Gateway International Journal of Innovative Research
Volume 2, Issue 1, March, 2023, pp 14-28.

A Study of Various Features and Challenges in Implication Firewalls in Data Security

***Sarita **Vikas Punia,**

Abstract

In the work use of a firewall within the framework of the suggested technique offers protection on many different levels. Encryption has been used in order to make certain that the data is kept in a secure environment, and session security makes it possible for users to initiate a session even when data is in the process of being transferred. IP filters deny access to Internet Protocol (IP) addresses that have not been previously validated. A user-defined port number, which is included as part of the multilayer firewall security, enables the user to make use of a customized protocol. This ability is made possible by the firewall.

Keywords: Firewall, Security, Network, Traffic etc.

Introduction

A firewall is a security system that monitors incoming and outgoing traffic and decides whether or not to allow it based on a set of rules that have been established. Firewalls have been the first line of defense for protecting networks for over twenty years. Both software-only and hardware-based firewalls are viable options. Firewalls are used to protect a network from outside attacks by screening out potentially malicious data.

[*] Research Scholar, Faculty of Engineering & Technology, Jagannath University, Jhajjar.

[**] System Administrator, ICAR-IASRI, Delhi-110012

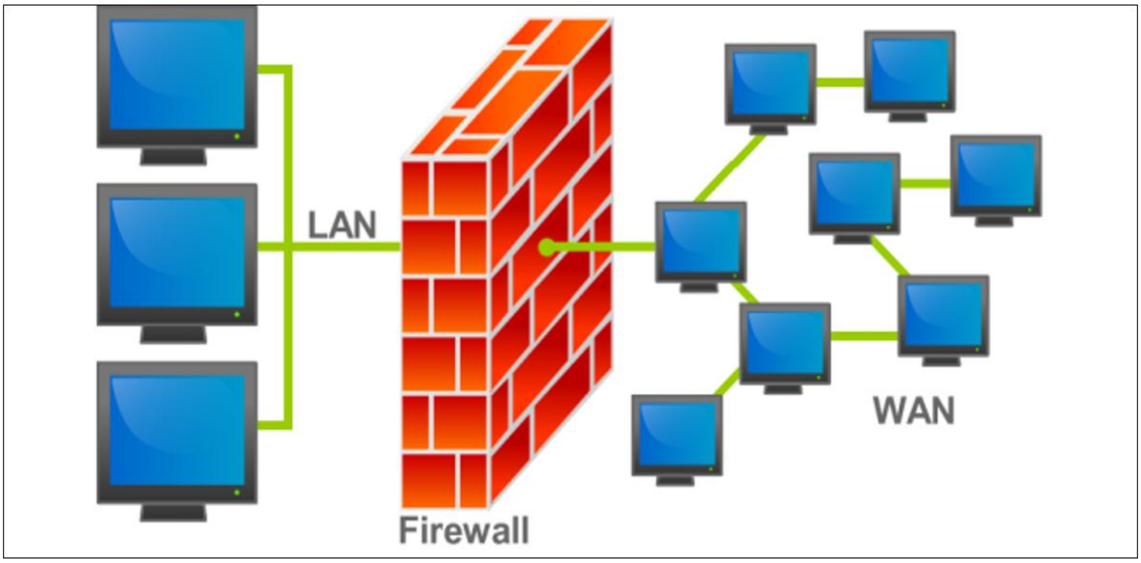


Fig. 1.Connection between Firewall, LAN and WAN

Outside connections, such as the Internet, are kept out of a trusted system or network by it. Although a firewall is a physical barrier, it is more like an electronic filter, allowing only trustworthy data to pass through it. There are certain firewalls that accept traffic from any IP address except those on a blacklist.

Software and Hardware Firewalls

Firewalls may be software-only, hardware-only, or a hybrid of the two. Both hardware and software firewalls are often used. It is more necessary to utilize a firewall than to choose which kind to employ, even though both have benefits and downsides.

Hardware

Hardware that lies between your computer and the internet is known as a firewall, preventing unwanted access (or other network connection). Several companies and Internet service providers (ISPs) provide routers designed specifically for use in home offices and small businesses that include firewall protection. Protecting many computers and controlling the traffic that attempts to get through the firewall is a job best suited for a hardware firewall. An extra layer of security is provided by hardware-based firewalls, which are able to protect desktop computers. Because they are independent devices that must be supported and maintained by experienced specialists, they have a disadvantage.

