ABSTRACT:

A firewall is a necessary part of any modern network security system. Filtering incoming and outgoing traffic, they serve as a barrier between a secured network and the outside world, thwarting threats and hostile actors.

This report offers a thorough overview of firewalls, including information on their history, significance, goals, reach, and constraints, as well as how they operate, various firewall architectures and types, typical cyberattacks and how firewalls defend against them, best practices for deployment and configuration, their function in network security.

TABLE OF CONTENT

LIST OF FIGURES

1. INTRODUCTION

1.1 Background and Importance of Firewalls:

Network security tools called firewalls keep an eye on and regulate all incoming and outgoing network traffic in accordance with pre-established security regulations. They serve as a line of defence against unwanted access and filter harmful traffic, standing between a secured network and the outside world [1].

The importance of firewalls has grown in the digital age due to the rise in both the volume and complexity of cyberattacks. Firewalls are essential tools for businesses and organizations of all kinds to safeguard their vital information and systems.

History:

Firewalls have a long history, dating back to the late 1980s when the internet was just being started. Because computer networks were becoming more interconnected at the time, there was rising concern about their security [1].

1987	DEC engineers develop the first firewall, a simple packet filter.
1991	AT&T Bell Labs develops the first stateful firewall
1994	The first commercial firewall product, Firewall-1, is released by Checkpoint Software Technologies.
1996	Squid, a popular open-source web caching proxy, is released.
1998	Snort, a popular open-source intrusion detection system (IDS), is released.
2000	The International Organization for Standardization (ISO) publishes the first standard for firewalls (ISO/IEC 13291).
2003	The first cloud-based firewall is launched.
2010	The introduction of next-generation firewalls, or NGFWs. NGFWs incorporate web filtering and intrusion prevention systems (IPS) along with standard firewall functions.

Artificial intelligence (AI) and machine learning are being utilized to create new firewall systems that are more adept at identifying and thwarting sophisticated attacks.

1.2 Objective and Scope:

It is no longer appropriate to think of a school or organization's network as an isolated local area network (LAN). Everyone want access to the Internet and to be online. Attackers looking to compromise the network and obtain its resources are drawn to this accessibility. It is impractical to try to safeguard workstations separately. Using a firewall to separate the local area network (LAN) from the Internet and monitor all network traffic is a preferable approach.

A secure gatekeeper is necessary for the integration of intranets and the Internet in order to defend against attacks on network security. Typically, firewalls keep the network safe from these types of attacks while still enabling communication with the outside world. Therefore, it is incorrect to define a firewall as a device that offers perimeter security. Some internal users still have an Internet connection that gets behind the firewall, despite system administrators' best efforts to force their network traffic to go through it [1].

In order to protect users' privacy and prevent identity theft, a firewall must ensure that only authorized users may access an operating system or a computer linked to a network. This is done by protecting private information. Firewalls typically prevent unapproved access that users of computers are unaware of.

1.3 Advantages of Firewalls:

In order to protect the internal network's security and privacy, firewalls operate as a barrier. By allowing administrators to limit access to particular resources, apps, and services in accordance with pre-established rules, firewalls improve network security as a whole. Firewalls protect sensitive data by preventing malware, hacking attempts, unauthorized access, and other cyber risks from accessing the network [2]. Administrators are able to monitor network activity, identify suspicious activity, and take rapid action in response to security issues because to the comprehensive logs and real-time monitoring that firewalls provide. By providing granular control over certain apps and protocols, advanced firewalls may inspect and filter traffic at the application layer, improving both productivity and security.

1.4 Disadvantages of Firewalls:

Firewalls can affect network speed and cause latency, particularly when processing a lot of traffic or examining deep packet content. Complex firewall rule configuration demands a thorough grasp of network security and protocols, which can be difficult for novice administrators. Firewalls can produce false negatives, which let dangerous content through and create security flaws, or false positives, which stop lawful traffic. Firewalls may not be able to adequately defend against internal dangers like unauthorized access by partners or workers since they are primarily designed to counteract exterior attacks .It is crucial to have redundancy and failover methods in place because if a firewall fails, the security of the entire network could be jeopardized .Firewalls may have difficulties while examining encrypted traffic, which can restrict their capacity to identify security risks in encrypted channels of communication. Acquiring, implementing, and maintaining robust firewall solutions can be costly [2].

2. UNDERSTANDING FIREWALLS:

2.1 Definition and Basic Functionality:

An apparatus used for network security, a firewall keeps an eye on and regulates both inbound and outgoing network traffic in accordance with pre-established security standards. It serves as a firewall, blocking harmful communications and preventing illegal access, between a secured network and the outside world.

Network traffic is examined by firewalls and is then compared to a set of rules. A data packet is permitted to flow over the firewall if it complies with a rule. If not, the packet is either blocked or dropped [4].

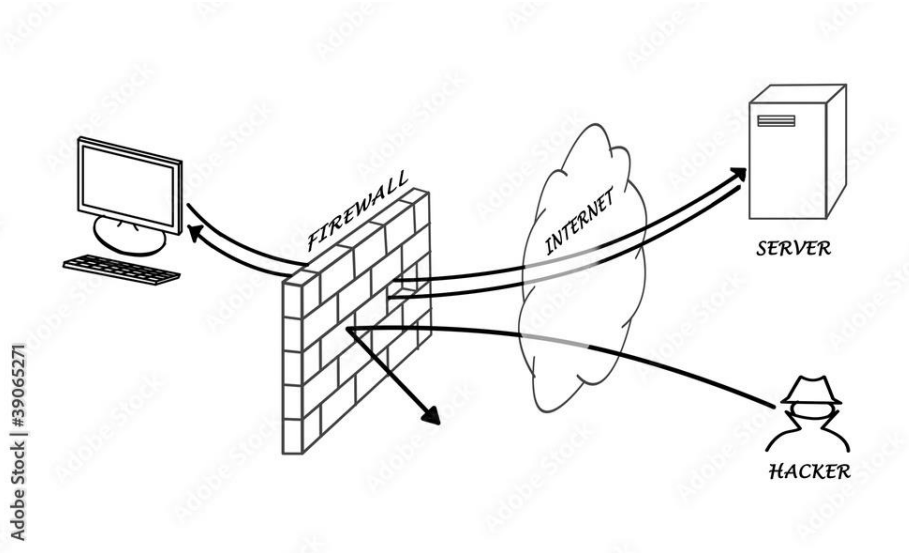

Figure 1 Firewall as Barrier

Firewalls can be deployed in a variety of ways, but they all share the same basic functionality:

Packet filtering: IP address, port number, and protocol are three criteria that firewalls can use to filter network traffic. This enables them to restrict particular kinds of communications, such email and file transfer protocol (FTP).

