Securing a Network: How Effective Using Firewalls and VPNs Are?

Chapter · January 2020

DOI: 10.1007/978-3-030-12385-7_71

5 authors, including:

Sonali Chandel
New York Institute of Technology
14 PUBLICATIONS **155** CITATIONS

SEE PROFILE

Securing a Network: How Effective Using Firewalls and VPNs Are?

Sun Jingyao, Sonali Chandel(✉), Yu Yunnan, Zang Jingji, and Zhang Zhipeng

New York Institute of Technology, Nanjing, China
{jsunl9, schandel, yyul8, jzang, Zzhang36}@nyit.edu

Abstract. With the tremendous amount of increase in cyber threats on the Internet, the security of data traveling over a network has become a significant concern for all the netizens. As a result, a large number of Internet users have started using firewalls and VPN (Virtual Private Network) to ensure more protection for their data on the go. Though mostly considered as defenders of our network security, sometimes firewalls and VPNs can also pose some serious threats to its users. Our research focuses on addressing these security flaws by providing a specific illustration of the working principles and performance of the firewalls and VPNs, including the technologies behind them and their benefits, significant potential risks it may bring due to some considerable loopholes in their architecture, and the possible solutions to those security issues. We hope that our research will bring a better understanding of these security issues and their solution to help users and organizations to deal with these security threats and risks in a better way.

Keywords: Firewall · VPN · Network security

1 Introduction

The importance of the Internet and its security was never as great of a concern as it is now because of the amount of data that is exchanged through it 24 × 7. Plenty of threats and risks exist in the cyber world that can affect the network security in a big way. Hacking is one of the most common cyber threats to a network as it allows the hackers aka malicious users to manipulate and attack the loopholes of vulnerable networks and take control of it. Besides the external damage, which mainly reflects the destruction caused by hackers by mostly using malware, virus or DDoS attacks, the threat of resource openness because of using the computer network in a shared environment, cannot be ignored at all. The exponential growth of security risks and dangers that exists outside of a network in the present times can strictly confirm the necessity for people to use and study the firewalls and VPNs so that the attacks can be prevented and detected, and the network can be protected from getting damaged [1].

Firewall is a technology that is used to control the degree of interconnection between different networks. It can prevent the external network from accessing the internal network equipment and network resources using unauthorized ways. This means a firewall can protect internal network and system from potential threats of a

K. Arai and R. Bhatia (Eds.): FICC 2019, LNNS 70, pp. 1050–1068, 2020.
https://doi.org/10.1007/978-3-030-12385-7_71

network attack. This technology fully combines the potential of hardware and software in a computer network and realizes active filtering and screening of potential threats and risks to a network. A firewall usually is the first step to intercept an external attack to accomplish the adequate protection for computer network security [2]. Figure 1 [3] introduce the connection schematic of Firewall, Intranet, and the Internet. The essential features and primary functions of Firewalls are shown in Table 1 [3].

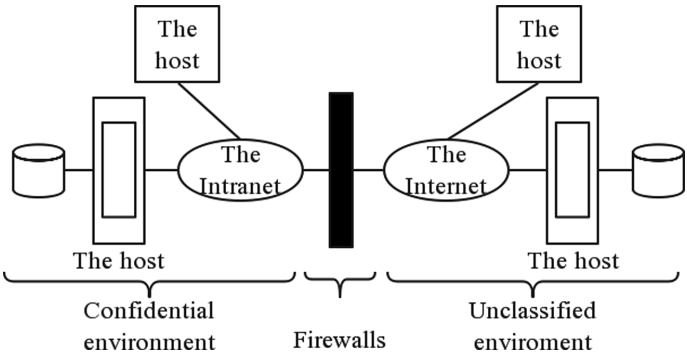

Fig. 1. The connection schematic of a Firewall, Intranet, and Internet

Table 1. The basic features and main functions of a firewall

Basic features	Main functions
All network data between the external and internal networks must pass through the firewall	Firewall is a barrier to network security
Only data flows that conform to security policies can pass through a firewall	It can strengthen network security strategy
The firewall itself should have powerful immunity against attacks	It can monitor and audit network access
	It prevents leakage of internal information

A VPN is a virtual encrypted tunnel between the user and a remote server operated by a VPN service. All external Internet traffic is routed through this tunnel, so our data becomes safe from the data hunters. On the other hand, the IP address of the VPN server becomes the user's IP address, enabling them to hide their actual identity [4].

