phase 2, data transfer and IPSec tunnel termination. For example, the phase 1 step occurs when devices establish a channel to communicate after Internet Key exchange (later referred to as IKE) security policy negotiation. The phase 2 occurs when devices negotiate how to protect the data. (Tiller 2004)

IKE is used for authentication between two parties and security key establishment. IKE communication consists of a request and response messages exchange. (D. Harkins, D. Carrel, cisco Systems 1998)

Another protocol, which is the oldest VPN protocols, is called Point—to—Point Tunneling protocol (later referred as PPTP). This protocol is not used as much in today's world because its security mechanisms were not as developed as other protocols. PPTP mostly relies on authentication and it usually uses MSCHAP—v2 (Microsoft Challenge— Handshake Authentication Protocol) authentication method. It is worth to mention, that it also allows X.509 certificates.
PPTP working principle is built on two channels— setting up the connection and data transportation through GRE protocol. (K. Hamzeh, Ascend Communications,

[15] Message—digest algorithm that is used for hash function.

[16] Secure Hash Algorithms is a hash function family.

G. Pall, Microsoft Corporation, W. Verthein, 3Com, J. Taarud, Copper Mountain Networks, W. Little, ECI Telematics, G. Zorn 1999)

To eliminate weak points of PPTP and Layer 2[17] forwarding protocols Layer two tunneling protocol (later referred to as L2TP) was created. Because it does not offer any encryption mechanisms, it is usually paired with IPSec. Like PPTP L2TP utilizes two control channels for establishment, maintenance, and clearance, of tunnels. (W. Townsley A. Valencia cisco Systems A. Rubens Ascend Communications G. Pall G. Zorn Microsoft Corporation B. Palter Redback Networks 1999)

Then there is a OpenVPN which is an open—source VPN protocol, often called an SSL—Based VPN, that uses HMAC[18]. It uses virtual network adapters as an interface. This protocol has very strong key encryption called AES—256, authentication 2048—bit RSA and hash algorithm SHA1. The biggest problem of the OpenVPN protocol is that its speed is slower than other protocols because of its strong security. (Crist and Keijser 2015)

Lastly, there is Microsoft Secure Socket Tunneling protocol (later referred as SSTP) which lets a user access a private network via HTTPS, while encapsulating Point—to—Point protocol. It uses 2048—bit SSL/TLS[19] certificates for authentication and 256—bit SSL keys for encryption. (Microsoft Corporation 2021)
The above-mentioned technologies have their own working principles, however, users' authentication, data encryption and decryption, is a huge part of it.

2.5 Authentication

[17] Layer 2 refers the second layer of OSI model. It is called the data link layer and it is used to transfer data between nodes.

[18] Hash—based message authentication code is message authentication code, which involves hash functions and secret cryptographic keys.

[19] Transport Layer Security an improved version of SSL.

Authentication is one of the most important parts of security because this process lets confirm the identity of a user and origin of the data. For authentication to be successful it must comply few principles defined by a security standard model called CIA. “The model defines characteristics that cyber environment should have in order to be claimed as secure. Originally, the CIA model consists of three characteristics: confidentiality (the C), integrity (the I), and availability (the A)” (Boonkrong 2021)

The identification of users can be divided into few parts, such as: RSA, digital signature, pre—shared key, EAP, RADIUS.

RSA (Rivest—Shamir—Adleman[20]) is a public key cryptosystem that follows four steps: generating key, distributing key, encrypting, and decrypting key. In this case, a private key is used to decrypt the received message. RSA must follow few rules: the entity to generate keys’ pair (a public key and a private key) should be easy, also, it should be easy to generate the corresponding ciphertext; no additional challenges should be provided to decrypt the message by using the shared private key; while the generation of the keys should come easy, however, the identification of a private key’s inside should be impossible and any recovery of the plaintext to third parties should be infeasible. The mathematics behind the keys’ generation is this: firstly, two large prime numbers are randomly selected (noting that they should be similar size) p and q, then, they both are multiplied and stored in a variable called n. Next, Euler’s phi function is being used: $\phi(n)=(p—1) * (q – 1)$. To fully calculate the public key’s greatest common divisor another new variable is used: $\gcd(k, \phi(n))$, this leads into variables n and k being a full public key. To generate a private key extended Euclidean algorithm is used with a new additional variable called d: $d=(1/k) \bmod \phi$.

A digital signature algorithm is another asymmetric—key cryptography method. This technique is very similar to RSA— a pair of keys, a private and a public key,

[20] RSA was named after the inventors last names.

is created and the private key is used to generate a digital signature. The signature can be verified by using a public key.

Another user identification method is called pre shared key is a set password that is used by both machines (a initiator and a receiver) simultaneously. While it is one of the easiest methods to configure, moreover, it has few faults in itself— this method interferes with scalability as it must be set mechanically; it could hinder the security as the created password must meet the standard, which consists of rules of complexity, uniqueness and secrecy.

Also. There is EAP (Extensible Authentication Protocol) which is rather an authentication framework than one specific authentication mechanism. Itself it can support multiple authentication systems without a need for pre—negotiation. The working principle of EAP is that the authenticator sends a Request message to authenticate a peer, while the peer replies with a valid Respond message. They continuously exchange additional messages till the authenticator can and/or cannot authenticate the peer. (B. Aboba,Microsoft, L. Blunk, Merit Network, Inc, J. Vollbrecht, Vollbrecht Consulting LLC 2004)

Finally, there is RADIUS (Remote Authentication Dial In User Service). This protocol is used to control network access by authentication, authorization, and accounting, also called AAA process. RADIUS protocol is a UDP[21]—based connectionless protocol, which uses a hop—by—hop security model. This protocol is stateless (does not keep track of shared information from previous sessions) and supports PAP[22] and CHAP[23] authentications via PPP[24], it uses MD5[25] security algorithm. (Hassel 2010)

[21] User Datagram Protocol is a communications protocol like TCP.

[22] Password authentication protocol.

[23] Challenge handshake authentication protocol.

[24] Point—to—point protocol lets two routers communicate directly without any host between.

[25] This is MD algorithm which produces 128—bit hash value.

2.6 Encryption and decryption

Encryption is as important as authentication. It is a tool of cryptography that ensures confidentiality by making the data (plaintext— an unencrypted message) incomprehensible. It consists of an algorithm called a cipher and a secret value called a key. Meanwhile, decryption is a reverse technology that turns encrypted messages back to the original state.

The encryption algorithms are divided into two groups— symmetric encryption and asymmetric encryption. While symmetric encryption uses the same key for data encryption and decryption, asymmetric encryption uses two separate keys— a public key and a private key.

Symmetric encryption consists of block ciphers, stream ciphers, hash functions, hash function with a secret key, authenticated encryption. A block cipher consists of encryption and decryption algorithms. The encryption algorithm uses a key and a plaintext block to produce a ciphertext block, while the decryption algorithm is the inversion of encryption algorithm. The block cipher uses two values: a block size and a key size.

A stream cipher uses determinism to allow decryption by generating pseudorandom bits which are used for encryption. It uses a key (a secret value) and a nonce (a unique value intended for the key), then it produces a pseudorandom stream of bits (a keystream).

A hash function uses a long input value and produces a short output value which is called a hash value. “Hash functions are by far the most versatile and ubiquitous of all crypto algorithms.” (Aumasson 2018), the author made this statement because the main hash function’s purpose is to be unpredictable. Another strength of the hash function is that it can be inverted.

Meanwhile, keyed hashing uses message authentication code (later referred to as MAC) which authenticate messages and secures its integrity. Also, it uses pseudorandom functions that produce random hash—sized values.

Lastly, authenticated encryption has features of a normal cipher and a MAC. It can be divided into three parts: authenticated encryption using MACs, authenticated ciphers, authenticated encryption with associated data. Authenticated encryption using MAC lets users encrypt the plaintext and, also, authenticate it. Authenticated ciphers task is to return an authentication tag with the ciphertext. Authenticated encryption with an associated data algorithm allows to attach plaintext data to a ciphertext, which would validate if the ciphertext is corrupted or not.

Opposite of symmetric encryption, asymmetric encryption consists of *RSA, Diffie—Hellman, Elliptic Curves.* The same RSA method is used in authentication and encryption. With encryption RSA works like this: after the key pair is created and the public key is shared, the padding scheme is used to insert random data (called paddle) and an encrypted message is generated. Mathematically this could be done by getting a new variable called m and calculating the following function: $c=m^e \bmod n$. This lets to encrypt the message, however, to encrypt it the encrypted variable m must be turned into plaintext with a function $m=c^d \bmod n$.

Then there is Diffie—Hellman key exchange protocol which allows two parties to create a shared secret password (or a key) without prior knowledge of another party. (Aumasson 2018)

Lastly, there is elliptic curve cryptography. This cryptography method uses elliptic curves over finite fields[26] . The main advantage of this method is that it uses smaller keys to reach the same level of security. (Ciesla 2020)

2.7 Conclusion for technologies

[26] A field containing finite numbers.

To format a conclusion, a creation of four criteria is needed to decide which technology is the most appropriative to continue the project. The criteria are: user identification, data encryption and decryption, convenience (into convenience standard goes not only a user easily understandable graphic interface but also a technology installation process), computer network administrators project installation experience level. .

The provided table below (referring to Table 1), shows that all technologies use certain identification, however, other criteria shows that there are some technologies lacking in some parts.

Table 1 Technologies and their suitability

Technology name	**Identification**	**Encryption**	**Convenience**	**IT specialist level**
RDS	+	+	-	Medium
SSH	+	+	-	High
MPLS	+	-	+	Low—medium
VPN	+	+	+	Low

The MPLS technology itself does not use encryption for sent information. This leads to MPLS being not suitable for this project. The VPN technology has user—friendly authentication, also, the technology does not require a huge amount of experience or knowledge, meanwhile, SSH technology is more suitable for users who understand command lines.

In the presence of large quantities of devices it is hard to install RDS and SSH technologies because individual configuration will require not only a huge amount of time but also human resources. All listed technologies do not require big amounts of expensive. The table provides information that the VPN technology is the most eligible for this project. Nevertheless, the VPN has another concurrent, which is not mentioned above, it is peer—to—peer cable line laying. This method physically provides an opportunity to make devices join another LAN easily and safely. However, the main peer—to—peer problem is that laying cables while

there is a great geographical distance costs a lot and smaller business would not be able to integrate this method. Additionally, using physical technology wastes more time and resources, than virtual technology.

3 SPECIFICATIONS

The VPN technology was chosen for this project because of its advanced safety protocols and easy installation. Since this project's main purpose is to connect different LANs through the Internet, a VPN type called site—to—site is a perfect choice. The VPN technology is the most advanced in several factors, such as: for computer network administrators this technology is easy to prepare and install; after the technology is implemented it can be removed without additional consequences— the network will still work without interruption; an encrypted tunnel is created, meaning that the data is safely transmitted between sites; authentication is used and only the client, to whom the packet belongs to, can read the data; with the right equipment and choosing a non—commercial type of the technology, this technology does not require additional software fees— i.e., IT administrators can set up a private virtual network in their companies for free.