Stateful inspection: When determining whether to permit or prohibit traffic, stateful firewalls keep track of the status of network connections. They can now fend off attacks like denial-of-service attacks with more effectiveness [4].

Proxying: Firewalls can also serve as proxies for particular kinds of applications. This enables them to more thoroughly examine and filter traffic for particular purposes.

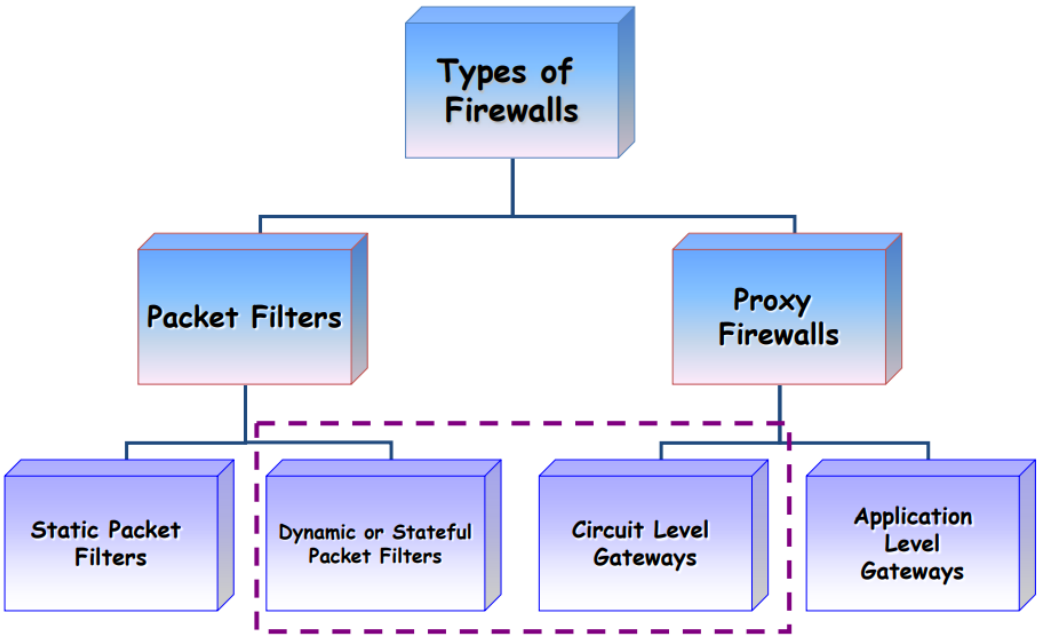

Figure 2 Basic Functionality of Firewalls

Network Address Translation (NAT): To map several private IP addresses to a single public IP address, firewalls frequently employ NAT. As a result, several devices connected to a private network might share an internet connection and appear to the outside world to have a single IP address. Because NAT hides internal network architectures, security is improved.

Virtual Private Networks (VPNs) Support: By enabling VPNs, firewalls can enable safe remote access. They can set up safe online connections via encrypted tunnels for branch offices or distant users to connect to the internal network.

2.2 Types of Firewalls:

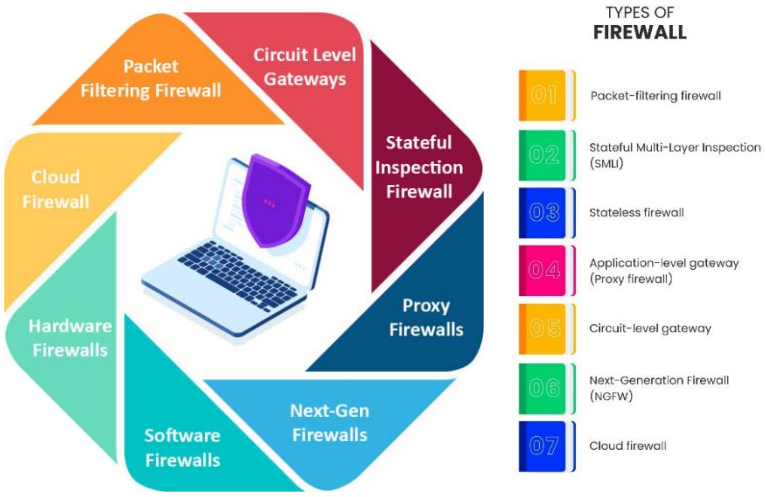

Figure 3 Types of Firewalls [1]

A. Traditional Firewalls:

1) **Packet Filtering Firewall**:

The first firewall was the packet filtering firewall. By keeping an eye on both incoming and departing packets, it filters packets. It filters them using a set of rules based on the protocols, ports, and Internet Protocol (IP) addresses of the packets [8].

The packet filtering firewall can filter packets effectively and is simple to configure due to its fundamental features. Nevertheless, payload, which is situated at the OSI model's application layer, is not checked by the packet filtering firewall. Moreover, it lacks user authentication and is susceptible to IP spoofing. Consequently, this kind of firewall is not very safe against advanced threats.

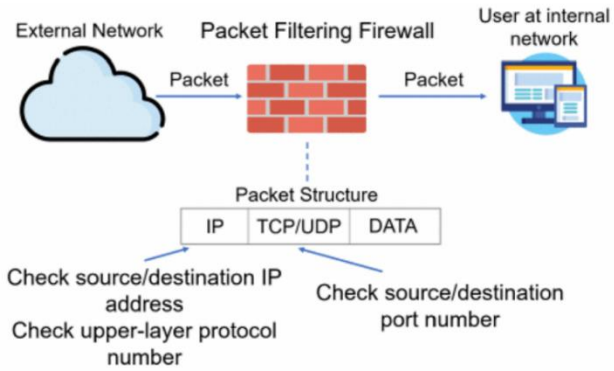

Figure 4: Packet Filtering Firewall [8]

2)**Stateful-Firewall**:

Updated packet filtering firewall is known as stateful-firewall. The three-way handshake procedure in TCP serves as the foundation for its operation. With stateful firewalling, all packets inside the traffic flow in both directions are tracked, as well as established flows. The firewall keeps track of each traffic flow thanks to a cache that it has inside of it in order to accomplish this. Based on the header data of this traffic, including IP addresses and port numbers, a profile is generated for each new connection that enters a syn-packet in a TCP flow. The stateful firewall compares each subsequently attempted connection to this list of records. The packet is permitted to flow across the firewall if the connection is indeed present in the cache. If the connection is not present in the cache, the stateful firewall will use the fundamental packet filtering rules to determine whether the connection qualifies to be listed in the cache [8].

