UDC 004.49
DOI: 10.24025/2306-4412.3.2023.284551

# ORGANIZATIONAL STRUCTURE OF TECHNICAL PROTECTION OF INFORMATION AT THE NETWORK LEVEL USING VPN TECHNOLOGY

**Oleksandr Havrysh**[1]
PhD, Associate Professor
https://orcid.org/0000-0003-4621-9510, e-mail: o.havrysh@chdtu.edu.ua
**Yurii Obruch**[2]
https://orcid.org/0000-0002-7451-8772, e-mail: ndekc.ck@gmail.com
**Anatolii Chepynoga**[1]
PhD, Associate Professor
https://orcid.org/0000-0003-3921-6557, e-mail: a.chepynoha@chdtu.edu.ua
**Artem Honcharov**[1]
PhD, Professor
https://orcid.org/0000-0003-4043-5300, e-mail: a.honcharov@chdtu.edu.ua
**Olena Panasko**[1]
PhD, Associate Professor
https://orcid.org/0000-0002-0510-7742, e-mail: o.panasko@chdtu.edu.ua
[1]Cherkasy State Technological University,
Shevchenko Blvd., 460, Cherkasy, 18006, Ukraine
[2]Cherkasy Scientific Research Forensic Centre MIA of Ukraine
Pasterivska Str., 104, Cherkasy, 18000, Ukraine

**Abstract.** Recently, connecting employees to the company's internal network remotely through public resources has become widespread among small and medium-sized companies. In this case, the issue of information protection has become acute since a certain share of information may circulate through an unprotected network. Currently, VPN technology, which has many options for implementing networks for different purposes of use, is widely used. Among the variety of implementations, this research has chosen the construction of a VPN network based on Cisco equipment as an object of research. This approach has been chosen because of the prevalence and availability of equipment, and the availability of a simulator to design, set up and test the network. The organization structure, in which employees can work both inside and outside the corporate network, has been described. At the same time, each of the employees is supposed to have equal opportunities to connect to servers securely and work with data related to the organization's activities. Accordingly, for the employees who work remotely, the issue of information security is specifically acute. Therefore, the authors propose a network model, which consists of three zones: the main office, the remote worker's workplace, and a segment with servers located in the demilitarized zone (DMZ). The demilitarized zone provides an additional level of security for the local network, which minimizes damage in the event of an attack on one of the publicly available services: an external attacker has direct access only to the equipment in the DMZ. The VPN technology will be used as a means of protecting the connection of employees to servers with the organization's data. The network hardware is selected. The Cisco 2811 router which is used to cover the needs of small organizations (up to 36 workplaces) is chosen to combine all segments into one network. Practical implementation of the VPN technology settings in the presented distributed network of the organization has been conducted. The computer network is simulated in the Cisco Packet Tracer environment. As a result of fulfilling the assigned tasks, security policies have been implemented in the network based on the use of Cisco VPN technology. This tool makes it possible to organize a secure VPN channel for connections from within the organization's network, which, in turn, allows a remote employee to access the organization's servers and data. The results of this work can be used by the companies or individual users who plan to integrate the VPN architecture, based on Cisco equipment, into their network infrastructure.

**Keywords:** network, demilitarized zone, Packet Tracer simulator, Cisco, VPN tunnel, cryptographic map.

DOI: 10.24025/2306-4412.3.2023.284551

## Introduction

Modern business is reaching out far beyond the region and country borders. As a result, the enterprises' structural components have become more distributed. Accordingly, communication and exchange of information between the enterprise's branches is realized through the Internet. The pandemic also contributed to the trend when remote work became the norm for many organizations. In Ukraine, this phenomenon received an additional impetus with the full-scale war of the Russian Federation against Ukraine, which spurred an extensive migration of specialists, posed threat to the employees' safety during missile attacks, which made remote work a new reality. Organizations introduced special policies regarding remote employees. It is obvious that the growth of the number of users, the amount of information and its value naturally requires a solution to the problem of information protection (Zhilin *et al.*, 2021). Information in the modern world has become a value that must be reliably protected (Buriachok *et al.*, 2019). Every year, huge amounts of money are spent on the information security of enterprises, state institutions and organizations, but does not guarantee a complete protection of information systems, since the methods of external intervention are being improved, the initiators of which can be either ordinary cybercriminals who aim to enrich themselves or obtain a competitive advantage, or even organized groups of specialists acting in the interests of the country, whose policies and activities are aimed at the infrastructure and critically important information resources of another state (Mohan *et al.*, 2015). It is obvious that protection should be targeted at the main properties of information: integrity, confidentiality, and availability (Mykytyshyn *et al.*, 2016).

The relevance of information protection at the network level lies in the fact that there is a key need to ensure the confidentiality of data transmitted within the network (Graivoronsky *et al.*, 2009). On the scale of the office, it is quite possible to create a secure network, but this will only partially solve the security problem, because in modern conditions some employees have remote access, so it is necessary to expand the security policy of the organization to the entire network infrastructure (Semenov *et al.*, 2014).

The security policy of the organization is developed in accordance with the provisions of ND TZI 1.1-002-99 and recommendations of ND TZI 1.4-001-2000.

