IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2320-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 10, Issue 4, April 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.512

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004006

The Role of Firewall as an Important Network Security Tool in Anomaly Detection

Anand Digambarrao Kadam [1], Vijayshri Chandrasen Thaware [2], Sachin Bhagwanrao Shelke [3]

Research Scholar, Department of Computer Science & Information Technology, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India[1]

Research Scholar, Department of Library & Information Science, Dr. Babasaheb Ambedkar Marathwada University, Aurangabad, Maharashtra, India[2]

P.G. Student, Dr. G.Y. Pathrikar College of Computer Science & IT, Aurangabad, Maharashtra, India[3]

ABSTRACT: The vast spreading of Internet has made the world a small village. The majority of business and corporate work is done on internet. However, diversity and capabilities of increasing communication tools and access, sharing and storing information is very fast and easy. As a result, a vast database is generated everywhere. Today's corporation networks are very large and interconnected with other networks. Also, the devices and applications connecting and using corporate networks are continually increasing in complexity and thus network security has become a global focus in the world. Therefore Firewall has become an important security tool in recent era. Often, there are many data entries that do not fit properly into the model which known as outliers or anomalies. This becomes a big issue in very large databases. The present paper focus on the role of firewall as a security tool and it also depicts the importance of firewall logs in Anomaly detection.

KEYWORDS: Firewall, Network, Security Tool, Anomaly detection.

I. INTRODUCTION

With the great explosion of information technology, Internet has become the most used communication method across the world that allows corporations to increase their productivity and extend activity. Today, diversity and capabilities of increasing communication tools and access, sharing and storing information is very fast and easy. It is a worldwide trend, and with the advent of internet technology, day to day work has been shifted over the Internet and thus network security has become a global focus in the world. Further, computer networks constantly change human society in accompanying with information and network security issues which becomes more sophisticated every day.

In the recent era, all enterprises and Organizations (small, big, public or private) use firewalls to enforce their security policy. Firewall acts as a router that connects different network zones together. A firewall is an essential component for a network connected to the Internet. It is the most common and important technique for enforcing network security. Therefore, without a firewall, you're not even doing the minimum step toward protecting your computers and network. A firewall is your network's guard that only allows certain packets and people to pass in or out the network. However, efficient and unrestricted control of anomalies rules is becoming increasingly difficult in large networks. Further, Firewalls are becoming more complex and their rule sets may have anomalies.

While the use and setting of firewalls is the first important step towards network securing, firewall policy rules have proved to be error-prone and sensitive especially in large networks. These rules are written and tailored to filter out any malicious traffic passing through the network. Because of the continuous growth of security threats, writing and managing Firewall rules is a sophisticated and complex task and any inappropriate management of these rules will cause anomalies. Moreover, the inappropriate configuration of Firewalls could enable malicious content or unauthorized users to pass through the network.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004006

II. ANOMALY – A MAJOR NETWORK SECURITY ISSUE

Often, there are many data entries that do not fit properly into the model which known as outliers or anomalies. This becomes a big issue in very large databases. If a model is developed including these anomalies, then the model may not behave well for the data. Actually, anomalies occur infrequently; however, their consequences affect the network security where it occurs and becomes a big issue. Anomalies create critical problem and risk in networks, releasing voluntaries and made it easily exposed to threats. Therefore, the network administrator must prepare and plan a set of firewall policies to prevent such problems and necessary to be aware of the consequences of these anomalies.

Discovering anomalies in a dataset is known as anomaly detection and it is mainly concerned with detecting hidden changes, patterns, anomalies and associations in the dataset. Detection of anomalies is based on patterns or profiles reflecting normal behavior of hosts, network users and identifies attacks as variations from these patterns or profiles. It is a significant data analysis process that detects abnormal or anomalous data from a specified dataset. It is an important discipline of data mining as it includes rare and unusual patterns in a dataset. Anomaly detection is broadly utilized and applied in many domains such as fraud detection, public health, intrusion detection, image processing, robots behavior, sensor networks, etc.

