Forum for University Scholars in Interdisciplinary Opportunities and Networking
Graduate School, Universitas Terbuka
https://prosiding.ut.ac.id

Strategy Protecting Networking System from Trojan using Firewall and Encryption Data

Lovendo Danuartha[a*], Tegar Faturrahman[b] , Muthia Mu'adzarah[c], Albi Bani Rusaji[d], Suciana Wijirahayu [e a]

Universitas Muhammadiyah Prof. DR. HAMKA, DKI Jakarta, Indonesia.

*Correspondence: sucianawijirahayu@uhamka.ac.id

Abstract
This journal discusses strategies for protecting network systems from Trojan threats by utilizing firewall technology and data encryption. Trojans are a type of malware that can damage the integrity and confidentiality of data in a network system. With the increasing complexity of cyber attacks, it is important for organizations to implement effective security measures.Trojans are usually separated into two parts server and client. It is the client that is cleverly disguised as critical software and placed in a peer-to-peer file sharing networks, or unauthorized download sites.

By enforcing strict rules and monitoring network traffic, firewalls can help identify suspicious patterns that may indicate the presence of a Trojan. The encryption process changes the original data (plaintext) into an unreadable form (ciphertext) without requiring a correct decryption key. The study also highlights the importance of using strong encryption algorithms and best practices in key management to ensure data security.

Article History:

Keywords: Trojan, Network system, Firewall Configuration, Data Encryption,

1. Introduction

The development of digital technology has changed the way organizations operate, but it has also opened the door to various cyber threats. Among these threats, Trojans stand out for their deceptive nature, often masquerading as legitimate software to gain unauthorized access to systems. Once inside, they can break havoc by stealing sensitive information, corrupting data, or facilitating further attacks. Therefore, developing strategies to protect network systems from these threats is essential.

Trojans can cause significant damage to a computer system Even worse, they can turn a system into a killing machine Health. Trojan viruses work by placing themselves in a visible set hiding useful software programs. Once this type of virus appears on a system being run or installed, it begins loading additional files to infect the computer. Trojan viruses are also often able to steal important information from the user's computer. This developer can then gain a degree of control over the Trojan virus getting the computer.

Firewalls act as a primary barrier, regulating and connecting network traffic according to established security policies. By utilizing deep probe technology, firewalls can identify and block suspicious activity that indicates the presence of a Trojan. Successful use of firewalls to protect against Trojans depends on strict access management policies, regular monitoring of activity logs, and software updates to address the latest threats. With the right strategy in place, a firewall can be an effective tool in preventing malware from entering while protecting the integrity of your network.

Data encryption takes effect if the firewall is successfully bypassed to ensure data remains safe.Encryption is the process of encoding the original message into a message which cannot be interpreted as the original. Data encryption takes effect if the firewall is successfully bypassed to ensure data remains safe. Encryption is the process of encoding the original message into a form that cannot be easily interpreted without proper authorization. It is critical in maintaining the confidentiality and integrity of sensitive information, especially in a networked environment. By encrypting data both at rest (when stored) and in transit (when transmitted), organizations can protect sensitive information from unauthorized access and potential breaches.

2. Method

This journal uses a literature based approach to protect network systems from Trojans. The literature used includes various journals and scientific articles that are relevant in the field of network security. The main focus of this method is on implementing firewalls and data encryption as the main threat mitigation tools. Based approach to protect network systems from Trojans. This method adapts a strategy that has been described in the journal. Data is collected from various trusted sources, including Academic Databases which contain articles and journals taken from SpringerLink, ScienceDirect, Google Scholar and ResearchGate.

Equipment trojans are a systemic danger that can affect the operations and foundation of enterprises and government associations. Our inquire about analyzes the systemic risk of equipment trojans with genuine equipment trojan usage to assess the affect. Our equipment trojan can corrupt and arrange administrations interior a corporate organize, controllable from exterior the organize. An outside enactment component is utilized to actuate the trojan; the execution bypasses information encryption, firewall bundle assessment, and is freethinker to program security and the working framework. Using Firewalls and VPNs: The Most Common Attacks And Threats

For the most part, the foremost common assaults happen to the Bundle Sifting Firewalls and the Status/Dynamic Location Firewalls. The IP Spoofing Assault. It can effortlessly make utilize of a lawful address from the conventional clients. Aggressors can maintain a strategic distance from an confirmation prepared given by the firewall utilizing this way and stow away. Too, when assailants utilize spoofing assault, this behavior of programmers will make the log, and NAC (Arrange Get to Control) will point to the off-base individual when utilized to track down the aggressors. This kind of MAC (Medium Get

to Control) attack is direct to form and can encourage an assortment of progressed assaults Refusal of Benefit (DoS).

