Information Systems at Enterprise. Design of Secure Network of Enterprise

N Y Saigushev, U V Mikhailova, O A Vedeneeva, A A Tsaran

Nosov Magnitogorsk State Technical University, 38 Lenina Ave., Magnitogorsk, 455000, Russia

email: nikolay74rus@mail.ru

Abstract. No enterprise and company can do without designing its own corporate network in today's information society. It accelerates and facilitates the work of employees at any level, but contains a big threat to confidential information of the company. In addition to the data theft attackers, there are plenty of information threats posed by modern malware effects. In this regard, the computational security of corporate networks is an important component of modern information technologies of computer security for any enterprise. This article says about the design of the protected corporate network of the enterprise that provides the computers on the network access to the Internet, as well interoperability with the branch. The access speed to the Internet at a high level is provided through the use of high-speed access channels and load balancing between devices. The security of the designed network is performed through the use of VLAN technology as well as access lists and AAA server.

1. Introduction

No enterprise and company can do without designing its own corporate network in today's information society. It accelerates and facilitates the work of employees at any level but contains a big threat to confidential information of the company. Dynamic development of the modern world community is accompanied by the aggravation of the crisis phenomena in the political, economic, environmental and cultural sphere [1]. In addition to the data theft attackers, there are plenty of information threats posed by modern malware effects, often able to cause damage, hundreds of millions and even billions of dollars. Development of information technologies led to the emergence of a new kind of extremism - cyber extremism. Cyber extremism is a commitment to extreme views, ideas and measures aimed at achieving its objectives using a mix of different means and methods of collecting, processing and transmission of data in cyberspace [2]. The network threats are constantly changing, attackers often use combinations of multiple types of attacks to achieve their goals [3,4]. In order to make full use of the capabilities of the enterprise a network must provide a secure transmission of information over the network. A properly constructed corporate network meets modern security standards, allows one to access the necessary information, protecting against unauthorized access to confidential data, providing the company a stable communication at all levels of workflow. In this regard the computational security of corporate networks is an important component of modern information technologies of computer security for any enterprise.

2. Technology transfer of digital information over a network
The technology of building local area networks (LAN) is at the core of corporate networking. It is difficult to imagine a modern office today without a local area network, no company can do without information and computing networks [5]. The appointment of a local information network is access to shared or network (shared) resources (computers, servers, faxes, scanners, printers, etc.), data and programs [6]. LANs are widely used as part of the information system in a firm. Nowadays the local-area network is in every office, at industrial enterprises, in various buildings, banks, etc. The local network is a communication system in general owned by the same organization. Networking technologies and standards are used to design local area networks (e.g., Ethernet, Arcnet, Token Ring, Token Bus, FDDI).

Network technology is a coordinated set of hardware and software (e.g., drivers, network adapters, cables and connectors), as well as data transmission via communication lines sufficient to build a network. Standard LAN technology is based on the same switching principle, which is used when transmitting traffic data in global computer networks, namely the principle of packet switching [7]. The developers of Ethernet have brought a lot to the organization of work of users, and so they became easier and easier to work with, to access shared network resources in the global networks. Tight integration of local and global networks has led to considerable interpenetration of the respective technologies [8]. Convergence in the methods of data transmission occurs platform digital data transmission through fiber optic communication lines. This transmission medium is used in all LAN technologies for high-speed exchange of information at distances over 100 meters. Primary highway networks SDH and DWDM offering their digital channels for enterprises equipment global computer networks were built on it then. The high quality of digital channels has changed the requirements for protocols of computer networks. A great contribution to the convergence of local and global networking has made the dominance of the IP Protocol. This Protocol can operate on top of any technology LAN / WAN (Ethernet, MPLS, Token Ring, ATM, Frame Relay), combining multiple subnets into a single composite network. The process of technology transfers from the global Internet in the local networks has gained such a massive scale that there is even a special term “intranet” [9,10]. For many years Ethernet has been the technology of local networks but is updated with new features and new levels of speeds, this technology (referred to in this embodiment, Carrier Ethernet, i.e. Ethernet carrier class) prevails on the lines of communication and global networks. In the first decade of the XXI century the dominance of Ethernet technology was the simplification of the structure of both local and global networks. The Ethernet Protocol works in the vast majority of subnets, and subnets are combined in a composite network using the IP Protocol. Another sign of the convergence of local and global networks is the emergence of networks that is intermediate between local and global networks. An urban network or a network of megacities (Metropolitan Area Network, MAN) is designed to service a large city. These networks use digital communication lines, often fiber, with speeds to the backbone 10 Gb and above. They provide a cost-effective Ethernet connection between them, as well as access to the global network. The MAN was originally developed only for data transmission, but now the range of their services has expanded, in particular they support video conferencing and integrated voice and text. Modern networks MAN are different in variety of services allowing its customers to combine communications equipment of various types, including PBX.