The network administrators of most networks and computer systems depend on periodic audit data or logs to get an idea about the status of the networks. Out of many different places, data mining can come. One of log mining's major advantages is that it's not limited to some kind of method. Data mining has a big role in anomaly detection, because this process involves the comparing between unexpected behaviors and expected behavior, and effectively can be used in anomaly detection process.

Data Mining is nothing but finding the expected useful data from the huge data collection. It is a predictive model and methodology which focuses on exploring a huge amount of dataset in order to determine interesting patterns in a large dataset. Furthermore, it guides decision for further dataset analysis [6]. The two most promising data mining techniques are classification and association rule mining algorithms. Association rule mining discovers the relationships or associations between different items. Classification algorithms' main objective is to develop an effective and solid predictive rule set based on the rules extracted. Integrating the rule mining association and classification enables a hybrid model or system to be implemented.

III. OVERVIEW OF NETWORK SECURITY

Computer networks constantly change human society in accompanying with information and network security issues which becomes more sophisticated every day. With the advent of internet technology, day to day work has been shifted over the internet and thus network security has become a big issue in the world and a need for survival for an organization. All computers and systems in computer networks that connected to the Internet are vulnerable to attacks. Depending on the computer system and Internet for banking, stock price, news, receiving emails and online shopping has increased enormously.

Today's corporation networks are very large, run both standards and propriety protocols and interconnect with other networks. Also, the devices and applications connecting and using corporate networks are continually increasing in complexity. The excessive use of communication networks increases the need for a secure and safe system to overcome threats and attacks. Moreover, every computer network is vulnerable to unauthorized access to private and sensitive information. Computer network security is commonly deployed in two ways:

1. Establishing a powerful external blockade to prevent unauthorized users from accessing a network.
2. Monitoring the network for attack traces.

In general, a powerful security system consists of a set of network security tools, and these tools can work together and exchange information with each other, these tools are:

1. Firewalls that regulate incoming-outgoing network traffic through the network and block unwanted traffic on the basis of a set of pre-defined policy rules.

2. Intrusion detection systems (IDS) that are used for detecting intruders attempting or accessing networks.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004006

3. Data encryption to ensure that the server provides the data for only authorized users using either symmetric key encryption or asymmetric key encryption.

4. Authentication technology to verify the authentication of the entity. It is based on cryptography, message authenticity, access authority, authenticity identity and finally digital identification.

5. Vulnerability assessment tools that are used to find and fixed security Vulnerabilities present in networks.

IV. NETWORK SECURITY GOALS

To secure computer systems we should assure the three primary goals of network security: availability, authentication, integrity and confidentiality. Further, we have to develop new methods to improve computer network security, so that the three major goals of network security, data integrity, confidentiality and availability, will be guaranteed. The network security's three primary objectives are discussed below:

i. **Integrity:** Data integrity assures that the data has not been changed or modified in transit and during transmission between computers. Also, it ensures that a no attack changes data that is stored on the computer network systems.

ii. **Confidentiality:** Data confidentiality assures to keep data private. It implies no disclosing information to unauthorized people. It involves physically or logically restricting access to the data or encrypting traffic passing the network.

iii. **Availability:** The availability of data assures that the data and information on a network can be requested when it is needed. It is a measure of the data accessibility.

V. FIREWALLS IN NETWORK SECURITY

Firewalls are the mainly significant component of the established security mechanisms that serve as a bridge between threats between the internal and the external networks. Firewalls are often described as systems that defend the network from external threats; they also avoid the spread of an unwanted situation by reaching the external network. Computer-to-computer data connections are a very useful process for information transfer; however, they carry a diversity of risks, such as the safe transmission of transmitted information and the security of transmitting systems.

Firewalls are the most important element of the established security mechanisms that serve as a connection between inside network and the external network. Although they are often described as systems that protect the network from external threats, they also prevent the spread of an unwanted situation by reaching the external network. The information that will be entered into and transferred to outside the institution must be secured. Firewalls are the most effective solution at this stage.

