УДК 681.324

І.С. ПЯТІН, Д.А. МАКАРИШКІН, Л.В. КАРПОВА
Хмельницький національний університет

ЗАХИСТ ІНФОРМАЦІЇ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

Розвиток локальних і глобальних комп'ютерних мереж збільшує ризики перехоплення конфіденційної інформації. В роботі проаналізовані розповсюджені методи захисту інформації. Показані способи використання міжмережевих екранів з метою створення демілітаризованої зони для захисту серверів від несанкціонованого доступу. Розглянуті варіанти створення віртуальних приватних мереж, що дозволяють об'єднати декілька географічно віддалених мереж організації в єдину мережу з використанням глобального інформаційного простору без створення додаткових каналів зв'язку. Захист інформації можна здійснювати на рівні програмного обо апаратного забезпечення. Для підвищення рівня захищеності інформаційних ресурсів необхідно поєднувати використання міжмережевих екранів зі створенням віртуальних приватних мереж.

Ключові слова: захист інформації, міжмережевий екран, віртуальна приватна мережа.

I.S. PYATIN, D.A. MAKARYSHKIN, L.V. KARPOVA
Khmelnytsky national university

INFORMATION PROTECTION IN COMPUTER NETWORKS

Abstract – Development of local and global networks increases the risk of interception of confidential information. The article analyzes common methods of data protection. The authors have shown how to use firewalls to create a demilitarized zone to protect the servers from unauthorized access. The versions of creation of virtual private networks have been studied that can combine some geographically distant networks in one network using global information space without creating additional connection channels. Information security can be made at the level of software or hardware. A firewall protects the perimeter of the local network and virtual private network protects information while sending it by means of a global network. To enhance the security of information resources using of firewalls should be combined with creation of virtual private networks.

Keywords: information security, firewall, virtual private network.

Introduction of information technologies in production requires significant attention to questions of technical protection of information, as interception of confidential information may occur. Questions of technical protection of information are divided into two large classes of problems [1]:

- information protection from unauthorized access;
- information protection against leakage by technical channels. Technical channels are channels of spurious electromagnetic emissions, acoustic channels, optical, etc.

Protection from unauthorized access can be exercised in different components of the information system: the applied and system software; hardware of servers and workstations; communication equipment and connection channels. Using of firewalls is prospective to block attacks from the external environment and using of intrusion detection systems (IDS) is prospective to detect unauthorized access from outside and inside the network.

Information protection against leakage by technical connection channels is provided by using of shielded cable and shielded constructions; establishment of high-frequency filters on line connections, etc.

Methods of information protection in global networks

Information protection in local networks is necessary for all companies that store and process the information in the information systems.

To ensure reliable protection of corporate information resources of the system we should use modern technologies of information protection:

- cryptographic data protection;
- use of management infrastructure by PKI (Public Key Infrastructure);
- authentication technologies to control users and network objects through the use of one-time passwords, tokens (smart cards, USB-tokens) and other means of authentication;
- access control on user level and protection from unauthorized access to information;
- firewall technology to protect the corporate network from external threats while connecting to public networks;
- technology of virtual protected channels and networks VPN to protect information, transmitted through open communication channels;
- technologies of protection from malware and spam using complexes of anti-virus protection.

Information security in corporate and wireless networks provides the ability to detect and prevent attacks directed on the network infrastructure of the company, to exclude the possibility of leakage of confidential information, reduces the risk of unauthorized connection to infrastructure and the use of corporate resources, provides an opportunity to objectively evaluate the state of safety and to take the necessary measures that will increase the protection of the resource.

Information security by using the firewall

A firewall is a complex of hardware or software that controls and filters network packets passing through it, according to the specified rules. The firewall has two main objectives: protection from penetration into the computer from the outside (evil) and protection against unauthorised data transfer from a computer to the network [2].

Firewalls are usually installed at the entrance of the network and are divided into internal (private) and external (shared). One of the key rules of building a secure network configuration is to establish all network objects that need to share information, and type of generated traffic. All other traffics between these objects must be rejected.

Consider the protection of information on the example of the demilitarized zone (DMZ). Demilitarized zone is the technology of the protection of information perimeter, in which the servers that respond to requests from the external network, are in a particular network segment (known as the DMZ) and limited in access to basic segments of the network by a firewall, with the aim to minimize damage in case of unauthorized access to one of the public services.

It is expedient to allocate the company's servers in a separate network protected from Internet users and internal users. Fig. 1 shows two possible outcomes: a DMZ is located between the two firewalls and DMZ is located on one of the ports of the firewall.