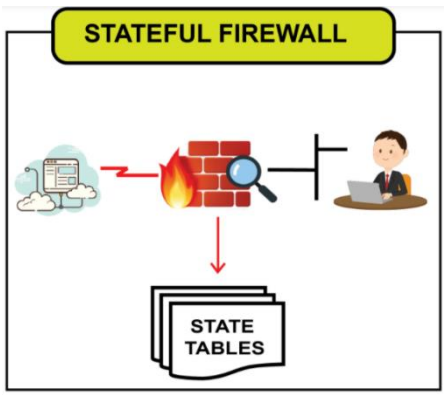

Figure 5 Stateful Firewall [8]

B. Application-Gateway Firewall:

In contrast to the firewalls stated above. Network traffic can be controlled at the application level with an application-gateway firewall. An application-gateway firewall is no longer a "wall" positioned between a traffic source and its destination. It functions more like to a "gateway," one that establishes sessions with distant users via proxies and inspects incoming packets at the application level.

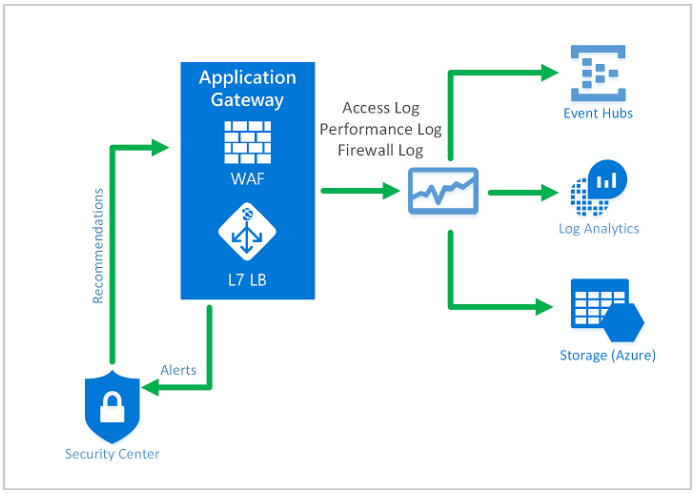

Figure 6: Application Gateway firewall [1]

Every time a client attempts to access a server's network resources, a secure gateway is formed. Every network resource that enters from the server first passes via the gateway before, upon request, being returned to the client.

By preventing the client from directly accessing the server's network resources, this adds an additional degree of security. The gateway will be impacted first and handled if any corrupted network resources exist; the client won't be impacted [8].

This additional security does have a price, though. Specifically, because of the secure gateway between the user and server, traffic between them typically moves more slowly.

C. Circuit-Gateway Firewall:

A circuit-gateway firewall functions as a "gateway" between the client and the server, much like an application-gateway firewall. Circuit-gateway firewalls don't function at OSI model layer 7, or the application layer, in contrast to application-gateway firewalls. Rather, it functions at OSI model layer 5, or the session layer. What does all this signify, though? The circuit-gateway firewall concentrates on the connections between the client and server rather than the network resources of the server. In addition to relaying TCP connections between the client and the server, a circuit-gateway firewall offers a proxy that establishes a transparent connection known as a virtual circuit that serves as an end-to-end link between the client and

the server. The circuit-gateway firewall verifies the legitimacy of the connections by performing this. Additionally, it ensures that requests and responses are consistent, meaning that the information coming from the server and the client's request match. There's a possibility that someone is attempting to steal data from the network if the answers do not match the queries.

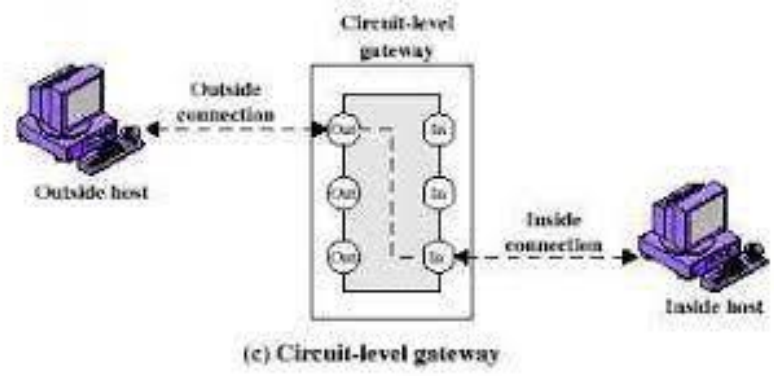

Figure 7: Circuit Gateway Firewall [5]

D. Web-Application Firewall:

One particular kind of application firewall that is only applicable to web applications is the web-application firewall (WAF). It is a security feature of an application proxy device that guards the web application server on the back end against various attacks. By examining network traffic patterns and HTTP/HTTPS request packets, it safeguards the web server. In the case that any malicious packets or patterns are discovered, WAF stops the assaults by either deleting the client-server session or blocking HTTP requests. When it comes to known online assaults like DDoS, SQL injection, and cross-site scripting (XSS), WAF is incredibly successful [8]. However, it is unable to handle zero-day exploits, or vulnerabilities that are not yet known to exist. because pattern recognition is the foundation of a WAF's threat detection system in large part. Because there is no pattern, it is hard for WAF to identify an attack that has never been observed before. As a result, it is challenging to repel them.

