Торайғыров университетінің
ҒЫЛЫМИ ЖУРНАЛЫ

НАУЧНЫЙ ЖУРНАЛ
Торайгыров университета

Торайғыров университетінің ХАБАРШЫСЫ

Энергетикалық сериясы

1997 жылдан бастап шығады

ВЕСТНИК Торайгыров университета

Энергетическая серия

Издается с 1997 года

ISSN 2710-3420

№ 3 (2020)

Павлодар

НАУЧНЫЙ ЖУРНАЛ
Вестник Торайгыров университета

Энергетическая серия
выходит 4 раза в год

СВИДЕТЕЛЬСТВО
о постановке на переучет периодического печатного издания,
информационного агентства и сетевого издания
KZ19VPY00029272
выдано
Министерство информации и общественного развития
Республики Казахстан

Тематическая направленность
публикация материалов в области электроэнергетики,
электротехнологии, автоматизации, автоматизированных
и информационных систем, электромеханики
и теплоэнергетики

Подписной индекс – 76136

SRSTI 50.41.21

https://doi.org/10.48081/AQBY3283

A. O. Dauitbayeva, E. N. Tulegenova, S. Omir, M. Kozhan
Korkyt Ata Kyzylorda University,
Republic of Kazakhstan, Kyzylorda

CONCEPT OF PROTECTED NETWORKS CREATION

Nowadays, it is important for users to know how to contact a corporate information system. There is a need for broadband connection, whether it's fixed line or Wi-Fi, as it's not rare for users to work on the road. At the moment, virtual technologies are widely popular, they have a high place in modern companies. Because they allow the voice server to communicate to one workplace. It does not require staff always to keep up-to-date with the Service, and there's no need to be there, so use remote access. Many institutions have been fixed or fixed through a mobile connection that ensures optimal connection of mobile workers through the terminal. They work with voice data transmission services. It ensures that employees are always in touch.

Keyword: Virtual Private Network (VPN), ATC Centrex (Central Exchange), Cisco, DES (Data Encryption Standard).

Introduction

In modern conditions of advanced information systems, the advantage of virtual private networks can not be overestimated. But before you can highlight the most obvious, useful ways to create virtual private networks, you need to understand its own point of view.

Nowadays, it is important for users to know how to contact a corporate information system. There is a need for broadband connection, whether it's fixed line or Wi-Fi, as it's not rare for users to work on the road. At the moment, virtual technologies are widely popular, they have a high place in modern companies. Because they allow the voice server to communicate to one workplace. It does not require staff always to keep up-to-date with the Service, and there's no need to be there, so use remote access. Many institutions have been fixed or fixed through a mobile connection that ensures optimal connection of mobile workers through the terminal. They work with voice data transmission services. It ensures that employees are always in touch. When there is a remote connection, there is a question about the user's ability and autentification. It is especially important

to focus on the issue of switching from one to the other on a public network, especially when it comes to virtual private network or virtual private network – the sharing of data to a public user network through a virtual private LAN connection. In this context, the Internet or other intra network may be delivered through a public user network.

Several years ago, we could not imagine how life style and work would change. In many institutions, the work of an additional or distant worker is used. They work at desktop computers as well as use an internet cafe or a common area with a wireless network [1].

Computers, networks, the Internet have become an integral part of our everyday life. Our rapidly developing world of technology is dependent on computer technologies and networks everyday. However, this dependence did not occur immediately. It is not surprising that every year, the financing of computer technology is increasing and therefore, these technologies are practically all human activities.

Many networks are currently connected to the Internet. Therefore, it is necessary to take specific measures for the security of such a large system, since any computer can access the network of any institution, and there is no risk of physical damage to the computer.

One of the pressing issues in the use and creation of distributed information systems and networks, due to the wide application of the Internet, is the solution of the problem of information security.

Due to the rapid development of networks with collective capacities in the world, there was a qualitative leap in the distribution and availability of information. The users have access to cheap and affordable communication channels.

Striving to save money, the enterprise uses such channels to provide critical commercial information. However, on the principle of creation, the Internet has allowed the wicked to steal information. It does not provide reliable local protection from the penetration of the criminals in corporate and branch networks.