## Literature review

One of the common approaches to solving the problem of information security is setting up and using virtual private networks (Virtual Private Network or VPN) (Galkin *et al.*, 2016; Vasylyna *et al.*, 2013). This technology is widely spread since, in addition to the security advantages it offers, it allows the user to bypass certain network restrictions, for example, it provides access to sites and resources that are prohibited in the country or by organization regulations. With this aim, for example, you can use the Opera browser above version 40 to easily enable a free VPN option. In addition to specialized software that complements the operating system with VPN functions. In addition, there are other methods, including software and hardware and integrated solutions that employ various tools, such as a router with the function of filtering network traffic, network screens, proxy servers, software-hardware encryptors etc. (A Framework for IP Based Virtual Private Networks; Pure hardware VPNs uale high-availability tests).

The idea of building virtual VPN networks is based on a fairly simple reasoning about building a secure tunnel between two nodes of an open network, which, through cryptographic algorithms, is inaccessible to outside observers, which will ensure confidentiality and integrity of information (Medvedev *et al.*, 2002).

DOI: 10.24025/2306-4412.3.2023.284551

Cisco Systems (Cisco IOS Quality of Service Solutions Configuration Guide) is the leader in the market of network equipment used in creating and using VPN technology. The company has specifically implemented the following technologies: Cisco ASA for network screens, Cisco Secure IDS for the intrusion detection system, Cisco VPN for virtual private networks (Bartlett *et al*., 2016; Bollapragada *et al*., 2005).

VPN technology offers an opportunity to establish a network connection over another network. A VPN connection provides users with secure access to an organization's corporate network while limiting access for the attackers. To equip a network connection with such a property, it is necessary to implement three basic principles: tunneling, encryption, and authentication (Douglas Crawford). Data transfer between sender and receiver network nodes takes place through multiple nodes of an open public network, but due to tunneling, the traffic passes as if they were combined into one local network. This is implemented due to an asymmetric cryptographic encryption algorithm, which generates additional information transmitted along with the main data packet. On the receiving side, this additional information is used for data authentication, which ensures their security.

The most commonly used protocols to establish a VPN are IPSec, PPTP, PPPoE, L2TP, L2TPv3 and OpenVPN (VPN protocols; We choose the VPN protocol; What is SSL?).

VPN service providers use encryption and a set of IPSec protocols to encapsulate user data for reliable protection (IPSec is a protocol for protecting network traffic at the IP level). Cisco IOS SSL VPN technology provides access to the corporate network using the SSL cryptographic protocol and provides data transmission of various types, including those with increased bandwidth requirements (audio and video files).

## Materials and methods

*The purpose of the research*: building a model of information protection at the network level using Cisco VPN technology.

*Research objectives:*

1) describe the organization (institution) and construct a model of its distributed network, where the information protection system is implemented;

2) implement the VPN technology settings in the presented distributed network of the organization and test the information protection system.

When developing an information protection system, the developer should be guided by regulatory documents that stipulate the minimum requirements for its creation.

Here, we consider a simple model of the organization, which can be expanded and supplemented in the future. This approach will demonstrate the basic principles of implementing information protection based on Cisco VPN technology. Suppose that the institution for which an information protection system is being implemented is engaged in work related to commercial secrets and at the same time has a limited budget funding and a small staff. Therefore, for the proper functioning of the system, it is necessary to take maximum security measures, which would not exceed the limited budget.

Suppose that the staff in this organization consists of three workers who are installed in the main office and an employee who performs the duties remotely. At the same time, each of the employees must be equally enabled to securely connect to servers and work with data related to the company's activities.

One of the factors contributing to better information protection from unauthorized access and interference from the outside is to divide the network into three zones: the main office (LAN), the remote worker's workplace (Branch) and the premises with servers located in the demilitarized zone.

DOI: 10.24025/2306-4412.3.2023.284551

The Demilitarized Zone (DMZ) is a network with limited access that separates a private network from a public network. The DMZ hosts various servers, such as: file (FTP), domain name (DNS), mail (MTA), proxy, IP telephony (VoIP), etc. The purpose of DMZ is to ensure the security of a private network by providing the company with access to untrusted networks (the Internet). If you provide open access to the necessary resources of the external network, then the internal network will be at risk. The solution to this complication can be to install the necessary servers in an isolated DMZ network, which is separated from the private one by means of a firewall that will filter the traffic between them. In turn, the DMZ server is protected by another firewall, which acts as a buffer between the restricted access network and the external network. Thus, the existence of a DMZ creates two additional barriers for an attacker, whose task is to compromise the system's operation in the DMZ first, then break the protection of the internal security system, and gain access to confidential information. At the same time, if the first barrier is broken, a security breach notification will be issued. To monitor the state of the system, companies can install a proxy server inside the DMZ, which will allow monitoring user activity and filtering traffic, giving employees access to the global network. However, the efficiency of DMZ protection does not include private networks and cannot guarantee information protection in case of internal attacks.

VPN technology will be used as a means of protecting the employees' connection to servers containing the company's data. The structure of the company's distributed network built in the Cisco Packet Tracer environment (Melnyk *et al.*, 2018; Cisco Packet Tracer) is shown in Fig. 1. This simulator allows you to design network models, configure its components (routers and switches) using Cisco IOS commands, and simulate interaction between several users. The addressing of devices in the network is presented in Fig. 2.