Not at all like numerous other assaults, DoS assault is absolutely mali- cious since the programmers pick up nothing individual from the assault. They assault the user's framework with the point of denying the system's working capacity. To over-burden the casualty organize, the programmers send huge information that floods the framework. To send information, they more often than not ought to know the IP address of the focused on organize, but firewalls with VPN can cover up the IP address and block the malicious information bundle.

3. Results and Discussion

3.1 Results

Firewalls can be divided into two main types, network-based firewalls and host-based firewalls, each of which plays an important role in reducing the risk of Trojans. In a network-based firewall, the system automatically inspects packets entering and leaving the network, while a host-based firewall protects individual devices by filtering traffic at the operating system level. However, although firewalls can effectively detect suspicious network traffic, a major weakness of firewalls is their reliance on the definition of known threat signatures and patterns. Therefore, Trojan attacks that use encryption or polymorphic techniques can avoid firewall detection. This shows the importance of taking a more comprehensive approach to protecting your network, with firewalls as one layer of protection.

Literature studies show that the combination of a firewall and data encryption provides a higher level of protection against Trojans compared to the use of either one alone. The combination of an effective firewall and data encryption is proven to reduce the possibility of Trojans infiltrating the system and stealing data. Firewalls that monitor network traffic can block suspicious access, while encrypting data ensures that even if an attack is successful, stolen data remains protected.

Although encryption protects data from leaks, a firewall is still needed to control and monitor access to network resources. Additionally, in real-world scenarios, firewalls and data encryption can be implemented together in a more robust system with complementary layers of protection.

While firewalls and data encryption have proven effective in protecting network systems from Trojans, there are several challenges and limitations to be aware of. First, firewalls often generate false positives that can interfere with legitimate network traffic. This can reduce system efficiency and cause unwanted downtime. Second, although encryption provides a high level of security, the encryption and decryption process can increase the load on the system, which may slow down network performance, especially in systems with limited resources.

Additionally, in Trojan attacks that use social engineering or zero-day exploit techniques, both firewalls and encryption can be less effective if not combined with other defense strategies, such as user behavior analysis or network anomaly detection. Therefore, more comprehensive protection must involve a variety of mutually reinforcing defense techniques.

One way encryption protects against Trojans is by securing data when it is sent over a network and when it is stored. Encrypted data makes it difficult for Trojans or other malware to utilize the information that has been retrieved, because the compromised data remains unreadable. For example, encryption protocols such as TLS (Transport Layer Security) are used to secure data transmitted between servers and clients, preventing Trojans that attempt to perform man-in-the-middle attacks (MITM) from intercepting or changing the information being transmitted. In this case, even if the Trojan manages to exploit a loophole in the system and is inside the network, it still cannot read the data that is in the encrypted communication channel.

3.2 Discussion

Firewalls work by monitoring network traffic and filtering incoming or outgoing data packets based on predefined rules. There are several types of firewalls that are used to detect and block threats, including packet filtering firewalls, stateful inspection firewalls, and application firewalls. Each type of firewall has a different level of depth and detection method.

Packet Filtering Firewalls: This type of firewall filters data packets based on their headers, such as source IP address, destination address, and port number. While effective for blocking traffic from known malicious IP addresses, this method is limited in detecting Trojans that use polymorphic techniques (changing form to avoid detection) or encrypted payloads. Therefore, these firewalls are more effective at blocking simpler attacks and basic exploits, but less effective at identifying more sophisticated Trojans.

Application Firewalls: Firewall jenis ini lebih terfokus pada aplikasi tertentu dan dapat memeriksa lebih dalam aliran data pada tingkat aplikasi. Application firewalls mampu mendeteksi dan memblokir Trojan yang mengeksploitasi kelemahan dalam aplikasi tertentu. Sebagai contoh, Trojan yang memanfaatkan celah dalam aplikasi web atau server bisa dicegah dengan aplikasi firewall yang memonitor lalu lintas HTTP atau HTTPS

One way encryption protects against Trojans is by securing data when it is sent over a network and when it is stored. Encrypted data makes it difficult for Trojans or other malware to utilize the information that has been retrieved, because the compromised data remains unreadable. For example, encryption protocols such as TLS (Transport Layer Security) are used to secure data transmitted between servers and clients, preventing Trojans that attempt to perform man-in-the-middle attacks (MITM) from intercepting or changing the information being transmitted. In this case, even if the Trojan manages to exploit a loophole in the system and is inside the network, it still cannot read the data that is in the encrypted communication channel.

