Advances in Social Science and Culture
ISSN 2640-9682 (Print) ISSN 2640-9674 (Online)
Vol. 5, No. 3, 2023
www.scholink.org/ojs/index.php/assc

Original Paper

The Critical Role of NIDSNIPS in Protecting Internet Infrastructure

Ding Jiawei[1] & E Yunpeng[1]

[1] School of Information science and Technology, Northwest University, Xi'an, Shaanxi Province, China

Received: June 13, 2023 Accepted: July 29, 2023 Online Published: August 03, 2023

doi:10.22158/assc.v5n3p66 URL: http://dx.doi.org/10.22158/assc.v5n3p66

Abstract

With the rapid development and wide application of the Internet, network security has become an important issue in modern society. Network attacks such as network worms, botnets and computer viruses are constantly emerging, bringing serious threats and economic losses to the Internet infrastructure. In this context, Network Intrusion Detection/Prevention System (NIDS/NIPS) plays a key role in protecting the Internet infrastructure. By monitoring network traffic in real time, NIDS/NIPS is able to detect and identify internal and external security intrusions in a timely manner and take appropriate measures for defense. Ensuring the high performance of NIDS/NIPS is an important topic in network security research, because the increase of Internet traffic and the variety of attacks make it face great challenges. In this paper, we will explore the fundamentals and functions of NIDS/NIPS and their key role in protecting the Internet infrastructure. We will also discuss key techniques to improve the performance of NIDS/NIPS and look at future directions in this area. An in-depth understanding and study of the theory and technology of NIDS/NIPS is an important reference for professionals in the field of network security.

Keywords

NIDS/NIPS, Internet, network security

1. Introduction

With the rapid development of the Internet and information technology, computer networks have penetrated into all aspects of modern society and become an indispensable part of people's life and work. However, the popularization of the Internet is also accompanied by an increasing number of network security threats. Network worms, botnets, computer viruses and other network attacks have emerged in an endless stream, and they have not only invaded and hijacked a large number of computer systems, but also abused computer network resources, causing serious threats and damage to the

Internet infrastructure, resulting in incalculable economic losses and social impact.

In this information age, it has become crucial to protect the security of Internet infrastructure. To cope with the growing network security threats, network security devices play a key role. In particular, Network Intrusion Detection/Prevention System (NIDS/NIPS), through real-time monitoring of network traffic, can detect and identify potential security intrusions in a timely manner and take corresponding defensive measures. NIDS/NIPS can not only protect the Internet infrastructure from internal and external attacks, but also provides real-time online security detection, providing strong support for network security.

However, with the continuous increase of Internet traffic and the evolution of network attack methods, NIDS/NIPS face severe performance challenges. High-speed packet processing, accurate threat identification, and timely response capability are all key issues that NIDS/NIPS needs to overcome. Therefore, improving the performance of NIDS/NIPS has become an important topic in the field of network security research, which is crucial for protecting the security of Internet infrastructure.

In this paper, we will delve into the key role of NIDS/NIPS in protecting the Internet infrastructure. We will first introduce the basic principles and functions of NIDS/NIPS to further explore its importance in the field of network security. Then, we will focus on the performance challenges faced by NIDS/NIPS and explore key techniques and approaches to improve NIDS/NIPS performance. Finally, we will look forward to the future direction of NIDS/NIPS development to provide useful references and guidance for network security research and practice.

2. Basic Principles and Functions of NIDS/NIPS

NIDS/NIPS (Network Intrusion Detection/Prevention System) are very important devices in the field of network security, and they play a key role in protecting the security of Internet infrastructure. With the rapid development and wide application of the Internet, computer networks have become the information infrastructure of modern society, but also face increasingly complex and widespread network security threats. The emergence of attacks such as network worms, botnets and computer viruses has brought serious threats and economic losses to the Internet infrastructure. Therefore, protecting the security of Internet infrastructure has become an important topic in today's network security research.

