Ministry of Education of the Republic of Belarus

Educational Institution

Belarusian State University of Informatics and Radioelectronics

UDK004.056.5:004.353.2

AL-JEBNAWE MUTHANNA JABBAR ABDULREDHI

ENSURING OF SECURITY CORPORATE NETWORK USING FIREWALLS

Dissertation

for the Degree of Master of Science

Specialization1-45 80 02 «**Telecommunication Systems and Computer Networks**»

The scientific adviser
Ass. Prof. ,Ph. Dr. V.Yu. Tsviatkov

Minsk 2015

INTRODUCTION

Ensuring of security of corporate network means protecting the corporate network from unauthorized access both from within the corporate network and externally. System objects are either tangible or nontangible. In a computer network model, the tangible objects are the hardware resources in the system, and the intangible object is the information and data in the system, both in transition and static in storage [**1**].

Securing corporate networks is difficult for several reasons. New attack vectors, or ways of attacking networks, emerge every year. Old attack vectors that were once thought of as “solved” are repurposed using newer technology, media, or protocols. Creating secure networks is a process that requires continual education and adaptation.

The administrators of corporate networks must also have access to state-of-the art security tools, protocols, techniques, and technologies and should always remain aware of malicious activities and have the skills and tools to minimize or eliminate the threats associated with those activities [2].

Corporate network security is composed of domains of network security and network attacks are classified. Viruses, worms, and Trojan Horses are specific types of network attacks. More generally, network attacks are classified as reconnaissance, access, or Denial of Service attacks (DoS).

Surely, it cannot just rely on a single type of security to provide protection for information systems. Likewise, and, it cannot rely on a single product to provide all of the necessary security for your computer and network systems. The reality of the situation is that no one product will provide total security for an organization. Many different products and types of products are necessary to fully protect an organization’s information assets [31].

The firewalls are computer security systems that protect the computers and network from intruders, hackers & malicious code. Firewalls protect systems from offensive software that may come to reside on your systems or from prying hackers. The firewalls use predefined rules for permitting or denying traffic. Firewalls may be a software features added to existing networking devices, such as routers.

Over time, several companies developed standalone, or dedicated firewalls that enable routers and switches to offload the memory and processor-intensive activity of filtering packets. Firewall is a network perimeter security, a first line of defense of the organization’s network that is expected to police both network traffic inflow and outflow. This perimeter security defense varies with the perimeter of the network.

Firewall enforces an access control policy between two or more security domains. Firewalls have interfaces that connect into the network. In order for a firewall to do its job, all traffic that crosses a security domain boundary must pass through the firewall.

In effect, a firewall becomes the only pathway or “chokepoint” to get in or out of the security domain. Permissive rules are usually added to a firewall by intrusion prevention systems (IPS) and antivirus systems, which are tools that react to things that are detected on the network in real time.

Intrusion Prevention System (IPS) that provides security against unauthorized access and malicious activities at the network level and intrusion Detection System (IDS) that only monitors the network traffic, an Intrusion Prevention System also ensures protection against intrusions that takes place on the network. Main function of an Intrusion Prevention System is to analyze all the inbound and outbound network traffic for suspicious activities, and perform appropriate actions instantaneously to prevent the intruders from entering into the internal network.

This thesis discuss the ensuring the security of corporate network that used of firewalls as a part of information and communication security solution to protect the network form external threads.

GENERAL DESCRIPTION OF WORK

The purpose and objectives of the research

The purpose of this research is to study the methods and the recommendations development of security of corporate networks with the firewall.

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

- **Analyze** the principles of construction and operation of corporate networks;
- **Analyze** protocols, providing the transmission, routing, and security of data in corporate networks;
- **Analyze** security threats and vulnerabilities of corporate networks;
- **Investigate** the attack on the corporate network;
- **Explore** the methods and tools to ensure the security of corporate networks;
- **Develop** integration schemes firewall to the corporate network and recommendations on how to configure and use.

Object of research are the methods and means to ensure the security of corporate networks. Subject of research - firewalls and methods of their use for the protection of corporate networks.

Communication with major scientific programs

Research conducted under performed at the Department of networks and devices of telecommunications educational establishment «Belarusian State University of Informatics and Radio Electronics» research state budget theme GB 11-2033 «Research and development of methods and technologies for construction of multi-local mobile networks».

Personal contribution of Master's degree student

All the main results presented in the thesis, obtained by the author alone. The co-author of published works include: the development of schemes of recommendations to protect the corporate network using the firewall, processing, analysis and interpretation of the results, formulation of conclusions.

Approbation of dissertation results

The Main provisions and results of the thesis were presented and discussed at the conference «Information Security Means» (Minsk, BSUIR, 2014) and international scientific and technical seminar «Telecommunications systems and technology, algebraic coding and data security» (Minsk, BSUIR, 2014 .).

Publication of dissertation results

By results of researches presented in the thesis, published abstracts and papers in the proceedings of the seminar.

CONCLUSION

For practical part of this thesis is implement by configuration of Cisco ASA 5520 firewall as first line of defense for corporate network by enforcing access control policies between inside, DMZ, and outside networks, after complete configuration of all devices, we conclude the following:

1. An analysis of the principles of construction and operation of corporate networks show that the one of the main and important components of the corporate network security is a firewall.

2. The analysis of the communication and routing protocols and the security of data in corporate networks show that the role of the protocols IP, TCP, UDP, SCTP, FTP, TFTP, NFS, SMTP, POP3, SNMP, DNS, ICMP, DHCP, ARP, IGMP, RARP, HTTP corporate networks.

3. The analysis made on security threats and vulnerabilities of corporate networks. It was found that the main target of attacks on corporate networks are hardware, software and data.

4. Investigated attacks on corporate networks establish the basic types of passive and active attacks.

5. Study of the methods and means to ensure the security of corporate networks show that the most effective means of ensuring the security of basic services (e-mail, HTTP and other) on the corporate network.

6. Developing integrated internetworking firewall Schemes of the corporate network and recommendations on how to configure and use. For example, the firewall Cisco ASA 5520 shows the options for its use in the corporate network. Designed codes setting Cisco ASA 5520 for basic applications.

LIST OF PUBLICATIONS

1. Цветков, В.Ю. Модель неравномерного криптографического кодирования многоракурсных изображений на основе матрицы перекрытия / В.Ю. Цветков, К.С.Ш. Аль-Саффар, А.Д.К. Аль-Гейзи**, М.Д.А. Аль-Джебнаве** // Технические средства защиты информации: Тезисы докладов XII Бел.-рос. н.-т. конф. 28-29 мая 2014 г., Минск. – Минск: БГУИР, 2014. – С. 41.

2. Доля, Н.А. Захват и анализ сетевого трафика с помощью технологии SPAN на базе сетевого анализатора CiscoNAM 2304 / Н.А. Доля, А.А. Антонович, А.В. Артамонов, О.Ю. Минченко**, М.Д.А. Аль-Джебнаве** // Телекоммуникации: сети и технологии, алгебраическое кодирование и безопасность данных: материалы междунар. научно-технич. семинара. Минск, апрель–декабрь 2014 г. – Мн.: БГУИР, 2014. – С. 21-25.