NETWORK SECURITY TOOLS

Omonov Fayziddin Komil o'g'li
Student of the Faculty of Telecommunication Technologies of Tashkent University of Information Technologies
Telefon: +998(94) 111 14 02 fayziddinomonov7@gmail.com
Abduraxmonova Dilnoza Alisher qizi
2nd year student of Oriental University, Pedagogy and Psychology

Abstract: *In this article, network security tools , network shielding, session level packet filters, routing technology, a budget of information resources Information about cross-network protection is provided.*

Key words: *electronic , cryptogates , VPN , MAC-addresses, port , TCP/UDP .*

Annotatsiya: *Mazkur maqolada tarmoq xavfsizligini ta’minlovchi vositalar, Tarmoqlararoekranlash, seans sathining paket filtrlari, marshrutlash texnologiyasiga, amaliyotda axborot resurslarining tarmoqlararo himoyasi haqida ma’lumotlar berilgan.*

Kalit so’zlar: *elektron, kriptoshlyuzlar, VPN, MAC-adreslar, port, TCP/UDP.*

Аннотация: *В данной статье представлена информация об инструментах сетевой безопасности, сетевом экранировании, фильтрах пакетов сеансового уровня, технологиях маршрутизации, сетевой защите информационных ресурсов на практике.*

Ключевые слова: *электронные, криптошлюзы, VPN, MAC-адреса, порт, TCP/UDP.*

INTRODUCTION

New technologies, electronic services have become an integral part of our daily life. As society becomes increasingly dependent on information and communication technologies, the protection and use of these technologies is critical to the national interest .

Currently, network security tools include basic network access restriction tools (internet firewall) and secure data transfer tools (cryptogateways and VPN solutions), as well as additional network tools that provide protection, traffic monitoring tools, rogue network badges, etc. concerned.

REFERENCES AND METHODOLOGY

Inter-network screening. Inter-network screening (firewall, brandmaver) is a basic means of restricting the use of the network based on the traffic filtering mechanism. The filtering mechanism provides for comparing the passing traffic with certain rules (filters) and making a decision on whether to pass network packets or not.

Network interfaces are generally classified according to the filtering technology used and the base layer of the OSI model.

Managed switches used at the channel level allow traffic filtering to be performed based on, for example, MAC addresses, ports, and other parameters derived from frame headers. As an advantage of managed switches, it can be stated that it is convenient to manage a group

of network devices and increase local network performance. Limited functionality, inconvenience of physical reconfiguration, and vulnerability to MAC-address replacement attack are disadvantages of managed switches.

Network-level packet filters and routers use IP address, ports, protocol type, etc. allows to perform the task of filtering by Limited functionality of the network and transport layers and vulnerability to IP address spoofing attack are disadvantages of packet filters.

Session level packet filters, sessionsgamos allows you to perform filtering, taking into account a large number of filtering parameters.

RESULTS

Intermediaries are intermediate network devices that perform their own connection and process traffic on an additional device. This, in turn, allows you to perform the following tasks:

- authentication;
- – asynchronous communication of clients and servers; - broadcasting and hiding of addresses;
- to change the address in order to redistribute the network load;
- hashing in order to improve exchange performance; - recording traffic.

At the same time, when using intermediaries, it is necessary to solve the problem of ensuring the desired performance at the network perimeter, since the traffic is processed repeatedly at the additional device.

Special attention should be paid to the routing technology implemented by the intermediary. According to it, the translation of network addresses (Network Address Translation, NAT) is carried out, that is, the internal address of the host is replaced by the private address of the intermediary. In other words, NAT implements the policy of hiding internal network addresses from the outside and makes it possible to assign a single IP address to an internal network device. Address broadcasting can be specified statically and dynamically.

A SOCKET Secure (SOCKS5) broker with session layer brokers, high performance, efficient address masking hardware, and TCP/UDP traffic separation capabilities. HTTP/HTTPS proxies and FTP proxies are commonly used as proxies. These mediators allow filtering by application protocol content.

Status inspectors (extensible session-level filters), session derived from the protocol headers of the layer performs intelligent filtering based on data. This allows you to get a filtering effect at high levels. Such cross-network screens do not require the installation of an intermediary. Therefore, network performance does not decrease, but the required level of security is ensured. To the advantage of the status inspector can be added the ease of scaling.

CONCLUSION

In practice, the concept of UTM (Unifield Threat Management) devices and next-generation inter-network screens (Next Generation, NG firewall) can be found in the provision of network protection of information resources.

UTM is a comprehensive solution to the issue of device perimeter protection is considered Unint archive includes intrusion detection systems, streaming antivirus, anti-spam solution, cryptogateway, etc., in addition to network screening modules. may exist.

The NG firewall is similar to UTM and is designed to combine port filtering techniques, intrusion warning systems, and application-level traffic filtering.

REFERENCES:

1. S.K.Ganiev, T.A.Kuchkarov. Tarmoq xavfsizligi (Mobil tarmoq xavfsizligi). O‘quv qo‘llanma. –T.: «Aloqachi», 2019, 140 b.

2. S.K.Ganiev, M.M.Karimov, Z.T.Xudoyqulov, M.M.Kadirov. Axborot xavfsizligi bo‘yicha atama va tushunchalarning rus, o‘zbek va ingliz tillaridagi izohli lug‘ati. –T.: «Iqtisod-moliya», - 2017, 480 bet.

3. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. –T.: «Fan va texnologiya», 2016, 372 bet.

4. S.K.Ganiev, M.M.Karimov, K.A.Tashev. Axborot xavfsizligi. Axborot-kommunikatsion tizimlar xavfsizligi. O‘quv qo‘llanma. –T.: «Aloqachi», 2008, 382 bet.

5. Stamp M. Information security: principles and practice // John Wiley & Sons, 2011, - P. – 606.