MANTECH Publications

Journal of Computer, Internet and Network Security
Volume 8 Issue 2
ISSN: 2457-0176 (Online)

# *Network Security and the Role of Traditional Firewalls and AI Firewalls*

***David A. Sinha[1], Ashish Kumar Sharma[2]***

*Student[1], Professor[2]*

*Department of CSE*

*ALLEN Career Institute "Sankalp" CP-6, Indra Vihar, , Kota, Rajasthan 324005*

***Corresponding Author's Email**: - ashishsharma.pce@gmail.com[2]*

***Abstract***

*In this paper, we have analyzed different types of network security aspects, including topology, infrastructure and protocols. The idea is to first understand what a mobile/computer network is, how it works, and how data packets are sent across a network. We have focused on how these data packets which contain essential data, might also contain malicious code, viruses, malware, and thus the need to set up a series of systems in place to control malicious attacks, block malicious IP addresses, packet monitoring, virus scanning. We have analyzed how the different network security systems work individually and collectively to enable a secure networking environment, which is critical in this day and age, an aspect that is very important for business, academic and military applications. Finally, we have focused on an important aspect of Network Security Firewalls – both the "simple" software firewall and a more complex dedicated device called a hardware firewall (also called appliance firewall). We look into the pros and cons of each and discuss them, and heading to our conclusion, we focus on the emerging role of AI/machine learning in AI Firewalls and the unique way they function to counteract the upcoming emerging threats in a completely connected world.*

***Keywords-*** *Network Security Firewalls, AI Firewalls, Machine Learning, IP addresses*

## INTRODUCTION

What is a network? At the very basic level a network is a connection between two or more devices (It could be computers, mobile devices, IoTs – Internet of Things, etc). This connection enables the devices to communicate with each other, share resources, etc. They may be connected wirelessly (via Bluetooth, Wi-Fi, Infrared, etc.) or via physical cables (ethernet cables, phone lines, etc.). Two commonly used networks are LAN (local area network) where two ormore devices are connected to each other (for example in a home or a school). Devices can be connected to each other without a centrally managed device (like router) – that is called an ad hoc network. Once we set up an ah doc network permanently, it becomes a LAN. When two or more different LANs (Local area networks) are attached to each other, like via the Internet, that could be called a WAN (wide area network).

### Network Protocols

### What is a network protocol?

A network protocol is essentially an established set of rules that determine how data is transmitted between different devices in the same network

A brief look into types of network protocols (we have not gone into details, as they are beyond the scope of this current paper).

1. Address Resolution Protocol (ARP).
2. Border Gateway Protocol (BGP)
3. Domain name system (DNS)
4. Dynamic Host Configuration Protocol (DHCP)
5. File Transfer Protocol (FTP)
6. Hypertext Transfer Protocol (HTTP)
7. Internet Protocol (IP). IP is commonly paired with TCP to form TCP/IP, the overall internet protocol suite.
8. Open Shortest Path First (OSPF)
9. Simple Mail Transfer Protocol (SMTP)
10. Telnet, not common nowadays due to lack of security.
11. Transmission Control Protocol (TCP)
12. User Datagram Protocol (UDP), an alternative to TCP.

**Network topology**

A network topology is the physical and logical arrangement of nodes and connection in a network. In layman's terms, we can refer it to "layout" of the network.

A brief mention of types of network topologies is needed to get a better understanding of networking. Few types of topologies are. These mainly refer to a wired network (to make understanding a bit more clear).

1. Bus – Devices are connected on single cable (ends are NOT connected)
2. Ring – It is just like a bus topology, but the ends are connected.
3. Star – Each node is connected to a central hub.
4. Tree – It is a combination of bus and star topology, where nodes are connected to each other in a hierarchal manner.
5. Mesh – Device are connected to each other in a redundant manner, with multiple path between devices. Mainly used for Wi-Fi networks.
6. Hybrid – Combination of different topologies, using different links and nodes. This kind of topology is the most reliable, flexible, scalable, and effective.

**What are the different types of network security devices and tools?**

Different networking security tools can be used in the line of services. Some of these include:

1. Access control. This is a simple way of restricting users to sensitive sections of the network. Using security policies, one can restrict network access to only recognized users and devices or grant limited access to noncompliant devices or guest users.