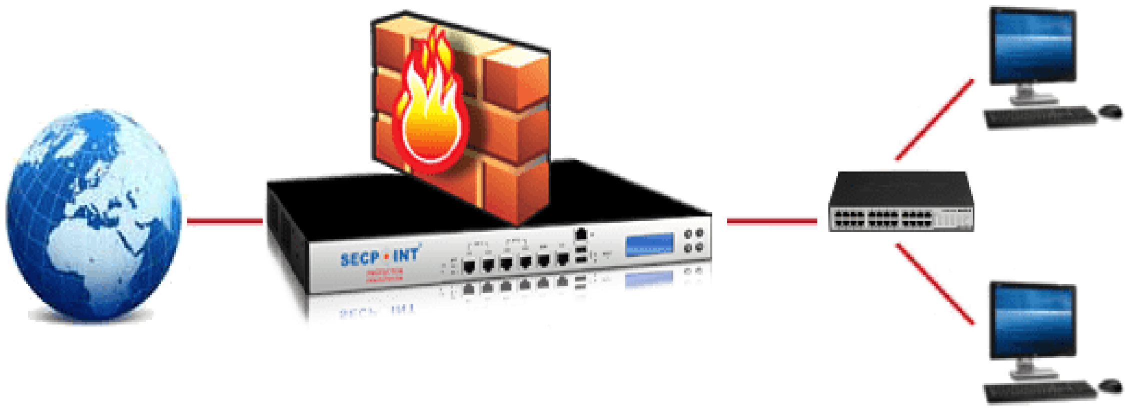


Fig. 2 Hardware Firewalls

Physical devices with their own processing power make up hardware firewalls. As gateways between the internet and internal networks, they prevent traffic from entrusted sources from entering the private network and requesting data. Businesses with several devices on the same network might benefit from physical firewalls. Insider attacks are not protected by these technologies because they stop malicious communication before it reaches any of the end points. As a result, your company's network will be well-protected if you use both software and hardware firewalls.

Software

Most operating systems come with a firewall already installed but turning it on is still a good idea. You're ISP, local computer store, or software provider may also sell standalone firewall software. Check the source of the firewall software before downloading it from the internet. Make sure it's from a trusted source. Individual programmes on a system may have their own distinct network behavior regulated by software firewalls. As a software firewall, it's commonly installed on the same system that it's supposed to protect. Being installed on the same computer as the firewall might hinder its capacity to recognize and stop hazardous activity. Software firewalls may have certain drawbacks, such as the fact that each computer on a network will need its own firewall to be updated and administered.

Each computer has its own software firewall. Because they may provide access to just certain programmes or functions while blocking others, they provide more precise management. For one thing, administrators must set up and manage them individually for each device that hosts a virtual machine, which consumes a lot of resources. A single software firewall may not be compatible with all of the devices on an intranet; therefore several firewalls may be required.

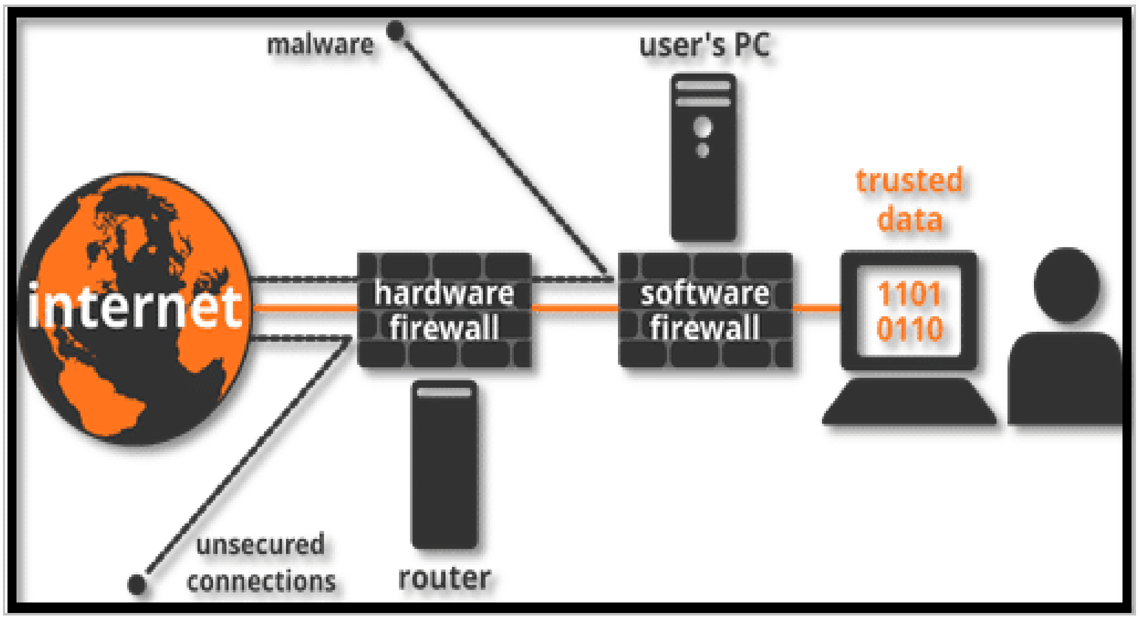


Fig. 3 Hardware and Software firewall

Firewall Architectures

The configuration that works best for a particular organization depends on three factors: The objectives of the network, the organization‘s ability to develop and implement the architectures, and the budget available for the function. There are four main firewall architectures to choose from. Filtering routers, firewalls with screened hosts, dual-homed firewalls, and firewalls with screened subnets are all examples of this kind of technology in action.