The designed object in this project is a computer network and its purpose is to be updated with security measures. After the security implementation the designed object will have functions like this:

1) The security of the company's computer network will be ensured;
2) Users identification in the network;
3) Transmitted information encryption and decryption;
4) Data transmitted between the required network nodes will be guaranteed to be unchanged and high—quality .

There are some crucial necessities for this project. For example, it is vital that selected hardware would support a VPN and financial spending power on this technology would not exceed small business' economic limit. Another essential part of

this project is a device power— processing power must handle encryption/ de-cryption processes and maximum data transfer speed should be sufficient to transmit packets through a VPN tunnel.

Hardware criteria should be divided into these parts:

1) VPN technology support;
2) Price;
3) Random—access memory size being no less than 64 MB;
4) The maximum data transfer speed being no less than 100 Mbit/ s.

Depending on the workload of a network, the minimum data transfer speed could differ from 1.5 Mbps to 15 Mbps. In this case, for less than four users the minimum amount of traffic should be 2.5 Mbps, while for more than four users the minimum amount should be greater than 3 Mbps. If necessary, the speed may be limited, however, it should not exceed the minimum data flow limit.

Internet providers (later called ISP) should be chosen adequately considering the service price, speed, and Internet type. The requirements are shown in Table 2.

Table 2 Requirements for the Internet providers offered services: technology type, speed and price.

Internet type	**Mb/s**	**Price €/ month**
Internet	< 60	<20
Internet	< 100	<25
Fiber optic	< 100	<30
Fiber optic	< 300	<40
Fiber optic	< 1024	<65

After the VPN technology is implemented, no additional advanced maintenance will be required; less experienced IT network administrators, IT engineers, can keep surveillance of the technology. To keep close observation on the VPN logs of specified entries should be made.

It is required that any router and nodes information, such as IP addresses and passwords, would be known only to network engineers and certain administrators. To reduce the probability of the data leak risk the information needs to be stored in an enclosed electronic space. Enclosed space could consist of servers, where only few people have access to and it cannot be reached from outside the intranet, or a cloud.

There are no additional demands to specify the format of the information storage file. Programs, such as Microsoft Excel are suitable. However, it is recommended that the file would be encrypted and a password, for accessing it, would be set and required.

4 PROJECT DESIGN

The principle of a VPN implementation is quite straightforward, with only need for three tools. Regardless of the VPN type an encrypted tunnel can be set by having a connection initiator, a data transmission medium and a client.

It is abstractly depicted in Figure 8, which appropriately shows the tools— two routers physically transmit data between each other with electromagnetic waves, making the data flow through an encrypted tunnel to destinated LANs.

This means that the first (referring to Router 1) and the second router (referring to Router 2) at the same time can be both— a connection initiator and a client.

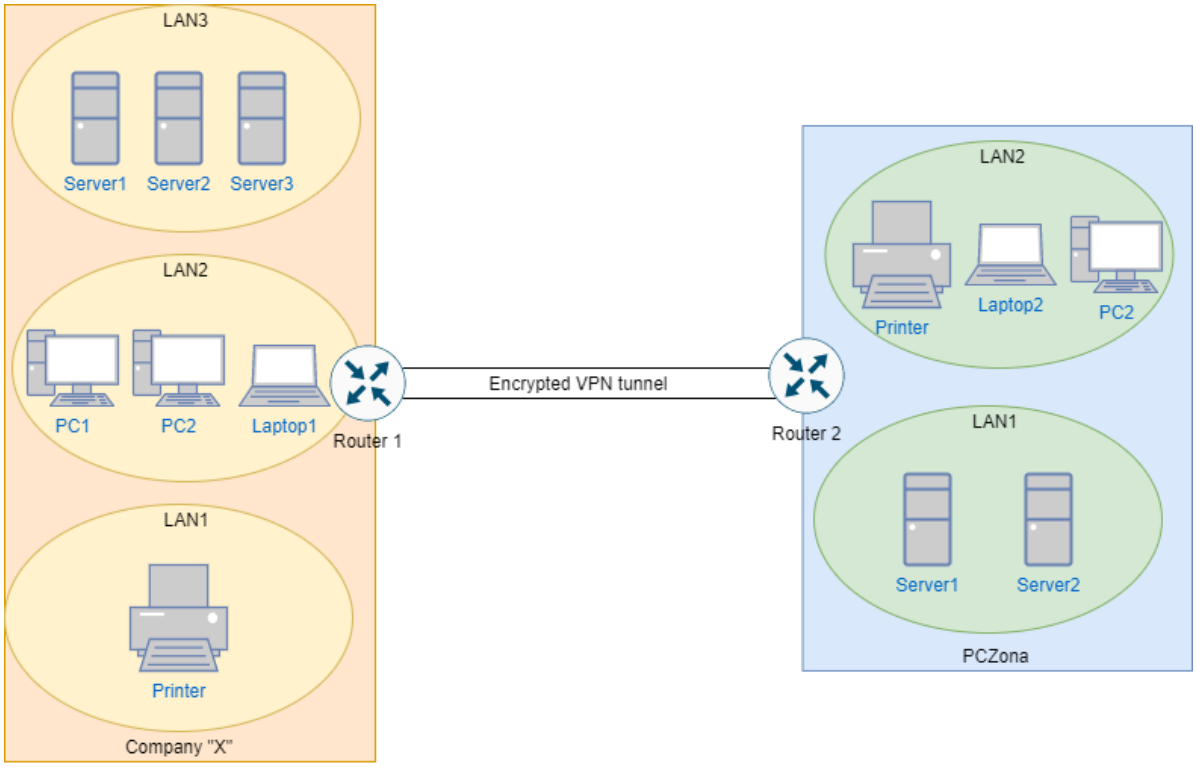

Figure 8 Abstract VPN scheme

Even if this bachelor's thesis focuses on a guide's design creation, the VPN deployment principle still stands and it is essential to integrate measures that would be in consideration of these questions: does existing hardware meet the defined requirements to be a connection initiator and a client, and does the telecommunication provider offers the needed product for the VPN installation?

Additionally, for deployment other questions should be answered: what IP addresses should be used and how; how the used equipment should be labeled; what simulation environment should be chosen; how VPN technology should be implemented in routers; how the installed technology will be known to be working?

4.1 Hardware subsystem

By using the characteristic, which were already determined in specification sector (referring to a chapter Specifications), it is possible to adjudge if the existing router in Pczona is suitable for this project.

Pczona has been already established many years ago and the company is most comfortable using one device vendor— MikroTik. MikroTik is a Latvian company that started its activities in 1996, with the main goal of developing routers and wireless systems, that could provide Internet connectivity by Internet service providers. The company offers a wide spectra of networking devices, which has their own trademarked software system called RouterOS installed. MikroTik currently supplies hardware and software to many countries around the world, including Lithuania and Finland.

One of the network devices Pczona uses from MikroTik is a router called RouterBOARD 750 GL (later referred as RB750GL). The router can be seen in Figure 9.

Figure 9 A picture of RB750GL

The RB750GL[27] router uses MIPSBE[28] architecture with one core central processing unit called AR7242 that has a nominal frequency of 400 MHz. It has 64 MB[29] of random—access memory and the same amount of storage size of NAND type. The router is physically small and compact intended for home and small business.. Because of its size it only has five 10/100 Ethernet ports.

[27] The official page for the product: https://mikrotik.com/product/RB750GL

[28] Microprocessor without Interlocked Pipelined Stages and big—endian

[29] Megabyte is a multiple of the unit byte.

RouterOS exploits six license levels, which provides certain features for a period of time. Starting at 0— this level is used for routers capabilities testing (a trial version); level 1— it offers a free demo version; level 3 is intended for wireless Internet service providers' (later referred to as WISP) customer premises equipment (meaning that it can act as a WAN client and a port); levels 4 and 5 are both used for WISP, however, the only difference between them is the price and count of provided setting; lastly, the level 6 is used as a controller. The RB750GL provides 4 license level, which is enough to create VPN tunnels.

4.2 Internet provider

An Internet provider is critical for deploying the VPN because it provides physical data transfer medium. Few factories should be taken in account to choose the Internet provider: cost, reliability, availability, troubleshooting speed, geographic coverage.

According to the Communications Regulatory Authority of the Republic of Lithuania, there are currently 89 (eighty—nine) data transmission service providers. Naturally, many companies survey for telecommunication providers which suits their defined standards best, and usually the nationally well—known suppliers are first looked at. In Lithuania few of these suppliers are: Telia, Cgates, Init, Mezon, Baltnet. The companies, where the VPN technology is prepared to be installed, are using different Internet suppliers— Telia (referring to Telia (Table 3), Cgates (Table 4), Baltnet (Table 5).

While it is recommended that the Internet server provider would be the same for each cooperating company, however, as long as the supplier does not create obstacles for VPN deployment, it can differ.

Table 3 Telia Internet cost

Internet type	**Mb/s**	**Price €/ month (terminated contract)**	**Device count**

Internet	<60	25	1—2
Internet	<100	34	3—5
Fiber optic	<300	46	5—10
Fiber optic	<1024	69	10—20

Table 4 Cgates Internet cost

Internet type	**Mb/s**	**Price €/ month (terminated contract)**	**Device count**
Fiber optic	<100	27	1—2
Fiber optic	<400	40	5—10
Fiber optic	<1024	60	10—20

Table 5 Baltnet Internet cost

Internet type	**Mb/s**	**Price €/ month (terminated contract)**
Fiber optic	<50	35
Fiber optic	<100	65
Fiber optic	<500	150

4.3 Simulation environment

In this section. a simulation environment will be chosen, IP addresses will be distributed, devices names chosen, a network topology created, and a VPN implemented in simulation environment.

First, a simulation environment was chosen to be Graphical Network Simulator—3. Graphical Network Simulator—3 (later referred to as GNS3) is open—source free software, which emulates network with the combination of virtual and real hardware. The emulation can be done because GNS3 mimics the actual hardware of a device (for example a real Cisco IOS copied from a physical Cisco router) and then the software simulates the features and functions of the device. The network simulator consists of two parts: GNS3 software with a graphic user

interface (also called GNS3 all—in—one software) and a GNS3 virtual machine (later referred to as GNS3 VM).

GNS3 all—in—one software requires that the created devices would be hosted and run by a server, which can be a local GNS3 server, local GNS3 VM, remote GNS3 VM.

