Ministry of education of the Republic of Belarus
Educational Institution
Belarusian state university of informatics and radioelectronics

UDK 004.056

Albigharbi
Husham Abduihusein

Evaluation of the security of information resources using network analysis

AVTOREFERAT

for the degree of master of science
on a speciality 1-98 80 01 «Methods and systems of information protection, information security»

_____
Scientific supervisor
T.V. Viktor Tsvitkov
Doctor of science, professor
_____

Minsk 2016

INTRODUCTION

Many modern IT developments are aimed at simplifying the communication between people and to provide new opportunities for communication. Development of maps coverage and bandwidth capacity of the Internet, both fixed and mobile, allows people to be online almost all the time, with the services of high-speed and low-latency performance. Interaction between people opens a lot of new possibilities.

The flip side of the information society is the growth of security threats. Appeared and continue to develop new methods of illegal access to the information transferred on networks both stored on servers and personal computers. In this connection special importance is the problem of network security. Active research in this area are carried out throughout the world and focused on the creation of active and passive protection systems both information and network nodes from different types of attacks.

The urgency of addressing the problem identified purpose of the thesis: A study of information resources protection by using methods and tools for network analysis.

To achieve this goal in the thesis the following tasks are solved:

- the analysis of the subject area in which considered classification of network security, network potential vulnerabilities and potential attacks;
- addressed the specific network security technologies such as IPSec, VPN, and firewalls;
- investigated modes Firewall CISCO ASA 5520, and especially its application in the enterprise network;
- developed recommendations for installing and configuring the firewall in the enterprise network, made their experimental testing in laboratory conditions on CISCO equipment;

The object of the research are the methods and tools to ensure network security. The subject of the research are the structural and functional applications of firewalls in corporate networks.

Doctoral studies are based on the protection of information theory, the theory of telecommunication systems and networks, Telegraphic theory.

The practical significance of the results of the research is to develop a set of laboratory studies on the Firewall CISCO ASA 5520 screen.

GENATAL DESCRIPTION OF THE WORK

Objectives and task of the research

The purpose of this paper is to evaluate the effectiveness of VPN technology to ensure network security.

To achieve this goal it is necessary to solve the following problems:

- to discover and explore the VPN technologies that's using in modern computer networks and the effects of these technologies on the each parts of the effect types of networks;

- to discover and explore the devices and tools that support the VPN technologies and devices and Algorithms and the benefit of apply these tools on networks security;

- to analyze and plan a particular computer networks security that's used in VPN technologies and tunneling techniques that help to prepared the particular part of dissertation;

- using modeling system to simulate the particular computer networks to apply the different types of security Methods and Measurements of VPN technologies.

The objects of study of this paper are the methods and means of ensuring network security.

Subject of research - methods and tools for network security based on VPN-technology.

Communication with large research programs

The studies were conducted as part of the department for telecommunications networks and devices of the educational establishment "Belarusian State University of Informatics and Radio Electronics" on the theme GB 11-2033 "Development and research of methods and technologies for construction of multi-service mobile networks."

Personal contribution of Master's degree student

Contents of dissertation work demonstrate personal contribution of the author. Main scientific and practical results were obtained personally be the author.

In works published in cooperation, the author focused on vulnerability analysis of mobile self-organizing networks and practical issues of uneven cryptographic coding and simulation of data network.

Scientific advisor V. Tsviatkou, Ph.D, associated professor, is a co-author of main results and publications. He formed the objectives and task of the research, decided in research methods, participated in work planning and result discussion, interpreted and summarized obtained results.

Approbation of dissertation results

Main results of dissertation were published at XI Belarusian-Russian Scientific and Technical Conference «Technical Means for Information Protection» (Minsk, 2013); XII Belarusian-Russian Scientific and Technical Conference «Technical Means for Information Protection» (Minsk, 2014); International Scientific Workshop "Telecommunications networks and technologies, algebraic coding, and data security" (Minsk, 2013).

Publication of dissertation results

In accordance with research results, presented in dissertation, 2 works were published.

THE BASIC CONTENT OF WORK

In introduction The urgency of addressing the problem identified purpose of the thesis: A study of information resources protection by using methods and tools for network analysis.

In chapter one. The aim of the work is to build a safe and secure corporate network using a firewall Cisco ASA 5520.

Historically, the main purpose of organizing a network of several computers was resource sharing: computer users or applications connected to the network are able to automatically access a variety of resources of other computers on the network, which include:

- peripherals such as disk drives, printers, plotters, scanners, etc .;
- the data stored in memory or on an external storage device;
- processing power (due to the remote start of "own" programs on "foreign" computers).
- Below in figure 1.1 is an example of a simple network consisting of two computers and AD.