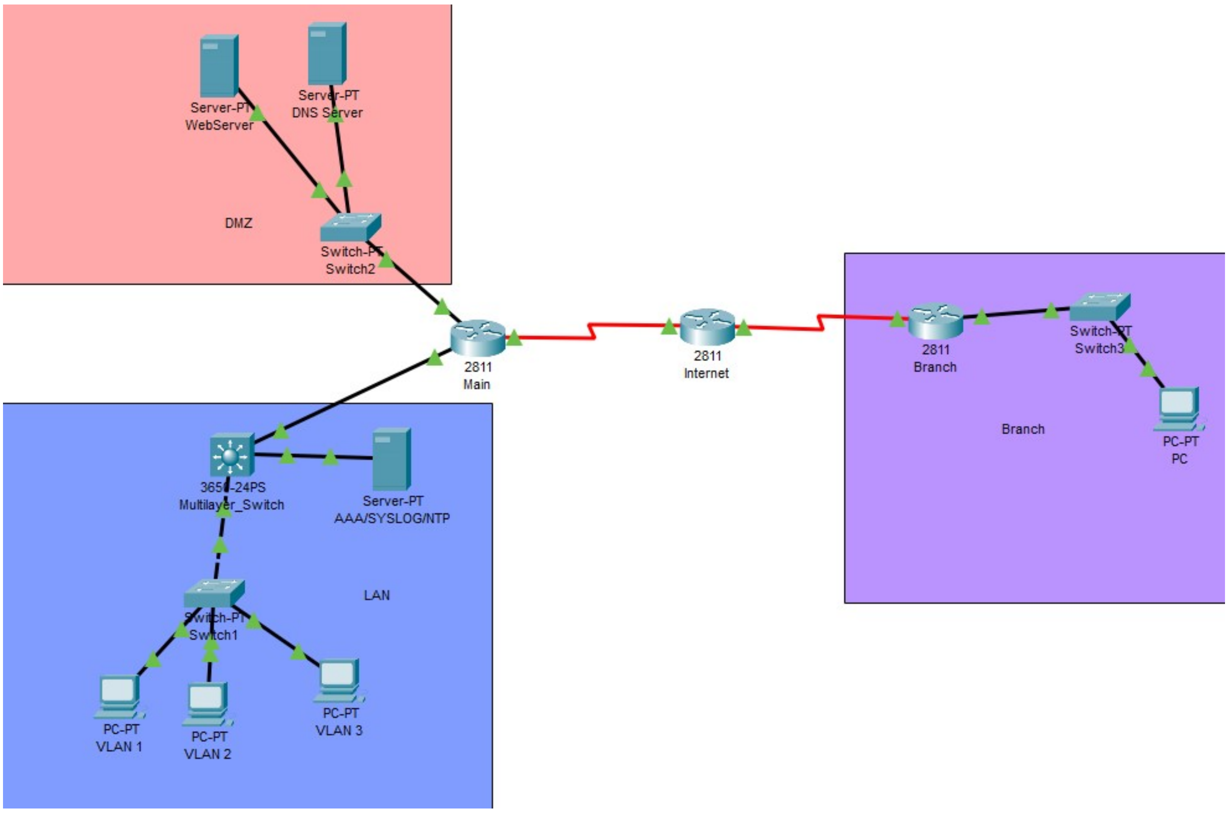
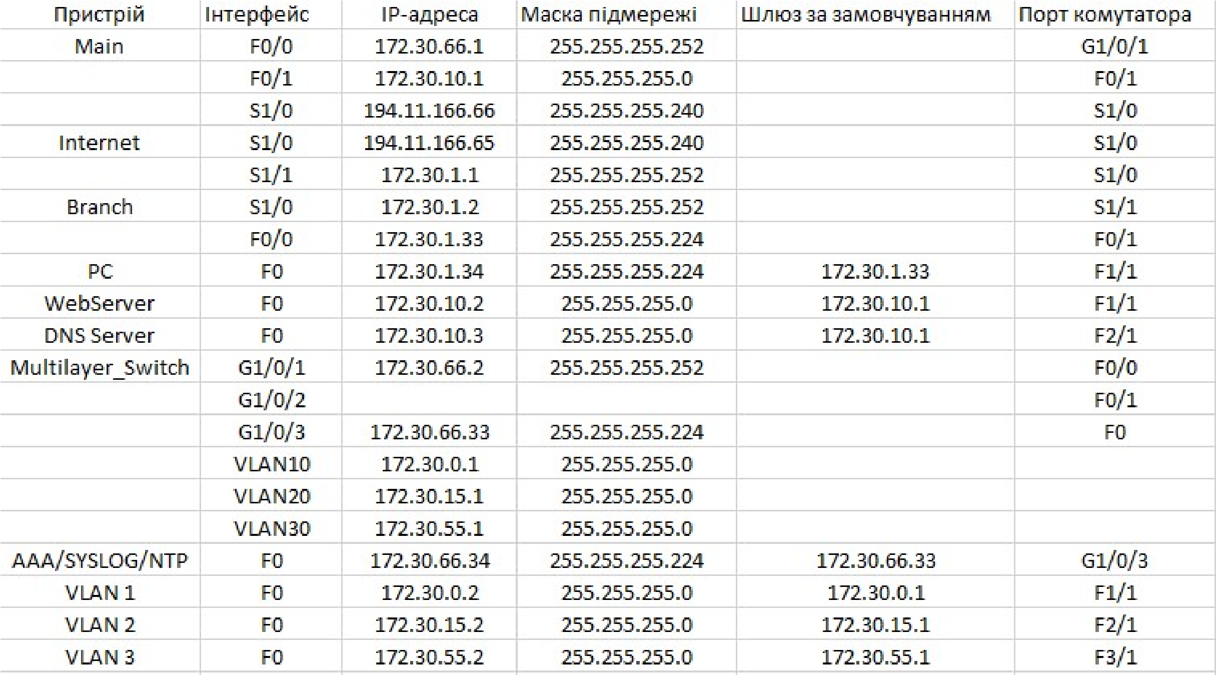