The difference between these servers is that the VM server requires virtualization software (such as VMware Workstation, VirtualBox, Hyper—V). It is recommended to use a VM server on Windows since it can run IOS[30]/IOU[31]/KVM[32]. There were few choices of simulation environment, In this case it there were few alternatives between GNS3, Cisco Packet Tracer and separate virtual machines. The comparison between few choices of simulation environments could be seen in Table 6.

Table 6 Simulation environments comparison

GNS3	**Cisco Packet Tracer**	**Virtual machines environment**
Allows to create a network topology and emulate network devices and their functions. Devices operating systems can be easily downloaded and installed to the environment. It is lightweight on the host.	Similar to GNS3, however, is meant for Cisco devices and can only simulate their work. It does not require a lot of resources and is very light on the host.	Allows to virtually emulate devices by using host resources. While it is like other environments, however, it relies too much on existing resources.

30 Cisco Internetwork Operating System a group of network operating system used for Cisco devices.

31 It is IOS version, that it is compiled to run on a workstation.

32 Kernel—based Virtual Machine, which allows kernel to function as a hypervisor.

Additionally, while installing GNS3 other extra tools were presented for optional installation. It is important to mention, that while it is possible to not install the tools, however, some of them are necessary for GNS3 to work well. The tools are:

1) WinPCAP;
2) Npcap;
3) Wireshark;
4) Dynamips;
5) QEMU 3.1.0 and 0.11.0;
6) VPCS;
7) Cpulimit;
8) TightVNC;
9) Viewer;
10) Solar—Putty;
11) Virt—viewer;
12) Intel Hardware Acceleration Manager (also referred as HAXM).

A network topology was chosen to represent a minimal real-life space by having routers communicate through a network and end devices on each LAN. Its model can be referred to hub—and—spoke because it has a centralized router, which communicates to other routers. The network topology (Figure 10) was created with a GNS3 environment**.** The colors represent a LAN queue number— the blue is the first LAN, the red is the second LAN, the yellow is the third LAN, and the green is the fourth LAN.

Devices used in this topology are Virtual PC Simulator (called VSPC), which allows to simulate a person computer with only DHCP and ping functions, basic GNS3 ethernet switches, MikroTik routers. Internet is represented by a MikroTik router, that is used in a bridged mode to let other routers communicate without additional configurations.

The branding system in the logical topology is simple— each device takes a letter or letters from their representative title and then it is combined with numbers. The labels not only represent the tools, but they also indicate companies and LANs.

For example, the main router R1, which is used for the company Pczona, takes the latter “r” in an uppercase form. The latter is taken from the first latter of a word “router”, while the number represent routers order. The following routers are called R2, R3, R4, and each are distributed to different companies.

The switch, which is connected to R1, has a number at the beginning and at the end. The begging number declares to which router the device belongs to, while the last number states device’s order. Two first letters are taken from the word “switch”. The switch of R1 is called 1—SW1. Also, it is important to note, that each switch represents a LAN.

Analogically to switch end—devices use the similar branding system, however, an additional number is attached to differentiate when there are more than one same end—devices. 1—Printer1.1 means that the printer is distributed to R1 and 1—SW1, and it is the first printer in the LAN.

Another important thing to mention is that the end—devices do not represent the real number of devices in companies, in topology they are there for testing and experimenting purposes. In real life environment there could be dozens of LANs and devices.

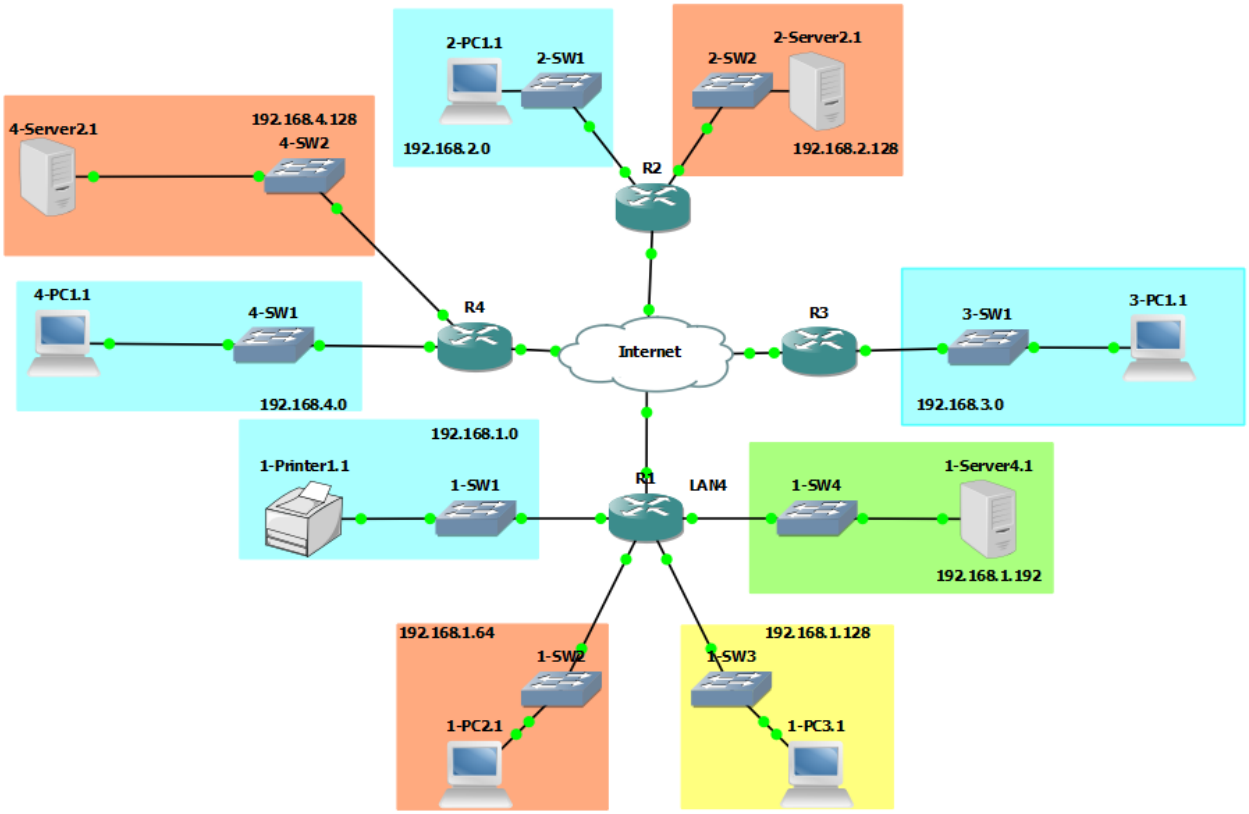

Figure 10 Network topology

The represents IP addresses distribution with the Pczona router (referring to R1). A network/ Subnet address has a purpose of being either a WAN or a LAN.

A “A” class network 10.10.10.0 is used to connect routers between each other. In the R1 case, the address 10.10.10.2 will be used as a WAN interface, while the address 10.10.10.1 will be used as a router’s gateway.

A “C” class addresses are used for LANs to distribute IP addresses for end—devices.

For the R1 a network 192.168.1.0 is used for end—devices. The network is divided into four parts where each part has 62 usable hosts, meaning that 62 addresses can be assigned to devices. However, the first usable address in a subnet is used as a LAN gateway. For example, the first subnet will have a 192.168.1.1—192.168.1.62 IP addresses range available; the address

192.168.1.1 will be used as gateway and the left addresses will be distributed as wished. It is shown in Table 7.

Table 7 R1 IP addresses table

Router name	**Network /Subnet address**	**Network purpose**	**Subnet mask**	**Usable hosts per subnet**
R1	10.10.10.0	Connect router to another routers (WAN)	28	14
	192.168.1.0	First subnet for devices	26	62
	192.168.1.64	Second subnet for devices	26	62
	192.168.1.128	Third subnet for devices	26	62
	192.168.1.192	Fourth subnet for devices	26	62

The represents IP addresses' distribution with the first maintained company's router (referring to R2). The technique is identical to R1 IP addresses distribution. The10.10.10.0 network is used for connection between the routers, meanwhile an address 10.10.10.4 is used for a WAN interface, while an 10.10.10.3 address is used as a gateway.

Like with R1, a "C" class network 192.168.2.0 is divided into two parts with 126 usable hosts available per a subnet. The addresses 192.168.2.1 and 192.168.2.129 are assigned as gateway addresses, while the one hundred twerty—five (125) addresses, which are left, are available to be distributed between devices. It is depicted in Table 8.

Table 8 R2 IP addresses table

Router name	**Network /Subnet address**	**Network purpose**	**Subnet mask**	**Usable hosts per**

				sub-net
R2	10.10.10.0	Connect router to another routers (WAN)	28	14
	192.168.2.0	First subnet for devices	25	126
	192.168.2.128	Second subnet for devices	25	126

In the router R3, a 10.10.10.0 network is, also, used to connect between the routers, while an address 10.10.10.6 is used for a WAN interface and an 10.10.10.5 address is used as a gateway.

A “C” class network 192.168.3.0 is used with 254 available hosts. The address 192.168.3.1 is assigned as a gateway address. These parameters are represented in Table 9.

Table 9 R3 IP addresses table

Router name	**Network /Subnet address**	**Network purpose**	**Subnet mask**	**Usable hosts per subnet**
R3	10.10.10.0	Connect router to another routers (WAN)	28	14
	192.168.3.0	First subnet for devices	24	254

Lastly, by using identical steps R4 addresses are distributed in a table below (referring to Table 10). A 10.10.10.0 network is used to connect between the routers and an address of 10.10.10.8 is used as a WAN interface, while 10.10.10.7 address is used as a gateway.

A “C” class network 192.168.4.0 is divided into two parts, with 126 usable host available per subnet. The addresses 192.168.4.1 and 192.168.4.129 are assigned as gateway addresses, meanwhile the one hundred twenty—five (125) available addresses are distributed between devices.

Table 10 R4 IP addresses table

Router name	**Network /Subnet address**	**Network purpose**	**Subnet mask**	**Usable hosts per subnet**
R4	10.10.10.0	Connect router to another routers (WAN)	28	14
	192.168.4.0	First subnet for devices	25	126
	192.168.4.128	Second subnet for devices	25	126

To ease the workload of configuring every end device manually and represent the real—world dynamic host configuration protocol (later referred to as DHCP) was chosen.

The DHCP allows to automatically allocate IP addresses to clients (end—devices). This protocol is crucial to reduce the workload for a computer network administrator— the employee is not required to configure IP addresses of every computer one by one, leading to saving time.

To implement DHCP in a network a network topology, allocated and unused addresses, subnets, gateways, DNS servers, are needed. Tables above have shown information about allocated addresses and gateways. This data provides enough information to easily create usable IP addresses ranges in each LANs.

