IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A SURVEY ON EMERGENT FIREWALL TECHNIQUES OVER TRADITIONAL FIREWALLS

[1] Pratyush Sanadhya, [2] Vanshika Thakur and [3]B. Chandra Mohan

[1] UG Student, [2] UG Student, [3]Associate Professor (Senior)

School of Computer Science and Engineering

VIT Vellore, India

Abstract: Now-a-days the effectiveness in firewall become major requirement due to huge hackers, hence comparison of Emergent Firewall Techniques (EFT) with Traditional Firewall Techniques (TFT) is focused in this paper. TFT has been the most commonly used security approach in the past. This paper highlights the limitations of TFT in protecting against emerging security threats, whereas the EFT uses a more dynamic approach which allows for real-time security adaptation and response to emerging threats. The paper analyzes a range of EFT techniques such as Machine Learning-based EFT, Cloud-based EFT, and Software-Defined Networking (SDN) based EFT, and provides evidence of superior performance compared to TFT in terms of threat detection, response time, and accuracy. The results of this survey paper demonstrate that EFT is a more effective approach for securing modern networks against ever-evolving security threats, and highlights the need for organizations to consider the adoption of EFT in their security strategies.

Index Terms **- Information Security, Firewall, Machine Learning, Software Defined Network.**

I.INTRODUCTION

In recent years, the security landscape has changed dramatically, with increasingly sophisticated cyber threats emerging on a daily basis. Network security is a system created to keep an eye on malicious activity and protect the network. It includes information access authentication within a network and is managed by the network administrator[1]. A tool or piece of software that monitors and regulates network traffic is called a firewall in a network security system.

There are multiple threats in the network, some of them are given below:

1. Malware: Malware, such as viruses, worms, and trojan horses, can infect a network and cause significant damage. Emergent firewall techniques can detect and block known malware signatures, as well as use behavior-based analysis to detect and block unknown malware.
2. Denial of Service (DoS) Attacks: A DoS (denial-of-service) attack make the targeted device unavailable to the users. This is accomplished when a single computer sends a large number of requests to the device resulting which it cannot process the requests which are legit.DoS attacks aim to overload a network by sending a large number of requests to a server. Emergent firewall techniques can detect and block DoS attacks by analyzing the traffic and blocking suspicious requests.
3. Intrusion: Intruders can gain access to a network and steal or damage sensitive data. Emergent firewall techniques can detect and block suspicious activity, such as unauthorized access attempts, and prevent intruders from gaining access to the network[7].
4. Man-in-the-Middle (MitM) Attacks: In a M-i-t-M attack, an attacker seizes the communication between two users and can eavesdrop or manipulate the conversation. Emergent firewall techniques can detect and block M-i-t-M attacks by analyzing the traffic and blocking suspicious requests.
5. Phishing: Phishing attacks use social engineering to trick users into divulging sensitive information, such as login credentials. Emergent firewall techniques can detect and block phishing attempts by analyzing the traffic and blocking suspicious requests.
6. Ransomware: Ransomware can encrypt a user's files and demand payment in exchange for the decryption key. Emergent firewall techniques can detect and block ransomware by analyzing the traffic and blocking suspicious requests[6].

Traditional Firewall Techniques (TFT) have been the mainstay of network security for many years, but their limitations in adapting to emerging threats have become increasingly apparent. In contrast, Emergent Firewall Techniques (EFT) offer a more dynamic and adaptive approach to network security, providing real-time threat detection and response. This survey paper provides an overview of the effectiveness of EFT compared to TFT in addressing the security challenges of modern networks. The paper examines the underlying principles of EFT, including Machine Learning-based EFT, Cloud-based EFT, and Software-Defined Networking (SDN) based EFT, and assesses their performance in terms of threat detection, response time, and accuracy. By providing a comprehensive analysis of EFT, this paper highlights the superiority of this approach compared to traditional security techniques, and the need for organizations to consider adopting EFT in their security strategies to better protect their networks from emerging cyber threats[18].