**Figure 1.** Scheme of the company's distributed network

DOI: 10.24025/2306-4412.3.2023.284551



| Пристрій | Інтерфейс | IP-адреса | Маска підмережі | Шлюз за замовчуванням | Порт комутатора |
|---|---|---|---|---|---|
| Main | F0/0 | 172.30.66.1 | 255.255.255.252 | | G1/0/1 |
| | F0/1 | 172.30.10.1 | 255.255.255.0 | | F0/1 |
| | S1/0 | 194.11.166.66 | 255.255.255.240 | | S1/0 |
| Internet | S1/0 | 194.11.166.65 | 255.255.255.240 | | S1/0 |
| | S1/1 | 172.30.1.1 | 255.255.255.252 | | S1/0 |
| Branch | S1/0 | 172.30.1.2 | 255.255.255.252 | | S1/1 |
| | F0/0 | 172.30.1.33 | 255.255.255.224 | | F0/1 |
| PC | F0 | 172.30.1.34 | 255.255.255.224 | 172.30.1.33 | F1/1 |
| WebServer | F0 | 172.30.10.2 | 255.255.255.0 | 172.30.10.1 | F1/1 |
| DNS Server | F0 | 172.30.10.3 | 255.255.255.0 | 172.30.10.1 | F2/1 |
| Multilayer_Switch | G1/0/1 | 172.30.66.2 | 255.255.255.252 | | F0/0 |
| | G1/0/2 | | | | F0/1 |
| | G1/0/3 | 172.30.66.33 | 255.255.255.224 | | F0 |
| | VLAN10 | 172.30.0.1 | 255.255.255.0 | | |
| | VLAN20 | 172.30.15.1 | 255.255.255.0 | | |
| | VLAN30 | 172.30.55.1 | 255.255.255.0 | | |
| AAA/SYSLOG/NTP | F0 | 172.30.66.34 | 255.255.255.224 | 172.30.66.33 | G1/0/3 |
| VLAN 1 | F0 | 172.30.0.2 | 255.255.255.0 | 172.30.0.1 | F1/1 |
| VLAN 2 | F0 | 172.30.15.2 | 255.255.255.0 | 172.30.15.1 | F2/1 |
| VLAN 3 | F0 | 172.30.55.2 | 255.255.255.0 | 172.30.55.1 | F3/1 |

**Figure 2.** Representation of addressing in the network

Next, we briefly consider the main segments of the network presented in Fig. 1.

- Central network device – Cisco 2811 router (connects all network segments into one) (Overview of Cisco Interface Cards for Cisco Access Routers).
- The LAN zone (highlighted in blue) is the main office (the workplaces of three employees are located).
- Demilitarized zone (highlighted in pink).
- Branch (highlighted in purple) is the branch where the remote employee's workplace is located.

A VPN tunnel is to be established between the Branch and the central device of the network called Main, because in this case, the employee from the branch will be protected from attacks on the data transmitted as a result of working inside the network and, at the same time, will be able to remotely access the company's data and work with it safely (Construction of a secure Internet access node).

*Practical implementation of VPN technology settings.* Network configuration will take place in the Cisco Packet Tracer environment. The simulator has a device library that contains all the necessary components, including various series of Cisco routers, switches and firewalls, servers for various purposes and other network equipment. The repository also presents a wide nomenclature of various types of connections between computer network elements (Melnyk *et al.*, 2018). To add a new network element, the user may simply drag the desired element to the workspace and set the connection type by clicking on the corresponding devices in turn. The Cisco Packet Tracer simulator allows you to successfully create complex network layouts, check network topology for operability. However, the implemented functionality of the devices is limited and corresponds to the equipment capacity in the real-life setting.

*Configuring security policies including VPN.* ISAKMP (Internet Security Association and Key Management Protocol) and IPSec are required to build and encrypt a VPN tunnel. ISAKMP, an alternative name for which is IKE (Internet Key Exchange), is a negotiation

DOI: 10.24025/2306-4412.3.2023.284551

protocol that allows two nodes to agree on how to establish an IPsec tunnel. ISAKMP alignment consists of two phases: Phase 1 and Phase 2.

During phase 1, the first tunnel is established to protect subsequent ISAKMP negotiation messages. During phase 2, a tunnel is established to protect the data. Then, IPSec is launched to encrypt the data using appropriate algorithms, provide authentication, and replay protection.