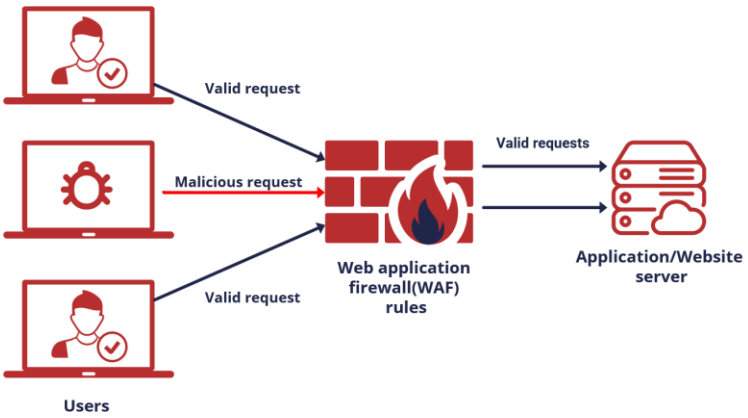

Figure 8 Web Application Firewall [5]

E. Unified Thread Management:

Unified Threat Management (UTM) is a strategy that, as its name suggests, combines many security features that may handle various cyberthreat kinds into a single software or hardware device. In contrast to the firewalls described before, UTM offers a plethora of protection techniques, including rule matching packet filtering, stateful inspection, deep packet inspection, intrusion detection (or prevention) systems, applications, circuit gateways, and more.

UTM offers defence against spam and phishing in addition to the conventional firewall defensive measures through thorough content inspection. Easy to deploy and install, UTM minimizes the hassle of managing various firewalls for distinct objectives. It is among the top options for safeguarding industrial networks.

But because it has multiple layers of security in one gadget. It has a single point of failure, meaning that if one protection layer failed, the entire network would be impacted. Additionally, because the packets must pass through numerous stages of inspection and scrutiny, it significantly reduces network performance.

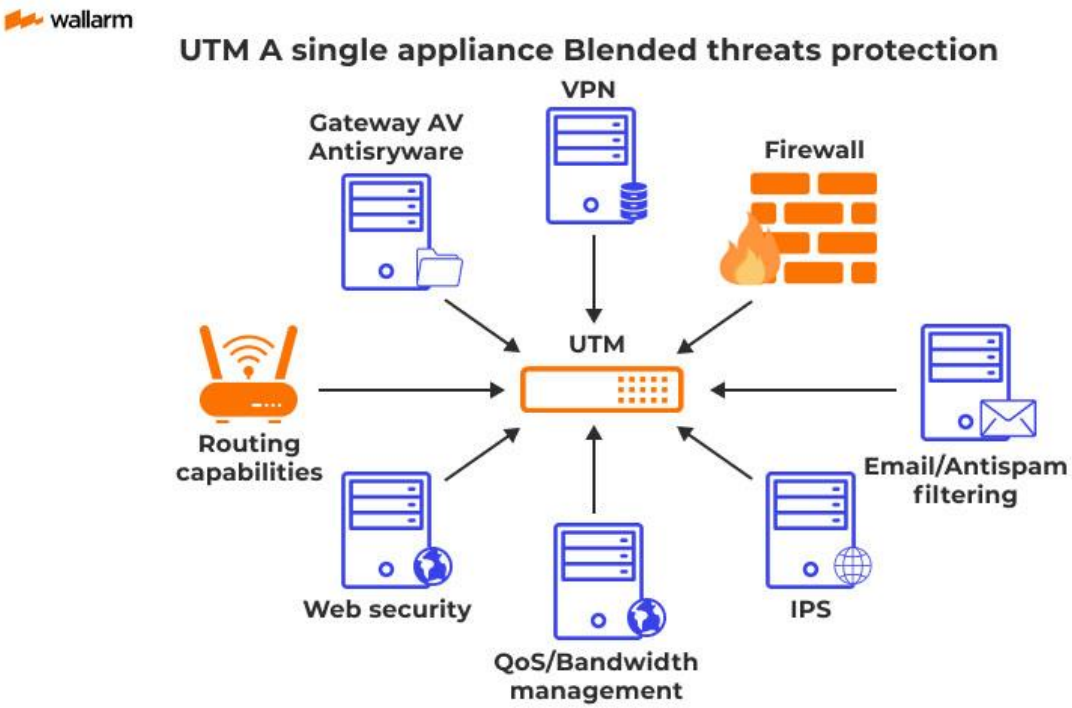

Figure 9 UTM Management [1]

2.3 Evolution of Firewalls:

Packet filtering firewalls were the earliest type of firewalls. In the year 1988, Digital Equipment Cooperation (DEC) developed it. Its sole purpose was to shield the network from undesired packets coming from specific source IP addresses; it was not intended to detect viruses or other network dangers. The stateful firewall was created in 1990 by AT&T Bell Laboratories with the goal of improving the effectiveness of packet filtering networks. The application-gateway firewall, designed to identify network threats, was created by DEC in 1991 as the internet became progressively more popular. Subsequently, in order to safeguard web servers, the web application firewall was unveiled in 1997. This firewall proved to be quite effective in identifying network intrusions. [5]

In 2004, about ten years after the first idea, UTM was unveiled. The idea of UTM was to integrate various firewall types into a single, large device. The idea of UTM changed into the idea of NGFW in 2009. The specifics of the distinction between UTM and NGFW will be covered in later parts. Ten years later, NGFW is still the most widely used option for protecting corporate and industrial networks, particularly when paired with machine learning and other cutting-edge intrusion detection methods. Every kind of firewall will be thoroughly covered and explained in the upcoming sections. Please take note that host firewalls will not be covered in this paper; all firewalls described are network firewalls.