Packet Filtering

Routers Most companies with Internet connections use a router to link their internal networks to the external service provider's network at the organization's perimeter. Many of these routers may be set to reject packets that are not allowed into the network. One of the most effective ways to protect the company from external threats is by using this basic strategy. Auditing and stringent authentication are among the system's downsides. Access control lists, which are used to filter packets, may become more complicated, which can have a negative impact on network performance.

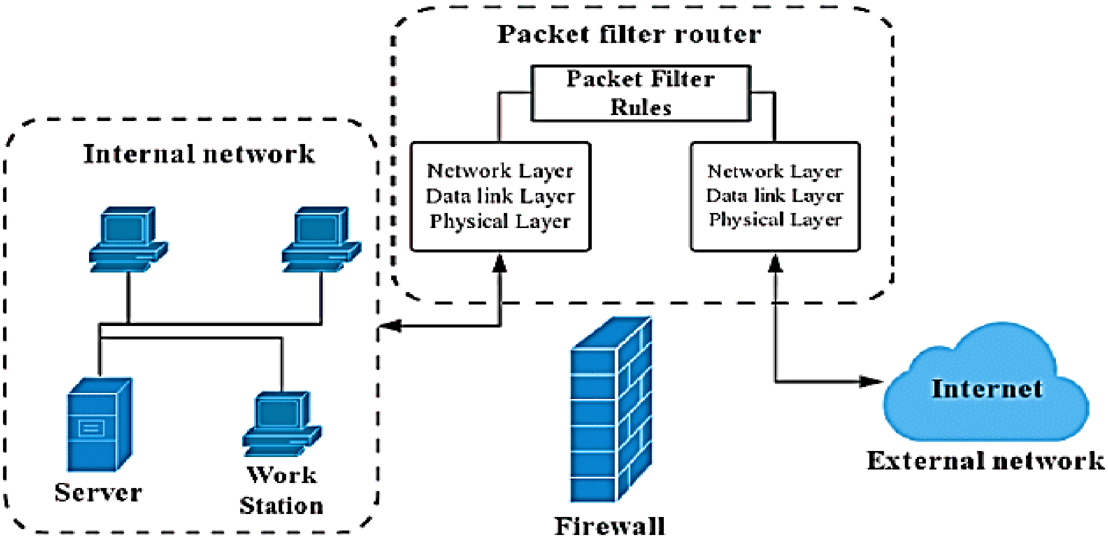


Fig. 4 Packet Filtering

Screened Host Firewalls

The packet filtering router is combined with a separate, specialized firewall, such as an application proxy server. It allows the router to pre-screen packets in order to reduce network traffic and internal proxy burdens. In order to provide proxy services, the application proxy analyses an application-layer protocol, such as HTTP. As a bastion host, this distinct computer should be well-protected against external threats. It is a common term for this kind of computer. However, even though the bastion host/application proxy is only a cache of internal Web content, it still presents a good target since it may expose internal network configurations and perhaps provide internal information to external sources if it is compromised. The bastion host is also known as the Sacrificial Host because it serves as a slow defender on the network perimeter.

This setup has the benefit of requiring an external assault to compromise two independent systems before internal data can be accessed. As a result, the data is more protected by the bastion host than it is by the router alone.