Whether it is industrial, commercial, financial, or government-owned, its affiliates are involved in providing and protecting information. Any firm can not have its own access channel, where VPN technology helps, on the basis of which all units and branches are integrated, which ensures more flexibility and high security at the same time and saves costs.

Object of research: Virtual Private Network

Subject of the study: concept of protected networks creation

Purpose: The purpose of a VPN is to have a clean connection to network resources, where the user will usually do what he / she does, regardless of whether he / she is removed.

VPN, or Virtual Private Network, a virtual private network is a cryptic system that provides protection in the transmission of data over an unprotected network such as the Internet. This description is different, regardless of SSH and VPN crypto systems. SSH is designed as a tool that allows the user to access secure and remote computers remotely. For this reason, VPN has become popular among distant employees and offices that need to support resources together on regional networks.

Notwithstanding the use of the software, all VPNs operate on the following tasks:

• Each of the knots identifies each other before creating a trap. It sends the encrypted data to the required node.

• Both nodes indicate a tailored policy that specifies which protocols can be used to secure and encrypt data.

• Compares the coordinated policy of algorithms of nodes; if it does not, then the tunnel will not be installed.

• Upon reaching an agreement on algorithms, the key is created to encrypt, re-encrypt the data in a symmetric algorithm.

Research methods and results. A secure virtual network can offer many levels of security, including privacy, integrity, and authentication. Because VPN uses a network infrastructure, it can be implemented immediately, as there is no need to connect new communications networks.

Main part

Virtual Private Network (VPN) is a networked Internet-enabled network. If communication through the Internet has its own disadvantages, the key is to ensure that traffic over the Internet is transmitted over a local area network, whereas the most important is deficiency of protection or privacy capability. At the same time, virtual networks provide much more cost savings compared to private networks on a global scale [2].

The concept of creating VPN-protected virtual private networks is a simple idea: if there are two nodes in the global network, then it is necessary to create a virtual tunnel to ensure the integrity and privacy of the information transmitted through open channels, which will be complicated by all possible active and inactive external controls. The term «virtual» is not interconnected between the two nodes of the network, and only the traffic over the network is available.

The advantage of the company in creating such virtual tunnels is that it saves more financial instruments.

The main benefit for remote VPN access is the sum of the most affordable network environment for using personal information and high security levels. A secure virtual network can offer many levels of security, including privacy, integrity, and authentication. Because VPN uses a network infrastructure, it can

be implemented immediately, as there is no need to connect new communications networks. From a security kit price point of view, VPN can consider commercial communication as a solution.

These components fulfill the requirements for safety, productivity and interoperability. The correct implementation of VPN architecture depends on the correct execution of the requirements. The definition of the claims should include the following aspects:

VPN server

The VPN server is a computer running the VPN connection terminal (Figure 1).

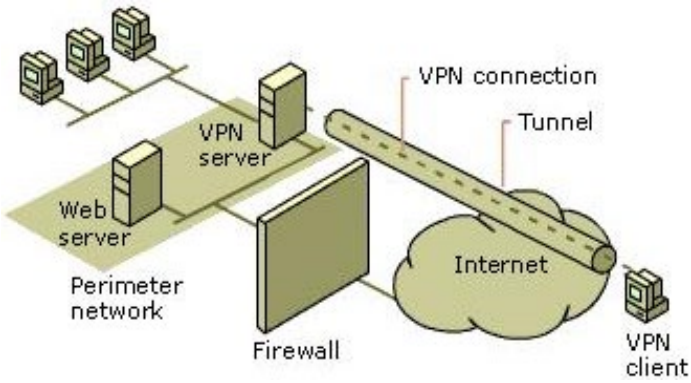

Figure 1 – Configuration of VPN server

This server must have a sufficiently descriptive description of the expected load support. Most VPN software vendors have to submit a proposal based on the number of VPN-enabled connections that run simultaneously on processor performance and memory configuration. It is necessary to have a system with corresponding parameters, but also to make it possible to further modernize it.

Encryption algorithms.

The encryption algorithm used in the VPN encryption algorithm should be the standard power algorithm of encryption. The following question arises: What is the best encryption system? All standard and powerful algorithms can be used effectively in the creation of VPNs. Different manufacturers use different algorithms depending on the distribution range of the product, its licensing aspects and its programming basics. Having received a VPN software package, you need to listen to the specialists' suggestions and make sure that the manufacturer uses a powerful encryption algorithm.