NIDS/NIPS provides strong support for protecting Internet infrastructure by detecting and preventing network intrusions through real-time monitoring of network traffic. NIDS relies heavily on the capture and analysis of network traffic to identify potential security threats. First, NIDS capture network traffic packets that pass through network interfaces or network switches. They then reorganize and reconstruct the captured packets to restore the original state of network communications. Next, NIDS perform in-depth analysis of the reconstructed traffic, including protocol parsing and traffic feature extraction, to identify security threats in the network. Based on predefined rules, signatures, or behavioral patterns, NIDS matches and detects traffic for potential intrusions. Once abnormal or suspicious network activity

is detected, NIDS generates alerts or reports to notify administrators or security teams to take appropriate countermeasures.

In contrast, NIPS not only has the capability to detect potential security threats, but can also take proactive steps to stop and defend against them. The fundamentals of NIPS include threat detection, threat response, real-time updates, and logging and analysis. NIPS analyzes and detects network traffic to identify potential intrusions through NIDS-like technology. Once a security threat is detected, NIPS will take appropriate defense measures, such as blocking traffic or blocking the source of the attack, according to pre-set policies and rules. At the same time, NIPS needs to be kept in sync with the latest threat intelligence and defense policies, by updating them in real time to cope with evolving network attacks. NIPS records all security events and response operations, and generates detailed logs for subsequent auditing and analysis.

As network security devices, NIDS/NIPS play a key role in protecting the Internet infrastructure. They help secure network systems and data by monitoring network traffic in real time, identifying security threats, taking defensive measures, and providing detailed reports. The functions of NIDS/NIPS are not limited to detecting intrusions, but also include real-time response and defense, in-depth analysis and reporting, and threat intelligence and updates. Continuous research and improvement of NIDS/NIPS technologies and methodologies are critical to securing the Internet infrastructure. Future directions may involve more efficient data processing, intelligent threat identification and more flexible defense mechanisms to address evolving cybersecurity challenges. Through continuous innovation and improved performance, NIDS/NIPS will play an even more important role in securing Internet infrastructure.

3. Challenges Faced by NIDS/NIPS

NIDS/NIPS (Network Intrusion Detection/Prevention System), as a network security device, plays a key role in protecting the Internet infrastructure. However, with the increase in Internet traffic and the continuous evolution of network attack methods, NIDS/NIPS is facing serious performance challenges. How to improve the performance of NIDS/NIPS has become a hot topic in the field of network security research.

First of all, large-scale Internet traffic requires NIDS/NIPS to be able to handle massive packets and quickly and accurately identify and classify potential security threats. The popularity of the Internet makes the scale and complexity of network traffic increase greatly, which puts forward higher requirements on the performance of NIDS/NIPS. NIDS/NIPS needs to have efficient packet processing capabilities, and be able to process a large number of data streams in real time in a high-speed network environment, and accurately analyze and judge the security threats in them. In addition, with the continuous growth of network traffic, NIDS/NIPS also need to have scalability, can flexibly adapt to changing traffic load.

Secondly, the diversity and complexity of network attack methods also put forward higher requirements

for the performance of NIDS/NIPS. Traditional security rules and signature detection methods have been difficult to meet the detection needs of new types of attacks. Network intruders continue to innovate and evolve, using more covert and complex attacks, such as zero-day vulnerability exploitation, behavior-based intrusion and so on. This requires NIDS/NIPS to have more intelligent and adaptive detection capabilities that can identify and stop new types of security threats, not just limited to known attack patterns. Therefore, researchers need to continuously conduct research on new algorithms and techniques to improve the detection capability of NIDS/NIPS for unknown attacks.

In addition, NIDS/NIPS needs to be highly reliable and stable. Due to its critical position in network security, any loss or omission of packet detection may lead to potential security risks. Therefore, NIDS/NIPS needs to have strong fault tolerance and fault recovery mechanisms to ensure continuous system operation and data integrity. In addition, NIDS/NIPS needs to have the self-protection capability of the defense mechanism to avoid being bypassed or damaged by attackers.