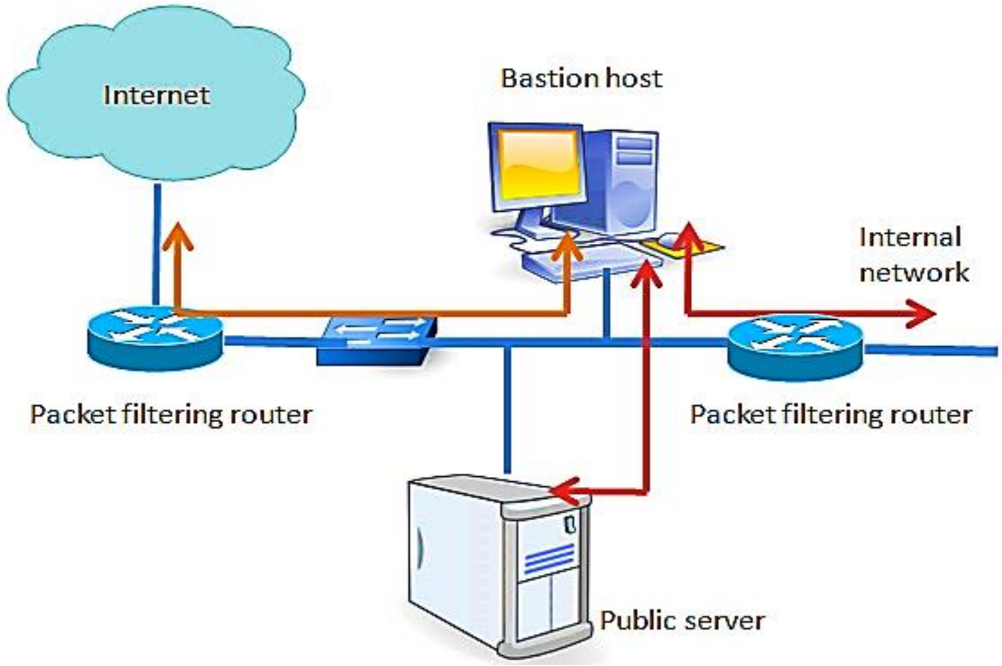


Fig. 5 Screened Host Firewalls

Dual-Homed Host Firewalls

With a dual-homed host, the complexity of a firewall rises even more. In contrast to the bastion host's single NIC, when this architectural approach is used, the bastion host possesses two NICs. Additional security is provided by using two NICs, one for the external network and one for the internal network. All communication between the internal and external networks must physically pass through the firewall using TWO NICs.A lot of times, NATs are used in the implementation of this architectural design. NAT is a technique for converting genuine, routable external IP addresses into non-routable internal IP addresses, hence further thwarting attacks from the outside.

NAT uses three separate ranges of internal addresses. There are more than 16.5 million Class A addresses available in the 10.x.x.x range. The 192.168.x.x range, which has around 65,500 Class B addresses, may be used by organisations. Last but not least, smaller organisations may utilise the c172.16.0.0 to 172.16.15.0 range, which has around 16 Class C addresses or over 4000 useable addresses, if they just require a few Class C numbers.

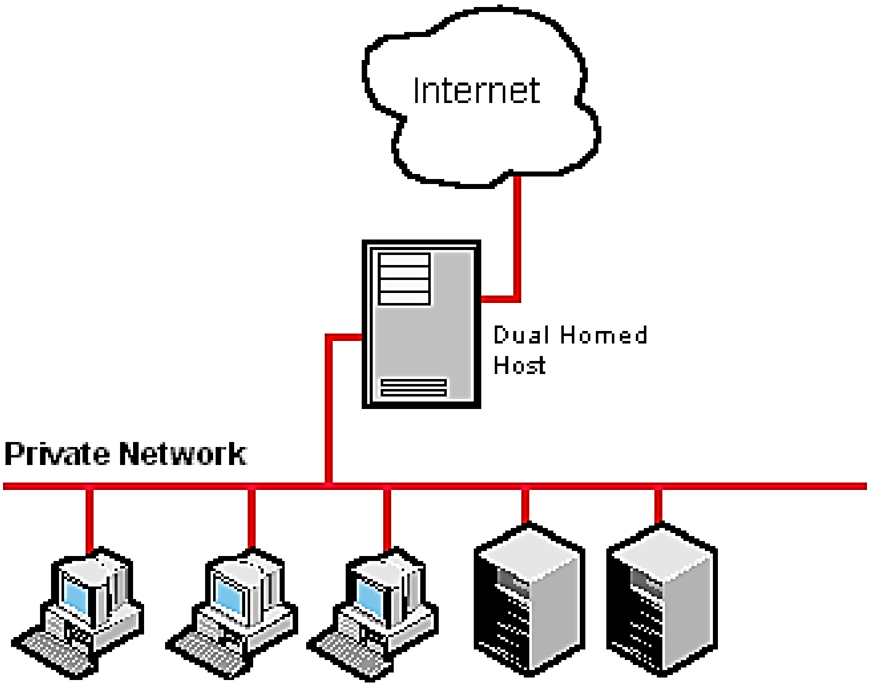


Fig.6 Dual-Homed Host Firewalls

Since the NAT server is bypassed by messages delivered to one of these three internal use addresses, no traffic can be routed over the public network. NAT uses this to prevent external assaults from affecting internal computers with addresses in certain ranges. Multi-homed bastion hosts, such as a NAT, may convert between public network naming authorities' real, exterior IP addresses and internal, non-routable ones. This is done by giving dynamic IP addresses to internal communications, then using sessions to keep track of which messages are received in response to which messages sent out.

Token Ring, Fiber Distributed Data Interface (FDDI), and Asynchronous Transfer Method (ATM) are just some of the protocols that may be translated between a dual-homed host and its data connection layer (ATM). Cons: If this dual-homed server is hacked, the external network connection will be lost, and the system would become overburdened as traffic volume grows. This design, on the other hand, offers superior overall security at a lower cost than more complicated alternatives.