For further correct operation of the VPN configuration, the Security Technology package must be installed. This step may not be necessary with some versions of Cisco routers. Therefore, enter the following commands:

```
Main(config)# license boot module c1900 technology-package securityk9
Main(config)# exit
```

After that, the router needs to be rebooted: *Main# reload*

The first step is to configure the ISAKMP Phase 1 policy:

```
Main(config)# crypto isakmp policy 10
Main(config-isakmp)# encryption aes 256
Main(config-isakmp)# authentication pre-share
Main(config-isakmp)# group 5
Main(config-isakmp)# exit
```

In the above commands, the individual parameters mean the following:

AES 256 is the encryption method that will be used in Phase 1 (state-of-the-art encryption methods are recommended).

Pre-Share implies using a pre-shared key (PSK) and as an authentication method.

Group 5 is the Diffie-Hellman group that will be used.

It is possible to use the commands hash md5 (hashing algorithm) and lifetime 86400 (the lifetime of the session key, which is expressed in seconds. This value is set by default.

It is necessary to create extended access lists of ACL access rights to sort potentially dangerous traffic (traffic that needs to be filtered):

```
Main(config)# access-list 110 permit ip 172.30.0.0 0.0.0.255 172.30.1.32 0.0.0.31
Main(config)# access-list 110 permit ip 172.30.15.0 0.0.0.255 172.30.1.32 0.0.0.31
Main(config)# access-list 110 permit ip 172.30.55.0 0.0.0.255 172.30.1.32 0.0.0.31
Main(config)# access-list 110 permit ip 172.30.66.32 0.0.0.31 172.30.1.32 0.0.0.31
```

The next step is to create a transformation set (Transform Set) used for data protection (named VPN-SET):

```
Main(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
```

In the above command, ESP-AES is the encryption method, and SHA is the hashing algorithm.

The next step is to create a Crypto Map. Crypto Map represents the last step of configuration and combines the previously specified ISAKMP and IPSec configurations.

```
Main(config)# crypto map VPN-MAP 10 ipsec-isakmp
Main(config-crypto-map)# description VPN to Branch
Main(config-crypto-map)# set peer 172.30.1.2
Main(config-crypto-map)# set transform-set VPN-SET
Main(config-crypto-map)# match address 110
Main(config-crypto-map)# exit
```

In the given sequence of commands, the name of the VPN-MAP cryptographic map is specified. The ipsec-isakmp tag tells the router that this corresponding map is an IPSec cryptographic map. Match address is a command that applies an access list to a cryptographic transformation.

DOI: 10.24025/2306-4412.3.2023.284551

The last step is to apply a cryptographic map to the router interface through which the traffic passes. In this case, the output interface is Serial1/0:

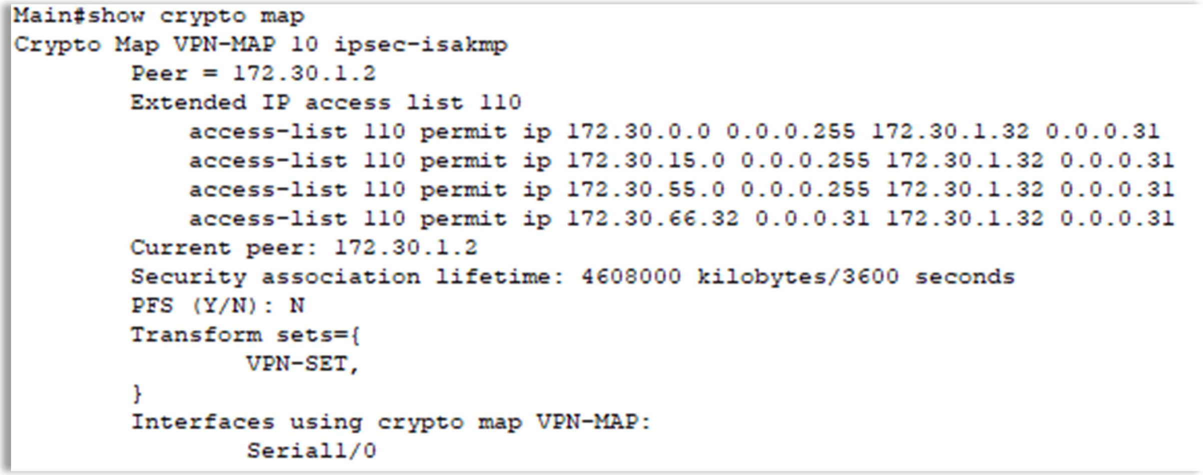
*Main(config)# interface Serial1/0*
*Main(config-if)# crypto map VPN-MAP*
*Main(config-if)# exit*

It should also be considered that only one cryptographic map can be applied to one interface.