Firewalls are the gateways to ensure the security of the internal network and VPNs are ways to access the internal network. There are always firewalls in the place where there are VPNs. VPNs can be used with or without firewalls, but they are not recommended to be implemented without firewalls as their primary purpose is to secure the network traffic. A VPN without a firewall makes VPN's encryption function useless. Using VPN with firewall further enhances the security of the Internet and network in general.

This paper aims to provide a detailed study of the security issues and its solutions that the users of a Firewall and a VPN should know. In this paper, we have proposed some suggestions for the safety and security in using the Firewalls and VPNs based on the literature survey that we did for our research. This paper is structured as follows: Related work is mentioned in Sect. 2. In Sect. 3, an overview of the firewall and VPN technologies has been discussed. Section 4 introduces the security issues related to using firewalls and VPNs. The most common threats and attacks in using firewalls and VPNs are discussed in Sect. 5. Solutions for the most common security issues in using firewalls and VPNs has been discussed in Sect. 6. In Sect. 7, the conclusions are drawn, and future work has been mentioned.

2 Related Work

In the past, the authors of [1, 3, 26, 30] focused on the security of firewalls and VPNs, but they did not discuss anything regarding the attacks or threats on firewalls and VPNs. [2] does not provide some specific methods about how to improve the security issues of firewalls. The authors of [9] and [12] present just one case study and focus on one aspect. [9] focuses on an example of a system using both Firewall and VPN. It presents a case of two firewalls with the same configuration in the same network node, which communicate with each other through a direct connection. [12] focuses only on the deep packet inspection technology of firewall. Furthermore, paper [10] is an old study that does not cover the recent problems and various attacks that happens in the cyber world presently. Paper [13] also talks about one model without its realization. In addition, some papers like [17, 19, 20, 24–26] only concentrate on one attack rather than its relationship with the firewalls. The work done by us will not only analyze firewalls and VPNs individually, but we will also compare them together to enhance their abilities in providing more security. It also means that the security loopholes and the solution will be related to both of them. We will analyze the better structure or system concerning the latest products like Web Application Firewall, Secure Web Gateway, and Next Generation Firewall to find the reasons behind them for being considered as safer than traditional firewalls and VPN setups.

3 The Working Principles of Firewalls and VPNs

3.1 The Working Principle of Firewalls

Firewall technology has been developing continuously since its birth. Various kinds of firewalls with different structures and functions are built into a network for getting more defense. Traditional firewall technology falls into three categories, and no matter how sophisticated the implementation of a firewall is, it is ultimately based on the following three technologies.

3.1.1 Packet Filtering

The working principle behind the Packet filtering firewall can be called as a network firewall because it works in the network layer. It usually decides whether to let the data packets pass, by examining the address, protocols, and ports of each packet. Figure 2 shows the principles of Packet filtering. The packet filter can be divided into a static packet filter and dynamic packet filter [5].

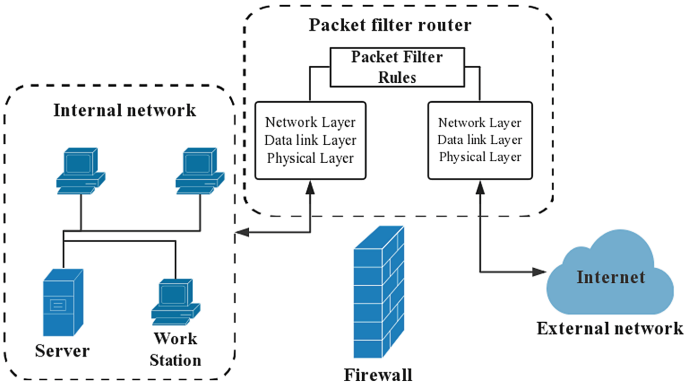

Fig. 2. The principle of packet filtering

- ***Static packet filter***. Static packet filter technology is a traditional packet filter. It decides whether these data packets can be passed according to the IP addresses of these data packets. If attackers set their mainframe IP addresses as legal addresses, they can quickly pass the static packet filtering firewall. Therefore, this kind of firewall is not secure enough.
- ***Dynamic packet filter***. It can automatically apply to create or delete packet filter rules according to dynamic practice application without administrators' intervention. However, the dynamic packet filter technology can only filter against data's IP address instead of the legality of users. It also does not have log records to check which brings enormous difficulties to daily network security management. Therefore, it has been replaced by a new technology called the Adaptive Proxy Protection firewall.

