International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048
Volume 10, Issue 4, pp 328-331, April-2026
https://doi.org/10.47001/IRJIET/2026.104047

Addressing the Key Issues in Network Security

[1]Nwile Beauty Nuka, [2]Daniel Matthias

[1,2]Rivers State University, Department of Computer Science, Port Harcourt-Nigeria
E-mail: [1]nwilebeauty@gmail.com, [2]daniel.matthias@ust.edu.ng

Abstract **- Network security is an essential aspect of modern business and organizations. It is important to implement a comprehensive security strategy that includes firewalls, intrusion detection and prevention systems, encryption, and regular security updates. Additionally, access controls and authentication mechanisms must be implemented to ensure that only authorized users have access to sensitive information. Network security is an ongoing process that requires constant monitoring and updating to stay ahead of emerging threats.**

Keywords: Network Security, Malicious Attacks, Intrusion Detection.

I. INTRODUCTION

Network security consists of the policies, processes and practices adopted to prevent, detect and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

The three primary goals of network security which are confidentiality, integrity and availability can be achieved by using firewalls. Firewalls provide security by applying a security policy to arriving packets. A policy is a list of rules which define an action to perform on matching packets, such as accept or deny (Ziegler and Firewalls, 2002). Determining the appropriate action is typically done in a first-match fashion, dictated by the first matching rule appearing in the policy and the time required to process packets increases as policies grow larger and more complex So Network firewalls must continually improve their performance to meet increasing network speeds, traffic volumes, and Quality of Service (QoS) demands. Unfortunately, firewalls often have more capabilities than standard networking devices, and as a result the performance of these security devices lags behind (Benecke, 1999). Furthermore, computer networks grow not only in speed, but also in size, resulting in convoluted security policies that take longer to apply to each packet (Wool, 2004),

Ziegler and Linux (2002). When a security solution cannot keep pace with the speed of incoming data, it either allows packets through without inspection or places incoming packets into a growing queue, thus becoming vulnerable to Denial of Service (DoS) attacks. With either of these possibilities, even a network with a perfect firewall policy (short in length and optimally ordered Fulp, 2005) is susceptible to attacks resulting in prolonged delays, data loss, or both, and it is for this reason that a new firewall architecture is necessary. Parallel firewall designs provide a low latency solution, scalable to increasing network speeds (Ziegler and Firewalls, 2002). Unlike a traditional single firewall, the parallel design consists of an array of firewalls, each performing a portion of the work that a single firewall performed. As network speeds increase, the additional load is distributed across the array, providing a solution that can be implemented using standard hardware. The firewall that will be discussed is Microsoft firewall which called Internet Security and Acceleration firewall (ISA). In this paper a standalone (ISA) and parallel (ISA) will be discussed and tested in different scenarios and their effect on network performance will be calculated. In this paper integrations will be applied with firewalls like integrate an antivirus with firewall to work as a gateway antivirus to scan every traffic which pass through the firewall another monitor program will be added to monitor the sessions that are established through the firewall, an integrated program which split or distribute the bandwidth to users will be added also and here the Microsoft firewall will have the responsibility to establish VPN connections. Therefore, lots oftest will be done to examine the performance of Microsoft firewall when it is in standalone and when using parallel Microsoft firewalls and a proposal will be presented to enhance the Microsoft firewall performance and this will happen by integration between Cisco and Microsoft products.

II. NETWORK SECURITY THREATS AND VULNERABILITIES

All data breaches and cyber-attacks start when a threat exploits weaknesses in your infrastructure. As a result, your network security vulnerabilities create opportunities for threats to access, corrupt, or take hostage of your network.

Any potential danger to your network must be considered a network security threat – however, security risks often begin with your infrastructure and its security. The best way to determine whether your network is vulnerable to these threats, is by getting a network security assessment from a trusted and qualified third party.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 4, pp 328-331, April-2026

https://doi.org/10.47001/IRJIET/2026.104047

1. Viruses

Viruses are malicious programs written to change the way your software or computer system operates. They are designed to spread between hosts, from one computer to another – if one computer in your network becomes infected, your entire network is at risk.

Often, this malicious software is a result of the user downloading infected application files. The subsequent infected code can spread throughout the system and completely alter the system operations

Viruses are most commonly downloaded from:

- Email attachments
- Internet advertisements
- Updating software and programs
- Infected software
- Malicious websites
- Pirating music, movies, and software

Viruses are cybersecurity threats that will typically threaten your network when there are vulnerabilities to exploit. This includes using outdated antivirus software, or a lack of anti-spyware, firewalls, and backup systems.

Without adequate security measures, your network are consistently open to threats and vulnerabilities that may:

- Damage or disable programs
- Copy your passwords and send them back to their sender/creator
- Create fake traffic in your network leading to massive downtime
- Take over your computers' processing power and memory

2. Insider Threats

Insider breaches typically occur as a result of actions from employees, former employees, or contractors. Although some of these breaches can occur from malicious attacks by employees, approximately 64% of insider threats are a result of employee negligent behavior or human error.

In order to block potential security threats within small businesses, business owners must establish a strong culture of security awareness in their organization. This includes creating employee cybersecurity policies, security threat training, and the implementation of additional security software to ensure that threats are identified and stopped before a potential breach occurs.

3. Spyware

Spyware is the malicious software (malware) that is designed to spy on your activities.

These programs embed deep into your computer files and programs, collecting sensitive information, including passwords, financial information, and employee identifications.

Like worms and viruses, spyware slows down your bandwidth and takes over other computing resources. It is categorized into Trojans, Adware, and tracking cookies.

Trojans are the seemingly legitimate programs that may be downloaded for your critical business functions. However, these programs may carry embedded malware that breaches security and clones' sensitive data.