2. Antivirus and anti-malware software. Malware, or "malicious software," is a common form of cyberattack that comes in many different shapes and sizes. Some variations work quickly to delete files or corrupt data, while others can lie dormant for long periods of time and quietly allow hackers a "back door" into your systems. The best antivirus software will monitor network traffic in real time for malware, scan activity log files for signs of suspicious behavior or long-term patterns, and offer threat remediation capabilities. Updates to antivirus and anti-malware programs are very important so that new malware/virus signatures can be easily identified by the antivirus product.

3. Application security. Each device and software product used in the devices within the network environment is a potential way in for hackers via vulnerabilities in the software architecture. Therefore, all programs be should be updated and patched to prevent cyber attackers from exploiting vulnerabilities to access sensitive data. Application security refers to the combination of hardware, software, and best practices you use to monitor issues and close gaps in your security coverage.

4. Behavioral analytics. In order to identify abnormal behavior, security support personnel need to establish a baseline of what constitutes normal behavior for a given customer's users, applications, and network. Behavioral analytics software is designed to help identify common indicators of abnormal behavior, which can often be a sign that a security breach has occurred. By having a better sense of each customer's baselines, MSPs (managed software provider) can quickly spot problems and isolate threats.

5. Data loss prevention. Data loss prevention (DLP) technologies are those that prevent an organization's employees from sharing valuable company information or sensitive data—whether unwittingly or otherwise —outside the network. DLP technologies can prevent actions that could potentially expose data to bad actors outside the networking environment, such as uploading and downloading files, forwarding messages, or printing. Even a basic closed-circuit TV monitoring set up can help with this.

6. Distributed denial of service prevention. Distributed denial of service (DDoS) attacks are becoming increasingly common. They function by overloading a network with one-sided connection requests that eventually cause the network to crash. A DDoS prevention tool scrubs incoming traffic to remove nonlegitimate traffic that could threaten your network, and may consist of a hardware appliance that works to filter out traffic before it reaches your firewalls.

7. E-mail security. Email is an especially important factor to consider when implementing networking security tools. Numerous threat vectors, like scams, phishing, malware, and suspicious links, can be attached to or incorporated into emails. Because so many of these threats will often use elements of personal

information in order to appear more convincing, it is important to ensure an organization's employees undergo sufficient security awareness training to detect when an email is suspicious. Email security software works to filter out incoming threats and can also be configured to prevent outgoing messages from sharing certain forms of data.

8. Firewalls. Firewalls are a very important element of a network security model. They essentially function as "gatekeepers" between a network and the wider Internet. Firewalls filter incoming and, in some cases, outgoing traffic by comparing data packets against predefined rules and policies, thereby preventing threats from accessing the network. Hardware firewalls, which are either embedded in some routers or placed in between the Internet and Router should be updated with patches and updates, so that it can recognize new threats. Software firewalls can be installed on devices within the network, and function in a similar way like a hardware firewall – but are limited to within the system they are installed on.Our paper will go into more detail with regards to firewalls.

9. Mobile device security. Mobile devices have become ubiquitous and all of them carry some form of personal and/or sensitive data. Hackers are aware of this and can easily take advantage of. Implementing mobile device security measures can limit device access to a network, which is a necessary step to ensuring network traffic stays private and doesn't leak out through vulnerable mobile connections. This can be done by software installed on the mobile device, encryption of data, regular updates, capability of remote wiping of data (in case of loss of device), etc.

10. Network segmentation. Dividing and sorting network traffic based on certain classifications streamlines the job for security support personnel when it comes to applying policies. Segmented networks also make it easier to assign or deny authorization credentials for employees, ensuring no one is accessing information they should not be. Segmentation also helps to sequester potentially compromised devices or intrusions.

11. Security information and event management. These security systems (called SIEMs) combine host-based and network-based intrusion detection systems that combine real-time network traffic monitoring with historical data log file scanning to provide administrators with a comprehensive picture of all activity across the network. SIEMs are similar to intrusion prevention systems (IPS), which scan network traffic for suspicious activity, policy violations, unauthorized access, and other signs of potentially malicious behavior in order to actively block the attempted intrusions. An IPS can also log security events and send notifications to the necessary players in the interest of keeping network administrators informed.