3.1.2 Application Proxy

Application Proxy firewall is also called as an Application Gateway firewall. This firewall participates in the entire process of a TCP connection through Proxy technology. The data packets sent from the inside are processed by the firewall to hide the Intranet structure. Network security experts recognize this type of firewall as the most secure firewall. Its core technology is the proxy server technology. The proxy server refers to the program that represents the client's connection request on the server. When the proxy server gets connection intentions from a client, they will verify the client's request and then handle connection requests through the specific secure proxy

applications. The request is transferred to the real server, which then accepts the server response. After further processing, the proxy will reply to the final client who makes a request. The proxy server plays the role of interconnecting the application of the external network to the internal network [5].

Adaptive Proxy Firewall

Adaptive proxy is a revolutionary technology implemented recently in commercial application firewalls. It combines the advantages of the safety of the Application Proxy firewall and the high speed of packet filtering firewall and improves the performance of the proxy firewall by ten times without losing the security.

3.1.3 Stateful Inspection

Stateful Inspection is an extension of the packet-by-packet filtering process, which tracks individual flows, enabling policy checks that extend across a series of packets [6]. It checks the handshakes in a communication network by exploiting detailed information of the communication protocol. It detects malicious activities by monitoring packet-by-packet connection and predicting the next move based on what happened. This makes it a more advanced tool than other firewalls [7]. These firewalls maintain a table of open connections, inspecting the payload of some packets and intelligently associating new connection requests with existing legitimate connections [8]. With modern firewalls, network administrators can control the network traffic in a more fine-grained fashion.

3.2 The Working Principle of VPNs

The mainstream applications that claim to provide VPN services are using one of the following three techniques [4]:

- **Proxy Server**. A proxy server is like a courier service that is responsible for only transcending the messages. The work of proxy servers is conducted in the HTTP layer and the Socket layer in the Open System Interconnection (OSI) model under most circumstances. Figure 3 explains how proxy server functions.

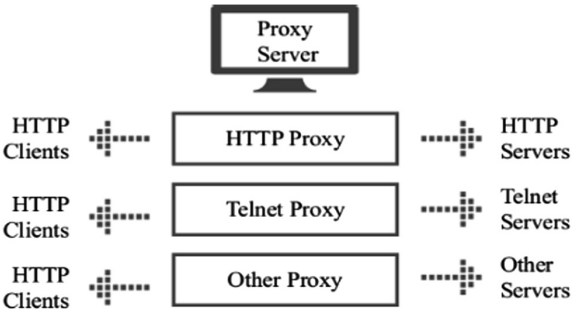

Fig. 3. The working architecture of a proxy server

- **IPSec**. IP Security (IPSec) is the most common method used by the VPN applications. It works in the third layer called the Network layer of the OSI model.
- **SSH**. An encrypted channel needs to be combined with the proxy server to overcome the blocked network. The tool that is used to scale the blocked network called SSH is, in fact, an SSH agent. In the TCP/IP 5-tier model, SSH is the security protocol that applies to the application layer and the transport layer. SSH is a remote shell, an application based on SSL. Although many people use SSH to transmit data, they merely use the SSL proxy function of SSHD software to get this job done.

3.3 Architecture of a System Using a Combination of Firewall and VPN

Figure 4 shows a typical network security architecture based on the combination of both firewall and VPN technology [9]. The system has a master node under which there are large nodes and links between them. Under the big node, there are intermediate nodes, and under the intermediate nodes, there are small nodes. The intermediate node and the small node is only connected with its own upper and lower levels. Between nodes, individual wire connections can also support other ways of connecting people, such as wireless connections. Security between nodes ensures the safe transmission of data through the virtual encryption channel between VPN array devices and VPN receiver devices.