Authentication system.

The third component of VPN architecture is the authentication system. The VPN authentication system must be two-factor. Users will be able to pass the authentication by using the data themselves and who they are. When using VPN benefits, the first two options are selected.

VPN protocol.

VPN determines how VPN interacts with other Internet systems, as well as traffic protection levels. If the institution concerned only uses VPN for internal information exchange, then the request for interoperability is ignored. If your organization uses VPN to communicate with other entities, it is unlikely that its protocols will be used. VPN protects the system's overall security level. This is because the VPN protocol is used to replace the encryption key between the two end nodes. If this replacement is unprotected, the malicious keys can be encrypted by removing all the benefits of VPN.

VPN encryption methods

Because virtual private networks are publicly accessible through the network, they must be protected from external sources. There are many VPN-protected protocols to protect the information you provide, but not all of them work in pairs and do not work in pairs:

Protocols for encapsulating data and generating VPN communications;

Encryption protocols in the built-in tunnel.

The first type of protocol sets a link to the threat, and the second type is directly responsible for data encryption. Let's take a look at world leaders who have recognized the whole world in the creation of some simple, operational homes.

Virtual private networks have several advantages over traditional networks. They are economical, flexible, and easy to use.

Cost savings. Even though VPN-networks have been partially disassembled for businesses, it has also been possible to limit the number of modems, access servers, communicative communications and other technical facilities. They were forced to add them to the company for their long-term benefits. In addition, virtual private networks allow users who use remote access to communicate over local telephone connections rather than on expensive network connections to the company's network resources.

Especially virtual private networks are profitable if the users are at a very remote distance, so wired connections are very expensive and at the same time, if there are so many users, then they need more wired connections. However, these privileges can be avoided. If the volume of traffic on the VPN-network is too high, the system will not be able to encrypt it will cause this situation. In order to avoid such sites, the enterprise needs additional installations.

In addition, due to the novelty of VPN technology and the complexity of the security tools used, the system administrator is more expensive than the traditional one for the virtual system[3].

Virtual Private Network (VPN – Virtual Private Network) is a networked Internet-enabled network. If communication through the Internet has its own disadvantages, the key is to ensure that traffic over the Internet is transmitted over a local area network, whereas the most important is deficiency of protection or privacy capability. At the same time, virtual networks provide much more cost savings compared to private networks on a global scale.

The concept of creating VPN-protected virtual private networks is a simple idea: if there are two nodes in the global network, then it is necessary to create a virtual tunnel to ensure the integrity and privacy of the information transmitted through open channels, which will be complicated by all possible active and inactive external controls . The term «virtual» is not interconnected between the two nodes of the network, and only the traffic over the network is available.

The advantage of the company in creating such virtual tandels is that it saves a much smaller financial instrument.

The main benefit for remote VPN access is the sum of the most affordable network environment for using personal information and high security levels. A secure virtual network can offer many levels of security, including privacy, integrity, and authentication. Because VPN uses a network infrastructure, it can be implemented immediately, as there is no need to connect new communications networks. From a security kit price point of view, VPN can consider commercial communication as a solution.

Conclusion

VPNs and wireless technologies are not competing, they complement each other. VPN works on distributed users in general, which provides privacy as channel protocols (Layer Two Tunneling Protocol – L2TP) at the channel level, taking into account security precautions. By encrypting the data, the encryption protocol decrypts the receiver to prevent unauthorized access. Additional security only encrypts data itself, as well as the recipient's recipient's network address. The wireless local area network can be compared to a common user-defined network.

VPN is responsible for three terms: privacy, integrity, and availability. No VPN can be stable on DoS– or DDoS-attacks, and can not guarantee the physical capability.

Пайдаланған деректер тізімі

1 **Беделл, Пол Сети.** Беспроводные технологии / пол беделл. – М. : нт пресс, 2016. – 448 с.

2 **Николай Колдовский.** Построение безопасных сетей на основе VPN. – М. : ИНФРА-М, 2011.

3 **Андреа, Голдсмит.** Беспроводные коммуникации / Голдсмит Андреа. – М. : Техносфера, 2011. – 521 с.