Screened Subnet Firewalls (with DMZ)

In today's world, the screened subnet firewall is the most common design. A DMZ is provided by the design of a screened subnet firewall. Figure 6-13 shows a firewall device that connects to a single bastion server, or a screened subnet, with a dedicated port for the DMZ. Servers that provide services across an untrusted network were traditionally located in the DMZ until recently. Web servers, FTP servers, and certain database servers are examples of this kind of server. It has produced far more secure options.

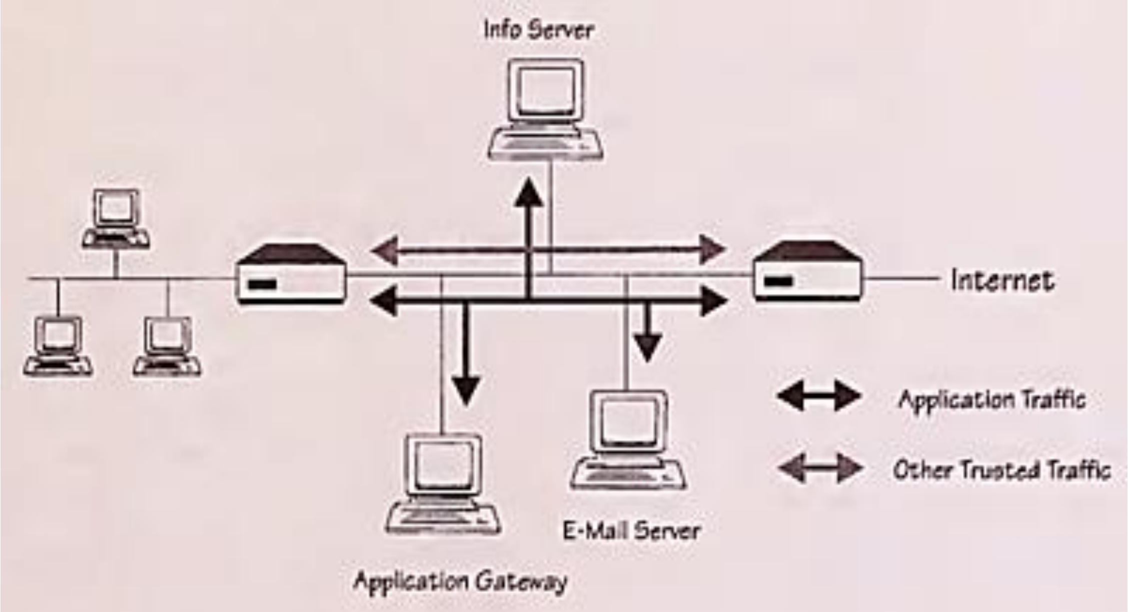


Fig. 7 Screened Subnet Firewalls (with DMZ)

Two or more internal bastion hosts behind a packet filtering router are popular configurations for a subnet firewall. Each host protects the trusted network. The screened subnet architecture may be implemented in a variety of ways. Two filtering routers and one or more dual-homed bastion hosts make up the first general model. It illustrates a second broad paradigm, in which connections are routed as follows:

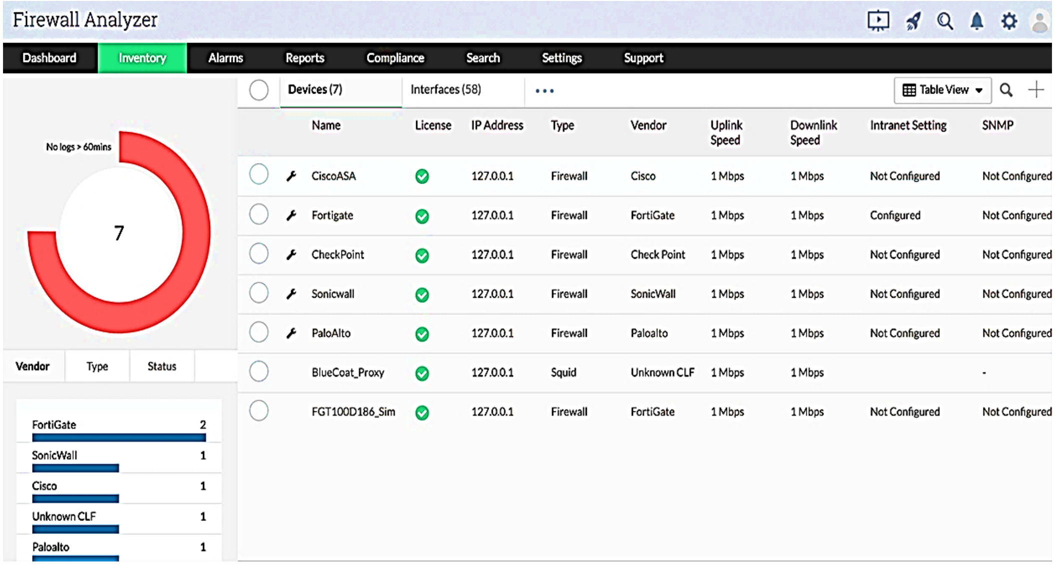
1. An external filtering router is used to redirect connections from the outside or from networks that are not trusted.
2. A routing firewall is used to redirect connections from the outside or untrusted network to the DMZ, a distinct network segment.