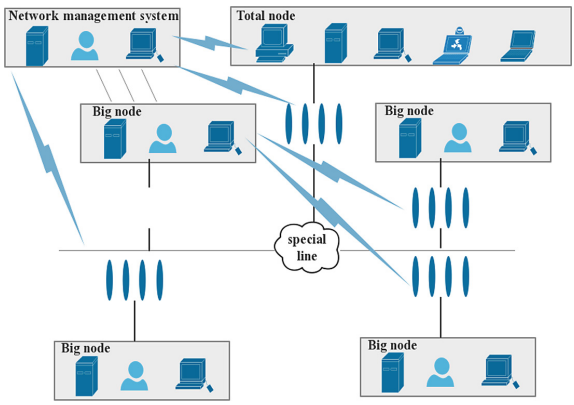

Fig. 4. A typical network security architecture based on firewall and VPN technology

The entire network adopts a network management system to manage, control and report congestion for various security devices, routers, switches and servers in the network, as well as fault management. The network management system will monitor equipment utilization, bandwidth utilization, packet loss rate, etc. Two firewalls with the same configuration are used in the same network node, and they communicate with each other through a direct connection. Under normal circumstances, one is working, which is the primary, and the other is in the backup state.

High availability is achieved through "heartbeat" mode. A direct connection between two firewalls of the same type creates the heartbeat line that uses fixed interval, master-slave equipment to exchange information. When the host accidentally crashes, or network fails, hardware failure happens. Master-slave firewall switch is a working state from the machine instead of the standard work of the host, to guarantee the regular use of the network. Switching process does not require a human operator. They also do not need the participation of other systems. The primary firewall's restore function will automatically return the control to the firewall, to assure the safety of the network. By deploying this network security system with firewall technology as the core, a VPN can realize the secure exchange of confidential information between nodes.

4 Security Issues in Using Firewalls and VPN

Even though firewalls and VPNs are used for protecting or mitigating the external attacks on a network or a system, but they are not full proof. In this section, we will discuss some of the shortcomings in both of these technologies.

4.1 Security Issues of Firewalls

With the increasing severity of network security issues and the continuous development of security defense, shortcomings of firewalls in the security aspect have gradually attracted much attention from security researchers and organizations. Due to the existing loopholes in the firewall architecture, a series of attacks can quickly destroy a network. Analyzing firewall's vulnerabilities and the attacks against it is of great significance to the development and improvement of firewall technology for complete network security.

The most common security flaws of firewalls are as follows:

- **Firewalls may sacrifice some useful network services**. Firewall's "either in or out" feature is bound to shut down some valuable ports due to security problems, sacrificing some helpful network services as well [10]. After the firewall receives network packets at the network layer (including the following link layer), it matches them one by one based on the rules. It then performs prearranged actions if they are consistent, such as allowing or denying packet access. This creates a lot of discomfort and challenges for the organizations and users alike to make sure that the good packets are not misunderstood and blocked as bad ones.
- **Firewalls cannot protect against attacks from internal network users**. Firewalls are the outlet for information between different networks or network security domains. It can control the flow of information in and out of the network according to the set security policy. This prevents the illegal information from flowing into the protected network without affecting the regular access of the protected network to the Internet. This feature of firewall determines that it can only filter packets between internal and external networks but cannot process packets from within the internal networks [11]. This makes it impossible to protect against attacks from internal network users commonly known as insider threats.

- **Firewalls are not secure against software or files with the virus**. Firewall for encrypted SSL stream of data is not visible. This means that the firewall cannot quickly seize the SSL data flow and do the decryption. Therefore, it cannot stop the attack of the application as well as cannot see the application firewall's encrypted data [12]. The firewall can recognize and intercept attack data only when the attacking behavior of the application layer matches the existing attacking behavior of the database in the firewall.
- **A firewall cannot extend depth detection**. It is impossible for a general firewall to extend depth detection that is based on the data package without increasing network performance accordingly. Profound detection capabilities for all network and application traffic require unprecedented processing power to accomplish a large number of computing tasks; including (1) SSL encryption/decryption function (2) Complete two-way payload detection (3) Ensure the normalization of all legitimate traffic (4) Extensive protocol performance. These tasks cannot run efficiently on standard PC hardware [13].

The weaknesses of five general kinds of firewalls are shown in Table 2 [13].

Table 2. The weaknesses of five general kinds of firewalls

Firewalls	Weaknesses in the security system
Packet filtering firewall	Hard to configure
Status/dynamic detection firewall	Delay in the network connection
Web application firewall	Limited range of user system
Network address translation firewall	Unable to mitigate the internal attacks and threats
Personal firewall	Unable to monitor and control multiple communication

4.2 Security Issues of VPNs

Any company or organization that implements a VPN to ensure their network security still cannot ignore the risks and threats that can destroy or sabotage their network without them even knowing or realizing it. The most common risks can be seen in Table 3.