4 **Мерритт, М.** Безопасность беспроводных сетей / М. Мерритт. – М. : Книга по Требованию, 2016. – 282 С.

References

1 **Bedell, Paul Seti.** Besprovodnye tehnologii [Wireless technology] / Paul Bedell. – Moscow : NT Press, 2016. – 448 p.

2 **Nikolai Koldovsky.** Postroenıe bezopasnyh setei na osnove VPN [Building secure VPN-based networks]. – Moscow : Infra–M, 2011.

3 **Andrea, Goldsmith.** Besprovodnye kommýnıkatsıı [Wireless communications] / Goldsmıt Andrea. – Moscow : Tehnosfera, 2011. – 521 c.

4 **Merrıtt, M.** Bezopasnost besprovodnyh setei [Merritt, M. Security for wireless networks] In M. Merritt (eds.). – Moscow : Knıga po Trebovanııý, 2016. – 282 p.

Материал 30.09.20 баспаға түсті.

А. О. Даутбаева[1], Е. Н. Тулегенова[2], С. Омир[3], М. Кожан[4]

Концепция создания защищенных сетей

[1,2,3,4]Кызылординский университет имени Коркыт Ата,
Республика Казахстан, г. Кызылорда.

Материал поступил в редакцию 30.09.20.

A. O. Dauitbayeva[1], E. N. Tulegenova[2], S. Omir[3], M. Kozhan[4]

Concept of protected networks creation

[1,2,3,4]Korkyt Ata Kyzylorda University,
Republic of Kazakhstan, Kyzylorda.

Material received on 30.09.20.

В настоящее время пользователям важно знать, как связаться с корпоративной информационной системой. Существует потребность в широкополосном соединении, будь то фиксированная линия или Wi-Fi, поскольку пользователи нередко работают в дороге. На данный момент виртуальные технологии широко популярны, они занимают высокое место в современных компаниях. Потому что они позволяют голосовому серверу связываться с одним рабочим

местом. Это не требует, чтобы персонал всегда был в курсе обслуживания, и нет никакой необходимости быть там, поэтому используйте удаленный доступ. Многие учреждения были закреплены через мобильную связь, что обеспечивает оптимальное подключение мобильных работников через терминал. Они работают со службами передачи голосовых данных. Это гарантирует, что сотрудники всегда на связи.

Ключевое слово: виртуальная частная сеть (VPN), ATC Centrex (Central Exchange), Cisco, DES (стандарт шифрования данных).

Nowadays, it is important for users to know how to contact a corporate information system. There is a need for broadband connection, whether it's fixed line or Wi-Fi, as it's not rare for users to work on the road. At the moment, virtual technologies are widely popular, they have a high place in modern companies. Because they allow the voice server to communicate to one workplace. It does not require staff always to keep up-to-date with the Service, and there's no need to be there, so use remote access. Many institutions have been fixed through a mobile connection that ensures optimal connection of mobile workers through the terminal. They work with voice data transmission services. It ensures that employees are always in touch.

Keyword: Virtual Private Network (VPN), ATC Centrex (Central Exchange), Cisco, DES (Data Encryption Standard).

Теруге 30.09.2020 ж. жіберілді. Басуға 14.10.2020 ж. қол қойылды.
Электронды баспа
2,99 Mb RAM
Шартты баспа табағы 23,30. Таралымы 300 дана. Бағасы келісім бойынша.
Компьютерде беттеген: А. Елемесқызы
Корректор: А. Р. Омарова
Тапсырыс № 3707

Сдано в набор 30.09.2020 г. Подписано в печать 14.10.2020 г.
Электронное издание
2,99 Mb RAM
Усл. печ. л. 23,30. Тираж 300 экз. Цена договорная.
Компьютерная верстка: А. Елемесқызы
Корректор: А. Р. Омарова
Заказ № 3707

«Toraighyrov University» баспасынан басылып шығарылған
«Торайғыров университет»
коммерциялық емес акционерлік қоғамы
140008, Павлодар қ., Ломов к., 64, 137 каб.

«Toraighyrov University» баспасы
«Торайғыров университет»
коммерциялық емес акционерлік қоғамы
140008, Павлодар қ., Ломов к., 64, 137 каб.
8 (7182) 67-36-69
e-mail: kereku@tou.edu.kz
www.vestnik.tou.edu.kz