In order to access the internal network, only DMZ bastion host servers are authorized to connect. One goal of the screened subnet is to provide an intermediate level of security for the DMZ systems and information while also safeguarding the internal networks by reducing the number of ways in which external connections may obtain access to the DMZ systems and information. The screened subnet, despite its high level of security, is difficult to deploy and operate. Costs must be justified by the value of the information it safeguards. The development of an extranet is one of the DMZ's other features. Additional authentication and authorization restrictions are implemented in an extranet to offer services that are not accessible to the general population. In this case, the consumer will be required to provide further authentication and authorization when he or she is ready to check out and make an order on the online retailer's website.

Advantages of Firewall:

Monitor Traffic

In order to perform its main function, a firewall must monitor every data that passes through its defenses. All information delivered via a network is done so in packet form. The firewall analyses every single one of these packets for any malicious code. If the firewall accidentally picks them up, it will immediately halt them.



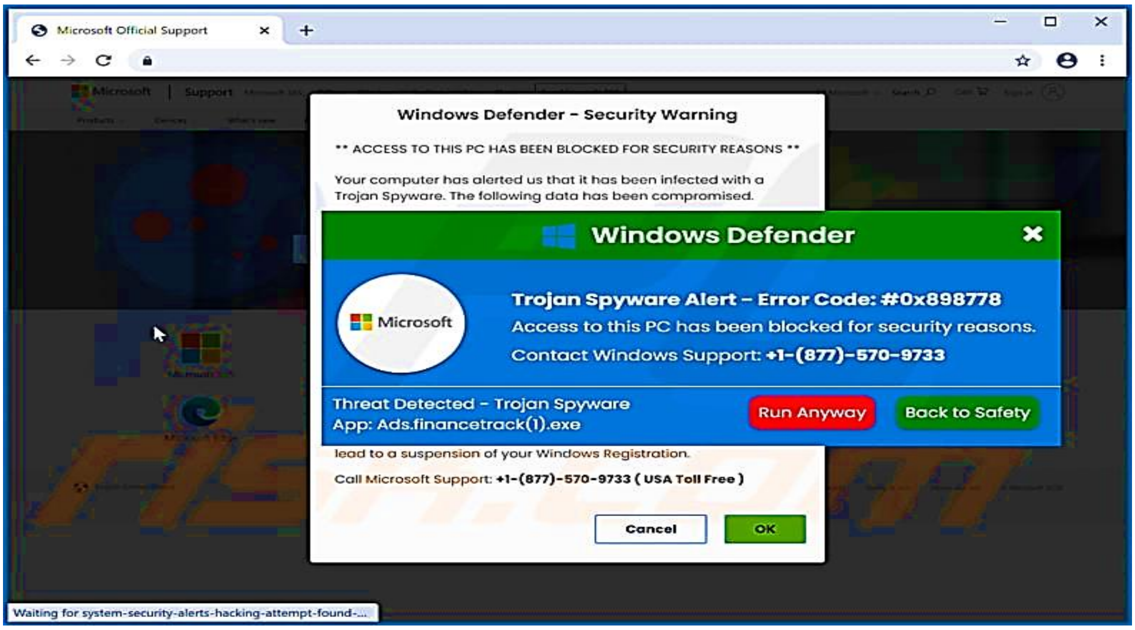
Name	License	IP Address	Type	Vendor	Uplink Speed	Downlink Speed	Intranet Setting	SNMP
CiscoASA	✓	127.0.0.1	Firewall	Cisco	1 Mbps	1 Mbps	Not Configured	Not Configured
Fortigate	✓	127.0.0.1	Firewall	FortiGate	1 Mbps	1 Mbps	Configured	Not Configured
CheckPoint	✓	127.0.0.1	Firewall	Check Point	1 Mbps	1 Mbps	Not Configured	Not Configured
Sonicwall	✓	127.0.0.1	Firewall	SonicWall	1 Mbps	1 Mbps	Not Configured	Not Configured
PaloAlto	✓	127.0.0.1	Firewall	Paloalto	1 Mbps	1 Mbps	Not Configured	Not Configured
BlueCoat_Proxy	✓	127.0.0.1	Squid	Unknown CLF	1 Mbps	1 Mbps		-
FGT100D186_Sim	✓	127.0.0.1	Firewall	FortiGate	1 Mbps	1 Mbps	Not Configured	Not Configured

FortiGate	2
SonicWall	1
Cisco	1
Unknown CLF	1
Paloalto	1

Fig. 8 Monitor Traffic

Protection against Trojans

Users should stay away from any virus, but Trojans in particular. Everything you do on your computer is being watched by a Trojan horse. Any data they gather will be uploaded to a server online. It's likely that you won't learn of their existence until your computer starts behaving erratically. This is where a firewall comes in handy; it will stop Trojans in their tracks.