Types of Firewalls

Firewalls have several types relating to their intended use and the techniques used in their construction. They are usually named according to their most important feature. Some sources classify the firewall based on its location in the OSI layer model. Basically, there are four types of firewalls:

1. **Packet Filtering Firewalls:** Packet-filtered firewalls accept or reject packets by looking at the header content of packets from network traffic. These firewalls run on the network layer which is the third layer of the OSI reference model. These types of firewalls, which obtain the header information of millions of packages and compare them according to the conditions in the rule list. Packet filtering firewall can filter packet according to the following fields in the packet header:
   - ✓ Source and Destination IP addresses
   - ✓ Source and Destination Port numbers
   - ✓ Packet types (UDP, TCP, etc)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004006

- ✓ Service protocols (Telnet, http, FTP, SMTP, IP Tunnel, etc.)

2. **Application Layer Firewalls**: These firewalls have many advantages over packet filters firewalls. Application-Proxy Gateway Firewalls are powerful in examining network address and port-based network connections. They also allow application-specific commands to be used in network traffic. Another advantage is that they can adapt to this situation regardless of the type of user authentication deemed appropriate for the enterprise infrastructure. Application-Proxy Gateway Firewalls is capable of authenticating users directly, while Packet Filter Firewalls verifies by network layer address. These types of firewalls have a very flexible structure in terms of closing and opening the port ports which are not needed by the users. They work on layer 7, the application layer of the OSI reference model. Therefore, they are often the preferred type of firewall. The ports used in attacks on the system can be analyzed with the help of firewall logs, and the port rule Table can be updated by the system administrator and these types of firewalls are now blocked before they reach the network.
3. **Application Level Gateway (proxy firewalls)**: proxy firewalls are used to filter traffic on the application layer so they are called application-level gateway. They give all the basic proxy functions and comprehensive packet analysis. The user must provide valid user id and authentication information to the proxy server to communicate with the destination service. A standard device-level gateway firewall can provide proxy protocol and application services such as: Telnet http FTP and SMTP.
4. **Circuit Level Gateway Firewalls:** Basically, it used for the connections of TCP. They check the handshaking of the TCP to guarantee the authenticity of the session from which the packet comes. These types of firewalls are much faster than other of firewalls. Because as soon as a connection has been formed all the session packets will pass through the gateway.

VI. THE ROLE OF FIREWALL LOGS IN ANOMALY DETECTION

Nowadays, with the increase in the number of electronic devices that can be connected to the internet and the transactions that can be performed, great data traffic has emerged. The dimensions of this traffic can reach TB (TeraByte) level. This data that occurs when electronic devices communicate with each other and with other network devices are often ignored. This is because it is an operation between the sender and the receiver and does not affect the connection. This data is important for network administrators. When network administrators want to investigate the cause of anomalies in the network, they use this data. The records of traffic on the network are called log or log. There are many methods for collecting logs. However, analyzing and interpreting these enormous data is a difficult and time-consuming task. The operating systems we use also log events occurring within the operating system. Firewalls log traffic to and from a private network in the log file. Keeping these logs is vital for network security. In next stages, these logs can be used for:

- Before making decisions to identify problems with the current network structure (expanding the network, changing bandwidth, etc.), system administrators can make decisions by looking at the traffic of subnets and backbone on the firewall and make future decisions.
- A successful attack as a result of attacks on the system indicates the weakness of your system if viewed positively. Therefore, a successful attack can be seen by looking at the logs and after this attack, the deficiency that causes vulnerability can be eliminated.
- By identifying the deficiencies of the attacked computers can be used in removing.
- The points where the network services used in the internal network are blocked can be seen and necessary arrangements can be made.
- When the sections in the network system are dense and underutilized, the resources in the less dense sections can be shared with the more dense sections to improve service quality.