Table 3. The risks involved in using a VPN

1	Securing against lateral network movement
2	Securing and connecting to cloud-based infrastructure
3	Blocking malicious insiders, over-privileged users, and compromised third-party access
4	Preventing malware from proliferating across the network
5	Efficiently integrating with business processes and identity management systems

IPSec VPN: This VPN has a robust communication protocol and encryption algorithm, so its security issues mainly come from its client's attacks [14].

- ***The local security configuration is not perfect***: The users control the local security configuration of the VPN's client-side themselves. It means there might be some security risks caused by human factors. For example, some clients may keep the license certificate on the local device. Once the attacker gets the control of these devices, they can open a VPN channel without even needing a login name and the password and bypass the authentication process altogether.
- ***Stealing VPN security information***: Attackers can steal VPN security information by using social engineering methods such as phishing. This security information includes the IP address of the VPN client, configuration parameters, user license certificates, etc. The attacker can forge a communication identity and pose a threat to the security of a VPN by using this security information.
- ***The internal security of VPN is weak***: The security protection requirements for trusted users are relatively low after VPN is successfully connected. Because there is no attack prevention strategy in the tunnel that decreases the security risk within the VPN.

SSL VPN: This VPN does not require specialized client software, but they use web browsers for its implementation. Therefore, the security threats of SSL VPNs are mainly focused on browsers and servers.

- ***Security problems caused by incorrect system operation***: If the user does not close the SSL VPN by logging out at the end of the browser and the server process, it may keep the SSL VPN server process open. The attacker can use this situation to bypass authentication and access the VPN, which brings a high-security threat to the VPN system.
- ***Malicious attacks on identity authentication***: SSL VPNs allow users to log on to the VPN system from any location through a browser. This increases the risk of leaking security information such as login id and passwords, especially when they log in from public places.
- ***The virus infects the internal network through the tunnel***: SSL VPN remote users can use any location of any client remote login within the enterprise network. Once the viruses at client-side connect to the internal network, the infected file will be able to use the SSL VPN tunnel to invade the internal network. At the same time, due to the limitations of the internal network boundary of the firewall, it cannot prevent the transmission of infected software or files effectively. As a result, the virus can infect the internal network through the tunnel.
- ***The security risks of the Web server itself***: Most of the SSL VPN system use Web server as its underlying platform. Therefore, the potential safety hazard of the Web servers, such as the back door or unauthorized leaks will also bring serious security problems to the SSL VPN system [14].

MPLS VPN: This VPN has adopted a strict routing information isolation mechanism. The security of user information transmission is guaranteed by using

MPLS VPN. However, as a technology based on IP communication, its transmitted information is not encrypted and authenticated, so there are still some security problems that exist in MPLS VPN [14].

- ***Attacks against VPN routing devices***. This attack usually occurs during the routing information release phase. The attacker disguised as an edge device establishes a session with the server equipment to connect and exchange routing information. This will cause the disclosure of the VPN's internal routing information. The attacker can also forge or tamper with the routing information to spread the user's data in the wrong direction to eavesdrop and steal the user's personal information.
- ***Security threats from the Internet***. In the case of users accessing the Internet through MPLS VPN, the attackers can attack the network by traditional attack means such as IP source address deception, session hijacking, and planting Trojan horse in the network. The user's data flow will be viewed, modified, forged and deleted by the hackers without their knowledge.

4.3 The Loopholes in Using Firewalls with VPNs

The firewalls with VPNs can provide a virtual private network on the unsafe Internet through the VPN function. Therefore, it can guarantee the security of the confidential data of the enterprise when the remote access happens. However, at the same time, there will be many loopholes in using this arrangement of firewalls with VPNs. The loopholes in using firewalls with VPNs are shown in Table 4 [15].

5 Using Firewalls and VPNs: The Most Common Attacks and Threats

5.1 The Attacks and Threats of Using Firewalls

Generally, the most common attacks happen to the Packet Filtering Firewalls and the Status/Dynamic Detection Firewalls [16]. In Table 5, we list the attacks that could corrupt the firewall security.