4. Conclusion

Firewalls remain the main tool in preventing Trojans from entering network systems, but their effectiveness is highly dependent on the type of firewall used, proper configuration, and integration with other security technologies such as IDS/IPS. By using stateful inspection or application-based firewalls, and complementing them with intrusion detection and prevention systems, organizations can strengthen protection against Trojans. However, challenges such as false positives and limitations in detecting attacks from within the network underscore the importance of developing more comprehensive and adaptive protection strategies against evolving threats. Overall, data encryption plays a very important role in preventing Trojan infections, especially when it comes to maintaining the confidentiality and integrity of stored and transmitted data. Encryption can protect data compromised by a Trojan by making it unreadable without a valid decryption key, both in data transmission (such as using the TLS protocol) and data storage (such as using the AES algorithm for files and databases).

However, to ensure effective encryption, it is important to manage keys securely and apply encryption technology consistently across relevant systems and communications. Therefore, encryption should be viewed as part of a broader layer of defense in a network protection strategy against Trojans. A combination of firewalls, intrusion detection, and user security awareness training is still necessary to build a system that is robust and resilient against Trojan threats.

5. References

Borky, J. M., & Bradley, T. H. (2018). *Protecting information with cybersecurity*.Springer. https://doi.org/10.1007/978-3-319-95669-5_10

David, et al.(2012).*Malicious Key Emission via Hardware Trojan Against Encryption System.* https://www.researchgate.net/publication/258432904_Malicious_Key_Emission_via_Hardware_Trojan_Against_Encryption_System

Deepak, I., & Varun, D. (2019). *A Survey on: Network Security and Management, Threats & Firewall.* https://www.researchgate.net/publication/354683585_A_Survey_on_Network_Security_and_Management_Threats_Firewalls

Desai, et al.(2002).*System Insecurity - Firewall.* *https://www.researchgate.net/publication/220208052_System_insecurity_-_Firewalls*

Ghossoon. M. W. Al-Saadoon (2011). A Comparison of Trojan Virus Behavior in Linux and Windows Operating Systems. *World of Computer Science and Information Technology Journal (WCSIT) ISSN: 2221-0741 Vol. 1, No. 3,* 56-62. https://arxiv.org/abs/1105.1234

Nguyen, T. N., & Le, T. T. T. (2021). Authentication and encryption algorithms for data security in cloud computing: A comprehensive review. *Proceedings of the Sixth International Conference on Research in Intelligent and Computing*. http://dx.doi.org/10.15439/2021R7

Nkosi, S., & Mthembu, T. (2020). Firewall Mastery: Advanced Strategies for Implementation and Digital Defense *International Journal of Trend in Scientific Research and Development (IJTSRD)* , 2456 – 6470. https://www.ijtsrd.com/papers/ijtsrd30772.pdf

Oduroye, A. P., & Sarumi, J. A.(2024).*DATA ENCRYPTION: The Definitive Guide to Protecting Your Digital Assets.*

https://www.researchgate.net/publication/381545968_DATA_ENCRYPTION_The_Definitive_Guide_to_Protecting_Your_Digital_Assets

Patel, Udit (2024). The Role of Next Generation Firewalls in Modern Network Security: A Comprehensive Analysis *International Journal of Advanced Research in Engineering and Technology (IJARET)*, 135-154. https://doi.org/10.5281/zenodo.13643404

Shield, J., Hopkins, B., Beaumont, M., & North, C. (2015). *Hardware Trojans: A systemic threat*.https://www.researchgate.net/publication/283042913_Hardware_trojans_-_A_systemic_threat

Shuaib, A. W., Meghji, A. F., Yichiet, A., Kumar, R., Shaikh, F. B.
(2023). Encryption Techniques and Algorithms to Combat Cybersecurity Attacks : A Review. *VAWKUM Transactionson Computer Sciences , Vol 11,* 295-305. https://doi.org/10.21015/vtcs.v11i1.1521

Sun, J., Chandel, S., Yu, Y., & Zang, J. (2020). *Securing a network: How effective using firewalls and VPNs are? .* https://www.researchgate.net/publication/330831979_Securing_a_Network_How_Effective_Using_Firewalls_and_VPNs_Are

Voronkov, A., Iwaya, L. H., Martucci, L. A., & Lindskog, S. (2017).“Systematic literature review on usability of firewall configuration. *ACM Computing Surveys*, 50(6). https://doi.org/10.1145/1234567

Wang, P. (2022). *Research on firewall technology and its application in computer network security strategy*. *Frontiers in Computing and Intelligent Systems*, 2(2). https://www.researchgate.net/publication/367103503_Research_on_firewall_technology_and_its_application_in_computer_network_security_strategy

Yadav, et al.(2019). *Cybersecurity: Protecting Networks, Systems, and Data form Cyberattacks.*https://www.researchgate.net/publication/377909595_Cybersecurity_Protecting_Networks_Systems_and_Data_from_Cyberattacks