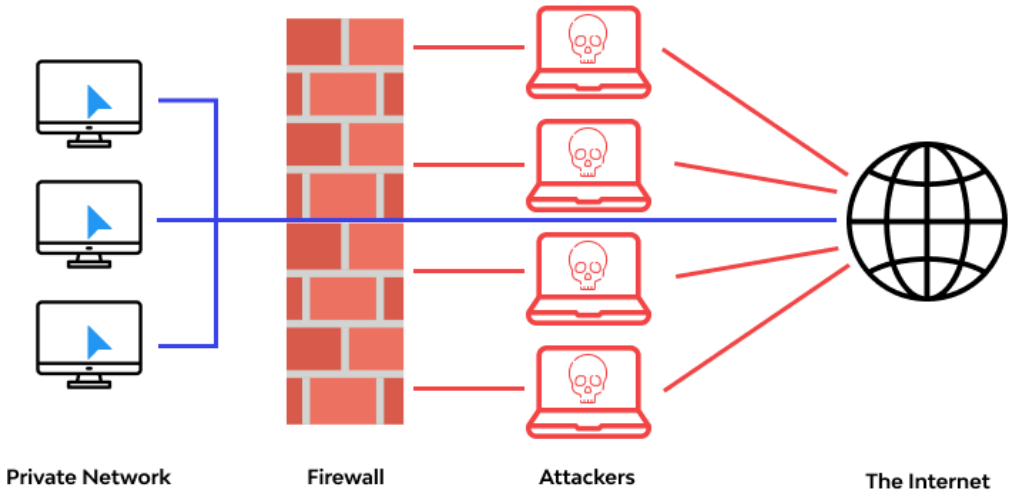

Figure 1. Working of Firewall[4]

An organized study was done to compare the efficiency of Emergent Firewall Techniques (EFT) with Traditional Firewall Techniques (TFT). The study focused on EFT and TFT methods to network security and included a thorough evaluation of the published research in pertinent academic publications, conference proceedings, and technical reports.

In conclusion, this review study offers an in-depth examination of the efficacy of EFT in comparison to TFT, based on a thorough investigation of the existing literature. Organizations looking to strengthen their network security posture and implement more powerful security controls to guard against new cyber threats may find benefit in the survey's findings.

For this study secondary data has been collected. From the website of KSE the monthly stock prices for the sample firms are obtained from Jan 2010 to Dec 2014. And from the website of SBP the data for the macroeconomic variables are collected for the period of five years. The time series monthly data is collected on stock prices for sample firmsand relative macroeconomic variables for the period of 5 years. The data collection period is ranging from January 2010 to Dec 2014. Monthly prices of KSE -100 Index is taken from yahoo finance.

II. Review on Traditional Firewall Techniques

Traditional Firewall Techniques (TFT) have been the mainstay of network security for many years, and they typically rely on one or more of the following approaches:

2.1 Packet Filtering Firewalls:

This approach is based on filtering incoming and outgoing network traffic based on predefined rules. These rules can be based on a variety of factors such as source and destination IP address, port number, protocol, and other characteristics.

Firewalls carry out the most elementary tasks, such inspecting the packet header, and checking the IP address.They have the advantage of speed and efficiency because of how swiftly they operate. Packets can be filtered based on the following factors: source IP address, destination IP address, TCP/UDP source port, and TCP/UDP destination port. A firewall like this can block connections to and from specific hosts, networks and ports.They are inexpensive since they make use of softwares present in the router and offer a high level of security [1][13].

Packet Filtering Firewalls types are given below-

1. IP Traceback Based Intelligent Packet Filtering
2. On Dynamic Optimization of Packet Matching in High-Speed Firewalls
3. Detecting and preventing peer-to-peer connections by Linux IPtables
4. Discriminative Wavelet Packet Filter Bank Selection for Pattern Recognition
5. Modeling Filtering Predicates Composition with Finite State Automata[2][12]

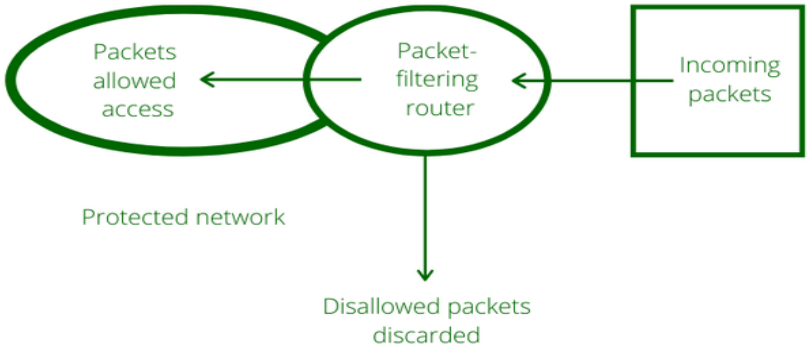

Figure 2. Packet Filtering Firewall[21a]

2.2 Stateful Inspection Firewalls:

Stateful Inspection Firewalls maintain a state table of the connections and traffic flowing through them. They use this state table to identify and filter traffic that is not part of an established connection or session, thereby blocking unauthorized access.

Stateful Inspection is an expansion of packet-by-packet filtering that keeps track of individual flows and allows policy checks to span multiple packet sequences. Stateful Inspection technology is used by many firewalls, including Cisico PIX[2], 3COM Secure Gateway [3], Netsreen Firewall[1], and Checkpoint FW-1[4]. A session table, whose entries typically list source and destination IP addresses and port numbers, is necessary for stateful inspection. A match is sought in the session table for each packet that arrives. When the first packet from an untracked flow appears, a session entry is created in the format src-addr, src-port, dst-addr, dst-port, ip-p, state, time>. An established session's subsequent packets are checked against the session table rather than the rule base. The performance of Stateful Inspection firewall mainly depends on the performance of processing session table[8][11].

