IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, March 2024

Next Generation Firewall (NGFW) and Datacenter Operations

Praveen Kumar Gopalakrishnan
ALSAC, Memphis, Tennessee, US

Abstract: *Network security, in the contemporary world, is a necessity due to the magnificent growth of the word wide web and the increasing dependence of the masses on the internet for majority of their day-to-day transactions. It ensures that both the integrity and usability of the data remains protected. The Next Generation Firewall (NGFW) becomes important to ensure this requirement of remaining secured is met in a rapidly changing technological environment where cybercrimes are developing by leaps and bounds and traditional means of protection fall grossly inadequate. This article delves into the area of data center operations and highlights the way NGFW had become an integral part of data security and an absolute necessity to ensure safe and sound operations.*

Keywords: Firewall, internet, security, datacenter, data protection, NGFW.

I. INTRODUCTION

The modern world functions much differently from the years when the world wide web (www) or the internet first came into operations. The internet is now a part of the everyday life of an individual and an indispensable part of the daily operations of any commercial establishment, especially where the markets have grown beyond the boundaries of the country and the business operations have spread internationally. This has also led to the generation of immense volume of online data which nowadays are stored and managed safely and professionally using data centers which are the very essence of modern-day global connectivity for both businesses and individuals[1]. With the development and progress of information and communication technology, the traditional tools for protecting data and their users have become obsolete and hence useless creating the need for development of new generation of data protection means and tools. Hence appeared the NGFW. The article discusses and establishes the need and importance of NGFW.

II. LITERATURE REVIEW

This piece of literature reviews contemporary literary and research works pertaining to firewalls, with a closer look at the practices and tools and technologies that have been proposed by specialists who are leaders in this domain. Around 30 references from a wide variety of sources created by experts and published by such reputed publishers provides the basis for this comparative analysis. The references shortlisted offer valuable insight into algorithms, firewall architectures, and various metrices used to measure performance which in turn provides the platform for an exhaustive exploratory research study. The systematic approach is devised to bring out the pros and cons of various practices, in comparison to other firewall methods employed is provided in the literature review.

Development of ICT & Data Centers

There has been rapid and exponential growth in the demand for digital services. 2010 onwards, there has been doubling of the number of uses of the internet across the globe and at the same time, the worldwide internet traffic has seen 25 times expansion[2]. This created a huge demand for data centers as faster connectivity and a growing number of computers led to a generation of a huge volume of data and a large number of businesses also made their appearance in the area data center operations for public clients[3].

The technological hub for the operations of a modern enterprise is its data center, which offers the crucial technical and IT infrastructure that is necessary for delivering the resources and services to employees of the establishment, its partners, and its clients across the globe[4].A data center is designed as to aid businesses stores, facilitate distribution, and interpretation of data by making use of an assortment of tools, both hardware and software, that assist IT

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, March 2024

departments in the management of data and maintenance of the IT infrastructure[5].It is possible for a medium or small business enterprise to frequently implement a helpful and convenient data center within the boundaries of a closet or any other appropriate room with few alterations and adjustments, that may be necessary [4] . The future of data center technology appears to be dynamical, fast-changing and transformative, on the back of progresses and developments taking place in both hardware and software technologies, ever-changing business needs, and environmental apprehensions [6] .

Figure 1: International Data Center Market

As stated by the P&S Intelligence report, the international data center market size, that stood at $263.34 bnin 2022 is anticipated to exceed $602 bn by 2030, expanding at a compounded annual growth rate (CAGR) of 10.9%[7].

Digitization, Growth of Data Centers & Need for Data Security

Our daily business activities, including financial transactions, have expanded massively by an extent that is unprecedented and this has increased our dependence on data, data churning and data crunching in the present-day digital age. Life has become increasingly data-driven and as a result the data centers of the present day have become economic hubs in today's world that is highly digitally connected[8].

A data center offers a common infrastructure that can be used by corporates to host data and applications and includes components for networking, computation, and storage. Industry standards pertaining to design, construction and maintenance of these facilities exist in order to make sure that the data and applications hosted within a data center remain secure and are easily available and accessible as and when required by these corporates[9]. In addition to data storage, data centers also support the platforms and apps which are being constantly upgraded and host the latest versions of these apps on their servers.

