JEL Classification: L15, L29. https://doi.org/10.35945/gb.2022.13.020

ACTUAL ISSUES OF BUILDING SECURE COMMUNICATION CHANNEL CONSIDERING MODERN TECHNOLOGICAL CHALLENGES

IOSEB KARTVELISHVILI

Associate Professor,
Georgian Technical University, Georgia
s.kartvelishvili@gtu.ge

TEA TODUA

Associate Professor,
Georgian Technical University, Georgia
tea_todua@gtu.ge

Abstract. In today's globalized, dynamic world, organizations' dependence on information and, consequently, their interest and demands for information is growing. Information technologies play a crucial role in effective functioning and control for modern companies and business. In the conditions of operational accessibility of necessary information it is possible to adequate evaluation of current situation and to make timely decision. At the same time, information must be available only to those to whom it is intended and unavailable - to all remaining. Computers are integrated into a common network for fast data transfer and efficient interaction. This connection must be reliable and secure. Modern companies are interested in possibility of using Internet channels. However, the principles of building of the Internet give the chance to malefactors to steal and distort information purposely. Corporate and broadcasting networks which are based on TCP/IP protocols and are constructed on standard Internet applications (E-mail, Web, FTP) have no warranty from invasion of unauthorised persons. In article the technology of creation of the virtual private networks (VPN), which is one of the optimal variants for creation of secure channel of communication, is considered.

KEYWORDS: INFORMATION TECHNOLOGY, VIRTUAL PRIVATE NETWORK (VPN), SECURE COMMUNICATION CHANNELS.

For citation: Kartvelishvili, I., & Todua, T. (2022). Actual Issues of Building Secure Communication Channel Considering Modern Technological Challenges. *Globalization and Business.* 13, 134-137. https://doi.org/10.35945/gb.2022.13.020

INTRODUCTION

Modern information technologies are a powerful tool for accelerating progress in all areas of social development. Of course, this is one of the important factors that determines the competitiveness of a country, region, industry and individual organization. Information is as important asset for organization as any other significant assets of management and needs to be properly managed. This issue becomes especially actual in an interdependent and related business environment.

In the modern information world information processing processes require more accuracy and reliability. As a result, organizations are consistently and step-by-step faced with the problem of adapting and implementing specific management models or practices to their own needs. Business partners are also more willing to work with organizations that see the need for correct, reliable and secure processing of information and take it into account in their work.

In order to effectively fight against cyber attacks in business or banking sphere and to ensure the active and secure use of the computer network, the concept of building virtual private networks - VPN (Virtual Private Network) was created and actively developed in the early 90s of the 20th century. A VPN is a network architecture implemented for the purpose of achieving privacy in a commonly accessible network. It has become a reliable and low-cost solution for network and telecommunication type organizations. Virtual private networks are quite profitable for any kind of IT industry as it enables huge cost savings on infrastructure at the expense of universally accessible internet usage so that communication channels are secure.

Problems of building secure connection channels

VPN technology implies that the connection between two nodes is temporary and it exists only when transmitting

information flows over a public network. The technical implementation of virtual private tunnels and networks has historically taken place in two directions:

- By using the built-in mechanisms of the organization of virtual channels, building a frame relay between the two points of the common infrastructure of network, which is isolated from other users.
- By using tunneling technology, building a virtual IP tunnel between two network nodes, during this process each IP packet is encrypted and moved to a special type of new packet data field.

The first modern network technology to create a virtual private network became the frame relay service. VPN simplifies creation of connections, in order to make it work, you only need to connect the node to the provider. Routers send data to the required address, using a VPN is much cheaper.

With the advent of network services for connecting separate network nodes, it has become possible to actively use an internet based VPN. As we mentioned above, such solution is much cheaper in comparison to previous approaches. All this made it possible to actively use one of the main virtues of the Internet - easy access. Therefore, with the help of internet connection, any person could easily connect to a bank or various companies from anywhere in the world. However, due to the openness of the Internet data, the data transmitted through this network is available to anyone to read or modify it. That is why Internet-based VPNs have the means to protect the information transmitted between VPN nodes.

The Internet-based VPN network is based on two main technologies: first - it is a tunnel that allows the creation of virtual channels, the second is the provision of confidentiality and security of transmitted information, as well as various methods of user authentication and authorization. Authentication is the proof of authenticity, the procedure of verifying the subject and its compliance, with the help of unique information, in the simplest case - by name and password. Authorization is the process of checking the necessary parameters, as well as the outcome of the process and the transfer of authority (access right) to a person or a group of persons to perform certain actions in different restricted access systems. The development of VPN technology has led to its connection to cryptographic methods of information protection.