At this point, the configuration on the Main device is completed, it is necessary to perform similar actions for the Branch device but specify unique IP addresses of ports and ACLs. The commands to configure VPN on the Branch device are given below:

```
Branch(config)# access-list 110 permit ip 172.30.1.32 0.0.0.31 172.30.0.0 0.0.0.255
Branch(config)# access-list 110 permit ip 172.30.1.32 0.0.0.31 172.30.15.0 0.0.0.255
Branch(config)# access-list 110 permit ip 172.30.1.32 0.0.0.31 172.30.55.0 0.0.0.255
Branch(config)# access-list 110 permit ip 172.30.1.32 0.0.0.31 172.30.66.32 0.0.0.31
Branch(config)# crypto isakmp policy 10
Branch(config-isakmp)# encryption aes 256
Branch(config-isakmp)# authentication pre-share
Branch(config-isakmp)# group 5
Branch(config-isakmp)# exit
Branch(config)# crypto isakmp key vpnpa55 address 194.11.166.66
Branch(config)# crypto ipsec transform-set VPN-SET esp-aes esp-sha-hmac
Branch(config)# crypto map VPN-MAP 10 ipsec-isakmp
Branch(config-crypto-map)# description VPN to Main
Branch(config-crypto-map)# set peer 194.11.166.66
Branch(config-crypto-map)# set transform-set VPN-SET
Branch(config-crypto-map)# match address 110
Branch(config-crypto-map)# exit
Branch(config)# interface Serial1/0
Branch(config-if)# crypto map VPN-MAP
Branch(config-if)# exit
```

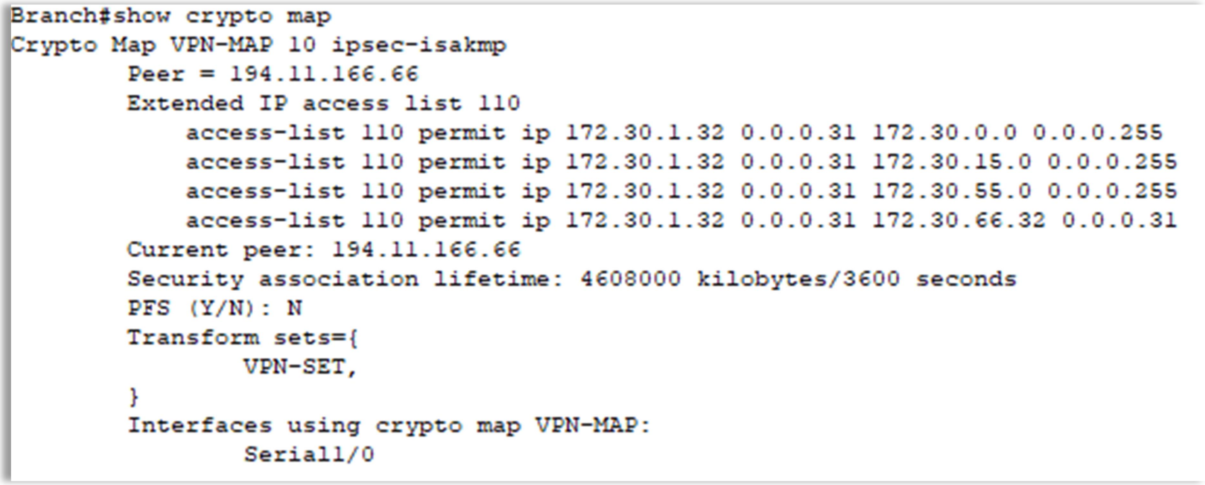
*Testing of the information protection system.* It is advisable to ensure that the VPN settings are correct using the show crypto map command. The result of the setting is shown in Fig. 3 and Fig. 4.



```
Main#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
        Peer = 172.30.1.2
        Extended IP access list 110
            access-list 110 permit ip 172.30.0.0 0.0.0.255 172.30.1.32 0.0.0.31
            access-list 110 permit ip 172.30.15.0 0.0.0.255 172.30.1.32 0.0.0.31
            access-list 110 permit ip 172.30.55.0 0.0.0.255 172.30.1.32 0.0.0.31
            access-list 110 permit ip 172.30.66.32 0.0.0.31 172.30.1.32 0.0.0.31
        Current peer: 172.30.1.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-SET,
        }
        Interfaces using crypto map VPN-MAP:
                Serial1/0
```

**Figure 3.** Result of VPN setup on Main device

DOI: 10.24025/2306-4412.3.2023.284551



```
Branch#show crypto map
Crypto Map VPN-MAP 10 ipsec-isakmp
        Peer = 194.11.166.66
        Extended IP access list 110
            access-list 110 permit ip 172.30.1.32 0.0.0.31 172.30.0.0 0.0.0.255
            access-list 110 permit ip 172.30.1.32 0.0.0.31 172.30.15.0 0.0.0.255
            access-list 110 permit ip 172.30.1.32 0.0.0.31 172.30.55.0 0.0.0.255
            access-list 110 permit ip 172.30.1.32 0.0.0.31 172.30.66.32 0.0.0.31
        Current peer: 194.11.166.66
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                VPN-SET,
        }
        Interfaces using crypto map VPN-MAP:
                Serial1/0
```

**Figure 4.** Result of VPN configuration on Branch device

## Results and discussion

Considering the growing trend of introducing remote work in many companies, this paper considers one of the possible options for protecting company information using VPN technology, which allows creating secure networks and significantly reduces possible threats of information leakage. The research was conducted with the equipment of the Cisco family.

With the help of the Cisco Packet Tracer simulator, a practical computer model of the company's distributed network was built, and its operation was simulated taking into account the capacity of real equipment from the same manufacturer.