Along with storage of important relevant information, data centers also support the contemporary apps and platforms that are being constantly technologically upgraded and host the latest versions of these apps on their servers. This has led to multiple corporate and government agencies becoming heavily dependent on data centers for the safe storage of assets (sensitive data) that are crucial because of their proprietary nature and are vital for the commercial operations of the organization, in a protected and centralized digital atmosphere[8]. With the growing digitalization of major commercial and operational activities across the world, data centers and data transmission networks are fast becoming important source of power for most organizations and business entities[2].

Many multi-national companies and even government organizations continue to remain fully reliant on these data centers for securely storing and even process their data in the current stage. These data centers have been entrusted with the safe storage of significant operational and proprietary data centrally in the digital environment. The pandemic was the key reason behind the exaltation of digital operation. It has resulted in a slingshot effect with regards to digital operations, with both work and study turning online allowing people to carryout their activities from remote locations

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, March 2024

resulting in an increase in data getting generated. This coupled with the improvement in internet access resulted in the increase in demand for large data[8].

Artificial intelligence (AI) and machine learning (ML) which are very recent technologies have taken charge and spearheaded us into a data-centric world. This rapid increase in volume and the abundance of data has spurred significant improvements and progression in several areas including finance and healthcare, transportation, communication and entertainment, redefining the ways in which modern man leads his daily lives, the way he carries out work and connects with this world[6].

This has led the data center market onto a growth trajectory, registering a distinctive growth in recent times, and this robust growth momentum is set to continue in the near future. Data centers continued to proliferated on a global scale inspite of economic hurdles, geopolitical instability and supply chain disruptions in various markets across the globe and across industries[10].At present over 7.2 million data centers operate all over the world as we continue to generate more than 2.5 million terabytes of data on a daily basis. This is supported and sustained by the advent of 5G, IoT and Industry 4.0 and it can, therefore, be forecasted that demand for data centers will grow astronomically over the next 5 years[8].

Use of Firewall for Data & Data Center Security

A firewall refers to the system of hardware that constantly keeps track of network traffic, both incoming and outgoing, and decides whether certain individual traffic should be allowed to come in or go out or blocked altogether. A set of clearly laid out security rules guides the screening of and the decision regarding the network traffic. This entire exercise is mainly designed to discourage attacks and firewalls scrutinize incoming traffic following some pre-programmed rules and thus filter traffic from both known and suspected malicious or unsecured sources. The traffic is protected by Firewalls at a computer's ports which are basically the points where the computer interfaces with external computers and data sharing occurs. A firewall could be a software or a hardware or a combination of both[11].

If not for the majority, for a large many number of enterprises, irrespective of the growth of cloud-based resources and an increase in the distributed workforce, the data center continues to play a crucial to many, if not most, enterprises. Containing applications that are critical for the organization's mission and for other indispensable equities of the business, the data center has undergone significant development to evolve as a better destination for secure data storage for future storage and retrieval. However, despite their frequent geographical dispersion, these data centers have continued to remain equally vulnerable. Facing the forever-increasing threats, IT departments across companies and sectors understand that whatever be the geographical location, safeguarding the data center from malevolent threats and unlicensed access remains imperative for commercial establishments[12].

Traditional Firewalls

Conventional firewalls or legacy firewalls predominantly control network traffic flow between an untrusted or public network and a trusted network. At present, the most widely employed firewall appliances are port-based or certain variations thereof[13]. According to researchers, the legacy firewalls are widely used because of their ease of operations and their maintenance being cost effective along with the fact that they do not clutter up network traffic nor cause the network traffic to slow down as a result of firewall application. Also, the existing design has been in use for over a couple of decades and have historically provided the desired outcome. The traditional firewall devices are relying on port-based filtering. Therefore, they inherently come with knowledge of Transfer Control Protocol (TCP)/ UDP built into their systems As the given devices are dependent on port-based filtering, understanding of TCP/UDP is mandatory [14].

Conventional firewalls operate using either stateless or stateful method for tracking flowing network traffic. Stateless monitored traffic firewalls just check each packet individually and is not able to determine or recognize a traffic flow. For traffic that is Statefully monitored, the firewalls keeps track of where the flow is within its lifetime (Wilkins, 2014.)