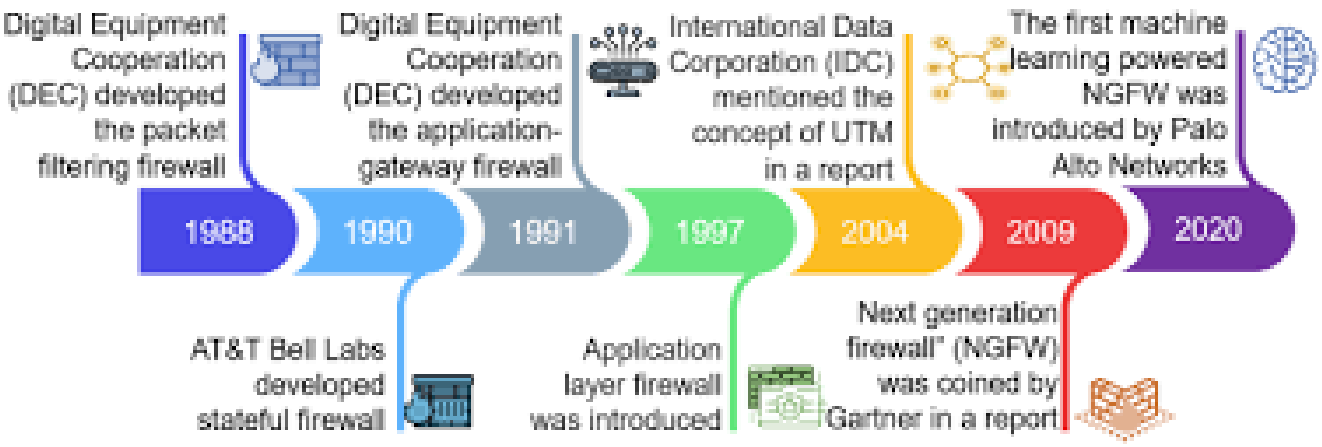

Figure 10: Evolution of Firewalls [3]

2.4 Next Generation Firewalls:

Next-Generation Firewall (NGFW) was invented around 2009 by Gartner. It was similar to the UTM in the early days and since then has evolved into a more innovative and more sophisticated product. Essentially, DPI firewall technology is applied by next-generation firewalls through the integration of application intelligence, control, and intrusion prevention systems (IPS) to visualize the content of the data being read and processed.

An NGFW is described as "a wire speed integrated network platform that performs deep inspection of traffic and blocking of attacks" by Gartner. [2]

An NGFW, according to Gartner, should offer non-disruptive, inline, bump-in-the-wire setup. Network Address Translation (NAT), SPI, Virtual Private Networking (VPN), and other common first-generation firewall features. integrated IPS engine based on signatures. granular control, full stack visibility, and application awareness. The ability to integrate data from external sources, such as directory-based policies, whitelists, blacklists, etc. Upgrade route to take into account upcoming information feeds and security threats .SSL decryption makes it possible to identify programs that are encrypted but not wanted.

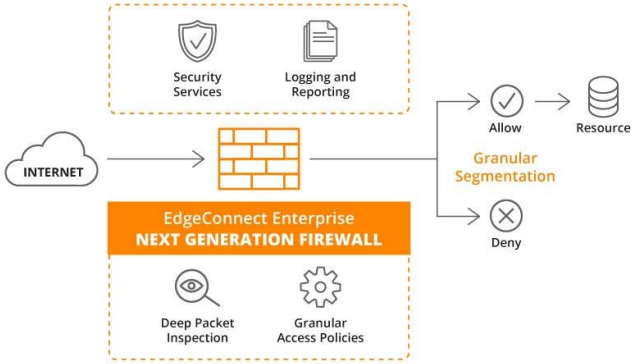

Figure 11: Next Generation Firewall [2]

Figure 12: Features of NGFW [2]

Benefits:

At multi-gigabit speeds, NGFWs may provide malware protection, SSL inspection, application intelligence and control, and intrusion prevention—all while being expandable to accommodate the highest-performing networks.

The most capable NGFWs can scan files of any size across any port without compromising security or performance, and they can control and manage both business and non-business apps to support network and user productivity. With high-end NGFWs, there is no restriction on the number of concurrent files or network streams, thus even under intense load, compromised files cannot evade detection. Moreover, NGFWs may apply all application control and security technologies to SSL encrypted traffic, preventing the introduction of new infection vectors into the network. When choosing a deep packet inspection firewall, IT managers should be aware that different processing architectures are used in different NGFW models. A few have opted for distinct security co-processors and general-purpose processors. Others still have opted to create Application-Specific Integrated Circuit (ASIC) platforms through design and construction. IT managers must make sure the NGFW solution they select has the most reliable performance, the most insightful and practical network analytics, and the least amount of effort to set up and maintain. It must also be fully scalable to meet their anticipated network performance requirements.[7]

Applications:

Type	Applications
Packet Filtering Firewall	Commonly used in routers and switches.
Stateful Firewall	Commonly used in enterprise networks and Data Centres
Application Gateway Firewall	Commonly used in proxy servers.
Circuit-Level Firewall	Typically used in dial-up connections and older networks.
Web Application Firewall (WAF)	Specifically designed for web applications and websites.
Unified Threat Management (UTM)	Used in comprehensive network security solutions.

3.FIREWALL ARCHITECTURES

3.1 Single Perimeter Firewall:

The most basic kind of firewall deployment is a single perimeter firewall architecture. The internal network and the internet are separated by a single firewall.

Small-scale networks usually utilize single perimeter firewalls to give a minimal level of protection against malicious traffic and unauthorized access.

A single perimeter firewall is economical and simple to set up and maintain nonetheless, creates a single point of failure and may be challenging to scale as the network expands.

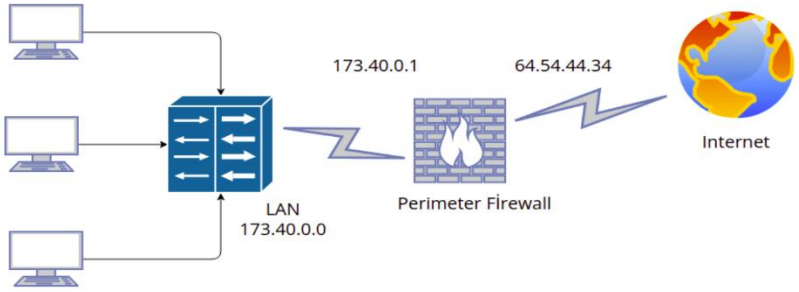

Figure 13 Single Perimeter [4]

For smaller networks, including those in homes and small offices, single perimeter firewalls are a good choice. They offer a minimal degree of protection without being very difficult or costly to set up and maintain.

It is crucial to remember that more sophisticated firewall architectures offer a higher level of protection than do single perimeter firewalls. For instance, attackers will have access to the whole internal network if the firewall is breached.

3.2 Dual Perimeter (Demilitarized Zone - DMZ) Firewall:

A demilitarized zone (DMZ) separates the two firewalls that make up a dual perimeter firewall system. A network segment that sits between the internal network and the internet is called the DMZ. It is usually used to host servers, such web servers and email servers, that must be reachable over the internet.