Example of addresses range distribution in R1: R1 has four subnets with sixty—two (62) available hosts. One host is immediately assigned to gateway making sixty—one (61) addresses available to end—devices. The LAN1 DHCP range

can be 192.168.1.2—192.168.1.63. The same logic applies to every router and LAN. The full distributed IP addresses ranges are show in Table 11.

Table 11 DHCP table

IP addresses range in each routers' LANs	**LAN1**	**LAN2**	**LAN3**	**LAN4**
R1	192.168.1.2 — 192.168.1.63	192.168.1.66— 192.168.1.126	192.168.1.129 — 192.168.1.190	192.168.1.193 — 192.168.1.254
R2	192.168.2.2 — 192.168.2.126	192.168.2.131 — 192.168.2.254		
R3	192.168.3.2 — 192.168.3.254			
R4	192.168.4.2 — 192.168.4.126	192.168.4.131 — 192.168.4.254		

MikroTik offers a possibility to configure a router by using a graphic interface software called WinBox, nevertheless. In this project command line interface was chosen because of its speed. The input commands are divided into three groups: basic configuration (commands used to declare names, interfaces, routers, etc.), IPSec configuration (commands used to implement VPN technology), additional commands (commands used to show information). All commands are referred from wiki.mikrotik.com website (Manual:IP/IPsec 2021).

Also, it is important to mention that R1 commands are shown as examples, other router commands could be seen in appendix sector (referring to Appendix 1). It is significient to use basic configuration at first. The first command is used to define hostname of a router because by the default all routers are name MikroTik. This command is mandatory and used to ease up the work by removing the confusion of what router is being used right now. The command syntax is "*/system identity set name=Router_name*", Router—name changed to the desired hostname, in this case all routers will be named to their names declared by created standards above.in

In a R1 command line interface the hostname would be set by executing a command**"*/system identity set name=R1"*.**

To set an interface, the command "/ip address add address=x.x.x.x/x interface=etherx" is used. The x should be changed to a IP address and a interface number. For example, in R1 there are one WAN interface and four LAN interfaces (Manual:IP/Address 2011). The commands would look like this: '

1) ***"/ip address add address=10.10.10.2/28 interface=ether1",***
2) ***"/ip address add address=192.168.1.1/26 interface=ether2",***
3) ***"/ip address add address=192.168.1.65/26 interface=ether3",***
4) ***"/ip address add address=192.168.1.129/26 interface=ether4",***
5) ***"/ip address add address=192.168.1.193/26 interface=ether5".***

A command for setting gateway is very similar to a command for interface *"/ip route add gateway=x.x.x.x"*. The x represents gateway address. In a R1 router the command would look like this "***/ip route add gateway=10.10.10.1".***

An additional NAT firewall rule is added with the action of the rule that is called masquerade. Masquerade is used when a public IP address randomly changes. The command for masquerade rule is **"*ip firewall nat add chain=srcnat action=masquerade*".**

Because the DHCP server is used, in a router the server can be set by executing a command ***"/ip dhcp—server setup"*** and following an installation wizard which lets a user choose DHCP range, gateway, lease time. (Manual:IP/DHCP Server 2020)

The IPSec configuration can be divided into optional and necessary. Optional configuration can be avoided because the default functions already exist, while necessary configuration is needed to set peers, source and destination IP addresses. Optional commands are used for profiles and security proposition creation.

The IPSec profiles are used to set parameters for IKE negotiation during phase 1. The command */ip ipsec profile add* adds a new profile, where a user can choose Diffie—Hellman group cipher strength, dead peer detection interval, maximum count of failures until the peer is considered dead, encryption algorithms, hashing algorithms, phase 1 lifebytes, phase 1 lifetime, how the profile is going to be named, if the NAT—traversal is used, how the phase 2 lifetime is going to be checked.

In R1 three profiles are created to each peer: R1—R2, R1—R3, R1—R4. The used commands:

1) ***"/ip ipsec profile add dh—group=modp2048 enc—algorithm=aes—256 name=R1—R2 hash—algorithm=sha256 proposal—check=strict",***
2) ***"/ip ipsec profile add dh—group=modp2048 enc—algorithm=aes—256 name=R1—R3 hash—algorithm=sha256 proposal—check=strict",***
3) ***"/ip ipsec profile add dh—group=modp2048 enc—algorithm=aes—256 name=R1—R4 hash—algorithm=sha256 proposal—check=strict".***

To create a proposal setting, to establish security association, a user can set parameters, such as: authorization algorithms, comments, is the item disabled, encryption algorithms, lifetime, the name of the proposal settings, what Diffie—Hellman group used for Perfect Forward Secrecy.

In R1 three proposal settings are set with names: R1—R2, R1—R3, R1—R4. The commands:

1) ***"/ip ipsec proposal add auth—algorithms=sha256 enc—algorithms=aes—256—cbc name=R1—R2 pfs—group=modp2048",***
2) ***"/ip ipsec proposal add auth—algorithms=sha256 enc—algorithms=aes—256—cbc name=R1—R3 pfs—group=modp2048",***
3) ***"/ip ipsec proposal add auth—algorithms=sha256 enc—algorithms=aes—256—cbc name=R1—R4 pfs—group=modp2048".***

Necessary commands are used to establish connection by setting identities, policies, importing the needed key pair and setting NAT rules and configuring peers.

To establish connection between IKE daemons peer configuration is needed. The main components for settings are remote peer address, port number, peer name and used profile name. However, additional settings could be defined— if the peers are used to match remote peer's prefix, ISAKMP phase 1 exchange modes, routers local address, if the passive mode is chosen, what port should be chosen, specify if the initial contact IKE packet is sent from this device or wait to receive the packet.

The codes for this in R1 are:

1) ***"/ip ipsec peer add address=10.10.10.4 port=500 name=R1—R2_peer profile=R1—R2",***
2) ***"/ip ipsec peer add address=10.10.10.6 port=500 name=R1—R3_peer profile=R1—R3",***
3) ***"/ip ipsec peer add address=10.10.10.8 port=500 name=R1—R4_peer profile=R1—R4".***

Setting identities is another crucial part. Identities main purpose is to verify peer's integrity and manage authentication. When setting it, a user can use these parameters: an authentication method (digital signature, EAP, EAP—RADIUS, pre—shared—key, RSA—key, pre—shared—key—XAUTH, RSA—signature—hybrid), certificate (if used), a comment, is identity used to match remote peer,

EAP—methods, to allow a peer to establish a security association for non—existing policies, what private key to use, peer's identity validation logic, if mode—config menu configurations are used and which are used, initiator ID, if raw firewall rule is added to match IPSec policy to specified chain, what password to use (if needed), a peer name, a policy template group, a remote certificate, remote ID, a remote key name, a secret, a username.

In R1, the used codes are:

1) **"*/ip ipsec identity add peer=R1—R2_peer auth—method=rsa—key key=R1—Key remote—key=R2—Key*",**
2) **"*/ip ipsec identity add peer=R1—R3_peer auth—method=rsa—key key=R1—Key remote—key=R3—Key*",**
3) **"*/ip ipsec identity add peer=R1—R4_peer auth—method=rsa—key key=R1—Key remote—key=R4—Key*".**

To determine if the security parameters should be applied to packets policies are configured. The settings can be: action of what to do with a packet matched by the policy, a comment, if the policy is used to match packets, a destination address (where the packets will be matched), a destination port, a policy group, IPSec protocols, specify what to do if a security association for a policy cannot be found, a peer name, a proposal template name, an IP packet protocol, a source address, a source port, a specific policy group, specify if a tunnel mode is used.

In R1, the used codes are:

1) ***"/ip ipsec policy add src—address=192.168.1.64/26 src—port=any dst—address=192.168.2.0/24 dst—port=any tunnel=yes action=encrypt proposal=R1—R2 peer=R1—R2_peer",***
2) ***"/ip ipsec policy add src—address=192.168.1.64/26 src—port=any dst—address=192.168.3.0/24 dst—port=any tunnel=yes action=encrypt proposal=R1—R3 peer=R1—R3_peer",***
3) ***"/ip ipsec policy add src—address=192.168.1.64/26 src—port=any dst—address=192.168.4.0/24 dst—port=any tunnel=yes action=encrypt proposal=R1—R4 peer=R1—R4_peer".***

The codes defines that all packets from network 192.168.1.64 to networks 192.168.2.0, 192.168.3.0, 192.168.4.0 are sent encrypted, to any port, while the tunnel mode is turned on.

For communication to be successful an RSA key generation and exchanging is very important. Each router needs to generate an RSA key, export it with a chosen name, fetch and import a needed RSA key (of another device) with a chosen name.

Generating a private key can be done with two parameters: the name of generated key and a key size (1024, 2048, 4096 bits). In R1 it was done by executing a command ***"/ip ipsec key generate—key name=R1—Key key—size=2048"***. Then the key was exported by using the command ***"/ip ipsec key export file—name=R1—Key"***, file—name does not have to be generated key name, it can be whatever name a user chooses.

After all keys are generated and exported they can be exchanged— a device must receive another device public key. With a tool called **fetch** it is possible to directly receive RSA keys into a router. The information which needs to be set: he source address, the wanted key's name, the device login information, by what protocol it is going to download the file, where it will store the file and how it is going to be named, what port is going to be used.

The commands used in R1 are:

1) ***"/tool fetch address=10.10.10.4 src—path=R2—Key user=admin password="" mode=ftp dst—path=R2—Key port=21 host="" keep—result=yes" ,***
2) ***"/tool fetch address=10.10.10.6 src—path=R3—Key user=admin password="" mode=ftp dst—path=R3—Key port=21 host="" keep—result=yes",***

3) ***"/tool fetch address=10.10.10.8 src—path=R4—Key user=admin password="" mode=ftp dst—path=R4—Key port=21 host="" keep—result=yes".***

After receiving the keys, they need to be imported for IPSec use. In R1 it was done by executing these commands:

1) ***"/ip ipsec key import file—name=R2—Key name=R2—Key",***
2) ***"/ip ipsec key import file—name=R3—Key name=R3—Key" ,***
3) ***"/ip ipsec key import file—name=R4—Key name=R4—Key".***

Finally, few NAT rules are added, which would let networks communicate between each other. Without it the IPSec peers could be established, however, the end—devices inside LANs could not communicate.

In R1 the commands are:

1) **"*/ip firewall nat add chain=srcnat action=accept place—before=0 \ src—address=192.168.1.64/26 dst—address=192.168.2.0/24",***
2) ***"/ip firewall nat add chain=srcnat action=accept place—before=0 \ src—address=192.168.1.64/26 dst—address=192.168.3.0/24",***
3) **"*/ip firewall nat add chain=srcnat action=accept place—before=0 \ src—address=192.168.1.64/26 dst—address=192.168.4.0/24".***

Lastly, there are additional commands which are used to check information—from the routers system to used functions. The output and example of information transmission can be seen in appendix pages (referring to Appendix 2).