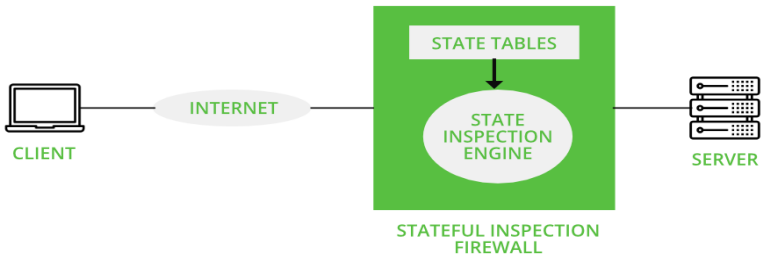

Figure 3. Stateful Inspection Working Methodology[22]

2.3 Application-Level Gateways:

Application-Level Gateways, also known as Proxy Firewalls, are designed to filter traffic at the application layer. ALGs are used to provide application specific proxies and are also used to inspect the packets in depth. After applying the security policies, the traffic is allowed to enter the inside network where the ALG evaluates and examines the traffic. They act as intermediaries between the network and the application, examining and filtering traffic based on the application protocol [9].

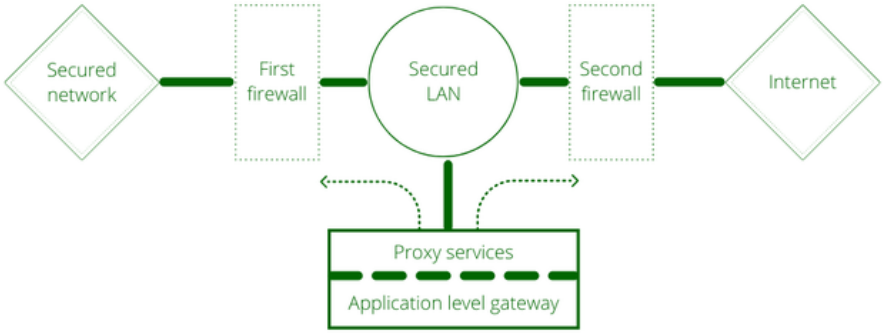

Figure 4. Application-Level Gateways[21b]

2.4 Unified Threat Management (UTM):

Unified Threat Management (UTM) or unified security management (USM) is a new trend in firewall security. In the network security industry, it is a solution. Traditional Firewall Technique can also do content filtering, load balancing, data leak prevention, and anti-virus duties that were previously handled by multiple systems[10].

Advantages of UTM:

1. Reduced complexity
2. Synergies with high-end software solutions
3. Easy to deploy
4. Low operator interaction
5. Easy Troubleshooting

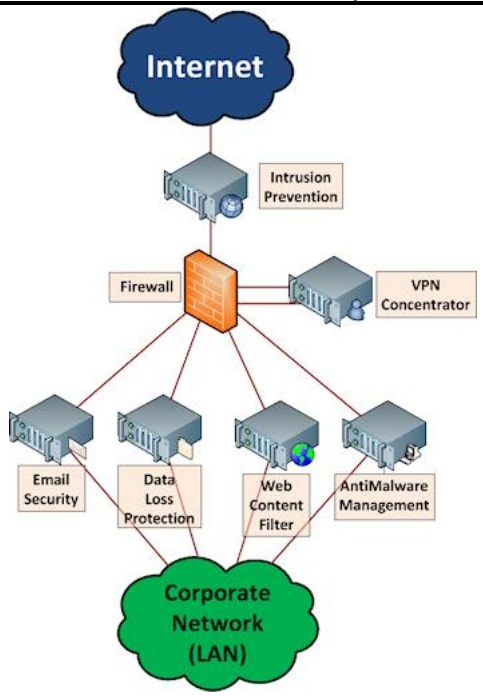

Figure 5. Example of Traditional Network Security[23]

III. Review on Emergent Firewall Techniques

While TFT has been effective in securing networks against known threats, they have limitations in adapting to new and emerging threats. Some of the key limitations of TFT include:

1. Inability to detect and respond to unknown threats: TFT is based on predefined rules and signatures, which means that it can only detect and respond to known threats. It is not effective in detecting and responding to new and emerging threats for which there are no predefined rules or signatures.
2. Limited visibility into application-level traffic: TFT is designed to filter traffic based on IP addresses, port numbers, and protocols, but it lacks visibility into the application-level traffic. This makes it difficult to identify and block threats that are hidden within legitimate application traffic.
3. Inability to scale with network complexity: TFT can become complex and difficult to manage as the network grows in size and complexity. It can also become a bottleneck in high-traffic environments, leading to performance issues.
4. Limited ability to adapt to changing network conditions: TFT is based on static rules and policies, which means that it cannot adapt to changing network conditions in real-time. This can result in false positives or negatives, leading to security gaps or unnecessary disruptions.
5. Inability to provide comprehensive protection: TFT typically provides only basic security features such as packet filtering and intrusion detection, which may not be sufficient to protect against more advanced threats such as zero-day exploits or advanced persistent threats (APTs).