To address these challenges, researchers and network security experts have proposed a number of key technologies and approaches to improve the performance and effectiveness of NIDS/NIPS. These include high-speed packet processing techniques, intelligent classification and identification algorithms, distributed and collaborative defense mechanisms, and real-time response and automated defense. By optimizing packet processing algorithms and hardware acceleration techniques, the packet processing speed and throughput of NIDS/NIPS can be improved. Using machine learning and artificial intelligence technology, intelligent classification of network traffic and threat identification can be realized to improve detection accuracy and efficiency. Establishing a distributed NIDS/NIPS system can realize the cooperative work between multiple nodes and improve the overall security defense capability. Combined with automated response technology, NIDS/NIPS can respond to security threats in real time, automatically take defense measures, and reduce the delay of human intervention.

4. Key Technologies to Improve NIDS/NIPS Performance

Improving the performance of NIDS/NIPS (Network Intrusion Detection/Prevention System) is an important research direction in the field of network security, aiming to cope with the increasingly complex network attacks and the growing Internet traffic. In order to improve the performance of NIDS/NIPS, researchers and network security experts have proposed a series of key techniques and methods. This section discusses these key techniques and explores how they can enhance the performance of NIDS/NIPS.

First, high-speed packet processing technology is the key to improving the performance of NIDS/NIPS. With the rapid growth of Internet traffic, NIDS/NIPS need to process a large number of packets and perform traffic analysis and threat detection in real time. To address this challenge, researchers have worked to optimize packet processing algorithms and hardware acceleration techniques. The use of high-performance processors and specialized hardware gas pedals can increase packet processing speed and throughput. In addition, the use of parallel processing and pipelining techniques can effectively

improve the efficiency of packet processing. There are also some emerging technologies, such as programmable data plane (p. 4) and user-state data plane (eBPF), which can improve the performance of NIDS/NIPS through flexible packet processing and programming.

Second, intelligent classification and identification algorithms are important techniques to improve the performance of NIDS/NIPS. Traditional rule- and signature-based detection methods have been difficult to cope with the ever-changing means of network attacks. In order to improve the accuracy and efficiency of detection, researchers have adopted machine learning and artificial intelligence techniques. By training and optimizing models, NIDS/NIPS can automatically learn and identify normal behaviors and abnormal patterns in network traffic, thus improving the accuracy of threat detection. At the same time, combined with technologies such as deep learning and behavioral analysis, unknown attacks can be detected and predicted, improving the ability of NIDS/NIPS to respond to new types of threats.

In addition, distributed and collaborative defense mechanisms are critical to improving NIDS/NIPS performance. In the face of increasingly complex and large-scale network threats, a single NIDS/NIPS device is often unable to meet the demand for real-time detection and defense. Therefore, the establishment of a distributed NIDS/NIPS system can effectively improve the overall security defense capability through the collaborative work of multiple nodes. This distributed architecture can share the traffic load and improve the scalability and fault tolerance of the system. At the same time, nodes can strengthen security defense capabilities by sharing threat intelligence and real-time collaboration to detect and respond to security threats faster.

In addition, real-time response and automated defense technologies play a key role in improving NIDS/NIPS performance. After detecting a security threat, NIDS/NIPS needs to be able to quickly take appropriate defensive measures to stop the attack traffic and protect the attacked system. To enable real-time response and automated defense, researchers have developed tools such as automated response techniques and programmable firewalls. These technologies automate the rapid response to detected threats, including blocking the source of the attack, adjusting network policies, etc., which reduces the delay of human intervention and improves defense efficiency.

5. Future Outlook and Challenges

NIDS/NIPS (Network Intrusion Detection/Prevention System) play a key role in protecting the Internet infrastructure, but still face many outlooks and challenges in the future. With the rapid growth of the Internet and the continuous evolution of cyber threats, the role of NIDS/NIPS will become even more important, but it also needs to meet the challenges of technology, scale and complexity.

First, as the Internet continues to expand, the scale and complexity of network infrastructure continues to grow. The interconnection of a large number of network devices, sensors, and end devices has led to a dramatic increase in the size of the network, posing even greater challenges to NIDS/NIPS.NIDS/NIPS need to be able to effectively process and analyze massive amounts of network traffic, as well as adapt to and understand complex network topologies and protocols.

Therefore, one of the future perspectives is to build NIDS/NIPS systems that are scalable and efficient in processing large-scale data to cope with the growing Internet traffic and complex network environments.