To check what are active IPSec peers (and if they were established), a command **"*/ip ipsec active—peers print"*** is used, to show their information a command **"ip ipsec peer print"** can be used**.** For installed security association settings, a command **"*ip ipsec installed—sa print"*** is used. Checking existing routes in routers could be done by a command **"/ip route print"**, to check infromation about them, a command **"/ip route print detail"** is used.

To check if the interfaces were set, a command ***"/ip address print"*** is used. For future use, all IPSec outputs are logged with a command ***"/system logging add topics=ipsec".*** *The* ***"/log print"*** command shows output information of the logs, it is very useful if the IPSec topic was put to be logged— it will shows information of packets, phase exchange, hashes, padding lengths, encryption and authentication information, etc.*;*

A command **"/ip ipsec policy print"** is used to show IPSec policies and assuring that encrypted tunnel was made. To print all established NAT rules, a command **"/ip firewall nat print"** is used**. "/ip address print"** command shows how were IP addresses distributed to interfaces; To see what IPSec peer were established, a command **"/ip ipsec active—peers print"** is used. More information offers a command **"/ip ipsec installed—sa print"**; this command shows Security Parameter Index identification tag, encryption and authentication algorithms, encryption key size, packets source and destination addresses; finally, to print DHCP server data, a command ***"/ip dhcp—server print"*** is used.

5 CONCLUSIONS

In summary this bachelor's thesis made it possible to thoroughly analyze existing cyber security measures and implement a specific one in chosen devices. In this work analyzed material were RDS, Telnet, SSH, MPLS, VPN technologies. The VPN was chosen to implement because the technology does not make any problems whit these principles: manageability, scalability, implementability. performance, availability. These principles means that the load for the network administrator will not increase while adding this security measure; it is adjustable to a network; it is simple to implement it; it has minimum impact on network performance; it is available to users.

The main goal of this project was to conclude if the VPN is the best for data protection, access control and network isolation and why it is chosen as security measure. This thesis provided information that the VPN is very adaptive to users'

needs and it provides a full spectrum of security— data protection and access control. It can isolate networks from public networks.

With created simulation environment the VPN technology as implemented into a chosen environment and it is ready to be used as a guide.

As a final observation VPN design could be enhanced, when further options would be thoroughly thought about and few questions would be answered: how to minimize packet fragmentation, how to minimize CPU overhead (with existing hardware), what encryption and authentication methods should meet consumer needs, what other network security functions could be used to improve VPN, how to avoid IPSec tunnel termination and implement multicast.

Additionally, authentication and encryption working principles were abstractly looked over. In summary authentication is a process, which lets exchange evidence of identities while attempting to authenticate.

REFERENCES

Andrea, Harris. 2014. *Cisco VPN Configuration Guide.*

Aumasson, Jean-Philippe. 2018. *Serious cryptogrpahy: A Practical Introduction to Modern Encryption.* William Pollock .

B. Aboba, Microsoft, P. Calhoun, Airespace. 2003. "RFC 3579." *IETF Tools.* September. Accessed March 10, 2021. https://www.ietf.org/rfc/rfc3579.txt.

B. Aboba,Microsoft, L. Blunk, Merit Network, Inc, J. Vollbrecht, Vollbrecht Consulting LLC. 2004. "RFC 3748." *IETF Tools.* June. Accessed March 10, 2021. https://tools.ietf.org/html/rfc3748.

Battu, Daniel. 2014. *New Telecom Networks : Enterprises and Security.* ISTE Ltd and John Wiley & Sons, Inc. .

Behringer, Michael H, and Monique J. Morrow. 2005. *MPLS VPN Security.* Indianapolis: Cisco Systems, Inc.

Bollapragada, Vijay, Mohamed Khalid, and Scott Wainner. 2005. *IPSec VPN Design.* Indianapolis: Cisco Systems, Inc.

Boonkrong, Sirapat. 2021. *Authentication and Access Control: Practical Cryptography Methods and Tools.* Nakhon Ratchasima: Apress.

C. Kaufman, Microsoft, P. Hoffman, VPN Consortium, Y. Nir, Check Point, P. Eronen, Independent. 2010. "RFC 5996 ." *IETF Tools.* September. Accessed March 08, 2021. https://tools.ietf.org/html/rfc5996.

Ciesla, Robert. 2020. *Encryption for Organizations and Individuals: Basics of Contemporary and Quantum Cryptography.* HELSINKI: Apress.

Crist, Eric F, and Jan Just Keijser. 2015. *Mastering OpenVPN.* Packt Publishing Ltd.

D. Harkins, D. Carrel, cisco Systems. 1998. "RFC 2409." *IETF Tools.* November. Accessed March 10, 2021. https://tools.ietf.org/html/rfc2409.

Dale Liu; Syngress; Stephanie Millers; Mark Lucas; Abhishek Singh; Jennifer Davis. 2006. *Firewall Policies and VPN Configurations.* Rockland: Syngress Publishing, Inc.

Downie, Ken. 2020. "Extensible Authentication Protocol (EAP) for network access." *docs.microsoft.* December 28. Accessed April 02, 2021. https://docs.microsoft.com/en-us/windows-server/networking/technologies/extensible-authentication-protocol/network-access.

Dwivedi, Himanshu. 2004. *Implementing SSH: Strategies for Optimizing the Secure Shell.* Wiley Publishing, Inc.

Ghein, Luc De. 2007. *MPLS fundamentals.* Indianapolis: Cisco Press.

Hassel, Jonathan. 2010. *RADIUS.* O'Reilly Media, Inc.

K. Hamzeh, Ascend Communications, G. Pall, Microsoft Corporation, W. Verthein, 3Com, J. Taarud, Copper Mountain Networks, W. Little, ECI Telematics, G. Zorn . 1999. "RFC 2637." *IETF Tools.* July. Accessed March 10, 2021. https://tools.ietf.org/html/rfc2637.

2011. *Manual:IP/Address.* Feburary 10. Accessed Feburary 15, 2021. https://wiki.mikrotik.com/wiki/Manual:IP/Address.

2020. *Manual:IP/DHCP Server.* January 21. Accessed Feburary 15, 2021. https://wiki.mikrotik.com/wiki/Manual:IP/DHCP_Server.

2021. *Manual:IP/IPsec.* April 1. Accessed Feburary 15, 2021. https://wiki.mikrotik.com/wiki/Manual:IP/IPsec.

Maxwell, Douglas ; Noble, James S. ; Inc. Staff Syngress Media. 2003. *Check Point NG VPN-1/FireWall-1 Advanced Configuration and Troubleshooting.* Syngress Publishing, Inc.

Microsoft Corporation. 2021. "[MS-SSTP]: Secure Socket Tunneling Protocol (SSTP)." *docs.microsoft.* April 7. Accessed March 08, 2021. https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-sstp/c50ed240-56f3-4309-8e0c-1644898f0ea8.

Montoya, Christian , Elizabeth Ross, Stef Ki, Theano Petersen, Liza Poggemeyer, and Justin Hall. 2017. "Welcome to Remote Desktop Services." *docs.microsoft.com.* Feburary 22. Accessed March 12, 2021. https://docs.microsoft.com/en-us/windows-server/remote/remote-desktop-services/welcome-to-rds.

Perez, André. 2014. *Network Security.* ISTE Ltd and John Wiley & Sons, Inc.

Postel, J.; Reynolds, J.; ISI. 1983. "RFC 854." *IETF Tools.* May. Accessed March 10, 2021. https://tools.ietf.org/html/rfc854.

Prasad, Neeli R., and Anand R. Prasad. 2005. *802.11 LANs and IP Networking : Security, QoS, and Mobility.* Artech House.

Rosen, E., and Y. Rekhter. 1999. "RFC 2547." *IETF Tools.* March. Accessed March 10, 2021. https://tools.ietf.org/html/rfc2547.

T. Ylonen SSH Communications Security Corp C. Lonvick, Ed. Cisco Systems, Inc. 2006c. "RFC 4252." *IETF Tools.* January. Accessed March 08, 2021. https://tools.ietf.org/html/rfc4252.

—. 2006b. "RFC 4253." *IETF Tools.* January. Accessed March 08, 2021. https://tools.ietf.org/html/rfc4253.

—. 2006d. "RFC 4254." *IETF Tools.* January. Accessed March 08, 2021. https://tools.ietf.org/html/rfc4254.

T. Ylonen, SSH Communications Security Corp, C. Lonvick, Ed., Cisco Systems, Inc. 2006a. "RFC 4251." *IETF Tools.* January. Accessed March 08, 2021. https://tools.ietf.org/html/rfc4251.

Tiller, James S. 2004. *A Technical Guide to IPSec Virtual Private Networks.* CRC Press LLC.

W. Townsley A. Valencia cisco Systems A. Rubens Ascend Communications G. Pall G. Zorn Microsoft Corporation B. Palter Redback Networks. 1999. "RFC 2661." *IETF Tools.* August. Accessed March 10, 2021. https://tools.ietf.org/html/rfc2661.

Zhang, Frank. 2021. "[MS-RDPBCGR]: Remote Desktop Protocol: Basic Connectivity and Graphics Remoting." *docs.microsoft.com.* April 07. Accessed March 10, 2021. https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-rdpbcgr/5073f4ed-1e93-45e1-b039-6e30c385867c?redirectedfrom=MSDN.