Windows Defender - Security Warning

** ACCESS TO THIS PC HAS BEEN BLOCKED FOR SECURITY REASONS **

Your computer has alerted us that it has been infected with a Trojan Spyware. The following data has been compromised.

Windows Defender

Trojan Spyware Alert – Error Code: #0x898778
Access to this PC has been blocked for security reasons.
Contact Windows Support: **+1-(877)-570-9733**

Threat Detected - Trojan Spyware
App: Ads.financetrack(1).exe

lead to a suspension of your Windows Registration.

Call Microsoft Support: **+1-(877)-570-9733 (USA Toll Free)**

Waiting for system-security-alerts-hacking-attempt-found-...

Fig. 9 Protection against Trojans

Stops Virus Attacks

A viral assault is one of the most effective ways to put an end to your digital activities quickly and completely. Your information technology infrastructure needs to be protected from the tens of thousands, if not hundreds of thousands, of new security risks that emerge every single day. The ability of a firewall to restrict your system's access points and protect it from malware attacks is one of the most obvious benefits of using a firewall. If a virus were to infect your computer systems, you could potentially lose everything, and the damage could be of unimaginable magnitude.

Prevents Hacking

Regrettably, as businesses become more reliant on digital operations, fraudsters and other malicious actors will become more likely to follow suit. As the number of instances of data theft and criminals acquiring control of networks continues to rise, the need of installing firewalls has only risen. They prevent hackers from gaining access to your data, emails, systems, and other information in any way they can. A firewall may either completely prohibit an intruder from accessing your system or stop them from trying to do so in the first place.

Stops Spyware

Protecting your computer systems from dangerous malware and preventing it from entering is an incredibly essential benefit in this day and age. The more complex and secure your systems get, the larger the number of entry points there will be for thieves to employ to break into them. Spyware and other forms of malicious software are types of computer programmes that are designed to infiltrate a computer system, change the data on the system, and steal the data from the system. This is one of the most common ways that access can be gained to a system. Firewalls are a crucial first line of defense when it comes to safeguarding a network from a variety of kinds of harmful software.

Disadvantages of Firewall

This section is presenting limitation of firewall:

Cost

Depending on the kind, there may be a cost associated with installing a firewall. Hardware firewalls often cost more than software firewalls. Hardware firewalls, on the other hand, need expensive setup and ongoing support. It is impossible to do these settings without the assistance of an IT professional. It's less expensive than a software firewall, moreover, the average user should have little trouble setting it up.

User Restriction

Firewalls are unquestionably effective in preventing network-based intrusions onto your system. The typical user may benefit from this, but huge enterprises could find it problematic. An overall decrease in production might ensue as a consequence of this. Employees may potentially be tempted to use backdoor attacks as a result of this. Due to the fact that these backdoor attacks are not thoroughly analyzed, this might create security issues.

Performance

Some firewalls, especially those that run on your computer's software, might slow it down significantly. The speed of a computer depends on a number of factors, including its processing power and memory. Software firewalls take more RAM and processing power when they are always running in the background. Consequently, the system's performance may be compromised. The system's performance is unaffected since hardware firewalls do not depend on computer resources.

Malware Attacks

The fundamental sorts of trojans can be blocked by firewalls; however it has been shown to be ineffective against additional varieties of malware. Malware of this sort might infiltrate your system by masquerading as legitimate data. As a result, even if your PC is protected by a firewall, you should still use an anti-malware programme. Because there is no other method to get rid of them except by running an anti-malware check.

Complex Operations

Despite the fact that firewall maintenance is made simple for small enterprises, it is not for big corporations. For big enterprises, firewalls need a dedicated team to maintain them. It is their job to make sure that the firewall is secure enough to keep outsiders out of the system.

Challenges in Firewall implication

Traditional solutions, on the other hand, have their limits and inconveniences. These flaws might jeopardise your safety while also draining your financial resources. The burden on your IT staff, network speed, and digital security budget must be considered when deciding whether or not to use a conventional firewall.

Application Awareness Limitations

When it comes to applications, conventional firewalls are unable to delve as deep as NGFWs. The user has the capacity to monitor which programmes are being used throughout the network and the ability to regulate particular use within those applications thanks to NGFWs, which enable both of these features. Traditional firewalls lack the capacity to limit access to this level of detail.