12. Web security. Web security software serves a few purposes. First, it limits internet access for employees, with the intention of preventing them from accessing sites that could contain malware. It also blocks other web-based threats and works to protect a customer's web gateway. These are often installed on the router or firewall or a managed network switch.

**Network Security**

The concept of network security has become important with the evolution of networks as they have become self-configuring and decentralized.

In the modern era, cyber security research has become very important. The amount of network data is huge, and it is necessary to use big data analysis and various machine learning algorithms to analyze and predict network security.

**Types of attacks on a network**

**Active Attack**

In an active attack, a miscreant tries to attack data while it is being sent to some other location. He can make changes to it or can hack confidential information while data is being transferred.

**Passive Attack**

In a passive attack, the hacker constantly monitors the system to gain valuable information through open ports. The attacker does not attempt to make changes to data.

**Auditing in Network Security**

Auditing in network security means checking whether the security policies and procedures are followed by the organization. This helps the organization to find any loophole in the security measures of the organization's network and hence implement network security.

**Firewall**

Firewall has been discussed above. It regulates the traffic on the network and is a security measure for communication on the network. It is an important aspect covered in our paper.

**End-point Security**

Endpoint Security is another approach for network security in which remote networks are secured. In this, devices follow certain security standards. It manages the user's access to the corporate network. The main components of this type of security are VPN(Virtual Private Network), operating system and an antivirus software. This security management process operates on the client-server model. Software as a Service is another model used in this case.

**Honeypot**

Honeypot is another security mechanism for network security. It detects, deflects and counteracts the unauthorized use of information systems. It consists of data which is isolated and monitored, but appears as if it is a part of the site. Honeypots are classified into two categories production honeypot and research honeypot.

Production honeypots capture only limited information and are easy to use whereas research honeypots collect information about the black hat communities who are trying to attack the network. Based on their design, honeypots can be classified as pure honeypots, low-interaction honeypots, and high-interaction honeypots.

**Hole Punching**

It is a computer networking technique that uses network address translation(NAT) for establishing the direct connection between the two parties. In this one or both the parties may be behind firewalls. For punching a hole, each of the clients connects to a third-party server which is unrestricted for temporarily storing external and internal address and port

information. Each client's information is passed on to the other through a server and using that direct connection is established. As a result, packets are transferred to each side.

**Malware Detection**

A malware is a software code which is designed to intentionally cause damage to the computer network. The malware code can be in the form of viruses, worms, Trojan horses, or spyware. The aim of malware detection is to find and remove any type of malware code from the network. Antivirus software, firewalls, and other such strategies help in detecting malware in the network. It is one of the good topics in network security for project and thesis.

**Information Security**

Information security refers to a set of strategies applied to prevent any type of threat to digital and non-digital information. It is also an interesting topic in network security. The strategies applied revolves around the CIA objectives which is expanded as confidentiality, integrity, and availability. These objectives ensure that only authorized users can access the information.

**Firewalls:**

Based on the configuration and use case scenarios, there are different types of firewalls, for e.g.,

- Packet-filter firewalls
- Circuit-level gateways
- Application-level gateways (Proxy Firewalls)
- Stateful multi-layer inspection (SMLI) Firewalls
- Next-generation Firewalls (NGFW), the latest variant is what we call AI Firewall. We have address this further in our paper.
- Threat-focused NGFW
- Network Address Translation (NAT) Firewalls
- Cloud Firewalls
- Unified Threat Management (UTM) Firewalls

At a physical level, these firewalls can be implemented on software firewalls or hardware firewalls.

**Comparing hardware and software firewalls**

As discussed earlier, there are a plethora of network security tools and devices, in this paper we focus on a very important aspect called the firewall. Typically, the term “firewall” is like a “wall of fire” that sits between your network and the outside Internet.

Hardware firewall:Also called appliance firewall.This is a hardware device which is dedicated in the role of firewall. Ideally, it is placed between the Internet and your network, so it can be placed after the modem. Typically, it looks like a network switch, but with far few ethernet porton them. This device is like a mini computer with processor, RAM and ROM. The software is embedded in this device, within its ROM/storage. They help protect your network from potential harm or from being used by bad actors to spread malicious data elsewhere.The software on the firewall should be updated regularly so that the device and detect emerging threats.