Second, the rise of emerging technologies and applications also brings new challenges to NIDS/NIPS. For example, the rapid development of technologies such as IoT, cloud computing, and edge computing has led to dramatic changes in network boundaries and topologies. This has also led to the expansion of new types of network security threats and attack surfaces. One of the future perspectives is to integrate NIDS/NIPS with these emerging technologies and applications to develop security monitoring and defense solutions adapted to the new network environment. This requires NIDS/NIPS to be able to adapt to dynamically changing network topologies and growing device types, and to be able to recognize and protect against specific threats targeting emerging technologies.

In addition, with the continuous evolution and improvement of network attacks, NIDS/NIPS needs to continuously improve its detection and defense capabilities. Traditional rule and signature detection methods are no longer able to cope with increasingly sophisticated and stealthy attack methods. Therefore, one of the future perspectives is to improve NIDS/NIPS detection capabilities for unknown attacks and zero-day vulnerabilities by introducing smarter and adaptive detection techniques, such as machine learning, behavioral analysis, and artificial intelligence. Such technologies can enable automatic learning and identification of anomalous behaviors to more accurately identify and stop new types of cyber threats. [12-13]

Another important future outlook is to enhance the real-time response and automated defense capabilities of NIDS/NIPS. For cyber security, rapid detection and response is critical. nIDS/NIPS need to be able to identify and stop security threats in a timely manner to minimize potential losses. One of the future perspectives is to enable real-time defense capabilities of NIDS/NIPS by introducing automated response technologies and programmable firewalls. This will enable NIDS/NIPS to automatically take defensive measures, such as blocking attack sources and adjusting network policies, based on predefined policies and rules, thus reducing reliance on manual intervention and improving the efficiency and timeliness of defense.

Despite many future prospects, NIDS/NIPS also faces some challenges. One of them is privacy and compliance issues. As data privacy and compliance regulations tighten, NIDS/NIPS needs to ensure that it does not violate users' privacy rights when performing traffic monitoring and analysis. In addition, NIDS/NIPS needs to fulfill various industry standards and compliance requirements, such as PCI DSS, GDPR, etc., to ensure that it meets the regulatory requirements in terms of data processing and security.

In summary, NIDS/NIPS plays a key role in protecting the Internet infrastructure and faces many future prospects and challenges. By building NIDS/NIPS systems that are scalable and adaptable to emerging technologies, enhancing detection and defense capabilities, and strengthening real-time response and automated defense capabilities, we can better respond to growing and evolving cyber threats and

protect the security and stable operation of Internet infrastructure. At the same time, there is a need to continue to focus on privacy and compliance issues and to ensure that NIDS/NIPS meet regulatory requirements for data processing and security to ensure public trust and data protection.

6. Conclusion

NIDS/NIPS (Network Intrusion Detection/Prevention System) plays a key role in protecting the Internet infrastructure. With the rapid development and wide application of the Internet, computer networks have become the information infrastructure of modern society. However, network attacks such as network worms, botnets and computer viruses are emerging, bringing serious threats and economic losses to the Internet infrastructure. NIDS/NIPS is able to provide real-time online detection of internal and external attacks through real-time monitoring of network traffic, thus protecting the security of the Internet infrastructure.

The basic principles and functions of NIDS/NIPS include network traffic capture and analysis, protocol parsing and feature extraction, threat detection, and alert generation, etc. NIDS/NIPS identifies potential security threats through the analysis and processing of network traffic packets and takes corresponding defensive measures. They can help secure network systems and data, stop intrusions and reduce potential losses. the functions of NIDS/NIPS are not limited to detecting intrusions, but also include real-time response and defense, in-depth analysis and reporting, and threat intelligence and update.

However, NIDS/NIPS still faces some challenges in protecting Internet infrastructure. First, the increase in Internet traffic and the growth in the types of cyber-attacks make NIDS/NIPS face severe performance challenges. They need to have efficient packet processing capabilities to be able to process a large number of data streams in real time in a high-speed network environment and accurately analyze and judge the security threats in them. Secondly, the diversity and complexity of network attacks require NIDS/NIPS to have intelligent and adaptive detection capabilities to identify and block new security threats, not just limited to known attack patterns.