LIST OF FIGURES

LIST OF TABLES

Used commands for routers

R2 commands (basic commands):

/system identity set name=R2

/ip address add address=10.10.10.4/28 interface=ether1

/ip address add address=192.168.2.1/25 interface=ether2

/ip address add address=192.168.2.129/25 interface=ether3

/ip route add gateway=10.10.10.3

/ip firewall nat add chain=srcnat action=masquerade

/system logging add topics=ipsec

/ip dhcp—server setup

R2 commands (IPSec configuration commands):

/ip ipsec profile add dh—group=modp2048 enc—algorithm=aes—256 name=R1—R2 hash—algorithm=sha256 proposal—check=strict

/ip ipsec proposal add auth—algorithms=sha256 enc—algorithms=aes—256—cbc name=R1—R2 pfs—group=modp2048

/ip ipsec peer add address=10.10.10.2 port=500 name=R1—R2_peer profile=R1—R2

/ip ipsec key generate—key name=R2—Key key—size=2048

/ip ipsec key export file—name=R2—Key

/tool fetch address=10.10.10.2 src—path=R1—Key user=admin password="" mode=ftp dst—path=R1—Key port=21 host="" keep—result=yes

/ip ipsec key import file—name=R1—Key name=R1—Key

/ip ipsec identity add peer=R1—R2_peer auth—method=rsa—key key=R2—Key remote—key=R1—Key/ip ipsec policy add src—address=192.168.2.0/24 src—port=any

dst—address=192.168.1.64/26 dst—port=any tunnel=yes action=encrypt proposal=R1—R2 peer= R1—R2_peer

/ip firewall nat add chain=srcnat action=accept place—before=0 \ src—address=192.168.2.0/24 dst—address=192.168.1.64/26

R3 commands (basic commands):

/system identity set name=R3

/ip address add address=10.10.10.6/28 interface=ether1

/ip address add address=192.168.3.1/24 interface=ether2

/ip address print

/ip route add gateway=10.10.10.5

/ip route print

ip firewall nat add chain=srcnat action=masquerade

/system logging add topics=ipsec

/ip dhcp—server setup

/ip dhcp—server ip pool print

/ip dhcp—server network print

/ip dhcp—server print

R3 commands (IPSec configuration commands):

/ip ipsec profile add dh—group=modp2048 enc—algorithm=aes—256 name=R1—R3 hash—algorithm=sha256 proposal—check=strict

/ip ipsec proposal add auth—algorithms=sha256 enc—algorithms=aes—256—cbc name=R1—R3 pfs—group=modp2048

/ip ipsec peer add address=10.10.10.2 port=500 name=R1—R3_peer profile=R1—R3

/ip ipsec key generate—key name=R3—Key key—size=2048

/ip ipsec key export file—name=R3—Key

/tool fetch address=10.10.10.2 src—path=R1—Key user=admin password="" mode=ftp dst—path=R1—Key port=21 host="" keep—result=yes

/ip ipsec key import file—name=R1—Key name=R1—Key

/ip ipsec identity add peer=R1—R3_peer auth—method=rsa—key key=R3—Key remote—key=R1—Key

/ip ipsec policy add src—address=192.168.3.0/24 src—port=any dst—address=192.168.1.64/26 dst—port=any tunnel=yes action=encrypt proposal=R1—R3 peer= R1—R3_peer

/ip firewall nat add chain=srcnat action=accept place—before=0 \ src—address=192.168.3.0/24 dst—address=192.168.1.64/26

/ip ipsec active—peers print

/ip ipsec installed—sa print

R4 commands (basic commands):

/system identity set name=R4

/ip address add address=10.10.10.8/28 interface=ether1

/ip address add address=192.168.4.1/25 interface=ether2

/ip address add address=192.168.4.129/25 interface=ether3

/ip address print

/ip route add gateway=10.10.10.7

/ip route print

ip firewall nat add chain=srcnat action=masquerade

/system logging add topics=ipsec

/ip dhcp—server setup

/ip dhcp—server ip pool print

/ip dhcp—server network print

/ip dhcp—server print

R4 commands (IPSec configuration commands):

/ip ipsec profile add dh—group=modp2048 enc—algorithm=aes—256 name=R1—R4 hash—algorithm=sha256 proposal—check=strict

/ip ipsec proposal add auth—algorithms=sha256 enc—algorithms=aes—256—cbc name=R1—R4 pfs—group=modp2048

/ip ipsec peer add address=10.10.10.2 port=500 name=R1—R4_peer profile=R1—R4

/ip ipsec key generate—key name=R4—Key key—size=2048

/ip ipsec key export file—name=R4—Key

/tool fetch address=10.10.10.2 src—path=R1—Key user=admin password="" mode=ftp dst—path=R1—Key port=21 host="" keep—result=yes

/ip ipsec key import file—name=R1—Key name=R1—Key

/ip ipsec identity add peer=R1—R4_peer auth—method=rsa—key key=R4—Key remote—key=R1—Key

/ip ipsec policy add src—address=192.168.4.0/24 src—port=any dst—address=192.168.1.64/26 dst—port=any tunnel=yes action=encrypt proposal=R1—R4 peer= R1—R4_peer

/ip firewall nat add chain=srcnat action=accept place—before=0 \ src—address=192.168.4.0/24 dst—address=192.168.1.64/26

/ip ipsec active—peers print

/ip ipsec installed—sa print

Output of implemented parameters in routers

```
[admin@R1] > /ip dhcp-server print
Columns: NAME, INTERFACE, ADDRESS-POOL, LEASE-TI
  #  NAME   INTERF  ADDRESS-PO  LEA
  0  dhcp1  ether2  dhcp_pool0  10m
  1  dhcp2  ether3  dhcp_pool1  10m
  2  dhcp3  ether4  dhcp_pool2  10m
  3  dhcp4  ether5  dhcp_pool3  10m
```

Figure 11 R1 DHCP server information

```
[admin@R2] > /ip dhcp-server print
Columns: NAME, INTERFACE, ADDRESS-POOL, LEASE-TIME
  #  NAME   INTERF  ADDRESS-PO  LEA
  0  dhcp1  ether2  dhcp_pool0  10m
  1  dhcp2  ether3  dhcp_pool1  10m
```

Figure 12 R2 DHCP server information

```
[admin@R3] > /ip dhcp-server print
Columns: NAME, INTERFACE, ADDRESS-POOL, LEASE-TIME
  #  NAME   INTERF  ADDRESS-PO  LEA
  0  dhcp1  ether2  dhcp_pool1  10m
```

Figure 13 R3 DHCP server information

```
[admin@R4] /ip/ipsec> /ip dhcp-server print
Columns: NAME, INTERFACE, ADDRESS-POOL, LEASE-TIME
  #  NAME   INTERF  ADDRESS-PO  LEA
  0  dhcp1  ether2  dhcp_pool0  10m
  1  dhcp2  ether3  dhcp_pool1  10m
```

Figure 14 R4 DHCP server information

```
[admin@R1] > /ip ipsec policy print
Flags: T - TEMPLATE; A - ACTIVE; * - DEFAULT
Columns: PEER, TUNNEL, SRC-ADDRESS, DST-ADDRESS, PROTOCOL, ACTION, LEVEL, PH2-COUNT
  #       PEER        TUN  SRC-ADDRESS      DST-ADDRESS     PRO  ACTION   LEVEL    P
  0  T *                  ::/0             ::/0            all
  1   A   R1-R2_peer  yes  192.168.1.64/26  192.168.2.0/24  all  encrypt  require  1
  2   A   R1-R3_peer  yes  192.168.1.64/26  192.168.3.0/24  all  encrypt  require  1
  3   A   R1-R4_peer  yes  192.168.1.64/26  192.168.4.0/24  all  encrypt  require  1
[admin@R1] > /ip firewall nat print
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=accept src-address=192.168.1.64/26 dst-address=192.168.2.0/24

 1    chain=srcnat action=accept src-address=192.168.1.64/26 dst-address=192.168.3.0/24

 2    chain=srcnat action=accept src-address=192.168.1.64/26 dst-address=192.168.4.0/24

 3    chain=srcnat action=masquerade
[admin@R1] > /ip route print detail
Flags: D - dynamic; X - disabled, I - inactive, A - active; C - connect, S - static, r - rip, b - bgp, o - ospf, d - dhcp, v
 - vpn, m - modem; + - ecmp
 0  AS  dst-address=0.0.0.0/0 pref-src="" gateway=10.10.10.1 immediate-gw=10.10.10.1%ether1 type=unicast distance=1 scope=30
 target-scope=10

   DAC  dst-address=10.10.10.0/28 gateway=ether1 immediate-gw=ether1 type=unicast distance=0 scope=10 local-address=10.10.10
.2%ether1

   DAC  dst-address=192.168.1.64/26 gateway=ether3 immediate-gw=ether3 type=unicast distance=0 scope=10 local-address=192.16
8.1.65%ether3

   DAC  dst-address=192.168.1.128/26 gateway=ether4 immediate-gw=ether4 type=unicast distance=0 scope=10 local-address=192.1
68.1.129%ether4

   DAC  dst-address=192.168.1.192/26 gateway=ether5 immediate-gw=ether5 type=unicast distance=0 scope=10 local-address=192.1
68.1.193%ether5
[admin@R1] > /ip address print
Columns: ADDRESS, NETWORK, INTERFACE
  #  ADDRESS            NETWORK         INTERF
  0  10.10.10.2/28      10.10.10.0      ether1
  1  192.168.1.1/26     192.168.1.0     ether2
  2  192.168.1.65/26    192.168.1.64    ether3
  3  192.168.1.129/26   192.168.1.128   ether4
  4  192.168.1.193/26   192.168.1.192   ether5
```

Figure 15 R1 information part 1

```
[admin@R1] > /ip ipsec active-peers print
Flags: R - RESPONDER
Columns: STATE, UPTIME, PH2-TOTAL, REMOTE-ADDRESS
  #     STATE        UPTIME  P  REMOTE-ADD
  0  R  established  18s     1  10.10.10.8
  1     established  59m11s  1  10.10.10.4
  2     established  59m11s  1  10.10.10.6
[admin@R1] > /ip ipsec installed-sa print
Flags: E - ESP
Columns: SPI, STATE, SRC-ADDRESS, DST-ADDRESS, AUTH-ALGORITHM, ENC-ALGORITHM, ENC-KEY-SIZE
  #     SPI         STATE   SRC-ADDRES  DST-ADDRES  AUTH-A  ENC-ALG  ENC
  0  E  0x58853B8   mature  10.10.10.4  10.10.10.2  sha256  aes-cbc  256
  1  E  0xB0FB518   mature  10.10.10.2  10.10.10.4  sha256  aes-cbc  256
  2  E  0x1E1EF20   mature  10.10.10.6  10.10.10.2  sha256  aes-cbc  256
  3  E  0xC6A5F22   mature  10.10.10.2  10.10.10.6  sha256  aes-cbc  256
  4  E  0x427BB04   mature  10.10.10.8  10.10.10.2  sha256  aes-cbc  256
  5  E  0xC5F2996   mature  10.10.10.2  10.10.10.8  sha256  aes-cbc  256
[admin@R1] > /certificate print

[admin@R1] > /ip ipsec peer print
Flags: X - disabled; D - dynamic; R - responder
 0     name="R1-R4_peer" address=10.10.10.8/32 profile=R1-R4 exchange-mode=main send-initial-contact=yes

 1     name="R1-R3_peer" address=10.10.10.6/32 profile=R1-R3 exchange-mode=main send-initial-contact=yes

 2     name="R1-R2_peer" address=10.10.10.4/32 profile=R1-R2 exchange-mode=main send-initial-contact=yes
```