The concept of building VPN is based on a fairly simple idea: if there are two nodes in a global network that want to exchange information, then between these two nodes it is necessary to build a virtual tunnel to ensure the confidentiality and inviolability of the information transmitted by public network. Access to this tunnel should be very complicated, for all possible active and passive outside observers. For example, by creating such virtual tunnels, banks can get significant savings in financial resources. The bank can refuse to build or lease expensive separate channels to set up its own Internet/extranet networks and use cheap Internet channels for which the speed and reliability of transmission are not inferior to those of separate lines. However, there are two major types of attack threats involved when connecting a corporate LAN to a public network:

- Unauthorized access to internal resources of corporate local networks, which is obtained by the perpetrator as a result of unauthorized access to this network;
- Unauthorized access to corporate data during the process of their transfer to the public network.
- In case of using local area networks and separate computers public networks, information security can be ensured by effectively solving the following tasks:
- Protection of local area networks connected to public channels, as well as individual computers connected to these networks through external unauthorized access;
- Protection of information in the process of its transmission through public channels.

Firewalls are commonly used to protect local area networks and individual computers from unauthorized access. They are placed between local and public networks. For the protection of a separate remote computer connected to a public network, network monitor software is installed on this computer. Such a network monitor is called a personal monitor.

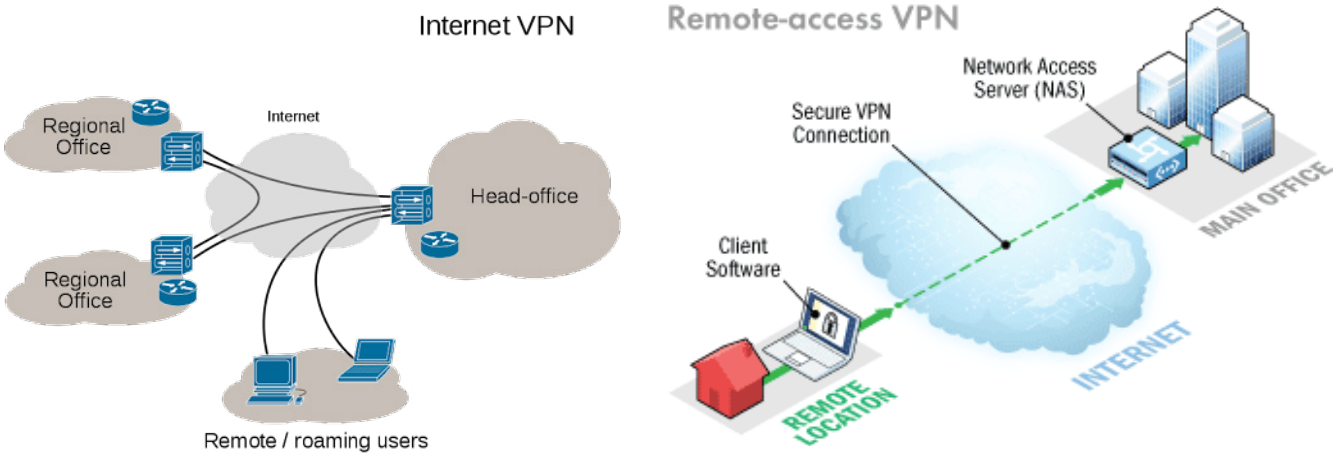
Data protection, in the process of its transmission through public channels, is based on the use of virtual protected networks. Virtual protected networks are the combination of local area networks and individual computers into a single virtual corporate network that ensures the security of circulating data. Virtual protected networks are formed by building virtual protected connection channels. These virtual protected connection lines are called VPN tunnels. The VPN network gives possibility by using VPN tunnels to connect central offices, branch offices, business partner offices, and users to securely exchange information over the Internet (Pic. 1).

A VPN tunnel transmits cryptographically protected information packets. Information security in the process of transmitting it through VPN tunnel is based on the following functions:

- authentication of interacting parties;
- cryptographic encryption of transmitted data;
- checking the authenticity and safety of the transmitted information.

