MCIT Modeling, control & information technologies

Concept and functions of building a private network (VPN)

https://doi.org/10.31713/MCIT.2021.04

Beridze Zebur
Batumi Shota Rustaveli State University, BSU
Batumi, Georgia
zazaber@mail.ru

Shavadze Jumber
Batumi Shota Rustaveli State University, BSU
Batumi, Georgia
ibraimd@mail.ru

Geladze Nona
Batumi Shota Rustaveli State University, BSU
Batumi, Georgia

Geladze Miranda
Batumi Shota Rustaveli State University, BSU
Batumi, Georgia

***Abstract* – As companies and organizations began to actively use computers in various areas of their work, these computers needed to be integrated into a common network for fast data transfer and efficient interaction. However, this connection must have been reliable and secure.**

***Keywords* – Virtual Private Network; network services; local area networks.**

I. INTRODUCTION

In order to effectively fight against network attacks and to ensure the possibility of active and secure use, the concept of building virtual private networks - VPN (Virtual Private Network) was created and is actively being developed.

The word `virtual VPN 'is included in the term to emphasize that a connection between two nodes should be considered as a temporary connection as long as it is not a permanent (hard) connection and exists only when transmitting information flows over an open network.

Since networking services for connecting separate network nodes have appeared, it has made it possible to actively use VPNs based on the Internet. All this made it possible to actively use one of the main virtues of the Internet - easy access. Therefore, anyone with the help of the Internet 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 everyone to read or change it. That is why VPN networks on the Internet have the means to protect the information transmitted between VPN nodes. This is why these networks are usually called VPNs (Virtual Private Networks). In this context, it means both "private" and "protected".

VPN technology soon became strongly associated with cryptographic methods of information protection and the creation of virtual protected networks - VPNs became one of the top priorities. Its main task is to solve 4 main problems: security-confidentiality, authentication, integrity and control of the participants (users). Cryptography is part of a mathematical technique involved in storing data protected from attackers. For example, cryptographic mechanisms have been developed to protect data privacy. Cryptographic schemes are designed in such a way that the information transmitted over the air (e.g., over a wireless system) is encoded and cannot be interpreted by attackers, although an attacker may obtain encoded data by accessing the data transmitted over the air. Cryptography can also be used to be sure that the data was indeed created by the entity that claimed its creation. This feature is also called data authentication.

Main part. The concept of building a VPN on virtual networks is based on a fairly simple idea: if there are two nodes in a global network that want to exchange information, then it is necessary to build a virtual tunnel between these two nodes to ensure the confidentiality and inviolability of open network information. Access to this tunnel should be very complicated, for all possible active and passive outside observers.

There are two major types of attack threats involved when connecting a corporate local area network to an open network:

- Unauthorized access to the 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 open network.

Securing information interaction with local area networks and individual computers, in particular the Internet, can be ensured by effectively solving the following tasks:

- Protect connections of local area networks and operating computers connected to open channels from outside unauthorized action;
- Protection of information in the process of transmission of its connection through open channels.

The protection of information through open channels in its transmission process is based on the use of virtual protected VPN networks. Virtual protected VPN 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 VPN networks are formed by building virtual protected connection channels. These virtual protected connection lines are called VPN tunnels. VPN network allows VPN tunnels to connect head office, branch offices, business partner

offices, remote users, and securely exchange information over the Internet

A VPN tunnel is an open network connection that transmits cryptographically protected information packets to virtual network messages. The protection of information in the process of transmitting it through its VPN tunnel is based on the performance of the following functions:

- Authentication of interacting parties;
- Cryptographic closure (encryption) of transmitted data;
- Checking the authenticity and safety of the transmitted information.

These functions are characterized by interrelationships. Cryptographic methods of information protection are used in their realization. The effectiveness of such protection is ensured through the joint use of symmetric and asymmetric cryptographic systems. A VPN tunnel formed by VPN devices has protected dedicated line properties. However, this protected breakdown line breaks down into a network frames with a common connection.

A VPN client is a software or software-hardware complex that is usually run on a personal computer basis. Its network software is modified to perform information flow encryption and authentication by which this device performs interchange operations with other VPN clients or VPN servers.

VPN-Server provides protection of servers from unauthorized access from the environment, as well as the organization of secure connection to computers of the local network segment protected by separate computers and local VPN-products.

The safety and service quality of wireless networks has become a subject of considerable and active research over the past few years, what is caused by a growing requirement for supporting the transfer of data packages. Any node which is located in the transmission range of a delivery node and which knows the operating frequency and other physical attributes (modulation, encoding, etc.) can potentially encrypt the signal so that a sender or an alleged recipient will not know anything about that interference. However, such interference in cable networks can occur if an attacker has an access to physical means of transmission (wires, fibers, etc.) what requires the accession to the facility. As wireless networks are not dependent on infrastructure-based resources, such as power stable source, high frequency, continuous connection or unchanging routing, they can be easily attacked.

CONCLUSION

An experienced hacker or accidentally snooper can easily track the unwanted packages and open the data in it, using the software means. Of course, the main danger is the fact that as a result of such an attack, some people can have access to important information such as usernames and passwords, credit card numbers and other.

VPN technologies allow secure tunnels to be organized both between offices and with separate workstations and servers. However, it does not matter which Internet provider is used by a particular workstation to connect to protected resources of the enterprise. All that is seen by a stranger observer is a stream of ordinary IP packets with unknown content. Instead of the traditional method of connecting Internet users via modems or dedicated lines, virtual private networks - VPNs are introduced, which allow users to communicate freely with each other via the Internet.

REFERENCES

[1]. Didmanidze Ibraim, Zaslavski Vladimir, Beridze Zebur, Didmanidze Didar. Analysis of wireless network security systems problems and those solutions. Works of conferences. No. 4 (2020), 5–7 november, Rivne, Ukraine, p. 139–140.

[2]. Beridze Z. Safety of informational interaction. XXXV international conference PROBLEMS OF DECISION MAKING UNDER UNCER-TAINTIES (PDMU-2020). ABSTRACTS. May 11-15, 2020, Baku-Sheki, Republic of Azerbaijan. p. 23.

[3]. Didmanidze Ibraim, Beridze Zebur. MAIN TASKS AND ALGORITHMS OF WIRELESS NETWORK SECURITY SUPPORTING AUTOMATED SYSTEM. PROBLEMS OF ATOMIC SCIENCE AND TECHNOLOGY, Series: Nuclear Physics Investigations (74), 2020, N 5(129). p. 86–93.

[4]. Beridze Z., Shavadze J., Geladze M. Main stages of designing automated system supporting wireless networks. XXXIII international conference PROBLEMS OF DECISION MAKING UNDER UNCERTAINTIES (PDMU-2019). ABSTRACTS. January 24-February 1, 2019, Hurgada, Egypt. p. 21–22.