Growing Cyber Crime

Information and communication technologies have become such inseparable part of the life of modern man that not only our society but also economy and crucial infrastructures have turnedhugely dependent on computer networks

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, March 2024

along with the solutions provided by information technology. Cyber attacks have become more rampant and more attractive with elevated level of threat and much higher damage potential as with the continuous growth in our dependence on information technology. As a consequence of the aggressive expansion and proliferation of the internet connectivity, there has been a significant growth in the incidents of cyber-attack, several of which have frequently had devastating and serious consequences. With the evolution of technology trends in cybersecurity have also evolved and incidents such as data breaches, ransomware attacks, and hacks have also turned increasingly common[15].Cybercriminals exploit the vulnerabilities in data center infrastructure that are used by the applications hosted by the data centers while remote desktop protocol (RDP) and virtual private networks (VPNs) that came to be used widely during the lockdowns during the COVID-19 pandemic provided new avenues to them for launching attacks. The new access points used during the COVID era helped these criminals exploit compromised credentials and unpatched vulnerabilities for gaining access to corporate systems where they could plant malware[9].

The principal weapon of choice for carrying out malicious intentions in the cyberspace is Malware, that is launched either through the exploitation of existing vulnerabilities or by using the unique features of developing technologies[13]. The advent of the technology called Internet of Things (IoT) has given rise to immense possibilities. However, in unison, it has thrown open several novel vulnerabilities creating routes that could be used for launching attacks that have the potential of compromising the availability, integrity, and confidentiality of associated systems[16].Since 2001, the number of victims falling prey to online crime has gone up by 16 times (to 91 victims per hour in 2023 from 6) along with a whopping 570+ times growth in financial losses, to nearly $1.2 million losses per hour from $2,000. Overall, cybercrimes have claimed victims in excess of 7,303,267 along with $36.4 billion losses during the last 22-year period that is being discussed[17].In 2023, the number of data compromises in the United States stood at 3,205 cases. Meanwhile, over 353 million individuals were affected in the same year by data compromises, including data breaches, leakage, and exposure. While these are three different events, they have one thing in common. As a result of all three incidents, the sensitive data is accessed by an unauthorized threat actor[18].

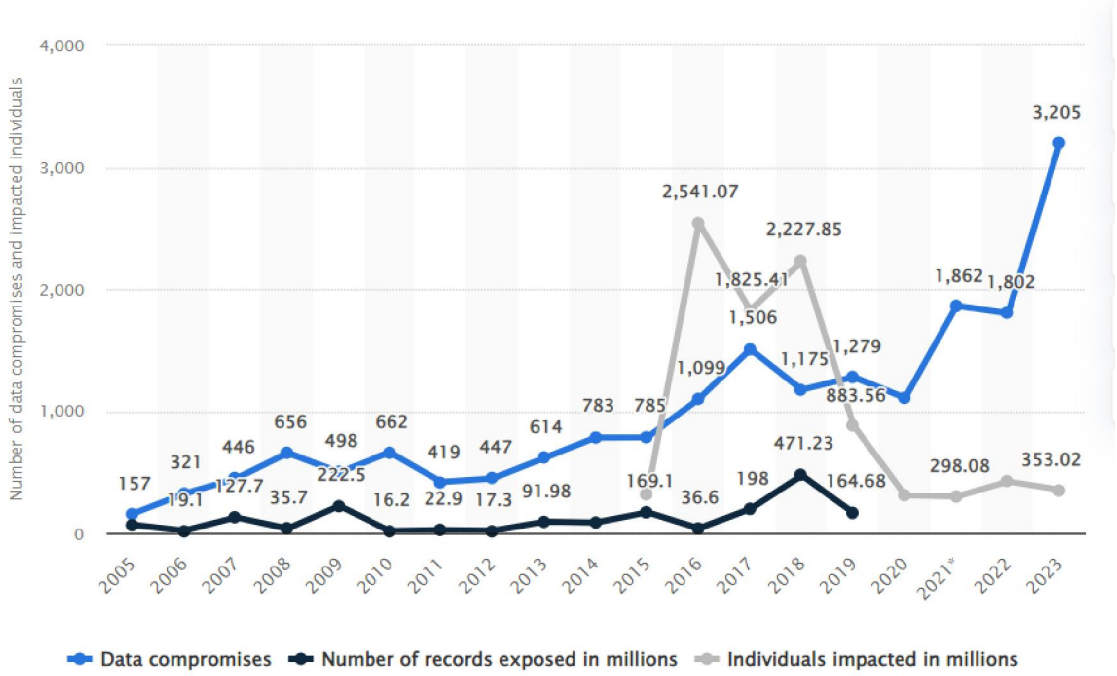

Figure 2: Cyber Crime[18].