The effectiveness of such protection is ensured at the expense of the joint use of symmetric and asymmetric cryptographic systems. A VPN tunnel formed by VPN devices has protected dedicated line properties. Besides this, Internet VPN devices in virtual private networks can play the role of VPN client or VPN server. A VPN client is a set of software or hardware that is usually executed on a personal computer basis. Its network software is modified to perform information flow encryption and authentication, which allows this

Pic.1. VPN network



device to exchange transactions with other VPN clients or VPN servers. A VPN server is a set of software or hardware that is installed on a computer and performs server functions. A VPN server ensures the protection of servers from unauthorized access, as well as the organization of secure connections to separate computers and local area segment computers protected by appropriate VPN products. A VPN server is a functional analogue of a VPN client for a server platform. It is primarily characterized by enhanced resources to support multiple connections to VPN clients. A VPN server can also support a secure connection to a smartphone user.

CONCLUSION

The technology of building virtually secure private VPN networks are very popular among large companies (banks, large government and private companies, etc.). The reason for such interest is that VPN technologies allow companies not only significantly reduce their expenses for managing dedicated channels to connect to distant branches, but also to increase the confidentiality of information exchange. The use of VPN ensures the organization of protected tunnels, both between the company's offices and with separate workstations and servers. However, it does not matter which ISP will connect a particular workstation to the enterprise's protected resources. All a foreign observer will see is a stream of ordinary IP packets with unknown content. Instead of the traditional method of connecting Internet users virtual private networks (VPNs) are introduced, which allow users to communicate freely with each other via the Internet.

There are different options for VPN classification. According to the technical solution architecture, there are three main types of virtual private networks: intra-corporate VPN, VPN with remote access, extranet VPN.

Intranet VPNs are designed to provide secure interactions between subdivisions within an enterprise that are connected by a corporate network, including dedicated lines.

Remote access VPN are designed to provide secure access between remote corporate information resources.

Extranet VPN is designed to ensure secure exchange of information between strategic partners. It also provides direct access from one company's network to another company's network and thus contributes to the reliability of the connection.

Based on the above, we can conclude that among the remote computers that use the Internet infrastructure to create a secure connection channel, VPN technology is one of the most optimal options today. The issue is highly topical, as a reliable connection through which confidential information can be transmitted is essential in many areas of human activity, such as banking, e-commerce, etc. VPN is very convenient to solve this problem, it is one of the most powerful and convenient technology to establish different types of connections in the global network.

REFERENCES:

Feilner, M. (2006). OpenVPN - Building and Integrating Virtual Private Networks. Packt Publishing.

Jyothi, K.K., & Reddy, D.I.B. (2018). Study on Virtual Private Network (VPN), VPN's Protocols and Security. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 3, 919-932.

Kartvelishvili, I., Darchashvili, M., & Okhanashvili, M. (2021). Virtual Private Network - VPN technology and the advantages of its use in the network. International scientific -technical conference - Information Society and Education Intensification Technologies. GTU Thematic Scientific Papers Collection, *Automated Management Systems*. 1 (32), Tbilisi. (In Georgian).

Kartvelishvili, I., & Todua, T. (2017). Issues of Security of Wireless Networks. Actual Problems of Knowledge Economy in Modern Globalization. 2-nd International Conference. Tbilisi.

Kartvelishvili, I., Shonia, O., Beridze, Z., & Shonia, I. (2012). Combined method of encryption of characters in virtual private networks (VPN). Georgian Technical University, *Automated Management Systems*. 1 (12), Tbilisi. (In Georgian).

Kartvelishvili I., & Shonia L. (2018).Virtual Private Network (VPN) construction concept, network functions and their classification. International Scientific-Technical Conference - International Society and Education Intensification Technologies. International Scientific Journal *Automated Management Systems*. 2 (26), Tbilisi. (In Georgian).

Kartvelishvili, I., Shonia, O., Kaishauri, T., Shonia, L., Beridze, Z., & Didmanidze, I. (2012). Algorithm of Combined Method for Symbol Encoding In Virtual Private Networks (VPN). *Journal of Technical Science & Technologies*. 2 (1). (In Georgian).

Kaur, K., & Kaur, A. (2019). A Survey of Working on Virtual Private Network. IRJET, 6, (9).

Sharma, Y.K., & Kaur, C. (2020). The Vital Role of Virtual Private Network (VPN) in Making Secure Connection Over Internet World. *International Journal of Recent Technology and Engineering* (IJRTE) ISSN: 2277-3878, 8 (6).

Singh, K., & Gupta, H. (2016). A new approach for the security of VPN. ICTCS ‹16: Proceedings of the Second International Conference on Information and Communication Technology for Competitive Strategies.