A dual perimeter design combines the strengths of both firewalls to offer more security than a single perimeter firewall. Traffic between the DMZ and the internal network is filtered by the first firewall, and traffic between the DMZ and the internet is filtered by the second firewall.

A single point of failure is what they offer. The other firewall will continue to defend the internal network even if one is compromised.

The internal network becomes more difficult for attackers to access as a result. The internal network can only be accessed by attackers who manage to breach both firewalls.

They make it possible for businesses to put in place more precise security measures. To prevent certain kinds of traffic from entering or exiting the DMZ, for instance, enterprises can set up their firewalls in this manner.

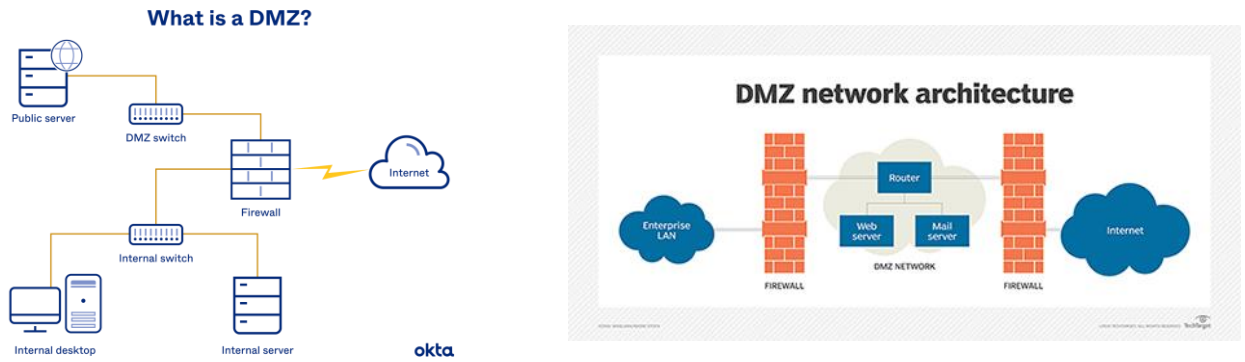

Figure 14 Dual Perimeter [4]

3.3 Multi-Layered Security: Using Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):

A robust defence against cyberattacks can be achieved by combining multiple security technologies through the use of multi-layered protection. One of the most crucial elements of multi-layered security architectures is the firewall.

In order to enable advanced threat detection and prevention, firewalls can be connected with IDSs and IPSs, two additional security technologies.

Intrusion Detection Systems (IDS):

IDSs keep an eye on network activity and spot questionable behaviour. An intrusion detection system (IDS) can produce an alarm or take additional measures, including traffic blocking, when it finds suspicious behaviour.

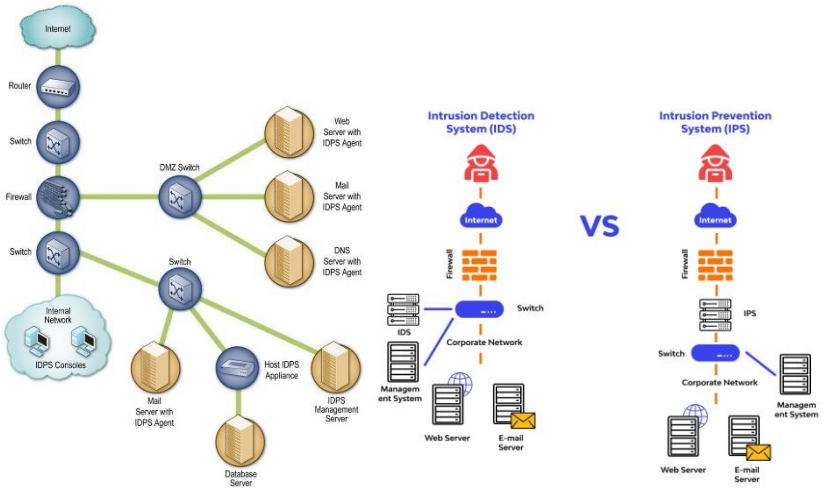

Figure 15: *Multilayer Security [11]*

Intrusion Prevention Systems (IPS):

IPSs are similar to IDSs, but they can also take action to prevent suspicious activity from occurring. For example, an IPS can block traffic that is known to be associated with a specific attack

Integrating Firewalls with IDS and IPS:

IDSs and IPSs can be connected with firewalls to offer a more complete defence against online threats. An IDS, for instance, can be used to keep an eye on traffic going through firewalls. The firewall can take action to stop the traffic if the IDS notices suspicious activity and notifies the firewall. In a similar vein, suspicious traffic can be stopped from entering or exiting a network by using an IPS. The IPS can be set up to cooperate with the firewall to log traffic or to prohibit particular kinds of traffic, among other things.

4. TYPES OF ATTACKS AND FIREWALLS:

In general, an attack is an unauthorized incursion. Attack tactics frequently focus on weaknesses (also known as holes or backdoors) in a particular operating system or network hardware [3,4]. Two broad categories of attacks exist: Attacks that are passive in nature, in which the hacker does not try to harm the system or tamper with it. However, he only keeps an eye on confidential information, which is typically in transit, and if required, performs cryptanalysis to try to crack any encryption that is in place. This is risky in any case [2]. Active attacks: these occur when a hacker tampers with data or resources within a system or network that they have targeted. These types of attacks include using the available resource, modifying or fabricating files or messages, and using address spoofing.

Computer-using criminals are those who violate system security. Because they are passionate about computers, hackers acquire unauthorized access to networks for enjoyment, spending hours developing programs to breach security systems. Crackers, on the other hand, intentionally compromise systems. Once they have gained access without authorization, they destroy crucial data, interfere with services for authorized users, and cause issues for their intended targets. [9]

Some of the most common attacks on firewalls are:

4.1 SYN Flooding Attack:

The three TCP session hand shakings are connected to this attack.