Inadequacy of Conventional Firewall

Fraudsters have become more sophisticated[19]. Cyber security being a continuously expanding field, day-in day-out new threats can appear in a company or organization's operations[20]. Data centers store and manage the sensitive data

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, March 2024

in an organization's possession, making their security a core part of a corporate data security strategy. Data centers need to be secured on the basisofazero-trust security model, which regulates and restrains access and permissions to the minimum required by business needs.[9].

By and large perimeter firewall had been the whole basis for data center security which was designed to provide protection to the in-house assets from malefic external players hiding amidst inward and outward traffic. But the proliferation of distributed networks and new-age applications, has made the network perimeter more and more leaky and hence vulnerable, making it imperative for the data centers to deploy highly developed and better disseminated firewalls that will be able to deliver detailed and more rigorous monitoring of data traffic in both direction thus ensuring better protection of internal data and assets[12].

Due to the dynamic nature of cybercrime, constant creation of novel technologies is necessary for combating hazards[16]. Despite the fact that the legacy software and hardware had once remained the columns on which digital innovation stood, have now turned into vulnerabilities in cyber security. though still in use, these legacy systems have now literally become latent "digital time bombs" that are ticking and it is just a matter of time before they explode and expose the data centers to the forever increasing risks of cyber security that need to be effectively addressed by businesses and individuals[21].

Even after passage of over 3 decades since the concept of network firewall made its debut in the cyber security arena, the technology continues to be an essential instrument in the network security arsenal of data centers and enterprises. The firewall provides the essential mechanism for filtering out malicious traffic before it can cross the network perimeter. Firewall has a proven track record over last couple of decades or so. As is the case with any indispensable technology, especially the ones that are being used daily for as extended time period, advancements and improvements have aided the progression of not only the capabilities of firewall but also the options for its deployment [22].

With the progression of technology older systems become outdated as the technological support for them starts diminishing. For developers and manufacturers newer systems always become their priority, which gradually reduces the availability of patches and updates for legacy systems, that are then phased away. The absence of constant updates also results in growing vulnerabilities in older software and hardware which become increasingly unaddressed, which makes the traditional firewalls become the easy and hence prime targets for cyber attacks that never stop becoming more advanced. This is the key reason why legacy systems are the more chosen route for hackers to attack and then easily reach cloud-based systems and data. Due to the outdated nature of legacy systems, breaking into is a much easier technique to gain access to old systems and hence data stored within public clouds[21].

Quite frequently current cyber security tools find it difficult to integrate with erstwhile security systems. The functionalities necessary for accommodation of advanced security measures might be lacking in the legacy systems which can create a gap in the defence framework along with the limited capacity to improve performance through the handing of growing volume of incoming and outgoing data that is the obvious outcome of a growing business[21]. Firewalls need to have the ability to accommodate the present need of an organization as also its potential future requirements that are bound to crop up as the organization grows. The firewall should be so designed as to allow easy scalability – both upwards and downwards, as per the organizational needs without causing any major disruption or overhaul to the existing operations or to its IT security stacks[23]. However, conventional firewalls are inadequate in this aspect due to limited scalability. More advanced and sophisticated methods are used by the next-generation firewalls for prevention of the network system from external malware attacks. It is a modified version of the traditional firewall and does a better job of bug prevention in network systems[24].

Discussion

On a daily basis, the modern man creates data in excessof350 million terabytes, which is inclusive of data generated freshly, copied data, consumed data and reprocessed data. With the rapid increase in popularity of the Internet of Things (IoT), this rate of generation of data will continue to see upward journey[6].A data center firewall being a software or a hardware device that is capable of monitoring the traffic entering and exiting the network of an organization [12] have a major role to play in the seamless operation of data centers. They not only provide protection against data theft but also ensure that the data is not contaminated. In a world where business and commerce has become heavily dependent on the usage of digital devices and a massive amount of transaction occurs online, companies shed significant amount on maintaining clean and relevant data – be it pertaining to internal operations, be it

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, March 2024

pertaining to providing superior customer service. This service is provided by datacenters which makes it imperative for them to run their operations smoothly and efficiently to ensure relevant data can be accessed by their users as and when required without facing much trouble. It also becomes imperative for them to ensured these volumed of sensitive data they store are not accessed by unauthorized persons.