Conversely, Adware is the malicious and unsolicited advertising that shows us pop-ups on your computer or mobile device. Clicking on these advertisements allows the advertiser to track your online activities – additionally, it slows down your computer and can open the door for future attacks.

4. Ransomware attacks

Ransomware, much like viruses and worms, can replicate itself across the network. This malicious program has the ability to lock you out of your computer applications, or alternatively, out of your entire computer system until a stated ransom demand is met.

One of the ways Ransomware gets into your network is through phishing and spam attachments that can automatically open on your computer. This network security threat encrypts your files, computer, or network – if this escalates, your computer files can no longer be opened without a program key. The key is only granted when the attacker is paid.

5. Phishing attacks

Phishing is one of the most common network security threats where a cyber-threat gains access to your sensitive information through a social engineering scheme, and is often disguised as a fake email from a recognizable source. By clicking on it, you may inadvertently share your credentials and other critical data.

Occasionally, the attackers may send Ransomware or a worm through these emails, linking to a website that has the ability to harvest sensitive or encrypted information. A weak email security structure is the most significant vulnerability exploited by phishing scammers.

International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 10, Issue 4, pp 328-331, April-2026

https://doi.org/10.47001/IRJIET/2026.104047

6. Rogue security software

This software misleads users into believing that there is a malicious attack on your network. As a form of ransomware, rogue security software often convinces users to pay a fee to have their network cleared of the false "attack."

These programs will also offer to clean up your system using a fake antivirus software. Once this is downloaded, you may end up installing malware on your computer.

7. DOS and DDOS attack

A denial-of-service DDoS attack happens when a threat overwhelms your network resources with traffic, preventing users from accessing crucial applications. A DOS attack eventually takes down your network through:

- Excessive amounts of false traffic directed to your network address (Buffer overflow)
- Multiple and fictitious connection requests to your server (SYN flood)
- Confusing data routing in your network, causing it to crash (Teardrop attack)

DOS attacks don't steal or damage your data. Instead, they aim to cause massive downtimes and extensive damage to your quality of service.

A DDOS or distributed denial of service attack is a DOS attack that happens through the use of several devices in your network. The damage scope in a service DDOS attack is broader, given that there are many computers involved on both the attacker's end, and your network.

8. Rootkit

A rootkit is a threat in the form of computer software that is designed to give the attackers unauthorized remote access to your computers and network. Rootkits work subtly, copying passwords and disabling antiviruses until it is completely through to your network.

A rootkit can arrive in your system through legitimate software. This malicious software can make its way into your network when you install the software and cause severe cybersecurity risks.

9. SQL Injection attacks

SQL injection is among a form of network security threats where the attacker sends information to websites or web applications that are overlooked by other security measures. The attackers are then able to delete, modify, or add data into your SQL database. SQL attacks affect websites and web apps that use an SQL database.

The attack compromises individual machines, but can also affect the entire network. SQL and other injection flaws happen when there is insufficient or unreliable scanning of data in the database query.

10. Man-in-the-middle attacks

This is a vulnerability that allows attackers to spy on or alter the communication between devices in your network. A man-in-the-middle attack could lead to the installation of viruses, warms, or Ransomware. Cybercriminals can carry out MITM through:

- IP spoofing
- DNS spoofing
- HTTPS spoofing
- SSL hijacking
- Wi-Fi hacking
- Machine learning

11. Hidden backdoor programs

A computer device manufacturer or software designer can develop tools to allow your system to be accessed via a backdoor. Usually, this is for use in technical support and diagnostic purposes. However, attackers can take advantage of this vulnerability to access your computer and networks illegally.

12. Superuser accounts

Superuser accounts can turn into network vulnerabilities. These accounts have unlimited privileges, data, and devices and are often used for administrative purposes by IT team leaders.

The user can create, modify, and delete files, install software, or copy information. If a cybercriminal gets hold of such an account, the damage to your network and your business could be catastrophic.

Benefits of network security

The main benefits of network security are:

- It ensures the functionality of the networks that businesses rely on.
- It ensures the confidentiality, integrity and availability of data on a network. This is known as the CIA triad.
- It ensures compliance with security regulations -- the HIPAA Security Rule, for example. Compliance is also important to the success of a business.

ISSN (online): 2581-3048
Volume 10, Issue 4, pp 328-331, April-2026
https://doi.org/10.47001/IRJIET/2026.104047

- It creates a safer marketplace overall when organizations take a proactive approach to security, and share their strategies continually with non-proprietary security frameworks like MITRE ATT&CK.
- It helps businesses build and maintain customer trust. Security breaches can damage a business's reputation.

REFERENCES

[1] Benecke, C. (1999). A parallel packet screen for high speed networks, in Proceedings of the 15th Annual Computer Security Applications Conference.

[2] O'Reilly, 2000A. Wool, "A quantitative study of firewall configuration errors," IEEE Computer, 3(6). 62 –67, June.

[3] Fulp,E. W. (2005) Optimization of network firewall policies using directed a cyclical graphs," in Proceedings of the IEEE Internet Management Conference (IM'05), 2005.

[4] Paul, O. and M. Laurent, "A full bandwidth ATM firewall," in Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000.

[5] Ziegler, R. (2002) Linux Firewalls, 2nd ed. New Riders.

[6] Zwicky, E. D. Cooper, S. and Chapman, D. B. (2004) Building Internet Firewalls.

[7] Ziegler. R. L. (2002). Linux Firewalls. New Riders, second edition.

Citation of this Article:

Nwile Beauty Nuka, & Daniel Matthias. (2026). Addressing the Key Issues in Network Security. *International Research Journal of Innovations in Engineering and Technology - IRJIET*, 10(4), 328-331. Article DOI https://doi.org/10.47001/IRJIET/2026.104047

****