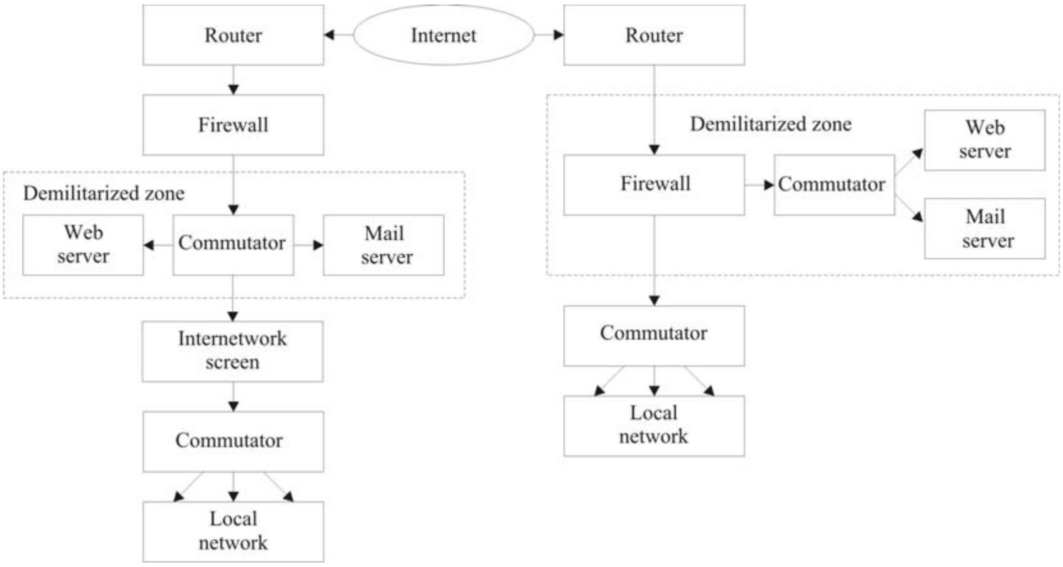

Fig. 1. Examples of network building protected from hacking

Firewall doesn`t protect network hubs from penetration because of programs` vulnerability; does not protect against many threats within the local network, first of all data leakage; does not protect you from downloading malicious software, including viruses. That is it protects the perimeter of the local computer network.

Using of virtual private networks

More powerful device of traffic security is virtual private network (VPN). This network creates for a user imagination that his private network exists within the world network. One of the basic properties of such private network is secure traffic from attacks. Technologies for VPN data security are divided into two classes: the data encryption technologies and traffic separation technologies. First class of technologies is based on a secure communication channels, uniting more customer networks. Representative of this VPN class is IPSec VPN technology.

The second class of VPN technologies is based on the technique of permanent virtual channels (PVC) that allows to reliably separate the traffic of one client from others. In this case, the encryption is not needed because one of the permanent virtual channel is not possible to attack another PVC. Virtual private networks of this class are constructed on the basis of technologies: ATM, Frame Relay, MPLS.

The main purpose of the IPSec (Internet Protocol Security – protected protocol IP) is to ensure the safe transfer of data over IP networks. IPSec using ensures the integrity, authenticity and confidentiality of data. The underlying technology, that allows achieving it, is encryption. The protocol operates on the third layer of the OSI model and can be used by Internet applications to transmit information.

VPM can combine, for example, several geographically distant organization's networks into a single network with the use of the global network.

An example of virtual network creating is encapsulating PPP in some other protocol – IP (this implementation is also called PPTP – Point-to-Point Tunnelling Protocol) or Ethernet (PPPoE). Some other protocols also provide the ability to create secure channels (SSH).

VPM consists of two parts: the "internal" (under control) network and "external" network with encapsulated connection (usually the Internet is used).

Connection of remote user to VPN is done by using a server that is connected to both (internal and external – public) networks. In the case of remote user connection (or connection with the other protected network) access server requires the completion of the identification process, and then the authentication process. After successful completion of both processes, the remote user (remote net) is authorized to work in the network, then there is the authorization process. An example of virtual private network creating is shown in Fig. 2.

VPN connection always consists of point-to-point channel, also known as the tunnel. The tunnel is created in an unprotected network, which is often the Internet. Point-to-point connection is established between the two computers, called hubs.

Each hub is responsible for data encrypting before they enter the tunnel and this data decoding after they leave the tunnel.