One simple type of firewall is called a packet filter, which examines the data itself. Because the data comes with information regarding its source and location, the firewall uses this to determine whether or not the data poses a threat to the system, then runs the information through a list of permissions in its database. If the data does not pass the permissions checklist, it is not allowed through. If, according to the permissions, the data is safe, it is allowed to pass.

Modern hardware firewalls will inspect data going in both directions. Similar to the mechanism for scrutinizing incoming traffic, the firewall applies a set of permissions to outgoing data as well. In this way, it can catch data embedded in the coding designed to use your computer to spread malicious code to other computers on the internet.

**Advantages of Physical Firewalls**

1. Single-device network control: A single hardware firewall provides protection for every computer connected to the network. This is big saving in terms of cost and time.

2. Simultaneous updates and protection updates for all computers on the network: Just like any software, hardware firewalls should be updated and patched regularly. This way the embedded software can detect new Update your protection settings once, and

all computers on the network benefit at the same time. This ensures all devices are safe from compromise and saves IT resources from updating each computer manually, trusting that every computer will be free and ready for an automatic update, or trusting that each user will take the appropriate steps to implement an update.

3. Constant protection: One major advantage of hardware firewalls is that stay up and running unless you to turn them off. There is no change in computer memory or processing power, there is no chance of losing protection and dangerously exposing the network.

4. Better security: Because hardware firewalls have their own, separate operating system, they are less prone to some of the attacks that software firewalls may suffer when a computer is compromised. This software is built ground-up on very stable platforms to provide robust network protection.

5. Prevention of threats from reaching internal devices: One can shield every device on your network from harmful. It is like a physical barrier between your devicess internal drives and incoming malicious code stops threats before they penetrate your device.

**Disadvantages of Hardware Firewall**

- Configuration of hardware firewalls need some technical know-how and in a bigger network, might require a dedicated IT support person(s) for this. Some newer hardware firewalls are a bit easier to configure, but still need some basic knowhow and experience. A badly configured hardware firewall can result in outage of the network!
- If not configured well, any malicious traffic that is traveling out of your network is considered safe by the hardware firewall. This poses to be a problem as the hardware firewall cannot detect internal malicious activities.

**Can routers be used as firewalls?**

Most modern routers can be used at a basic level as a firewall replacement, but cannot function in the role of a dedicated firewall in a complex system.

1. Protection from data without a predesignated destination: Unless a router knows which computer, incoming traffic is supposed to go to, it discards the data. In the case of

malicious data directed at the router, but not specifically requested by a computer on the network, the router would get rid of it because it would not know which computer to direct it to.

2. Blocking specific types of data: Some routers can be configured to block specific types of data exiting your computer. With this protection, your computer could not be used by malicious actors looking to make it a hub for attacks on other devices.

If a router is used in conjunction with another firewall, it can provide an extra layer of protection. It can also, if programmed properly, help prevent your computer from being turned into a “zombie” or “kidnapped” by malicious software.

However, routers are not well-equipped to provide a comprehensive security solution. For example, a router may allow malicious incoming traffic a user requests by clicking a link or visiting a site.It may not provide protection against this type of attack because it may interpret the click, or other action by the user, as a request for the malicious data. A firewall will block suspicious data even if it is “requested” by a user.

**Software Firewalls**

A software firewall is a program that is installed on a computer. It inspects data that goes in and out of the device. It can be customized by the user to meet their needs. Like hardware firewalls, software firewalls filter data by checking to see if it—or its behavior—fits the profile of malicious code.

Software firewalls can monitor traffic trying to leave your computer as well, preventing it from being used to attack other networks or devices. A software firewall has to be installed on each computer in the network. Therefore, a software firewall can only protect one computer at a time. They are also fairly simplistic in the rules that can be configured.

**Advantages of Software Firewall**

- Software firewalls are very economic options for homes and small offices. It is especially good where there are a limited number of computers.

- Software firewalls are easily configurable as you only have to follow a step by step installation program.
- A software firewall is flexible with the sources from which it blocks information. You can easily determine the applications that should be granted access when you are using a software firewall.
- Laptops which are often connected over various public networks such as in airports, cafes, restaurants, and so on can be attacked on such networks, but with a software firewall, you are always protected.
- Since a software firewall works from within the system it can better keep track of the activities of your system. Thus, if a malicious program has entered your system and trying to pass information out into the network, the software firewall detects such activities and prevents it!
- Software firewalls are often bundled with anti-virus software so it makes a lot of financial sense in that you get the protection of both!

