Building secure networks based on VPN

Slesar Maksym, Vladyslav Khotunov *

ISMA University of Applied Science, Latvia

Cherkasy state business college, Ukraine

**Corresponding author's e-mail:taldram375@gmail.com , vkhotunov@gmail.com*

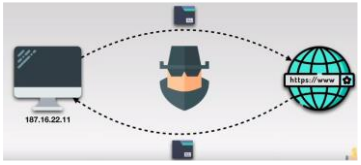
Abstract

Network security is becoming one of the main ideas of the present time. Internet provides tremendous ease in almost all industries such as online banking, online shopping, communications, businesses or organizations. Thus, the communication network requires the security of sensitive data that is stored or transmitted over the internet. Due to the rapid emergence of computerized gadgets and their access to the Internet has caused the unreliability of user data. Nowadays, security and privacy threats are becoming more and more complex, making increased demands on data protection on the Internet. In this article, a virtual private network (VPN) is introduced - a great way to protect devices and information from hackers. A VPN is a private network that operates over a public network, encrypting information so that attackers cannot use it. The main purpose of a VPN is to provide various elements of security, such as authenticity, confidentiality, and data integrity. VPN services are also available for smartphones, computers and tablets. VPN is an evolving technology that plays an important role in the WLAN by providing secure transmission of data over the Internet.

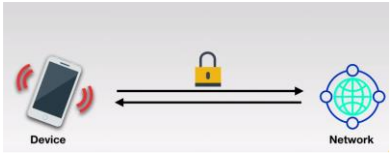
Keywords: encryption, protocol, virtual private network (VPN).

1 Introduction

A VPN is a network structure that affects public networks to protect sensitive data available for public access on the network. It is a cost-effective and correct solution in various networking and telecommunication organizations. A virtual private network (VPN) is the most important part of any IT business because it saves huge infrastructure costs, using the public Internet to create a secure communication environment from the corporate office to users' websites.



Typically, a VPN is a subscription-based service. This means the user has to download an app from their ISP and subscribe to use their private network to protect various devices. Free VPN apps are also available in the App Store for various OS. Before you use a VPN, keep in mind that your VPN provider may keep records of Internet activity that may well be available authorities.



Overview

Why do we use VPNs? From a consumer's perspective, the main advantages of VPNs are that they are much more cost-effective. The solution to using VPN technologies is a high-speed dedicated line. Such lines are expensive, difficult to manage and difficult to maintain. The Internet provides reliability for VPN users. Even in very remote locations, there are dial-up modem connections to the Internet. Virtual private networks guarantee a secure connection for users with a telephone connection. The Internet provides VPN precision services. Mobile users may not be able to use dedicated lines to connect to the corporate site, so VPN technology is the only possible solution.

Benefits of

- Virtual private networks get rid of geo-restrictions.
- Internet privacy is no longer compromised.
- Protects against cyber criminals.
- Data transmission is encrypted.
- Regional leased lines or even cable networks are all you need to connect to the Internet and use the public network to tunnel a private connection.
- Cost savings.

Decision

Potential customers have a wide range of hardware and software for VPN deployment: from integrated multifunctional and specialized devices to pure software products.

The main types of VPN solutions are as follows:

- software-based;
- integrated;
- specialized;

Software-implemented VPN products are inferior in

performance to dedicated devices, but have enough power to implement VPN networks. It should be noted that in the case of remote access, very little bandwidth is required Thus, pure software products can easily provide sufficient performance for remote access. The undoubted advantages of this approach are flexibility and ease of use, as well as relatively low cost. An integrated VPN solution includes, routing and switching functions. The main advantage of this method is the centralization of element management. For companies that do not need a high-performance corporate network, reducing the cost of network equipment is one of the primary objectives, and the most effective is an integrated solution that allows you to concentrate all functions on a single device. However, it should be noted that the more functions the device performs, the more obvious the performance loss will be. High performance is the main advantage of specialized VPN hardware. The higher speed of this type of system is due to the encryption performed by a special chip. The amount of computation needed to handle VPN packets is 50 to 100 times greater than the amount of computation needed to handle regular packets. If the enterprise network performs various activities that require high traffic exchange, it is recommended to use special equipment for efficient processing of VPN data packets. Dedicated VPN equipment provides a high level of security, but at a high cost.

Conclusion

Virtual private networks allow users and businesses to communicate over the public Internet with remote servers, branches or businesses while maintaining secure communications. A VPN is a highly reliable, versatile and inexpensive communication tool. In this article, we determined that various VPN technologies are popular, including SSL and IPsec. We also listed the different types of VPNs and noted that their versatility allows the user to choose which tool they want. Virtual private networks can provide a range of authentication, integrity and encryption algorithms.

Virtual private networks are expected to be used for secure communications in the future. The VPN industry is predicted to grow in the coming years. It is important that the requirements meet the needs of the consumer and maintain their universality.

Analyzing the main problems of information security in local or global networks as virtual private networks, we can conclude that such systems should provide detection of internal and external threats and intrusions, filtering of external traffic, control over the use of corporate network resources and prevent leaks of confidential information.

References

[1] 1. Kanuga Karuna Jyothi, Dr. B. Indira Reddy “Study on Virtual Private Network (VPN), VPN’s Protocols And Security”, Int © 2018 IJSRCSEIT | Volume 3 | Issue 5.
[2] Komalpreet Kaur, Arshdeep Kaur “A Survey of Working on Virtual Private Network” © 2019 IRJET | Volume 6 | Issue 9.
[3] https://scholar.google.com/citations?hl=en&user=OOI01CwAAAAJ
[4] https://www.servercake.blog/types-virtual-private-network-vpn/
[5] https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/
[6] D. Simion, M.F. Ursuleanu, A. Graur, A.D. Potorac, A. Lavric “Efficiency Consideration for Data Packets Encryption with in Wireless Tunneling for Video Streaming” INT J COMPUT COMMUN 8(1):136-145
[7] https://whatismyipaddress.com/vpn-comparison
[8] https://scholar.google.com/citations?hl=en&pli=1&user=ks9yhS0AAAAJ
[9] Charlie Scotte et al., “Virtual Private Network” Second Edition, O’Reilly, January 1999
[10] Ayhan ERDOĞAN, Dz. Yzb. “Virtual Private Networks (VPNs): A Survey”, https://pdfs.semanticscholar.org/bd27/4a3195cb2de780c87727ec6e6248dffb80e5.pdf
[11] https://scholar.google.com/citations?user=Js1wB70AAAAJ&h1=en&scioq=Dr.+Yogesh+kumar+sharma