Figure 16 R1 information part 2

```
[admin@R2] > /ip ipsec policy print
Flags: T - TEMPLATE; A - ACTIVE; * - DEFAULT
Columns: PEER, TUNNEL, SRC-ADDRESS, DST-ADDRESS, PROTOCOL, ACTION, LEVEL, PH2-COUNT
  #       PEER        TUN  SRC-ADDRESS     DST-ADDRESS      PRO  ACTION   LEVEL    P
  0  T *                  ::/0            ::/0             all
  1   A   R1-R2_peer  yes  192.168.2.0/24  192.168.1.64/26  all  encrypt  require  1
[admin@R2] > /ip firewall nat print
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=accept src-address=192.168.2.0/24 dst-address=192.168.1.64/26 src-address-list="" log=no log-prefi
x=""

 1    chain=srcnat action=masquerade
[admin@R2] > /ip route print detail
Flags: D - dynamic; X - disabled, I - inactive, A - active; C - connect, S - static, r - rip, b - bgp, o - ospf, d - dhcp, v
 - vpn, m - modem; + - ecmp
 0  XS  dst-address=0.0.0.0 pref-src="" gateway=10.10.10.3 type=unicast distance=1 scope=30 target-scope=10

 1  AS  dst-address=0.0.0.0/0 pref-src="" gateway=10.10.10.3 immediate-gw=10.10.10.3%ether1 type=unicast distance=1 scope=30
 target-scope=10

   DAC  dst-address=10.10.10.0/28 gateway=ether1 immediate-gw=ether1 type=unicast distance=0 scope=10 local-address=10.10.10
.4%ether1

   DAC  dst-address=192.168.2.0/25 gateway=ether2 immediate-gw=ether2 type=unicast distance=0 scope=10 local-address=192.168
.2.1%ether2

   DAC  dst-address=192.168.2.128/25 gateway=ether3 immediate-gw=ether3 type=unicast distance=0 scope=10 local-address=192.1
68.2.129%ether3
[admin@R2] > /ip address print
Columns: ADDRESS, NETWORK, INTERFACE
  #  ADDRESS           NETWORK        INTERF
  0  10.10.10.4/28     10.10.10.0     ether1
  1  192.168.2.1/25    192.168.2.0    ether2
  2  192.168.2.129/25  192.168.2.128  ether3
[admin@R2] > /ip ipsec active-peers print
Flags: R - RESPONDER
Columns: STATE, UPTIME, PH2-TOTAL, REMOTE-ADDRESS
  #     STATE        UPTIME  P  REMOTE-ADD
  0  R  established  59m17s  1  10.10.10.2
```

Figure 17 R2 information part 1

```
[admin@R2] > /ip ipsec installed-sa print
Flags: E - ESP
Columns: SPI, STATE, SRC-ADDRESS, DST-ADDRESS, AUTH-ALGORITHM, ENC-ALGORITHM, ENC-KEY-SIZE
  #     SPI        STATE   SRC-ADDRES  DST-ADDRES  AUTH-A  ENC-ALG  ENC
  0  E  0xB0FB518  mature  10.10.10.2  10.10.10.4  sha256  aes-cbc  256
  1  E  0x58853B8  mature  10.10.10.4  10.10.10.2  sha256  aes-cbc  256
[admin@R2] > /certificate print

[admin@R2] > /ip ipsec peer print
Flags: X - disabled; D - dynamic; R - responder
 0     name="R1-R2_peer" address=10.10.10.2/32 profile=R1-R2 exchange-mode=main send-initial-contact=yes
```

Figure 18 R2 information part 2

```
[admin@R3] > /ip ipsec policy print
Flags: T - TEMPLATE; A - ACTIVE; * - DEFAULT
Columns: PEER, TUNNEL, SRC-ADDRESS, DST-ADDRESS, PROTOCOL, ACTION, LEVEL, PH2-COUNT
  #       PEER        TUN  SRC-ADDRESS     DST-ADDRESS      PRO  ACTION   LEVEL    P
  0  T *                  ::/0            ::/0             all
  1   A   R1-R3_peer  yes  192.168.3.0/24  192.168.1.64/26  all  encrypt  require  1
[admin@R3] > /ip firewall nat print
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=accept src-address=192.168.3.0/24 dst-address=192.168.1.64/26

 1    chain=srcnat action=masquerade
[admin@R3] > /ip route print detail
Flags: D - dynamic; X - disabled, I - inactive, A - active; C - connect, S - static, r - rip, b - bgp, o - ospf, d - dhcp, v
 - vpn, m - modem; + - ecmp
 0  AS  dst-address=0.0.0.0/0 pref-src="" gateway=10.10.10.5 immediate-gw=10.10.10.5%ether1 type=unicast distance=1 scope=30
 target-scope=10

   DAC  dst-address=10.10.10.0/28 gateway=ether1 immediate-gw=ether1 type=unicast distance=0 scope=10 local-address=10.10.10
.6%ether1

   DAC  dst-address=192.168.3.0/24 gateway=ether2 immediate-gw=ether2 type=unicast distance=0 scope=10 local-address=192.168
.3.1%ether2
[admin@R3] > /ip address print
Columns: ADDRESS, NETWORK, INTERFACE
  #  ADDRESS         NETWORK      INTERF
  0  10.10.10.6/28   10.10.10.0   ether1
  1  192.168.3.1/24  192.168.3.0  ether2
[admin@R3] > /ip ipsec active-peers print
Flags: R - RESPONDER
Columns: STATE, UPTIME, PH2-TOTAL, REMOTE-ADDRESS
  #     STATE        UPTIME  P  REMOTE-ADD
  0  R  established  59m30s  1  10.10.10.2
```

Figure 19 R3 information part 1

```
[admin@R3] > /ip ipsec installed-sa print
Flags: E - ESP
Columns: SPI, STATE, SRC-ADDRESS, DST-ADDRESS, AUTH-ALGORITHM, ENC-ALGORITHM, ENC-KEY-SIZE
  #     SPI         STATE   SRC-ADDRES  DST-ADDRES  AUTH-A  ENC-ALG  ENC
  0  E  0xC6A5F22   mature  10.10.10.2  10.10.10.6  sha256  aes-cbc  256
  1  E  0x1E1EF20   mature  10.10.10.6  10.10.10.2  sha256  aes-cbc  256
[admin@R3] > /certificate print

[admin@R3] > /ip ipsec peer print
Flags: X - disabled; D - dynamic; R - responder
 0     name="R1-R3_peer" address=10.10.10.2/32 profile=R1-R3 exchange-mode=main send-initial-contact=yes
```

Figure 20 R3 information part 2

```
[admin@R4] /ip/ipsec> /ip ipsec policy print
Flags: T - TEMPLATE; A - ACTIVE; * - DEFAULT
Columns: PEER, TUNNEL, SRC-ADDRESS, DST-ADDRESS, PROTOCOL, ACTION, LEVEL, PH2-COUNT
  #       PEER        TUN  SRC-ADDRESS     DST-ADDRESS      PRO  ACTION   LEVEL    P
  0  T *                  ::/0            ::/0             all
  1   A   R1-R4_peer  yes  192.168.4.0/24  192.168.1.64/26  all  encrypt  require  1
[admin@R4] /ip/ipsec> /ip firewall nat print
Flags: X - disabled, I - invalid; D - dynamic
 0    chain=srcnat action=accept src-address=192.168.4.0/24 dst-address=192.168.1.64/26

 1    chain=srcnat action=masquerade
[admin@R4] /ip/ipsec> /ip route print detail
Flags: D - dynamic; X - disabled, I - inactive, A - active;
C - connect, S - static, r - rip, b - bgp, o - ospf, d - dhcp, v - vpn, m - modem; + - ecmp
 0  AS  dst-address=0.0.0.0/0 pref-src="" gateway=10.10.10.7 immediate-gw=10.10.10.7%ether1 type=unicast distance=1
       scope=30 target-scope=10

   DAC  dst-address=10.10.10.0/28 gateway=ether1 immediate-gw=ether1 type=unicast distance=0 scope=10
        local-address=10.10.10.8%ether1

   DAC  dst-address=192.168.4.0/25 gateway=ether2 immediate-gw=ether2 type=unicast distance=0 scope=10
        local-address=192.168.4.1%ether2

   DAC  dst-address=192.168.4.128/25 gateway=ether3 immediate-gw=ether3 type=unicast distance=0 scope=10
        local-address=192.168.4.129%ether3
[admin@R4] /ip/ipsec> /ip address print
Columns: ADDRESS, NETWORK, INTERFACE
  #  ADDRESS            NETWORK        INTERF
  0  10.10.10.8/28      10.10.10.0     ether1
  1  192.168.4.1/25     192.168.4.0    ether2
  2  192.168.4.129/25   192.168.4.128  ether3
[admin@R4] /ip/ipsec> /ip ipsec active-peers print
Columns: STATE, UPTIME, PH2-TOTAL, REMOTE-ADDRESS
  #  STATE        UPT  P  REMOTE-ADD
  0  established  30s  1  10.10.10.2
[admin@R4] /ip/ipsec> /ip ipsec installed-sa print
Flags: E - ESP
Columns: SPI, STATE, SRC-ADDRESS, DST-ADDRESS, AUTH-ALGORITHM, ENC-ALGORITHM, ENC-KEY-SIZE
  #     SPI         STATE   SRC-ADDRES  DST-ADDRES  AUTH-A  ENC-ALG  ENC
  0  E  0xC5F2996   mature  10.10.10.2  10.10.10.8  sha256  aes-cbc  256
  1  E  0x427BB04   mature  10.10.10.8  10.10.10.2  sha256  aes-cbc  256
```

Figure 21 R4 information part 1

```
[admin@R4] /ip/ipsec> /ip ipsec peer print
Flags: X - disabled; D - dynamic; R - responder
 0     name="R1-R4_peer" address=10.10.10.2/32 profile=R1-R4 exchange-mode=main send-initial-contact=yes
```

Figure 22 R4 information part 2

Example of packet's information shown by Wireshark

```
> Frame 359: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface -, id 0
> Ethernet II, Src: 0c:c2:b5:78:1c:00 (0c:c2:b5:78:1c:00), Dst: 0c:c2:b5:83:40:00 (0c:c2:b5:83:40:00)
v Internet Protocol Version 4, Src: 10.10.10.2, Dst: 10.10.10.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 156
    Identification: 0x727b (29307)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: Encap Security Payload (50)
    Header checksum: 0xdf97 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.2
    <Source or Destination Address: 10.10.10.2>
    <[Source Host: 10.10.10.2]>
    <[Source or Destination Host: 10.10.10.2]>
    Destination: 10.10.10.8
    <Source or Destination Address: 10.10.10.8>
    <[Destination Host: 10.10.10.8]>
    <[Source or Destination Host: 10.10.10.8]>
v Encapsulating Security Payload
    ESP SPI: 0x0e7c5cf3 (243031283)
    ESP Sequence: 1
```