**Disadvantages of Software Firewall**

- Once installed, a software firewall can make a computer slow up taking up resources.
- If you are installing it on a number of computers, you have to purchase a separate package for each computer, raising up the overall cost.
- Software firewall does not allow you to mask the IP address of your system.

**AI Firewalls**

The latest generation of NGFW, next generation firewalls are AI firewalls. NGFW typically used a set of static rules to direct traffic, so they are unable to cope with emerging threats, until the malicious threats are updated via software updates. An AI-based firewall, on the other hand can cope with emerging threats using intelligent detection engine. This relies on a massive database of samples and on top of that it continually optimizes modes based on the real-time traffic data. This is the forefront of firewall technologies and definitely the future of firewalls.

One has to remember that earlier traditional threats to Network Security was from viruses, Worms, DDoS, which have now progressed, but not limited to advanced threats, like phishing, trojans, web threats, ransomware, Intra-net threats and even M2M (machine to

machine) attacks. These advanced threats and not just persistent – they are constantly evolving.

Thus, there is a need for firewall with AI/machine learning to counteract these emerging and evolving threats. These new kinds of threats cannot be possibly controlled by traditional rule-based firewalls which are the majority of the firewalls deployed worldwide.

- Signature-based threat detection based on databases cannot cope with advanced and unknown threats.

Signature-based threat detection relies onstatic rule databases and can only describe known threats and hence the database is limited. The database cannot detect hitherto unknown and variant advanced threats.

**Multi-layer and covert threats pose new challenges for firewalls dealing with Network Security.**

IoT has become very popular these days, but with it comes more security threats. The number of threats from the inside (or intranet)is significantly increased. Hackers can infiltrate from the outside, gain remote control, spread to the inside, steal, and destroy important data, forming a complete kill chain. A traditional firewall matching packets with the database cannot identify the entire attack process. As a result, the NGFW cannot accurately mitigate attacks.

Nowadays, threats are becoming more covert using encrypted channels. Encrypted channels make it difficult for traditional firewalls to match the attack with the database and so the AI firewall should be able to analyze data from all aspects without decrypting the data, so that any threats can be exposed.

**• The need for technical personnel.**

Firewall deployment is never a one-time thing. An ongoing operations and management program are essential. Network administrators need to continuously update policies to cope with changing threats. AI firewalls must have automated data analysis and threat handling capabilities.

When integrated into NGFWs, AI algorithms can analyze vast amounts of network data, identify emerging patterns, and detect abnormalities, indicative of potential threats. Thus, networks can swiftly get rid of emerging threats, reducing incident response time and minimizing the potential impact of cyberattacks.

We strongly feel that traditional firewalls, both software and hardware, have to be completely changed to AI firewalls in the future to cope with the complex and evolving threats that are coming up.

## CONCLUSION

We believe the firewall is one of the most important tools to be used for network security, either software or hardware firewalls. While both types of firewalls have their own roles and there are advantages and disadvantages of both. Both of them are very capable of providing seamless protection in their own unique ways. The hardware firewall can act over a large network and protect all the systems connected to the network. However, the software firewall is capable of tracking the computer system's activities and pick up malicious activities.

A software firewall is much cheaper compared to a hardware firewall. However, both of them are economical in the environment they are used in. While software firewalls work very well for single computers, a hardware firewall can provide protection to all the systems attached to a network.

We think the best solution would be to use a combination of both. Both options bring with them unique features, and each of them can be very useful against different kinds of attacks. However, it is very important to keep updating the firewall installed in your system, either the software or hardware embedded firewall - to ensure an efficient degree of protection. The computer system (operating system) should also be updated regularly to aid the firewall in providing enhanced security.

No matter what system is used, we strongly feel that AI firewalls with machine learning is critical for network security for the coming times. Or else, huge networks are vulnerable to attacks like which we have never seen before. We also believe that as the adoption of AI

firewalls increases, this technology will trickle down to small businesses, home users and individual users. This will greatly help in overall network security as it will close off all loop-holes from where emerging threats can reenter the network spaces.

**REFERENCES**

1. https://en.wikipedia.org/wiki/Firewall_(computing)
2. https://en.wikipedia.org/wiki/Computer_network