The configuration of security policies, including VPN, is considered, which includes establishing and encrypting a VPN tunnel, specifying the AES 256 encryption method, using a pre-shared key (PSK) as an authentication method, filtering traffic, creating a transform set (Transform Set) used for protection of personal data, creating a cryptographic map and applying it to the interface of the router through which the traffic passes.

The Cisco Packet Tracer simulator assesses the correctness of VPN settings and, if necessary, introduces appropriate adjustments.

## Conclusions

The current study implemented the security policies in the company's network based on the use of Cisco VPN technology. This tool made it possible to organize a secure VPN channel for connections from within the company's network, which in turn allows a remote employee to access the company's servers and data.

*The scientific novelty* of the study consists in the construction of a model of information protection at the network level using Cisco VPN technology, which involves dividing the network into three zones and creating a VPN tunnel, which allows organizing a secure remote connection of users to their workplaces.

*The practical significance* of the obtained results is a test-verified model, which can be promptly implemented for practical use because it is oriented towards real equipment, taking into account its possible limitations of work in real conditions. This is especially important for companies whose employees connect remotely over unsecured network infrastructure, such as using public Wi-Fi networks.

DOI: 10.24025/2306-4412.3.2023.284551

*Prospects for further research.* The proposed model of information protection in a company where some employees work remotely is a complete, but basic model, but due to its flexibility, it can be scaled according to the requirements of a specific customer, taking into account their needs and wishes. A wide range of Cisco equipment will satisfy the needs of the most demanding customer. The described procedures for the practical implementation of the network infrastructure, the configuration of security policies and testing the correctness of the settings remain unchanged and will be extended to the added new devices.

## Acknowledgments

The authors would like to thank the Cisco Networking Academy for providing free access to resources for members of the Cisco Networking Academy Program.

## Conflict of Interest

The authors have no conflict of interest.

## References

A Framework for IP Based Virtual Private Networks. Retrieved from http://www.ietf.org/rfc/rfc2764.txt.

Bartlett, G., & Inamdar, A. (2016). *IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS*. Cisco Press.

Bollapragada, V., Mohamed, Kh., & Wainner, S. (2005). *IPSec VPN Design.* Cisco Press.

Buriachok, V.L., Anosov, A.O., Semko, V.V., Sokolov, V.Yu., & Skladannyi, P.M. (2019). *Technologies for ensuring network infrastructure security.* Kyiv: KUBG.

Cisco IOS Quality of Service Solutions Configuration Guide. Retrieved from https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos/command/qos-cr-book.pdf.

Cisco Packet Tracer. Retrieved from https://www.netacad.com/ru/courses/packet-tracer.

Construction of a secure Internet access node using VPN and tunneling technology. Retrieved from http://www.opennet.ua/docs/UAS/vpn_solution/.

Crawford, D. OpenVPN over TCP vs. UDP: What is the difference, and which should I choose? Retrieved from https://www.bestvpn.com/blog/7359/openvpn-tcp-vs-udp-differencechoose/.

Galkin, V.V., & Parkhomenko, I.I. (2016). The use of VPN technologies for the protection of information in the channels of corporate networks. In *Proceedings of the scientific and technical conference "Problems of Cyber Security of Information and Telecommunication Systems"* (KNU, Kyiv, March 10-11, 2016) (p. 66). Kyiv: KNU.

Graivoronsky, M.V., & Novikov, O.M. (2009). *Security of information and communication systems: a textbook for universities*. Kyiv: BHV.

IPSec is a protocol for protecting network traffic at the IP level. Retrieved from https://www.ixbt.com/comm/ipsecure.shtml.

Medvedev, N.G., & Moskalyk, D.V. (2002). *Aspects of the information system of virtual private networks*. Kyiv: European University.

Melnyk, H.M., Verbovy, S.O., & Voznyak, S.I. (2018). *Methodological recommendations for performing laboratory work in the discipline "Computer networks" for students of the bachelor's degree in specialty 123 "Computer engineering"*. Ternopil: TNEU.

DOI: 10.24025/2306-4412.3.2023.284551

Mohan, V. Pawar, & Anuradha, J. (2015). Network security and types of attacks in network. In *International Conference on Intelligent Computing, Communication & Convergence. Procedia Computer Scienc*e, 48, 503-506.

Mykytyshyn, A.G., Mytnyk, M.M., & Stuhlyak, P.D. (2016). *Complex security of information network systems: a study guide.* Ternopil: Publishing House of Ivan Pulyuy TNTU.

ND TZI 1.1-002-99 General provisions on the protection of information in computer systems against unauthorized access, order of the DSTSZI of the SBU dated 04/28/99 (Amendment No. 1 order of the State Special Communications Administration dated 12/28/2012 No. 806). Retrieved from https://tzi.com.ua/downloads/1.1-002-99.pdf.

ND TZI 1.4-001-2000 Standard provisions on the information protection service in automated systems, order of the DSTSZI of the SBU dated 04.12.2000 No. 53 (Amendment No. 1 order of the Administration of State Special Communications dated 28.12.2012 No. 806). Retrieved from https://tzi.com.ua/ downloads/1.4-001-2000.pdf.

Normann, R. We choose the VPN protocol. Retrieved from http://www.osp.ua/ win2000/2001/07/175027/.