There is a convergence of telecommunications and computer networks which are developed in several directions today. Technological convergence of networks is based on digital transmission of information of various types, a method of packet switching and programming services. An important step towards telephony, computer networks were primarily the representation of voice in a digital form, which made possible the transmission of telephone and computer traffic on the same digital channels. Telephone networks widely use a combination of methods of switching channels and packages. Thus, the protocols of packet switching are for transmitting service messages (call signaling messages). They are similar to the protocols of computer networks. And the traditional compound channel is for transmitting actual voice between subscribers. Nowadays packet switching techniques gradually push traditional telephone networking techniques circuit switching even for voice. This trend has quite an obvious reason. It is more efficient to use bandwidth communication channels and
switching equipment on the base of the method of packet switching. For example, pauses in a telephone conversation can be up to 40% of the total connection time, but only packet switching allows cut pause and use the freed bandwidth to transmit the traffic of other subscribers. Methods of QoS (Quality of Service) have been designed to minimize latency-sensitive in traffic, such as voice, and at the same time guarantee the average speed and dynamic transmission of pulsations for data traffic. However, it would be wrong to say that the methods of switching channels are outdated and have no future. In a new turn of the spiral of development they find their application, but new technologies, such as technologies for primary networks that serve as a basis for computer and telephone networks, Optical Transport Networks (OTN) and Dense Wavelength Division Multiplexing (DWDM). Computer networks borrowed from the telephone and television networks a lot. In particular they have adopted methods of ensuring resiliency of the telephone networks, by which the latter exhibit a high degree of reliability, sometimes missing the Internet and corporate networks. Telephone networks in turn adopt much from computer networks. It is especially evident in mobile telephone networks, which widely use IP Protocol in their technology of 3rd and 4th generations (3G and 4G). The term “info-communication network” means the two components of the modern network, information (computer) and telecommunication.

3. The design of the protected corporate network of the enterprise

Until recently the universal protection network from unwanted traffic was a firewall. Currently absolute safety cannot guarantee either one of the technologies. And current network epidemics occurring with surprising regularity show it. Network attacks are becoming increasingly sophisticated year by year. The use of social engineering techniques becomes increasingly intensive. The security of computer networks is time consuming and a complicated process which consists of the development and performance of the whole complex of organizational and technical measures aimed at achieving the following objectives:

1. A significant difficulty for an attacker is the opportunity to make the collection of information of interest to his network.
2. To minimize the opportunity for penetration of the intruder inside the protected perimeter of the organization and a connection to the local area network of the organization.
3. To except the situations of intercepting one’s network traffic by an attacker if the attempt to connect to a local area network "victim" still was a success.

The first thing that one must perform to ensure the safety of the designed network is its structuring. Local enterprise network in a secure execution is designed for the enterprise, which includes two five-story buildings, each of which has seven working groups, ten workstations each. In the process of designing the enterprise network planned the structure of the computer network. The original is a segmented computer network, the system then determines the addressing scheme and the selection scheme network traffic between the VLANs. The design was implemented in the package "Cisco packet tracer". The location of the PC and connecting them to the network equipment are shown in Figure 1. Traffic transmitted within local area network can be broadcasted and intended for the specific subscriber. When one connects a new computer to the computer network Ethernet the computer starts polling other computers on the network using the ARP Protocol by sending them broadcast ARP requests. After receiving their replies, the computer adds their MAC addresses in its ARP table. The amount of network traffic of the ARP will exceed all other types of traffic which will create extra overhead on the network infrastructure. Moreover, the possession of information about all the subscribers of the network for the average computer on the network is completely redundant. A typical subscriber is in the process, interacts on the network with a limited number of neighboring network site. And one has no reason to be aware of all devices on the network. And the possession of information about all devices on the network threatens network security, because the powers of the network nodes and their users, as well as the importance of the information they process and its nature, can vary considerably.