These limitations highlight the need for more dynamic and adaptive approaches to network security, such as Emergent Firewall Techniques (EFT), that can detect and respond to new and emerging threats in real-time.

Some of the key EFT techniques include:

3.1 Machine Learning-based Firewalls

Machine Learning (ML) algorithms can be used to analyze network traffic patterns and identify anomalies that may indicate potential threats. ML-based firewalls can adapt to changing network conditions and learn from past incidents to improve their accuracy in identifying and responding to threats[16].

This can be configured through a dedicated web-app. There are five basic points:

(1) Power on/off unit
(2) Training unit
(3) Parsing unit
(4) Classification unit
(5) Decision-making unit

When the WAF is active, the OS service contacts the database and retrieves the configurations to run WAF, activate the listener, and watch for incoming requests for the WAF that acts as a middleman between the client and the web server.In the first unit, the procedure starts with power unit. Using the chosen dataset and the chosen classification algorithm, the training process begins after running the WAF. After the training process is finished and the first and second units have finished their work, WAF is prepared to accept requests. When a request comes in, WAF's parsing unit is the first to handle it. It breaks down the request into its constituent parts, extract the features, and sends the features to the classification unit, which classifies the request using the classification technique that the administrator chooses in the training unit. The decision to pass or drop a request is made by the decision-making unit based on the results sent by classification unit.

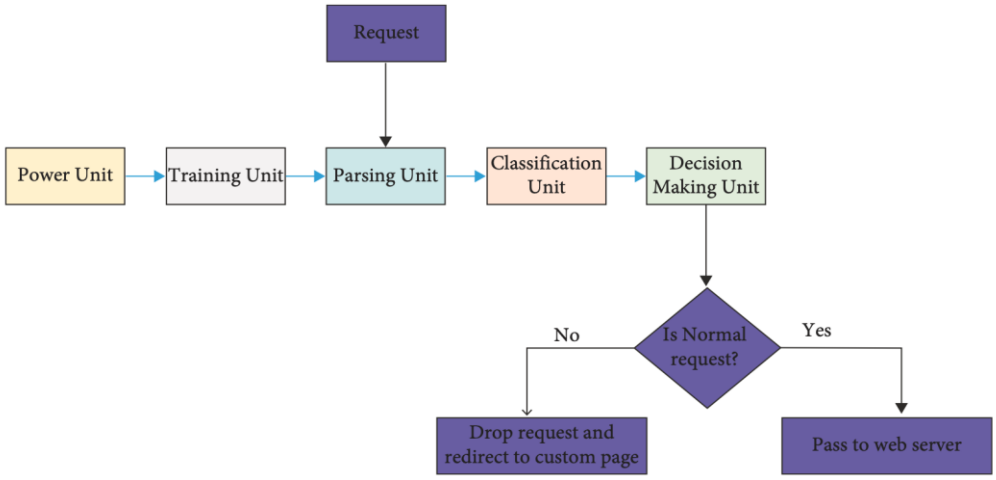

Figure 6. Units of proposal WAF (brief diagram) [25]

Machine Learning (ML)-based firewalls are a new generation of firewalls that use advanced machine learning algorithms to detect and prevent cyber threats. Here are some ways in which ML-based firewalls are better than TFT[15]:

1. Detection accuracy: ML-based firewalls can detect new and sophisticated cyber threats with greater accuracy compared to traditional firewalls like TFT. This is because ML-based firewalls can analyze large volumes of data and identify patterns and anomalies that are difficult for traditional firewalls to detect.
2. Automation: ML-based firewalls can automate the identification and mitigation of cyber threats, reducing the need for manual intervention. In contrast, TFT firewalls require manual configuration and monitoring, which can be time-consuming and prone to human error.
3. Scalability: ML-based firewalls are highly scalable and can handle large volumes of network traffic. TFT firewalls may struggle to keep up with the increased traffic during peak hours, which can lead to network slowdowns or downtime.
4. Real-time response: ML-based firewalls can respond to threats in real-time, automatically adapting their security policies based on the type and severity of the threat. This is in contrast to TFT firewalls, which may not be able to respond quickly enough to prevent a cyber attack.
5. Adaptability: ML-based firewalls can learn from past cyber attacks and adapt their security policies to prevent similar attacks in the future. This makes ML-based firewalls more effective than TFT firewalls at preventing cyber threats.

Overall, ML-based firewalls offer several advantages over traditional firewall technologies like TFT, including detection accuracy, automation, scalability, real-time response, and adaptability.