Need for New Age Data Security

The COVID-19 pandemic brought about some unwanted developments to the realm of data security creating greater exposure of the data to malefic entities because of the new modalities of working. Given the worldwide increase in work from home or remote work option during the COVID years and reparameterization as a reason of cloud deployment of next generation firewalls or NGFW, the construct of a next generation firewall has come under a lot of pressure. Shapingand outlining the fence between good and evil has become increasingly more difficult. Provision of the best-in-class endpoint security with the least number of false positives or negatives often makes it necessary for the enterprises and data centers to identify the communicating endpoint application[25]. As number of businesses that are moving to cloud-based computing is now growing significantly, selection of data centers, locatedremotely, for the management of IT systems and servers, storage of data and also data backup are proving to be beneficial in terms of actual cost saving and relief from the perils of vulnerabilitiesthat are the resultof creation and operation of their own in-house network infrastructure.

On a worldwide basis, the largest of the data centers remain equipped with and use improved, modern and advanced features and act as the pioneers as we move to the next generation of data centers [26].Very frequently, new-age gateway firewalls will have the intrusion detection (IDS/IPS) feature when it comes to the context of application, and the analysis of advanced threat which helps to assessrisks associated with the content of traffic that is passing through. To sum up, distributed firewalls are so designed as to filter the east-west data traffic (traffic among devices within a specific data center) Sand provide all-round data protection down to the workload level[12].

Emergence of NGFW

A decade ago, Gartner had introduced the idea of NGFW [27]. A key component of the third generation of firewall technology which has evolved to be a very important part of this novel age that is crowded with a huge number of digital advancements is the next-generation firewall. TheNex t-Generation Firewall (NGFW) presents a fruitful combination of a traditional firewall with the objective to filter a large number of functions through IPS (intrusion prevention system) and DPI (deep packet inspection)[24]. The next-generation firewall is a portion of the 3rd generation of firewall technology, which puts together the old-style firewall and other network appliance filtering functions (NAFF) for instance, as already mentioned, a combination of inline intrusion prevention system (IPS) as well as in a deep packet inspection (DPI) [28]. As the discussion indicates, next-generation firewall is DPI firewalls moving beyond the constriction of port and protocol inspection (PI) and also factors in blocking for adding application-level inspection (ALI), intrusion prevention, in addition to acquiring outside firewall intelligence [27]. Conventional firewalls are capable of working and are effective at Layer 3 and Layer 4, and they permit or block traffic on the basis of their port and protocol, with a leverage stateful inspection, and their decisions were madeon the basis oflaid out policies [28]. As ICT developed with time it is no longer makes sense or is safe and secure to carry out data center security policies in such manner that offer extremely limited flexibilityand is not transparent[29].

Use of NGFW in Datacenter Operations

Cybersecurity of data centers is a significant cause of concern in the digital era and calls for innovative approaches that canprovide protectionto sensitive information and systems. There are certain next-generation firewalls (NGFWs) that integrate artificial intelligence (AI) technologies for providing efficient data security. The traditional firewalls have proven to be inadequate in addressing innovative cyber threats.Theincorporation of AI presents a promising option for superior threat detection and mitigation of those risks[30].

Also, NGFWs are frequently able to execute user-based and group IDs based security policies. Additionally, they can control traffic according to their transport and application layer properties. NGFW provide basic features, including routing and NATting of traffic[25].A key benefitof next-generation firewall is malware blockage, protecting a network

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, March 2024

by blocking malware's entry into the network and defense against external attack. These firewalls are much better equipped to recognize Advanced Persistent Threats or the APTs. NGFWs will most likely have a path that facilitated storage of future updates for an organization, an extremely beneficial updated feature newly added to the NGFW. Next-generation firewalls prove monetarily advantageous for companies that looking for reasonably good but economical security systems having low maintenance withleast human intervention. Network protection demands significant attention and must include malware blockages and anti-virus among other things. The next-generation firewall provides a tool that integrates these essential features and uses them suitably and conveniently. NGFW firewalls seldom fail at protecting the networks for the organizations as they involve identification or detection, awareness, inspection services, as also malware protection[24].NGFWs provideadministrators with deeper awareness of and control over individual applications together with deeper inspection capabilities.