To eliminate the above-mentioned drawbacks of the network, let us use the technology of virtual
local area networks (VLANs). A VLAN has the same properties as a physical LAN, but allows end stations to be grouped together even if they are not in the same physical network. Such reorganization can be done through software instead of physically moving devices. Under this standard, virtual LAN is organized as follows:

1. Virtual LAN is announced by setting the label tag on network devices. This label is assigned to the network ports of the LAN switches connected to the virtual LAN segment in the network nodes.

2. Network traffic originating from devices is connected to coded ports labeled by attaching labels VLAN header to the Ethernet frame. That is why traffic becomes marked.

![Figure 1. Layout of PC enterprises and connecting them to the network hardware](image1)

To do this, VLAN has been configured on Cisco equipment with all working groups on all switches of the second level. Ports which switches the second tier connected to switches in the third level did trunk ports because they will receive traffic addressed to different devices. The result was the configuration shown in Figure 2. The similar setup but with a different numbering of VLANs has been done on all the switches of the second level.

![Figure 2. Configuration of switch settings of the second level](image2)
The switch of the third level unlike the switches of the second level will route traffic through IP addresses. For this reason, VLANs have been created for each network and each of them is assigned IP addresses from its network. For dynamic routing technology, interface is created in the local loop and lists the network to which there is access through the switch; it has been done in order not to write separate static routes on each device. Also, a static route has been set up from all networks on the port of the router to access the Internet. Obtaining IP addresses to PC is using a dedicated DHCP server. The router has been protected with a password, and for extra security one used the AAA server. The AAA server is used to store user accounts and it further enhances the security and ease of administration of the network through centralized account management.

4. Conclusion
The described design of the LAN of the company provides the access to the Internet on the computers of one’s network, as well interoperability with the branch. The access speed to the Internet is provided at a high level through the use of high-speed access channels and load balancing between devices. The security of the designed network is performed through the use of VLAN technology, as well as through the use of access lists and AAA server. The corporate network designed in the above-described manner will provide optimally secure transfer of enterprise data without the use of additional means of information protection. The use of special means of information protection will be necessary in case of the need for reinforced protection of information.

References
[1] Saigushev N Y, Savva L I, Gnevak O V, Tsaran A A, Vedeneeva O A Model of future engineers' self-determination during professional training in technical university 2017 The European Proceedings of Social & Behavioural Sciences EpsBS: Volume XXVI, Pages 1-1055 (17 July 2017) 93 851-857
[2] Savva L I, Dokolin A S The historiography of the problem – preparing students to confront cyber extremist activity 2015 Modern problems of science and education 6 516-524
[3] Barankova I I, Mikhailova U V, Lukiyano G I 2016 Automated control system of a factory railway transport based on ZIGBEE 2nd International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM - Proceedings
[4] Barankova I I, Mikhailova U V, Lukiyano G I 2017 Company railway transport control automation International Conference on Industrial Engineering, Applications and Manufacturing, ICIEAM – Proceedings
[5] Kryuchkov D K, Fedoseyeva O Yu Security Policy the INTERNET and the local network 2017 Youth and XXI century - 2017 proceedings of the VII International youth scientific conference 4 28-32.
[6] Zotova M A computer network with multiple queries as an open network, SMO 2014 Innovations and investments 5 187-190
[7] Markelov K S, Neiman A B 2012 Wireless Security Young scientist 4 63-66
[8] Tanenbaum A. Computer networks 2014 SPb.: Peter 960
[9] Imanov V Y, Chudinov S M Structure of the investigated range of threats to information security 2016 Problems of Radiotechnics 7 90-92
[10] Dimov E M, Maslov O N, Rakov A S Information security Management of the Corporation using criteria of risk and expected utility 2016 Information technology 22 8 620-627