Overview of Cisco Interface Cards for Cisco Access Routers. Retrieved from https://www.cisco.com/c/en/us/td/docs/routers/access/interfaces/ic/hardware/installation/guide /oview_ic.pdf?dtid=osscdc000283.

Pure hardware VPNs uale high-availability tests. Retrieved from https://web.archive.org/ web/20070923013848/.

Semenov, S.G. et al. (2014). *Information protection in computer systems and networks: education. manual.* Kharkiv: NTU "KhPI".

Vasylyna, A.V., Yalovy, M.M., & Tsibulyak, B.Z. (2013). Protection of qualified communication channels using virtual private network systems. In *Proceedings of the International academic-practical conference "Problems and Prospects of Civil Protection"* (Kharkiv, April 3-4, 2013) (pp. 266-268). Kharkiv: Publishing House of the National Center of Ukraine.

VPN protocols. Retrieved from https://www.cactusvpn.com/ua/beginners-guide-to-vpn/vpn-protocol/.

What is SSL? Retrieved from http://www.ods.com.ua/win/uas/security/ssl.html.

Zhilin, A.V., Shapoval, O.M., & Uspenskyi, O.A. (2021). *Information protection technologies in information and telecommunication systems: training manual*. Kyiv: KPI named after Igor Sikorskyi, Polytechnic Publishing House.

DOI: 10.24025/2306-4412.3.2023.284551

# ОРГАНІЗАЦІЙНА СТРУКТУРА ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ НА МЕРЕЖЕВОМУ РІВНІ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЇ VPN

**О. С. Гавриш**[1]
Канд. фіз.-мат. наук, доцент
https://orcid.org/0000-0003-4621-9510, e-mail: o.havrysh@chdtu.edu.ua
**Ю. Ю. Обруч**[2]
https://orcid.org/0000-0002-7451-8772, e-mail: ndekc.ck@gmail.com
**А. В. Чепинога**[1]
Канд. техн. наук, доцент
https://orcid.org/0000-0003-3921-6557, e-mail: a.chepynoha@chdtu.edu.ua
**А. В. Гончаров**[1]
Канд. техн. наук, професор
https://orcid.org/0000-0003-4043-5300, e-mail: a.honcharov@chdtu.edu.ua
**О. М. Панаско**[1]
Канд. техн. наук, доцент
https://orcid.org/0000-0002-0510-7742, e-mail: o.panasko@chdtu.edu.ua
[1] Черкаський державний технологічний університет
б-р Шевченка, 460, м. Черкаси, 18006, Україна
[2] Черкаський науково-дослідний експертно-криміналістичний центр МВС України
вул. Пастерівська, 104, м. Черкаси, Україна

**Анотація.** В останні роки для малих і середніх компаній поширилася практика дистанційного підключення працівників до внутрішньої мережі компанії через загальнодоступні ресурси. В цьому випадку гостро постає питання захисту інформації, оскільки її частина може циркулювати у незахищеній мережі. Нині широко використовується технологія VPN, яка має багато варіантів реалізації мереж для різних цілей використання. Серед різноманіття реалізацій в роботі розглянуто побудову VPN мережі на базі обладнання компанії Cisco. Такий підхід обумовлений поширеністю та доступністю устаткування, наявністю симулятора для проєктування, налаштування та апробації мережі. Здійснено опис структури організації, особливістю якої є те, що співробітники можуть працювати як всередині корпоративної мережі, так і за її межами. При цьому кожен із працівників повинен мати однакові можливості для захищеного підключення до серверів та роботи з даними, що фігурують при роботі організації. Відповідно для фахівців, що працюють дистанційно, гостро постає питання безпеки інформації. Тому була запропонована модель мережі, яка розділяється на три зони: головний офіс, місце роботи віддаленого працівника та сегмент із серверами, які знаходяться у демілітаризованій зоні (DMZ). Наявність демілітаризованої зони надає додатковий рівень безпеки в локальній мережі, який дозволяє мінімізувати збитки в разі атаки на один із загальнодоступних сервісів: зовнішній зловмисник має прямий доступ тільки до обладнання в DMZ. Як засіб, що буде захищати підключення працівників до серверів з даними організації, буде використовуватись технологія VPN. Здійснено вибір апаратного забезпечення мережі. Для поєднання усіх сегментів в одну мережу обрано маршрутизатор Cisco 2811, який використовується для потреб невеликих організацій (до 36 робочих місць). Проведено практичну реалізацію налаштувань технології VPN у представленій розподіленій мережі організації. Проведено моделювання комп’ютерної мережі в середовищі Cisco Packet Tracer. В результаті виконання поставлених завдань було впроваджено політики безпеки в мережі на основі використання технології Cisco VPN. Цей засіб дозволив організувати захищений VPN канал для підключень зсередини мережі організації, що, в свою чергу, дає змогу працівнику, який працює віддалено, отримати доступ до серверів та даних організації. Результати цієї роботи можуть використати компанії чи окремі користувачі, які планують інтегрувати архітектуру VPN, на базі обладнання Cisco, до своєї мережевої інфраструктури.

**Ключові слова:** мережа, демілітаризована зона, симулятор Packet Tracer, Cisco, VPN-тунель, криптографічна мапа.

*Дата надходження: 13.07.2023*
*Прийнято: 08.09.2023*

DOI: 10.24025/2306-4412.3.2023.284551