Proceedings of International Scientific-Practical Conference «Sustainable Development Goals: Youth Policy and Innovative Technologies», February 15-16, 2023, Oguz Han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan

WEB SERVER TECHNOLOGY TO PROVIDE CYBER SECURITY

Yuldashbay Kurambayev*

Oguz Han Engineering and Technology University of Turkmenistan, Ashgabat, Turkmenistan.

*Corresponding author

DoI: https://doi.org/10.5281/zenodo.7782319

Honorable President of Turkmenistan determined the digitization of the country's industry institutions as a priority for solving systemic tasks. In the era of the Revival of a new epoch of a powerful state, the "State Program for Ensuring Cyber Security of Turkmenistan for 2022-2025" approved by the decree of the deeply respected Turkmen President Serdar Berdimuhamedov, is oriented to develop the efficiency of the sectors of the national economy and the social system through the widely usage of reliable communication and information technologies.

The objective of paper: To create a modern new technology of data cyber security and to develop a new device model based on existing models for use in local conditions. Various technologies exist that help to build a strong basis for website security. For example, web application firewalls are one of the technologies that help protect data secure. SSL (Secure Sockets Layer) certificates are a technology that provides privacy and security by encrypting all data sent between the server and the user.

Currently, CDNs (Content Delivery Networks) have become an essential constituent of the website's architecture. CDNs operate by caching data content at multiple points distributed around the world. CDNs help ensure website security and improve web infrastructure reliability. CDNs are mainly used to provide security for servers hosting content [1, 2].

Web application security is a branch of information security that provides protection for Web sites and Web applications. Web software security differs from other areas of information security in that it focuses on vulnerabilities in software code discovered by users in real time on the Internet. Most attacks on web servers are made through firewalls and HTTP (80) or HTTPS (443) ports. Some of the most common hacking techniques include denial of service, exfiltration, site scripting, SQL injection, and data disclosure. In addition to traditional firewalls, various solutions are used at the application level to ensure the security of web applications. This includes external tools such as web application scanners (WAS) and firewalls (WAF) [3-5].

The paper analyses the advantages of three-layered technology in providing and protecting the cyberattacks in web servers and the architecture of protection device that was developed on the basis of that technology. Above mentioned CDN technology and its anti-attack capabilities are applied on developed technology. Web server data cyber security technology is deployed in front of the main web server in a CDN.

The developed firewall has been proven to protect against attacks from levels 1-6 of the OSI (Open Systems Interconnection) model by pre-blocking all open ports of the server, except ports 80 and 443, which are sufficient for the operation of web sites. The developed technology has been designed and implemented to simultaneously back up and analyze the flow so that the flow does not affect the request response time.

The findings of paper present the developed security hardware designed to ensure data security is not intended just for only CDN network system but in any system.

The new technology that has been developed, i.e., the protection device developed for the purpose of ensuring the information cyber security of the geographically dispersed (distributed)

network infrastructure capable of delivering the data of web-based services to the clients in a fast manner, can be proposed to be used as a firewall to protect any web server from cyber threats.

REFERENCES

[1]. Dom Robinson, Content Delivery Networks: Fundamentals, Design, and Evolution, John Wiley & Sons, Inc., New Jersey 2017.
[2]. Hu M., Luo J., Wang Y., Veeravalli B. Practical resource provisioning and caching with dynamic resilience for cloud-based content distribution networks. IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 8, 2014, pp. 2169-2179
[3]. П. Ключарев. “Высокопроизводительные алгоритмы специальной обработки данных для защиты компьютерных сетей, ориентированные на аппаратную реализацию”. Автореферат диссертации на соискание учёной степени доктора технических наук. Москва, 2022 (in Russian)
[4]. М.Самара. “Методика сбора и данных о качестве ip соединений для задач сетевой безопасности”. Автореферат диссертации на соискание ученой степени кандидата технических наук. Самара, 2022 (in Russian)
[5]. J. J. Fritz, J. Sagisi, J. James, A. S. Leger, K. King and K. J. Duncan, "Simulation of Man in the Middle Attack On Smart Grid Testbed," 2019 SoutheastCon, Huntsville, AL, USA, 2019, pp. 1-6