The two connection endpoints exchange three-way handshakes to start a TCP session. Let us say that host A wishes to attack host B, who we will refer to as the victim host, via SYN flooding. Initially, A transmits SYN packets to B; the source IP address host of these packets cannot be reached. B sends a SYN/ACK packet to the inaccessible address in response. B would thus have to wait an eternity for the unreachable address host to a TCP ACK packet to complete the three-way handshake. The machine's (host B) performance will suffer as a result. A popular ruse involves bombarding the victim with SYN requests. The compromised system not only takes time to respond with acknowledgements, but it also stays in a waiting state for the third exchange.

4.2 Ping of Death Attack:

Ping is an echo request packet sent over the Internet Control Message Protocol (ICMP). ICMP is a protocol that IP employs to transmit error messages, while IP is used by ICMP to transport messages. In order to target the victim server, the attacker impersonates its source address in this attack. The attacker then sends multiple ICMP packets to various destination addresses. Attackers using updated versions of this technique send ICMP packets to targets with broadcast addresses. Echo request is the most common ICMP message to send. The ping program will implement this at the application layer. A network probe with a specified destination address is sent out to check if a specific node is present. Any node receiving these ICMP echo replies is

sent to the victim machine rather than the spoofing machine. This is because the nodes that receive the echo request send an ICMP echo reply to the source address that appears in the packet. The victim machine would most likely be unable to carry out any helpful tasks when it received these ICMPs echo replies from numerous nodes.

4.3 IP Address Spoofing Attack:

IP spoofing is the most damaging active assault on the Internet since the attacker impersonates an author machine with one machine. Thus, an attacker would interact with a secured site as a legitimate user.

Attacker attacks the authorized machine with a denial-of-service attack. In a denial-of-service attack, the attacker bombards the server with requests to establish connections with fictitious servers. The server, inundated with thousands of additional false connection requests, attempts to connect to non-existent servers and waits for a response. As a result of being overloaded with false requests, the server starts to refuse service to actual users. The servers in the secured site could be directly targeted by the denial-of-service attack. Following a denial-of-service attack against the authorized machine, the attacker uses hardware address spoofing, which is partially reliant on the computer's card connection to the network. If the attacker is successful in going through the protected site and spoofing, he needs to make a better hole through which to breach the site.

4.4 Impersonate One Half of A Session:

If there is clear network connection between two nodes and you are aware of the protocol each node is using, you can use IP Address Spoofing Attack to mimic one of the nodes and disable the other. One of two methods can be used to disable a node: either physically store the node or overload it with constant network traffic. This hack differs from others in that it operates under the premise that message services must be exchanged as part of the protocol.

4.5 Session Hijacking Attack:

The idea of hijacking a session is straightforward. Traffic is sent in the clear between the communication session's two endpoint nodes. Because of where you are, any communication between these two nodes has to go via a node under your direct control. You can generate arbitrary IP traffic and sniff packets on your node by listening to the packets. If you want to trick both nodes into doing what you want, you have to manage both ends of the conversation.

5. A CASE STUDY: WINDOWS DEFENDER FIREWALL

As a stateful host firewall, Windows Defender Firewall is included with Windows 11, Windows 10, Windows 8, Windows 7, Windows Vista, Windows Server 2012, Windows Server 2008, and Windows Server 2008 R2. It helps safeguard the device by letting you establish rules that specify which network traffic can enter it from the network and which network traffic it can send there. Moreover, Internet Protocol security (IPsec) is supported by Windows Defender Firewall. This means that you can use IPsec to demand authentication from any device trying to connect to your system. Devices that are unable to authenticate as trusted devices are unable to communicate with your device when authentication is required.

The user-friendly Windows Defender Firewall interface located in the Control Panel is far less functional than the Windows Defender Firewall with Advanced Security MMC snap-in, which is also less flexible. Although they offer varying degrees of control over the same underlying services, both interfaces communicate with them. Although a single device in a home environment can be protected by the Windows Defender Firewall Control Panel tool, it lacks the centralized administration and security features necessary to effectively secure the more complicated network traffic seen in a typical large enterprise environment. [12]

Because the software on the protected host is connected to the host operating system and network protocols, the personal firewall is acting on it. It is based on personal firewall software and the Windows operating system. Windows-based operating system, personal firewall, and network packet interception technologies are the main components of the Windows operating system.

The protocol driver, for instance, calls out a distinct code sharing can be accomplished in a system where numerous apps use the same network protocol. All procedures can be called with a protocol driver, just like a DLL can be all EXE calls. As long as the interface performs as intended and is enabled in compliance with the proper action, the OS can thus reach agreements on the application that are transparent and unaffected by protocol implementations across all programs. [10]

The advantage of this hierarchical structure is that more security may be attained. When a program encounters issues, the system could become paralyzed. As a result, the operating system is split into two layers, each of which can have distinct operating rights.

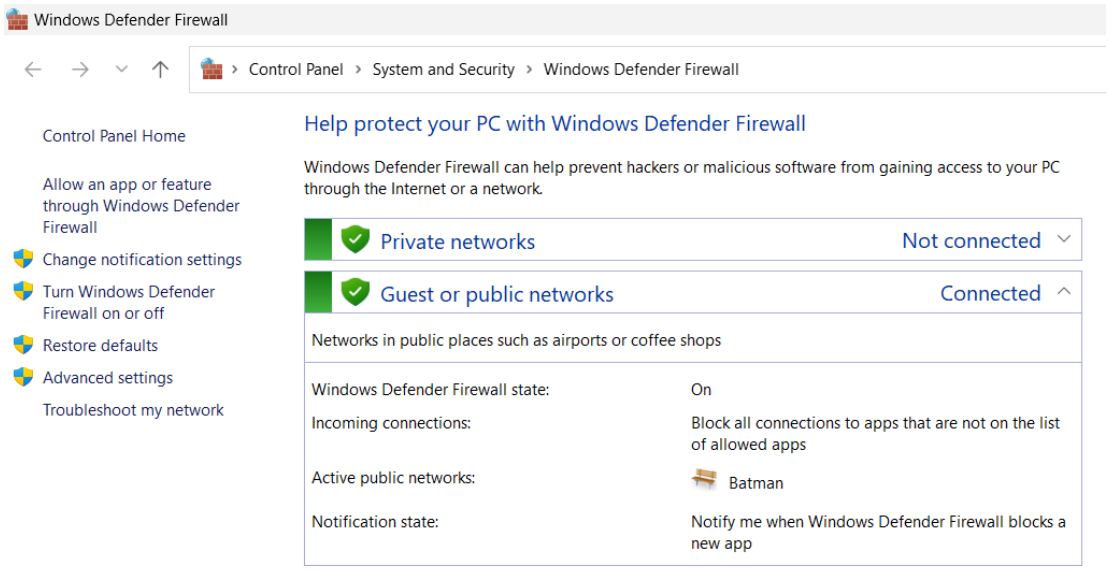

Figure 16 Windows Defender Firewall [12]

This indicates that all incoming connections to programs that are not on the list of approved apps are being blocked by the Windows Defender Firewall, which is now turned on. This is an excellent security precaution because it keeps unauthorized software off your computer.