Although the VPN-tunnel is always installed between two points, each computer can install additional tunnels with other hubs. For example, when three remote stations need to contact one office, three separate VPN-tunnels to this office are created.

This hub is called the VPN-gateway and the network behind it – encryption domain. Using of gateways is convenient because all users must pass through one device that simplifies management of security and control policy of inbound and outbound network traffic. If there is a gateway, the user connects to it, then the user will have access to the network.

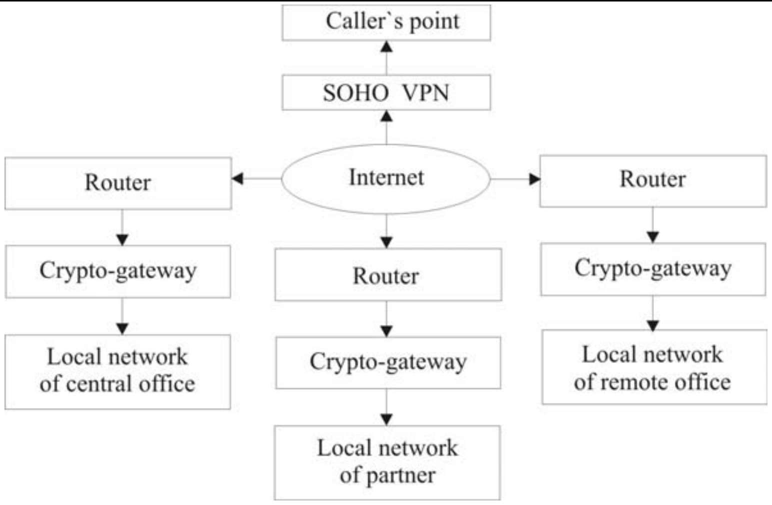

Fig. 2. Creation variants of virtual private networks

There are many variations of VPN-gateways and VPN-clients. It can be a hardware device or software that is installed on the router or PC. For example, OS FreeBSD comes with the software to create a VPN-gateway and configuration of the VPN-client. Own VPN-solutions exist for software of Microsoft.

Regardless of the used software, all VPN work on the following principles:

- each hub identifies each other before creating a tunnel to ensure that the encrypted data will be sent to the appropriate hub;
- both hubs require predefined policy that specifies protocols that can be used for encryption and data integrity;
- hubs compare policy to arrange the used algorithms; if it is not done, then the tunnel is not established;
- as soon as an agreement concerning algorithms is reached, the key is created that will be used in a symmetric algorithm to encrypt and decrypt data.

There are four basic ways to build a VPN that conventionally depicted in Fig. 2.

1. Version "Intranet VPN", which allows combining into a single protected network several distributed branches of the same organization, interacting through open communication channels.

2. Version "Remote Access VPN", which allows to implement a secure communication between the corporate network (central office or a branch) and a single user who is connecting to corporate resources from home (home user) or through laptop (mobile user). This option differs from the first one by the fact that the remote user, as a rule, does not have a static address, and he connects to the resource protected not by a dedicated VPN device, but right from his own computer with installed software that implements the functions of the VPN. In some cases, to implement a VPN SOHO (Small Office – Home Office) devices are used that do not require a complex configuration. Such devices are now widely spread abroad.

3. Version "Client / Server VPN", which provides protection of transferred data between two hubs of the corporate network. The feature of this variant is that the VPN is built between hubs, that usually are in the same network segment, for example, between the workstation and the server. This need very often occurs in cases, when some logical networks must be created in one physical network.

4. Version "Extranet VPN" is intended for those networks that are accessed by external users (partners, customers, clients and so on), the level of trust to them is much lower than to the employees.

Conclusions

Depending on the size of organization and the required level of security various means of information protection can be applied to. It is better to use firewalls for small businesses that use up to a dozen hubs. Systems that provide operative management of local firewalls and support virtual private networks are preferable for large enterprise.

A firewall protects the perimeter of the local network, and VPN protects information while sending it by means of the global network. So we have to use VPN and firewalls to ensure the necessary level of protection of information resources. The ideal solution is to combine in one device the functions of the firewall and VPN.

References

1. Olifer V.G., Olifer N.A. Computer networks. Principles, technologies and protocols. 3-d ed. SPb.: Piter, 2006. 958 p.

2. Tanenbaum E. Computer networks. 4-th ed. SPb., 2003. 992 p.

Рецензія/Peer review : 28.4.2014 р. Надрукована/Printed : 18.5.2014 р.
Рецензент: Шинкарук О.М., д.т.н., професор