In addition, NIDS/NIPS needs to have a high degree of reliability and stability. Any packet loss or missed detection can lead to potential security risks. Therefore, NIDS/NIPS needs to have strong fault tolerance and fault recovery mechanisms to ensure continuous system operation and data integrity. At the same time, NIDS/NIPS also needs to have the self-protection capability of the defense mechanism to avoid being bypassed or damaged by attackers.

In the future outlook, NIDS/NIPS requires continuous research and innovation to address the growing and evolving cybersecurity challenges. Building NIDS/NIPS systems that are scalable and efficient in handling large-scale data, enhancing detection and defense capabilities, and strengthening real-time response and automated defense capabilities will be the future direction of development. At the same time, the integration of emerging technologies and applications, such as IoT, cloud computing and edge computing, combined with NIDS/NIPS to develop security monitoring and defense solutions adapted

to the new network environment is also an important direction.

In conclusion, NIDS/NIPS plays a key role in protecting the Internet infrastructure. By monitoring network traffic in real time, identifying security threats, taking defensive measures, and providing detailed reports, NIDS/NIPS help secure network systems and data. However, challenges include performance pressure, new attack methods, and reliability requirements. Through continuous research and innovation to improve the performance of NIDS/NIPS, adapt to new network environments, and enhance real-time response and automated defense capabilities, we are able to better address the growing and evolving cybersecurity challenges, and protect the secure and stable operation of the Internet infrastructure.

References

Cui, M., Xiong, J., & Zhang, H. (2018). A review of network intrusion detection techniques in Internet infrastructure. *Computer Science and Applications*, *8*(9), 3-9.

Deng, J. H., Ouyang, Q., & Liang, Z. N. (2016). Research on network intrusion detection system in Internet infrastructure protection. *Modern Computer (Professional Edition)*, (13), 130-133.

Hu, Z. H., & Chen, Z. F. (2019). Research progress on network intrusion detection based on deep learning. *Information Network Security*, *3*(5), 50-58.

Huang, D., Zhu, J. D., & Cai, K. (2019). A research review of network intrusion detection techniques based on machine learning. *Computer Engineering and Design*, *40*(8), 2351-2357.

JANG, H. W., LI, J. M., & ZHU, Yang. Research review on network intrusion detection system based on data mining. *Computer Engineering and Applications*, *52*(1), 1-6.

Jie, Z., Yu, C. L., & Tang, H. L. (2019). Research and application of intrusion detection system for Internet infrastructure. *Modern Communication Technology*, (9), 19-24.

Lin, J., Chen, T., & Wang, C. Q. (2016). Research on key technologies for Internet infrastructure security protection. *Communication Technology*, *49*(9), 1105-1111.

Liu, B., Zhao, H. X., & Xue, J. (2017). Research review on network intrusion detection based on deep learning. *Computer Science*, *44*(9), 6-10.

LIU, X. F., LIU, W. J., & YAO, Z. (2020). A review of research on security situational awareness technology for Internet infrastructure. *Computer Science*, *47*(4), 17-22. https://doi.org/10.1016/j.procs.2020.08.003

Meng, Z., & Wu, W. H. (2017). Research review on network intrusion detection based on data mining. *Computer Engineering and Applications*, *53*(3), 50-55.

Tian, M. M., Yang, W. J., & Wang, D. S. (2018). A review of network intrusion detection techniques based on data mining. *Computer Science and Exploration*, *12*(2), 133-148.

Wang, J. B., Luo, L. L., & Hu, Z. H. (2015). A review of intrusion detection systems for Internet infrastructure. *Computer Science and Exploration*, *9*(4), 379-394.

WANG, Y. H., LIU, Y. J., & ZHAO, S. H. (2014). A review of research on security protection of

Internet infrastructure. *Journal of Network and Information Security*, *2*(1), 36-44.

Yan, X. D., Sun, J. Y., & Xie, H. B. (2018). A review of research on Internet infrastructure security protection. *Computer Science and Exploration*, *12*(1), 45-57.

Yuan, P. L., Chen, W. B., & Zhou, L. Y. (2015). A research review on network intrusion detection techniques based on machine learning. *Computer Science and Exploration*, *9*(6), 750-767.