Additionally, the firewall is set up to alert you whenever it bans a new application. You may use this to view which apps the firewall is blocking and choose which ones to allow, which might be useful for troubleshooting.

Click the "Allow an app or feature through Windows Defender Firewall" option to get a list of the apps that are permitted through the firewall. By selecting the "Add app or feature" or "Remove app or feature" options, you can also add or delete apps from the list.

You might want to think about turning on the "Guest or public networks" setting if you are connected to a public network, like the Wi-Fi network at an airport or coffee shop. This will assist safeguard your privacy by reducing the visibility of your computer to other networked devices.

An essential component of a tiered security approach is the Windows Defender Firewall with Advanced Security. Windows Defender Firewall prevents illegal network traffic from entering or leaving the local device by offering host-based, two-way network traffic filtering. Network Awareness is another feature that Windows Defender Firewall uses to apply security settings suitable for the kinds of networks the device is connected to. Windows Defender Firewall is also a crucial component of your network's isolation strategy since it integrates Internet Protocol Security (IPsec) configuration options into a single Microsoft Management Console (MMC) called Windows Defender Firewall.

CONCLUSION

Firewalls play an integral role in ensuring overall network security by acting as a crucial line of defence against unauthorized access and malicious activities. Firewalls monitor incoming and outgoing network traffic, analysing data packets based on predetermined security rules. By allowing or blocking specific connections, firewalls prevent unauthorized access attempts and filter out malicious content. Firewalls use intrusion detection and prevention techniques to identify and thwart potential attacks. They analyse patterns and behaviours in network traffic, enabling the detection of suspicious activities, such as DDoS attacks or port scanning, and blocking them in real-time. firewalls play a multifaceted role in network security by controlling access, inspecting traffic, preventing intrusions, supporting secure communication channels, and providing essential visibility into network activities. Their strategic placement and configuration are essential in creating a robust defence against cyber threats, ensuring the confidentiality, integrity, and availability of network resources.

Firm firewall systems are expensive, and organizations need to maintain them updated in order to properly defend their networks against ever changing cyberthreats.

REFERENCES:

[1] J. Liang and Y. Kim, "Evolution of Firewalls: Toward Securer Network Using Next Generation Firewall," *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, Las Vegas, NV, USA, 2022, pp. 0752-0759, doi: 10.1109/CCWC54503.2022.9720435.

[2] Florian_Malecki "Next-generation firewalls: security with performance " Volume 2012, Issue 12, December 2012,doi.org/10.1016/S1353-4858(12)70114-9

[3] C. Sheth and R. Thakker, "Performance Evaluation and Comparative Analysis of Network Firewalls," *2011 International Conference on Devices and Communications (ICDeCom)*, Mesra, India, 2011, pp. 1-5, doi: 10.1109/ICDECOM.2011.5738566.

[4] S. -d. Krit and E. Haimoud ,"Overview of firewalls: Types and policies: Managing windows embedded firewall programmatically," *2017 International Conference on Engineering & MIS (ICEMIS)*, Monastir, Tunisia, 2017, pp. 1-7, doi: 10.1109/ICEMIS.2017.8273003.

[5] B Rajkumar and G Arunakranthi " Evolution for a secured path using NexGen firewalls "

2022 OPJU International Technology Conference on Emerging Technologies for Sustainable Development (OTCON) 2023

[6] M. Schultz, E. Eskin, E. Zadok and S. Stolfo, "Data mining methods for detection of new malicious executables", IEEE Symposium on Security and Privacy, pp. 38-49, 2001

[7] Benfano Soewito and Charlie Erwin Andhika, "Next generation firewall for improving security in company and iot network" in 2019 International Seminar on Intelligent Technology and Its Applications (ISITIA), IEEE, pp. 205-209, 2019.

[8] M.G. Gouda and A.X. Liu, "A Model of Stateful Firewalls and Its Properties," Proc. IEEE Int'l Conf. Dependable Systems and Networks (DSN), pp. -128-137, June 2005. (Pubitemid 41538228)

[9] MyungKeun Yoon, Shigang Chen, and Zhan Zhang, "Minimizing the Maximum Firewall Rule Set in a Network with Multiple Firewalls" Proc. IEEE Transactions on Computers, Vol. 59, Issue. 2, pp. -218-230, Feb. 2010

[10] Ritchey, R. O'Berry, B. Noel, S., "Representing TCP/IP connectivity for topological analysis of network security", In Proc. IEEE Computer Security Applications Conference, 2002. Proceedings, pp.-25-31, 2002.

[11] H. Hamed, A. El-Atawy, and E. Al-Shaer, "On Dynamic Optimization of Packet Matching in High Speed Firewalls," IEEE J. Selected Areas in Comm., vol. 24, no. 10, pp. 1817-1830, Oct. 2006 (Pubitemid 44559596)

[12] Z. Yu, "The Program Design of Network Firewall Based on Windows," *2010 International Conference on Machine Vision and Human-machine Interface*, Kaifeng, China, 2010, pp. 553-556, doi: 10.1109/MVHI.2010.116.

ACKNOWLEDGEMENT

I acknowledge with great pleasure our deep sense of gratitude to Ms Pooja Pariyani (Teaching Assistant) , Department of Computer Science and Engineering, SVNIT Surat, for her constant encouragement and valuable guidance. I am very much indebted to her for suggesting this topic and helping me at every stage for its successful completion. The submission of this project gives me an opportunity to convey my gratitude to all those who helped me reach a stage. I would also like to thank my parents, and friends without whose support, I would not have been able to reach this important moment of our life.

Regards,

LANKA DEEPAK JOY