3.2 Cloud-based Firewalls

Cloud-based firewalls are designed to provide security at the network edge, using cloud-based resources to analyze network traffic and detect potential threats. They are highly scalable and can provide comprehensive protection against a wide range of threats. In recent years, firewalls have been installed between a secure internal network and an unsecured network that exists between a private network and the internet. Originally, firewalls were physical hardware components of an organization's or enterprise's data network. The firewalls enable or dis-allow network activity based on a predetermined set of criteria. Few firewalls permitted network managers to change or adjust their separate networks. With the introduction of cloud computing, there is no separation between an internal network and the internet. The cloud-based firewall thereby offers the necessary virtual barrier between the two.

Cloud-based WAFs are typically centrally orchestrated, which means that all of the service's customers can access information about threat detection. Together, we achieve higher detection rates and fewer false positives. One type of WAF is the Cloud-based Web Application Firewall. The host does not need to make any hardware or software changes because the CWAF is platform-independent. To route all web traffic through the WAF, where it is inspected, almost all providers demand a DNS change.

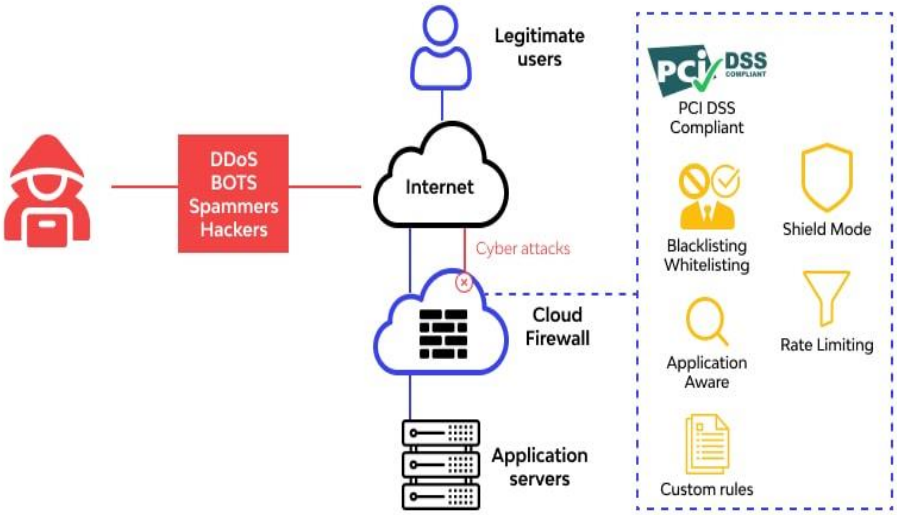

Figure 7. Working example of SaaS Firewalls[26]

Cloud-based firewalls are a type of firewall that is hosted in the cloud instead of being deployed on-premises like traditional firewalls, such as TFT (traditional firewall technology). Here are some ways in which cloud-based firewalls are better than TFT:

1. Scalability: Cloud-based firewalls can be easily scaled up or down based on changing network traffic demands, making them highly scalable. This is in contrast to traditional firewalls, which can be difficult and expensive to scale.
2. Flexibility: Cloud-based firewalls can be quickly and easily deployed, managed, and updated remotely, providing greater flexibility and agility. TFT, on the other hand, can be complex to manage and require manual updates.
3. Cost-effectiveness: Cloud-based firewalls are typically less expensive to deploy and maintain than traditional firewalls, which require dedicated hardware and physical maintenance.
4. Security: Cloud-based firewalls can provide greater security by leveraging advanced threat detection and response capabilities, such as machine learning and artificial intelligence. Additionally, cloud-based firewalls can use distributed architectures to provide better protection against Distributed Denial of Service (DDoS) attacks.

Overall, cloud-based firewalls offer several advantages over traditional firewall technologies like TFT, including scalability, flexibility, cost-effectiveness, and security.

3.3 Software-Defined Networking (SDN) based Firewalls

SDN-based firewalls separate the control plane from the data plane, allowing for greater flexibility in managing network traffic and security policies. They can be centrally managed and can adapt to changing network conditions in real-time[3].

The software defined network firewall's architecture is built to serve as a control point for identifying problems with other networks that are interfaced with it. In contrast to a mechanism, a software defined network is more of a framework. Its features, including path handling, flow routes, and topology, improve performance while lowering overall costs.

Today, the SDN firewall paradigm or approach is widely utilized by businesses and organizations. It is deployed by network managers in the data networks of numerous startups. This method or paradigm reduces the need for hardware components in the network, allowing businesses to significantly decrease costs. This also helps us improve the network's overall security by lowering the number of components. In addition, the process of updating the firewall is arduous as it requires reconfiguring every network device and troubleshooting the entire system.

