International Journal of Academic Pedagogical Research (IJAPR)
ISSN: 2643-9123
Vol. 5 Issue 1, January - 2021, Pages: 55-57

Virtual Protected Networks

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *In order to benefit from the ubiquity of the Internet, work has been done to create a virtual private network VPN that effectively resists network attacks and allows businesses to actively and securely use open networks. As a result, in the early 1990s, the concept of a virtual private network VPN was created. The term "virtual" was coined to indicate that a connection between two nodes is considered temporary. In fact, this connection is permanent, not fixed, and only exists when traffic passes over an open network.*

Keywords: VPN tunnel, IpSec, Network-level VPN-products encapsulate IP to IP.

INTRODUCTION

1. The concept of VPN and its types

2. Classification of VPN networks

3. Basic types of VPN network building

In order to benefit from the ubiquity of the Internet, efforts have been made to create a virtual private network VPN that can effectively resist network attacks and allow businesses to actively and securely use open networks. As a result, in the early 1990s, the concept of a virtual private network VPN was created. The term "virtual" was coined to indicate that a connection between two nodes is considered temporary. In fact, this connection is permanent, not fixed, and only exists when traffic passes over an open network.

METHODS

The protection of information during the transmission through the VPN tunnel is based on the following tasks:

• authenticate the parties involved;

• cryptographic encryption of transmitted data;

• Verification of the authenticity and integrity of the information provided.

Routers are used to create protected channels according to this method of building a VPN. Since all information from the local network passes through the router, it is natural to load it with encryption. Examples of router-based VPN devices are Cisco-Systems devices.

VPN based on firewalls.

Most manufacturers' firewalls support tunneling and data encryption functions. An example of a firewall-based solution is Check Point Software Technologies' Fire Wall-1. Personal

computer-based firewalls are only used in networks with relatively small amounts of transmitted information. The disadvantages of this method are the high cost of the solution per worker and the fact that productivity depends on the hardware that runs the firewall.

Software-based VPN.

While software-based VPN products lag behind a specialized device in terms of performance, they are powerful enough to implement VPNs. It should be noted that the requirements for the required bandwidth for remote use are not high. Therefore, the software products themselves provide sufficient performance for remote use. The undoubted advantages of software products are flexibility and ease of use, as well as relatively low cost.

VPN based on specialized hardware.

The most important advantage of VPNs based on specialized hardware is high productivity. Encryption in specialized VPN systems on chips allows for speed. Specialized VPNs provide a high level of security, but their cost is much higher.

VPN classification by OSI model

Channel level VPN

The VPN tools used in the channel layer of the OSI model allow encapsulation of various third-level (and higher) layer traffic and build virtual tunnels in a "point-to-point" language (from a router to a router or from a personal computer to a local area network gateway).

Network-level VPN.

Network-level VPN-products encapsulate IP to IP. One of the most common protocols at this level is the SKIP protocol. However, this protocol is gradually being pushed out by the IPSec (IPSecurity) protocol, which is called for authentication, tunneling, and encryption of IP packets.

Session-level VPN

Some VPNs use a method called "circuit proxy". This method works on the transport layer and retransmits a separate traffic for each socket from the protected network to the public Internet. (An IP socket is identified by a combination of a TCP connection and a specific port or UDP. The TCP / IP stack does not have a fifth session level, but socket operations are often referred to as session level operations.)

RESULTS

The VPN tools used in the channel layer of the OSI model allow encapsulation of various third-level (and higher) layer traffic and build virtual tunnels in a "point-to-point" language (from a router to a router or from a personal computer to a local area network gateway).

While software-based VPN products lag behind a specialized device in terms of performance, they are powerful enough to implement VPNs. It should be noted that the requirements for the required bandwidth for remote use are not high. Therefore, the software products themselves provide sufficient performance for remote use. The undoubted advantages of software products are flexibility and ease of use, as well as relatively low cost.

DISCUSSION

VPN based on firewalls.

Most manufacturers' firewalls support tunneling and data encryption functions. An example of a firewall-based solution is Check Point Software Technologies' Fire Wall-1. Personal

computer-based firewalls are only used in networks with relatively small amounts of transmitted information. The disadvantages of this method are the high cost of the solution per worker and the fact that productivity depends on the hardware that runs the firewall.

Software-based VPN.

While software-based VPN products lag behind a specialized device in terms of performance, they are powerful enough to implement VPNs. It should be noted that the requirements for the required bandwidth for remote use are not high. Therefore, the software products themselves provide sufficient performance for remote use. The undoubted advantages of software products are flexibility and ease of use, as well as relatively low cost.

CONCLUSION

In order to benefit from the ubiquity of the Internet, efforts have been made to create a virtual private network VPN that can effectively resist network attacks and allow businesses to actively and securely use open networks. As a result, in the early 1990s, the concept of a virtual private network VPN was created. The term "virtual" was coined to indicate that a connection between two nodes is considered temporary. In fact, this connection is permanent, not fixed, and only exists when traffic passes over an open network.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

4 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

5 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

10 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

6 See Tadjikhanov B.U. Ugolovno-pravovye mery borby s terrorizmom / Otv. ed. Ph.D. jurid. nauk A.S. Yakubov. - T .:, 2003. - S.4–20; Naumov A.V. Rossiyskoe ugolovnoe pravo. Obshchaya chast. - M., 1999. –162–163.

7 See Krylov V. Informatsionnye prestupleniya - novyy kriminologicheskiy object // Rossiyskaya yustitsiya. - 1997. - № 7 - S.22 - 23.

8 See Chichko L.. Kompyuternye xishcheniya // Rossiyskaya yustitsiya. - 1996. - №5. - S.45.

9 See Vexov V.B. Computer prestupleniya: sposoby sovershenіya i raskrytiya. - M., 1996. –S.163.

10 See Sorokin A.V. Computer prestupleniya: ugolovno-pravovaya characteristics, metodika i praktika raskrytiya i rassledovaniya. Internet resource: //http://kurgan.unets.ru/~procur/my_page.htm, 1999.

11 See Ugolovnoe pravo. Special time. - M., 1998. - S.546.

12 See Ugolovnoe pravo. Obshchaya chast / A.S.Yakubov, R. Kabulov et al. - T., 2005. - p. 112-119.

13 See Krylov V.V. Informatsionnye kompyuternye prestupleniya: Uchebnoe i prakticheskoe posobie. - M., 1997. - p. 40-44; Bogomolov M.V. Ugolovnaya otvetstvennost za nepravomernыy dostup k oxranyaemoy zakonom kompyuternoy informatsii. - Krasnoyarsk, 202. - S, 8 - 14; 62-64.

14 See Sottiev I.A. Legal means of combating organized crime: Textbook - T, 2005. - pp. 30-43.