By combining the three or more computers you need to consider the problem of addressing, or rather addressing of network interfaces. One computer can have multiple network interfaces. For example, to create a full-mesh structure of N computers, it is necessary that each of them had a N - 1 interface.

By the number of addressable interface addresses can be classified as follows:

- a unique address (unicast) is used to identify individual interfaces;
- group address (multicast) identifies multiple interfaces, so the data is marked with a multicast address are delivered to each of the nodes in the group;
- data directed to the broadcast address (broadcast), that delivered to all network nodes;

- mailing address of an arbitrary (anycast), defined in the new protocol version IPv6, as well as the multicast address, determines a group of addresses, but data sent to this address must be delivered to all addresses of this group, and any one of them.

Addresses can be numeric (eg, 81.26.255.255) and character (google.by). Symbolic address (name) is designed to remember people and therefore usually carry meaning. To work in a large network symbolic name can have a hierarchical structure, such as mail.google.com.

The set of addresses that are valid within certain addressing scheme is called an address space. Address space may have a flat (linear) organization (see figure 1.15) or a hierarchical organization (figure 1.16).

An example of a flat numeric address is the MAC address assigned to uniquely identify the network interfaces in LAN. This address is normally used only by apparatus, therefore trying to make possible a compact and recorded as a binary or hexadecimal number, for example 00: 83: 00: 6e: 22: a8. When setting the MAC address is not required to perform manual work, since they are usually built into the equipment by the manufacturer, so they are also called hardware addresses (hardware address). Using the flat of addresses is a tough decision - the replacement of equipment, such as a network adapter is changed, and the address of the network interface of the computer.

In the second chapter. Among the set of Internet protocols there is a transport connectionless protocol, UDP (User Datagram Protocol). UDP allows applications to send encapsulated connectionless IP-datagrams. UDP is described in RFC 768. UDP protocol use transmitted segments consisting of 8-byte header followed by a payload field. Subject is shown in figure 2.1. Two port numbers are used to identify sockets inside the sending and receiving machines. When a UDP packet arrives, the contents of its payload field is transmitted to the process associated with the destination port. This binding occurs when the BIND type of underlying transaction.

Imagine that port is a mailbox rented application. We'll talk more about them when discussing TCP, which uses the same ports. In fact, the whole point of using UDP instead of the usual IP is just as specifying the source and destination ports. Without these two fields it was not possible at the transport layer to determine the action that should be done with every incoming packet. In accordance with the fields of ports the delivery of embedded segments corresponding applications is made.

Information on the source port is required, first of all, when you create a response to the sender. By copying the field values from the incoming port of the source segment into the destination port field of the outgoing segment, the process of sending a response, may indicate to what exactly the process is intended on the opposite side.

UDP Length field consists of a header and data. The minimum length is the length of the title, that is, 8 bytes. The maximum length is 65,515 bytes - this is less than the maximum number, is recorded by a 16-bit, due to limitations on the size of the IP-packet.

Optional field The checksum is used to improve the reliability. It contains a header of checksum, and pseudo data. When performing checksum calculations field is set to zero, and the data field is supplemented by a zero byte, if its length is an odd number.

In the third chapter. Cisco ASA appliances provide a high class network protection and are designed for use in small, medium and large networks of organizations. The main features of the firewall are:

- Own operating system
- Using the algorithm ASA (Adaptive Security Algorithm)
- Support for user-based authentication (Cut-through proxy)
- Inspection of protocols and applications (Application-Aware Inspection)
- Virtual firewall (Security Context)
- Support for redundancy (Failover)
- Transparent Firewall (Transparent firewall)

Device Management via the Web interface (ASDM

CONCLUSION

In work characteristics and modes of Cisco ASA 5520 firewall were examined, and situation of using this device were simulated.

The main advantages of firewall include:

- Multifunctionality
- Reliability
- Set of application scenarios
- Flexibility

The usage of Cisco ASA 5520 Firewall screen for protecting of the corporate network is one of the best solutions on the market of telecommunications equipment.

Appendix A provides an example of a laboratory practical work skills to obtain and configure Cisco ASA 5520 firewall and the skills modeling network topologies.

LIST OF PUBLICATIONS

Алби Гарби Хушам Абдулхусейн Худайр Оценка безопасности информационных ресурсов с использованием сетевого анализа, 69-я научно-техническая конференция профессорско-преподавательского

состава, научных работников, докторантов и аспирантов Белорусского

национального технического университета. МЕЖДУНАРОДНЫЙ ИНСТИТУТ

ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ

КАФЕДРА «ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ», 11 мая, 2016 г.