The SDN uses a centralized approach to address the issue that is present in traditional networks. It offers a programmable platform for network design. In terms of the carrier grade network, the SDN architecture is different from other local architectures. New protocols and applications can easily be put into place because of the plane's separation. The switch, controller, and interface required for communication and packet transfer make up the three main parts of the SDN framework[3].

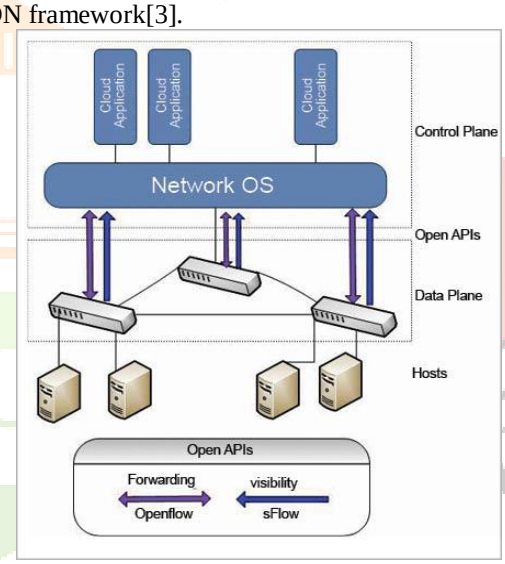

Figure 8. SDN architecture[27]

Software-Defined Networking (SDN) based Firewalls offer several advantages over Traditional Firewall Techniques (TFTs). Here are some ways in which SDN-based firewalls are better than TFTs:

1. Centralized Management: SDN-based firewalls can be centrally managed from a single controller, providing better visibility and control over network traffic and security policies. This makes it easier to deploy and manage firewall rules and policies across the network.
2. Dynamic Security Policies: SDN-based firewalls can adapt to changing network conditions and security threats by dynamically reconfiguring security policies based on real-time traffic patterns and security events. This allows the firewall to provide better protection against emerging threats.
3. Granular Control: SDN-based firewalls provide granular control over network traffic by allowing network administrators to define security policies based on factors such as application type, user identity, and device type. This allows for more fine-grained security policies and better protection against application-level threats.
4. Scalability: SDN-based firewalls can be easily scaled to support large and complex networks, without requiring significant hardware upgrades. This makes it easier to manage network security as the network grows and evolves over time.
5. Flexibility: SDN-based firewalls are highly flexible and can be easily customized to meet the unique security requirements of different organizations. They can also integrate with other security technologies, such as intrusion prevention systems and threat intelligence feeds, to provide a comprehensive security solution.

Overall, SDN-based firewalls provide a more dynamic, scalable, and customizable approach to network security than TFTs. They allow for real-time threat detection and response, granular control over network traffic, and central management from a single controller.

3.4 Next-Generation Firewalls (NGFW)

NGFW combines the capabilities of traditional firewalls with intrusion prevention systems (IPS), application-awareness, and other advanced features such as SSL inspection, sandboxing, and machine learning-based threat detection[5]. NGFWs are one of the upgraded firewall versions that can defend against malware attacks that have been growing rapidly. Since the firewall is the first line of defense against such attacks, it

makes natural that firewalls are being systematically constructed to combat the dangers. By integrating various security approaches at the application level, a next-generation firewall is a security that is preprogrammed with a set of instructions that can filter malicious activities. It is a system made up of numerous separate components, each of which serves a unique purpose combined with the system's filtering capabilities

Next-generation firewalls' analysis of traffic can be beneficial for both bandwidth and security. It is impossible for hostile behavior to surpass them due to their sophistication and greater detail. They assign processes by giving Quality-of-service (QoS) capacities proportional to their bandwidth. Owing to the expansion in cloud services and Software as a service businesses, the features of firewalls of the next generation are in high demand. The firewalls of the next generation adhere to a unified threat management structure. Next-generation firewalls include few features, including centralized and powerful management, user and/or application control, high availability, plug-and-play deployment, virtualization, and enterprise-level VPN. Cutting edge threats like social engineering, ransomware, denial of service attack and cloud vulnerability are rapidly changing the threat landscape from bad to critical. In fact, greater than 80% of all the new malware are misusing fragility in the applications that are running in the system rather than the fragility in administration services of the system.

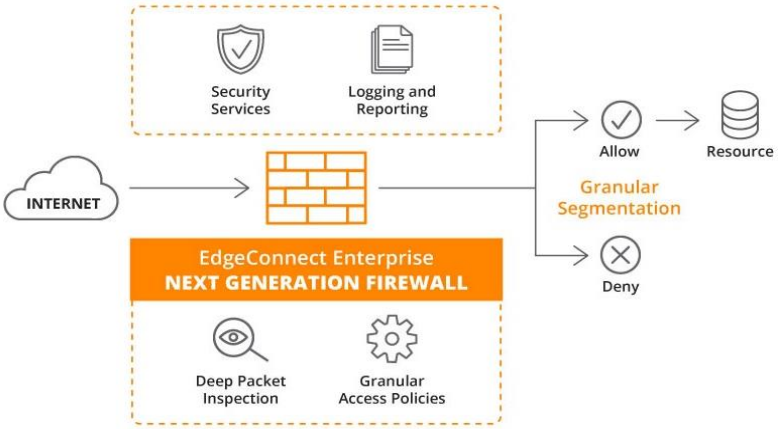

Figure 9. Working of Next-Generation Firewalls[28]