Figure 23 Packet sent from R1 192.168.1.64 LAN to R4 192.168.4.1 LAN 1

```
> Frame 358: 170 bytes on wire (1360 bits), 170 bytes captured (1360 bits) on interface -, id 0
> Ethernet II, Src: 0c:c2:b5:83:40:00 (0c:c2:b5:83:40:00), Dst: 0c:c2:b5:78:1c:00 (0c:c2:b5:78:1c:00)
v Internet Protocol Version 4, Src: 10.10.10.8, Dst: 10.10.10.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 156
    Identification: 0x12fb (4859)
  > Flags: 0x0000
    Fragment offset: 0
    Time to live: 64
    Protocol: Encap Security Payload (50)
    Header checksum: 0x3f18 [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.8
    <Source or Destination Address: 10.10.10.8>
    <[Source Host: 10.10.10.8]>
    <[Source or Destination Host: 10.10.10.8]>
    Destination: 10.10.10.2
    <Source or Destination Address: 10.10.10.2>
    <[Destination Host: 10.10.10.2]>
    <[Source or Destination Host: 10.10.10.2]>
v Encapsulating Security Payload
    ESP SPI: 0x07b0e3ed (129033197)
    ESP Sequence: 1
```

Figure 24 Packet sent from R4 192.168.4.1 LAN 1 to R1 192.168.1.64 LAN 1

It is shown in Figure 23 and Figure 24 that sent packets are with installed security measures because they use ESP an it is unknown to where are they sent (only routers WAN interface's addresses are known).

```
> Frame 1568: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface -, id 0
> Ethernet II, Src: 0c:c2:b5:78:1c:00 (0c:c2:b5:78:1c:00), Dst: 0c:c2:b5:83:40:00 (0c:c2:b5:83:40:00)
v Internet Protocol Version 4, Src: 10.10.10.2, Dst: 10.10.10.8
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 136
    Identification: 0x74ba (29882)
  > Flags: 0x4000, Don't fragment
    Fragment offset: 0
    Time to live: 64
    Protocol: UDP (17)
    Header checksum: 0x9d8d [validation disabled]
    [Header checksum status: Unverified]
    Source: 10.10.10.2
    <Source or Destination Address: 10.10.10.2>
    <[Source Host: 10.10.10.2]>
    <[Source or Destination Host: 10.10.10.2]>
    Destination: 10.10.10.8
    <Source or Destination Address: 10.10.10.8>
    <[Destination Host: 10.10.10.8]>
    <[Source or Destination Host: 10.10.10.8]>
v User Datagram Protocol, Src Port: 500, Dst Port: 500
    Source Port: 500
    Destination Port: 500
    <Source or Destination Port: 500>
    <Source or Destination Port: 500>
    Length: 116
    Checksum: 0x7f98 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
v Internet Security Association and Key Management Protocol
    Initiator SPI: 0885813c37e25d24
    Responder SPI: 01d8c22f4d1e93ae
    Next payload: Hash (8)
  > Version: 1.0
    Exchange type: Informational (5)
  > Flags: 0x01
```

Figure 25 ISAKMP information mode part 1

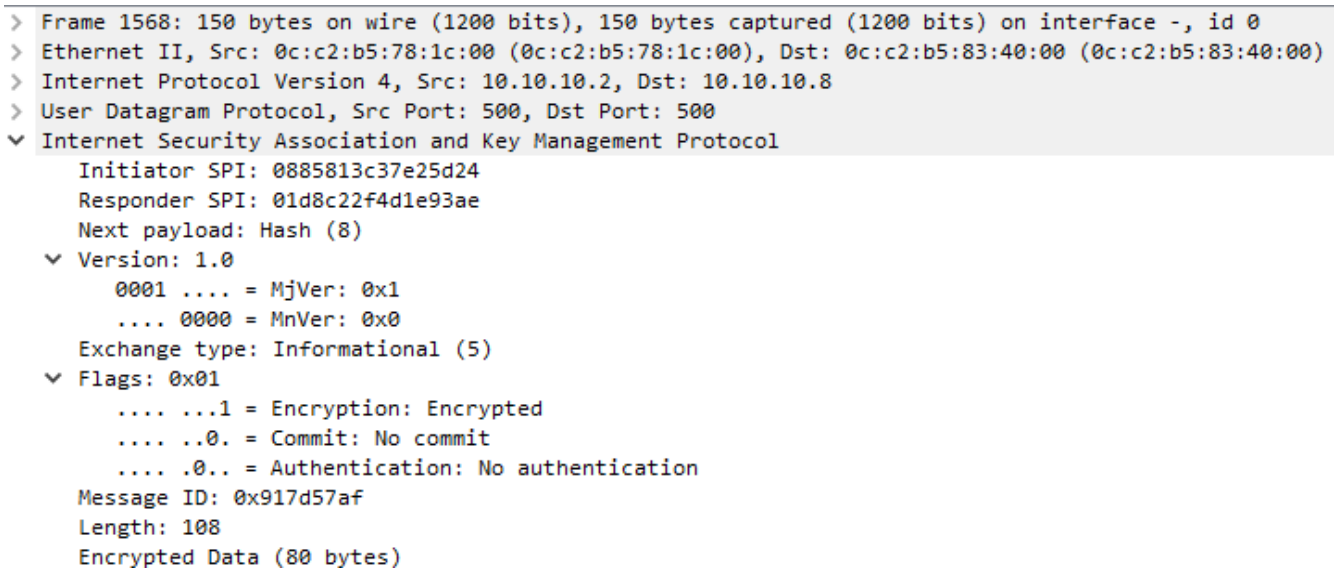

Figure 26 ISAKMP information mode part 2

It is important to mention that the depicted information in Figure 25, Figure 26, Figure 27, Figure 28 can differ from real life devices as it was tested with GNS3 environment. The pictures also show the phases process— the negotiation of authentication, hash and encryption algorithms, Diffie-Hellman group information; the chosen attributes such as: protocols and encapsulation mode.

```
> Frame 1604: 430 bytes on wire (3440 bits), 430 bytes captured (3440 bits) on interface -, id 0
> Ethernet II, Src: 0c:c2:b5:78:1c:00 (0c:c2:b5:78:1c:00), Dst: 0c:c2:b5:83:40:00 (0c:c2:b5:83:40:00)
> Internet Protocol Version 4, Src: 10.10.10.2, Dst: 10.10.10.8
v User Datagram Protocol, Src Port: 500, Dst Port: 500
    Source Port: 500
    Destination Port: 500
    <Source or Destination Port: 500>
    <Source or Destination Port: 500>
    Length: 396
    Checksum: 0xa6a8 [unverified]
    [Checksum Status: Unverified]
    [Stream index: 2]
  > [Timestamps]
v Internet Security Association and Key Management Protocol
    Initiator SPI: d2fb8c57dc22e7dd
    Responder SPI: 1b2f6da910128668
    Next payload: Key Exchange (4)
  v Version: 1.0
      0001 .... = MjVer: 0x1
      .... 0000 = MnVer: 0x0
    Exchange type: Identity Protection (Main Mode) (2)
  v Flags: 0x00
      .... ...0 = Encryption: Not encrypted
      .... ..0. = Commit: No commit
      .... .0.. = Authentication: No authentication
    Message ID: 0x00000000
    Length: 388
  v Payload: Key Exchange (4)
      Next payload: Nonce (10)
      Reserved: 00
      Payload length: 260
      Key Exchange Data: ec565458bb40ed25f23c3349c070145d8ba30586c8f7ec59…
  > Payload: Nonce (10)
  > Payload: NAT-D (RFC 3947) (20)
  > Payload: NAT-D (RFC 3947) (20)
```

Figure 27 ISAKMP protection mode

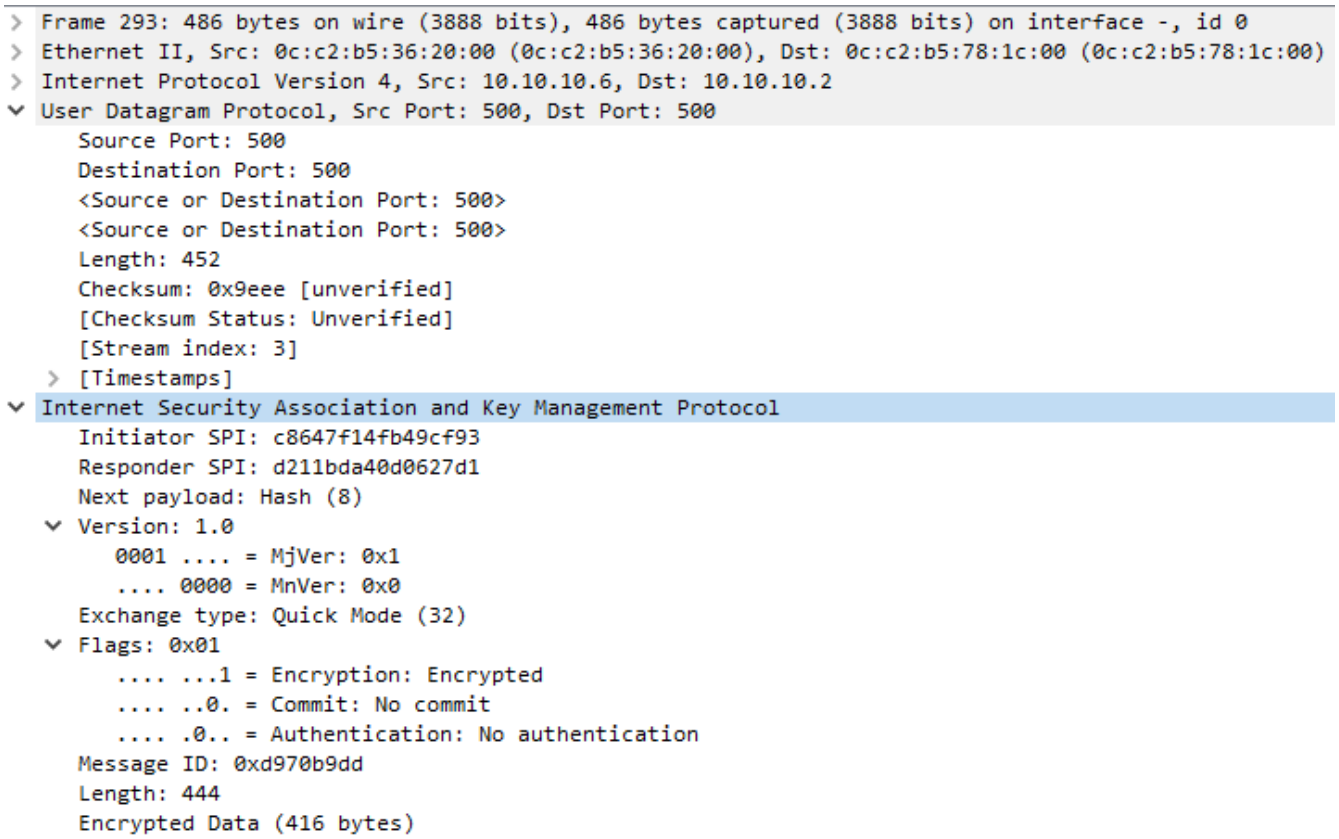

Figure 28 ISAKMP quick mode