III. CONCLUSION

Data is all around, with users who access it from around the world and from all types of devices. At the same moment, Information Technology (IT) teams are implementing analytics, cloud, as well as automation to quicken the delivery of innovative applications and drive business development. Massive expansion of online activities catapulted by the recent global pandemic and buoyed by exponential growth in internet connectivity has resulted in creation of mammoth data volume which need tobe stored and managed professionally, hence the need for efficient data centers that would also prove to be the safe harbor for sensitive information related to businesses and individuals.

A data center provides secure facilities where crucial data-driven and IT server equipment can be housed. The units can be vast with storage space available to rent or single-purpose units having only a single key occupant. But the thereat of data theft and cyber attacks had always been real and significant and at present growing not only in terms of numbers but also in terms of sophistication. This makes it absolutely essential for companies and data centers to use state-of-the-art protection technology as legacy systems prove grossly inadequate in a technologically dynamic environment.

NGFW is an important tool that equips organizations with such features as intrusion prevention, application control, and advanced visibility of their network. Therefore, the key function of a NGFW firewall is providing protection to these organizations through superior and safe data center operations. Besides protecting the devices from a wider spectrum of intrusions the toolis also available relatively inexpensive. Along with helping the networks with breach prevention, advanced protection,NGFW also provides huge comprehensive network visibility coupled with several flexible management and deployment options.

REFERENCES

[1] Faist, "Why are data centres so important?," 08 Nov 2023. [Online]. Available: https://www.faistgroup.com/news/data-centres/. [Accessed 15 Feb 2024].

[2] IEA, "Data Centres and Data Transmission Networks," 11 Jul 2023. [Online]. Available: https://www.iea.org/energy-system/buildings/data-centres-and-data-transmission-networks. [Accessed 15 Feb 2024].

[3] Express Computer, "The Evolution of Data Centers: From On-Premises to Cloud and Edge Computing," 04 Oct 2023. [Online]. Available: https://www.expresscomputer.in/guest-blogs/the-evolution-of-data-centers-from-on-premises-to-cloud-and-edge-computing/104256/#:~:text=The%20internet%20era&text=The%20internet%20emerged%2C%20the%20microprocessors,growing%20numbers%20of%20computer%20users.. [Accessed 15 Feb 2024].

[4] S. J. Bigelow, "How to design and build a data center," 18 May 2022. [Online]. Available: https://www.techtarget.com/searchdatacenter/How-to-design-and-build-a-data-center. [Accessed 15 Feb 2024].

[5] STL Tech, "Data Centers: What, Why and How?," 02 Jun 2022. [Online]. Available: https://stl.tech/blog/data-centers-what-why-and-how/. [Accessed 14 Feb 2024].

[6] V. Kumar, "13 Largest Data Centers In The World In 2024 [By Size]: RankRed," 02 Jan 2024. [Online]. Available: https://www.rankred.com/largest-data-centers-in-the-world/#:~:text=China%20Telecom%20has%20the%20largest,Mainland%20China%20and%20overseas%20markets.. [Accessed 18 Feb 2024].

[7] PS Market Research, "Data Center Market," Prescient & Strategic Intelligence, 2023.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, March 2024