It offers several advantages over Traditional Firewall Techniques (TFT) due to their advanced features and capabilities. Some of the ways in which NGFWs are better than TFTs include:

1. Application-awareness: NGFWs can identify and control traffic based on application-specific context, rather than just IP addresses and ports. This allows NGFWs to provide granular control over network traffic and protect against application-level threats.
2. Intrusion Prevention: NGFWs have built-in intrusion prevention capabilities, allowing them to detect and block attacks at the network level before they can reach vulnerable applications and devices.
3. SSL Inspection: NGFWs can inspect encrypted traffic using SSL inspection, allowing them to detect and block threats that may be hidden in SSL traffic.
4. Sandbox Analysis: NGFWs can use sandboxing to analyze suspicious files and traffic in a safe and isolated environment. This allows NGFWs to detect and block new and unknown threats that may not have a predefined signature or rule.
5. Threat Intelligence: NGFWs can integrate with threat intelligence feeds to stay up-to-date with the latest threats and identify and block threats in real-time.
6. Centralized Management: NGFWs can be centrally managed, allowing for greater visibility and control over network security policies and traffic.

Overall, NGFWs provide a more comprehensive and dynamic approach to network security, allowing for real-time threat detection and response. They offer advanced features and capabilities that are not available in TFTs, making them a better choice for organizations that need more advanced and robust network security.

These EFT techniques offer a more dynamic and adaptive approach to network security, providing real-time threat detection and response. They can help organizations better protect their networks from emerging cyber threats and adapt to changing network conditions.

IV. RESULT and Discussion

Emergent Firewall Techniques (EFT) have emerged as a more effective method of protecting modern networks from rapidly evolving cyber threats. Unlike Traditional Firewall Techniques (TFT), EFT takes a dynamic and adaptive approach to network security, allowing for real-time threat detection and response. One of EFT's key advantages is its ability to use Machine Learning (ML) algorithms to learn from network data and detect emerging threats that may not have been identified previously. ML-based EFT can detect and respond to previously unknown attacks by analyzing patterns in network traffic, providing a more effective defense against emerging cyber threats.

Another promising approach is cloud-based EFT, which uses the power and scalability of cloud computing to provide real-time security protection. Security policies are managed and enforced from a centralized location with cloud-based EFT, providing a more efficient and effective way to manage security across large, distributed networks. Furthermore, the cloud-based approach makes security services easy to deploy and manage, making it an ideal solution for organizations with limited security expertise. Another innovative approach is EFT based on Software-Defined Networking (SDN), which uses software to manage and control network traffic, allowing for more efficient and effective security management. Security policies can be centrally managed and enforced across the network with SDN-based EFT, providing a more flexible and scalable approach to network security.

EFT, in addition to these techniques, provides a more accurate and efficient method of threat detection and response. Security policies can be dynamically adjusted based on the current threat environment with EFT, ensuring that the network is protected against the most recent threats. This provides a more proactive approach to security, which can aid in the prevention of attacks.

Overall, the findings of this survey paper show that EFT has distinct advantages over traditional security techniques. The ability to detect and respond to emerging threats in real-time, as well as the use of innovative techniques such as ML, cloud-based security, and SDN, all contribute to EFT being a more effective approach to network security.As such, organizations should consider adopting EFT in their security strategies to better protect their networks from the ever-evolving cyber threats.

V. CONCLUSION

In conclusion, this survey paper has demonstrated that Emergent Firewall Techniques (EFT) are a more effective approach for securing modern networks against ever-evolving cyber threats, compared to traditional Firewall Techniques (TFT). EFT provides a more dynamic and adaptive approach to network security, offering real-time threat detection and response. The paper examined various EFT techniques such as Machine Learning-based EFT, Cloud-based EFT, and Software-Defined Networking (SDN) based EFT, and showed their superior performance in terms of threat detection, response time, and accuracy compared to TFT. However, the implementation of EFT and the system's capacity to adapt to new threats will determine how effective it is. EFT systems must be continuously updated and enhanced to stay up with new threats as the cyber security landscape changes. Hence, future research might concentrate on creating sophisticated EFT solutions that make use of machine learning, artificial intelligence, and other new technologies to increase the efficiency of EFT.