Issues with Network Speed

When it comes to speed, there's a problem. Because traditional firewalls create a bottleneck at the places where data is inspected, this may cause your company to run more slowly and cost you more money. This is not good for companies that anticipate growing and including additional rules, regulations, and security measures.

Logistical Drawbacks

For the most part, conventional firewalls are unable to keep up with the ever-evolving nature of business processes and systems. On addition to their clumsiness, these systems might be difficult to run in the cloud since they need so much management and upkeep.

In addition, it may be time-consuming and costly for IT staff to keep track of policy rules across a large network. This may not only provide opportunities for unauthorised access, but it also has the potential to create problems with the functioning of the system. It's possible that you won't be able to acquire access to the data and individuals you want because you don't have enough control over the security restrictions.

Lack of Evolution Capabilities

Every day, new dangers are discovered in the security environment. It is nearly impossible to keep up with the changes & provide proper help and protection without severely limiting the capabilities of your team or firm. It's costly, time-consuming, and sometimes dangerous to reinstall new solutions on every machine.

Fortinet Can Help

Proactively addressing your company's and network's security risks today may pay off in the future in terms of time, money, safety, and privacy. Additionally, NGFWs might provide you a marketing edge over your rivals who are behind the curve in terms of security.

References

Bavithra.G.R, Mahalakshmi.V, R.Suganya (2018), A Review on Firewall and its Attacks, Vol. 7, Issue 1, January 2018

Damodharan, Prabhat Kumar Srivastava (2018). A Review Paper on Computer Firewall. International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5, Issue 2, February 2018

Dr. Ajit singh, Madhu Pahal, Neeraj Goyat (2013), A Review Paper On Firewall, Vol. 1 Issue II, September 2013

Er. Shikha Pandit, Er. Pritam Kumar, Er. Deepak Malik (2014), Fire-Router: A new secure inter-networking device, Vol. 3, Issue. 6, June 2014, pg.279 – 285

I. Kashefi, Maryam Kassiri, Ali Shahidinejad (2013). A Survey on Security Issues in Firewalls: A New Approach for Classifying Firewall Vulnerabilities.

Khaled Salah, Khalid Elbadawi, Raouf Boutaba (2012), Performance Modelling and Analysis of Network Firewalls, Volume: 9 , Issue: 1 , March 2012

M. G. Mihalos1,*, S. I. Nalmpantis2 and K. Ovaliadis2 (2019). Design and Implementation of Firewall Security Policies using Linux Iptables. Journal of Engineering Science and Technology Review 12 (1) (2019) 80 – 86.

Miss. Shwetambari G. Pundkar & Prof. Dr. G. R. Bamnote (2014), Analysis of firewall technology in computer network technology in computer network security, Vol.3 Issue.4, April- 2014, pg. 841-846

Mohammad Imran, Dr.AbdulrahmanA.Algamdi, Bilal Ahmad (2015), Role of firewall Technology in Network Security, Volume 4, Issue 12 December 2015

Raed Alsaqour, 1 Ahmed Motmi, 2*Maha Abdelhaq (2021). A Systematic Study of Network Firewall and Its Implementation. IJCSNS International Journal of Computer Science and Network Security, VOL.21 No.4, April 2021

Raja Waseem Anwar 1,*ORCID,Tariq Abdullah 2 andFlavio Pastore (2021). Firewall Best Practices for Securing Smart Healthcare Environment: A Review. Appl. Sci. 2021, 11(19), 9183; https://doi.org/10.3390/app11199183

Richa Sharma & Chandresh Parekh (2017), A Study and Its Classification, Volume 8, No. 4, May – June 2017

Roumaissa Khelf; Nacira Ghoualmi-Zine(2018). IPsec/Firewall Security Policy Analysis: A Survey. DOI: 10.1109/SIVA.2018.8660973

Roza Dastres, Mohsen Soori (2021). A Review in Recent Development of Network Threats and Security Measures. International Journal of Computer and Information Engineering Vol:15, No:1, 2021.

Steven Thomason (2012), Improving Network Security: Next Generation Firewalls and Advanced Packet Inspection Devices, Volume 12 Issue 13 Version 1.0 Year 2012

Wojciech Konikiewicz & Marcin Markowski (2017), Analysis of Performance and Efficiency of Hardware and Software Firewalls, Vol. 9, No. 1, pp. 49

Xin Yue, Wei Chen, Yantao Wang (2009). The research of firewall technology in computer network security. DOI:10.1109/PACIIA.2009.5406566

Xinzhou He (2021). Research on Computer Network Security Based on Firewall Technology. doi:10.1088/1742-6596/1744/4/042037

Yuchong Lia, Qinghui Liu (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. https://doi.org/10.1016/j.egyr.2021.08.126.