[8] Sreejith G, "The growing importance of data centres in digitally connected world," 07 Sep 2022. [Online]. Available: https://timesofindia.indiatimes.com/blogs/voices/the-growing-importance-of-data-centres-in-digitally-connected-world/. [Accessed 15 Feb 2024].
[9] Check Point, "Data Center Threats and Vulnerabilities," 2023. [Online]. Available: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-data-center/data-center-threats-and-vulnerabilities/. [Accessed 22 Feb 2024].
[10] A. VINAY, "India has 14th highest number of data centres, but still a long way to go: The Hindu Business," 05 Nov 2023. [Online]. Available: https://www.thehindubusinessline.com/data-stories/data-focus/india-has-14th-highest-number-of-data-centres-but-still-a-long-way-to-go/article67484729.ece. [Accessed 19 Feb 2024].
[11] M. K. Kumawat, "Traditional Firewall vs Next Generation Firewall (NGF)," International Journal of Advanced Research in Science, Communication and Technology (IJARSCT), vol. 5, no. 2, pp. 163-167, 2021.
[12] VMware, "What is a data center firewall?," 2024. [Online]. Available: https://www.vmware.com/in/topics/glossary/content/data-center-firewall.html. [Accessed 20 Feb 2024].
[13] J. Jang-Jaccard and S. Nepal, "A survey of emerging threats in cybersecurity," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 973-993, 2014.
[14] K. Kokko, "Next-generation firewall case study: Bachelor's thesis Information Technology," 2017. [Online]. Available: https://www.theseus.fi/bitstream/handle/10024/139127/kokko_kalle.pdf?sequence=1. [Accessed 15 Feb 2024].
[15] Simplilearn, "20 Emerging Cybersecurity Trends to Watch Out in 2024," 07 Feb 2024. [Online]. Available: https://www.simplilearn.com/top-cybersecurity-trends-article. [Accessed 22 Feb 2024].
[16] U. Tariq, I. Ahmed, A. K. Bashir and K. Shaukat, "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," Sensors, vol. 23, no. 8, pp. 1-46, 2023.
[17] Surfshark, "Cybercrime statistics - Surfshark," 2023. [Online]. Available: https://surfshark.com/research/data-breach-impact/statistics#:~:text=Yearly%20growth%20of%20cybercrime%20costs&text=Since%202001%2C%20the%20online%20crime,%241.2%20million%20losses%20per%20hour).. [Accessed 22 Feb 2024].
[18] A. Petrosyan, "Annual number of data compromises and individuals impacted in the United States from 2005 to 2023: Statista," 12 Feb 2024. [Online]. Available: https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/. [Accessed 22 Feb 2024].
[19] FBI, "Internet Crime Report," Federal Bureau of Investigation, 2022.
[20] D. B. Ansari, Atteeq-Ur-Rehman and R. A. Mughal, "Internet of Things (IoT) Protocols: A Brief Exploration of MQTT and CoAP," International Journal of Computer Applications, vol. 179, no. 27, pp. 9-14, 2018.
[21] M. Olney, "How legacy software and hardware is a ticking cyber security risk timebomb: Integrity 360," 23 Aug 2023. [Online]. Available: https://insights.integrity360.com/how-legacy-software-and-hardware-is-a-ticking-cyber-security-risk-timebomb. [Accessed 19 Feb 2024].
[22] A. L. DeCarlo and R. G. Ferrell, "The 5 different types of firewalls explained," 19 Jan 2021. [Online]. Available: https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls. [Accessed 20 Feb 2024].
[23] Rahi, "How to Choose the Best Firewall for your Data Center," 10 May 2023. [Online]. Available: https://rahi.io/articles/how-to-choose-the-best-firewall-for-your-data-center/. [Accessed 22 Feb 2024].
[24] U-next, "Next Generation Firewall: Everything you need to know in 5 Easy Steps," 15 Oct 2020. [Online]. Available: https://u-next.com/blogs/cyber-security/next-generation-firewall/. [Accessed 22 Feb 2024].
[25] J. Heino, A. Hakkala and S. Virtanen, "Study of methods for endpoint aware inspection in a next generation firewall," Cybersecur (Singap), vol. 5, no. 1, p. 25, 03 Sep 2022.
[26] Nxtra, "Key Features of the World's Largest Data Center: Nxtra by Airtel," 02 Aug 2022. [Online]. Available: https://www.nxtra.in/blog/key-features-of-the-worlds-largest-data-center. [Accessed 15 Feb 2024].
[27] A. S. George and A. H. George, "A Brief Study on The Evolution of Next Generation Firewall and Web Application Firewall," IJARCCE, vol. 10, no. 5, pp. 31-37, 2021.
[28] ZSCALER, "What Is a Next-Generation Firewall?," 2024. [Online]. Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-next-generation-firewall. [Accessed 19 Feb 2024].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, March 2024

[29] Cyberdefense, "WAF vs NGFW," 07 Dec 2017. [Online]. Available: https://www.orangecyberdefense.com/be/blog/waf-vs-ngfw. [Accessed 15 Feb 2024].
[30] S. Ahmadi, "Next GenerationAI-BasedFirewalls: A ComparativeStudy," International Journal of Computer (IJC, vol. 49, no. 1, pp. 245-262, 2023.
[31] "A Systematic Literature Review on the Cyber Security," International Journal of Scientific Research and Management (IJSRM), vol. 9, no. 12, pp. 669-710, 2021.
[32] N. J. Palatty, "90+ Cyber Crime Statistics 2024: Cost, Industries & Trends: Astra," 24 Jan 2024. [Online]. Available: https://www.getastra.com/blog/security-audit/cyber-crime-statistics/. [Accessed 22 Feb 2024].