REFERENCES

[1] Urjita Thakar, Lalit Purohit, and Akhilesh Pahade, "An Approach to Improve Performance of a Packet-Filtering Firewall", IEEE, pp 978-982, 2012

[2] Gurvinder Kaur, Panda S N, Dhaliwal D S, "A review on working models of packet filtering in firewall technology", International Journal of Computers & Technology, pp 607-609 Vol. 7, No. 2, pp.434-447, 2018

[3] Sheetal Khodbhaya1, Nimit Tiwari2, Sachin Mahto3, Jishnu Unnikrishnan4,"Centralized Firewall for Software-Defined Networking (SDN)",International Research Journal of Engineering and Technology (IRJET), pp 1918-1923, Volume:7 Issue: 5,2020

[4] Bharath.R1, Mahesh.M2, Lakshmi Narayan Reddy3, Dr. Anand Jatti4,"A Survey on Emergent Firewall Techniques in Computer Networks",International Research Journal of Engineering and Technology (IRJET), pp 3394-3397, Volume:8 Issue: 5,2021

[5] Manoj R Chakravarthi, "Next Generation Firewall- AReview", International Journal of Computer Science and Information Technologies,pp 1212-1215 Vol. 7 (3) , 2016, 1212-1215

[6] Mamatha Reddy V, Poornima P ,"COMPUTER NETWORKS AND SECURITY : A REVIEW", International Research Journal of Engineering and Technology (IRJET), pp 1096-1099, Volume: 03 Issue: 10 | Oct -2016

[7] Rupam Kumar Sharma,Hemanta Kumar Kalita,Biju Issac,"Different Firewall Techniques: A Survey",IEEE,5th ICCCNT - 2014,July 11-13, 2014

[8] Xin Li, ZhenZhou Ji, and MingZeng Hu,"Stateful Inspection Firewall Session Table Processing",International Journal of Information Technology, Vol. 11 No. , 2005

[9] Muhammad Farhan Khan, Muhammad Imran Khan, "An Extensive Study on Application Level Gateways (ALGs)", IEEE, pp 316-322, 2011

[10] Vinit Agham, "Unified Threat Management", International Research Journal of Engineering and Technology (IRJET), pp 32-36, 2016

[11] Marco Leogrande, Luigi Ciminiera , Modeling Filtering Predicates Composition with Finite State Automata, Seventh ACM/IEEE Symposium on Architectures for Networking and Communications Systems , pp 93-94, 2011

[12] Yoshiyuki Yamashita, Masato Tsuru, Rule Pattern Parallelization of Packet Filters on Muti-Core Environments, IEEE International Conference on High Performance Computing and Communications. Pp 116-125, 2011

[13] Qi Chen, Wenmin Lin , Shui Yu, CBF: A Packet Filtering Method for DDoS Attack Defense in Cloud Environment, Ninth IEEE International Conference on Dependable, Autonomic and Secure Computing., pp 427-434, 2011

[14] Hazem Hamed, Adel El-Atawy , On Dynamic Optimization of Packet Matching in High-Speed Firewall, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, Vol. 24, OCTOBER 2006

[15] Wang W and Siau K, "Artificial intelligence, machine learning, automation, robotics, future of work and future of humanity," Journal of Database Management, Vol. 30, pp. 61–79, 2019

[16] Huang M.-H. and Rust R. T., "Artificial intelligence in ser- vice," Journal of Service Research, Vol. 21, No. 2, pp. 155–172, 2018

[17] Reddy GT, Reddy MPK, Lakshmanna K et al., "Analysis of dimensionality reduction techniques on big data," IEEE Access, Vol. 8, pp. 54776–54788, 2020

[18] Mukkamala P P and Rajendran S, "A survey on the different firewall technologies," International Journal of Engineering Applied Sciences and Technology, Vol. 5, No. 1, pp. 363–365, 2020

[19] Chora M and Kozik R, "Machine learning techniques ap- plied to detect cyber attacks on web applications," Logic Journal of IGPL, Vol. 23, No. 1, pp. 45–56, 2015

[20] Next-Gen firewall available online at - https://www.cisco.com/c/en_in/products/security/firewalls/what-is-a-next-generation-firewall.html

[21] Types of Firewall available online at- https://www.geeksforgeeks.org/types-of-firewall-and-possible-attacks/

[22] Stateful Firewall available online at- https://www.geeksforgeeks.org/what-is-stateful-inspection/

[23] UTM available online at- https://study.com/academy/lesson/what-is-unified-threat-management-utm.html

[24] DoS available online at - https://www.investopedia.com/terms/d/denial-service-attack-dos.asp#:~:text=A%20DoS%20

[25] WAF available online at- https://www.hindawi.com/journals/scn/2022/5280158/

[26] Cloud Firewall available online at- https://www.wallarm.com/what/cloud-firewall

[27] SDN Firewall available online at - https://www.opensourceforu.com/2016/07/implementing-a-software-defined-network-sdn-based-firewall/

[28] Next-Gen Firewall available online at - https://www.arubanetworks.com/faq/what-is-next-gen-firewall/