In addition, most firewalls provide statistical reports of available traffic. For example, it can graph the total number of received and sent packets daily, weekly, monthly, and yearly. Some firewalls can also do this in MS Word file format. Types of viruses that attack from logs, unauthorized access, and data traffic in GB, TB, and the number of blocked and allowed connections. It can also list the data traffic in order of maximum or minimum and graphically display it. However, these representations are made statistically. System administrators can use these graphs.

Due to the large size of the logs, these records constitute a serious data mine. Firewall logs for the implementation of data mining techniques are like a unique mine. In short, firewall logs can be analyzed with data mining methods.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512|

|| Volume 10, Issue 4, April 2021 ||

DOI:10.15680/IJIRSET.2021.1004006

In fact, because of the high amount of data, using data mining techniques is an ideal method for analyzing firewall logs. However, it is imperative that the data in the logs are still to be analyzed as it contains the raw data.

In general, firewall logs are like an aircraft black box that records flight data such as speed, height, etc. of an aircraft. Firewall logs are vital for improving the firewall, finding and addressing vulnerabilities in the corporate network, identifying new types of viruses, firewall policy rule anomalies, and addressing the grievances of network users exposed to attacks.

REFERENCES

[1] S. Agrawal, J.Agrawal ,(2015)," Survey on anomaly detection using data mining techniques," *Procedia Computer Science*, vol.60, pp.708-713.

[2] K. Golnabi, R. K. Min, L. Khan and E. Al-Shaer,(2006), "Analysis of Firewall Policy Rules Using Data Mining Techniques," *IEEE/IFIP Network Operations and Management Symposium NOMS, Vancouver*, BC, pp. 305-315.

[3] Winding, R., Wright, T., & Chapple, M. (2007) System anomaly detection: Mining firewall logs. In *2006 Securecomm and Workshops,* vol.5, (pp. 1- 5), IEEE.

[4] Al-Shaer, Hamed, Boutaba, Hasan,(2005) "Conflict classification and analysis of distributed firewall policies," *IEEE journal on selected areas in communications,* vol.23, pp. 2069-2084.

[5] Chandala, V., Banerjee, A., Kumar, V.(2009), "Anomaly Detection: A Survey, ACM Computing Surveys", *University of Minnesota*.

[6] Nalepa, G. J., & Ligeza, A. (2003). Designing reliable web security systems using rule-based systems approach. In *International Atlantic Web Intelligence Conference,* May, pp. 124-133, Springer, Berlin, Heidelberg.

[7] Andrew Simmonds, Peter Sandilands, Louis van Ekert. (2004) *Lecture Notes in Computer Science* Volume 3285.

[8] Chapter 6: Information Systems Security – Information Systems for Business and Beyond. (2014, February 28). [online] Available at: https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/. [Accessed 13 Jan. 2018].

[9] Large, D., & Farmer, J. (2009). Broadband Cable Access Networks. *The HFC Plant*.

[10] Siemens, G., & d Baker, R. S. (2012). Learning analytics and educational data mining: towards communication and collaboration. In *Proceedings of the 2nd international conference on learning analytics and knowledge,* April (pp. 252-254). ACM.

[11] JANOŠCOVÁ, R. (2016). Mining Big Data in WEKA. *11th IWKM, Bratislava, Slovakia.*

[12] Han, J., Kamber, M., & Pei, J. (2011). Data mining concepts and techniques third edition. *The Morgan Kaufmann Series in Data Management Systems*, 83-124.

[13] Bramer, M. (2007). Principles of data mining, Vol. 180. *London*:*Springer*.

[14] Niculescu-Mizil, A., & Caruana, R. (2005). Predicting good probabilities with supervised learning. In *Proceedings of the 22nd international conference on Machine learning,* August (pp. 625-632). ACM.

[15] Abie, H. (2000). An overview of firewall technologies. *Telektronikk*, vol. 3, pages 47-52.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor:
7.512

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details