The IP Spoofing Attack. It can easily make use of a legal address from the ordinary users. Attackers can avoid an authentication process provided by the firewall using this way and hide. Also, when attackers use spoofing attack, this behavior of hackers will make the log, and NAC (Network Access Control) will point to the wrong person when used to track down the attackers. This kind of MAC (Medium Access Control) attack is straightforward to create and can facilitate a variety of advanced attacks [17].

Denial of Service (DoS). Unlike many other attacks, DoS attack is purely malicious because the hackers gain nothing personal from the attack. They attack the user's system with the aim of depriving the system's working ability. To overload the victim network, the hackers send large data that floods the system. To send data, they usually need to know the IP address of the targeted network, but firewalls with VPN can hide the IP address and block the malicious data package.

Table 4. The loopholes in using firewalls with VPNs

Contents	Loopholes
Firewall rule virtual test	No work can detect the effect of the configured strategy
Intranet service permissions settings	No function
Quality of service loan allocation	In general, there is no VPN within QoS permissions
Multi-line superposition and backup of firewalls and VPNs	Only double backup
VPN maximum transmission unit	Manually modify maximum transmission unit based on the Internet environment
VPN dynamic IP addressing	We can only use dynamic domain name system and other third party's solutions. People control the use
Hardware binding authentication	No function. Only username, and password
USB key security policy storage and exchange	Only security certificates can be stored, and clients still need professional staff
Support for mobile users	Not supported or incorporated into through the PPTP protocol with little support and inadequate security
Protocol, encapsulation, and compression	Standard IPSec, using the network address translation standard. User datagram protocol encapsulation ensures that data is correct with other check fields. One by one packet encapsulation and no compression technology lead to low bandwidth utilization
VPN performance	Using low-end hardware components. Single channel connection speed is slow. The number of access support is limited, and performance is unprotected
Support for VPN channels	Unable to support a large number of branches and client access, network performance significantly decreased when there are more nodes
Software	No software VPN gateway
Convenience of implementation	It is complicated that it needs professional staffing
Support for access methods	It can only access with Internet IP and does not support new access modes such as cell broadband, WLAN, and GPRS

Table 5. The most common attacks on firewall

Types of firewall	Attack
Packet filtering	IP spoofing attack
	Denial of service
	IP fragmentation attacks
	Trojan attacks
Status/dynamic detection firewall	Protocol tunnel attack
	Passive FTP
	Rebound Trojan attack

IP Fragment Attack. In an IP fragment package, only the first fragment has the information of the TCP port. When the package is transmitted through the Packet Filtering Firewall, the firewall only checks the first fragment to decide whether to let it pass. In this case, the attacker can cheat the firewall by sending a legitimate first IP fragment, and then the rest of the malicious fragment can pass through the firewall and cause a threat to the network security [18].

Trojan Attack. It is the most effective attacking method to Packet Filtering Firewall because once the Trojan is installed inside the network, there is nothing a firewall can do to stop it. The reason is that the Packet Filtering Firewall usually only filter the packet at the lower port (1-1024) and most Trojan attacks through the higher ports [19].

Protocol Tunnel Attack. The attack of the protocol tunnel is similar to the idea of a VPN, and the attacker hides some malicious attack packets in the head of some of the protocols, so it can penetrate the firewall system and attack the internal network [20].

Passive FTP. It solves the issue of an FTP client's firewall blocking incoming connections. "PASV" is the command that is used by the FTP client to let the server know that it is in passive mode. This is a preferred mode for FTP clients behind a firewall and is often used for web-based FTP clients and computers connecting to an FTP server within a corporate network [21].

Rebound Trojan. The internal network's rebound Trojan periodically connects to a host controlled by an external attacker. Since the connection is initiated from within, the firewall considers it as a legitimate connection, causing the blind area of the firewall. A firewall cannot distinguish between a Trojan's connection and a legitimate connection. The limitation of this attack is that the Trojan must be installed inside the network first [22].

5.2 The Attacks and Threats to a VPN

Choosing a VPN is a good idea to get protection against a network, especially when it is a public Wi-Fi. However, use of a VPN can sometimes be a threat to security and bring some risks as well. VPN establishes a channel between the user and the server, so the user's trust in the VPN provider is essential because the provider can see and record all the data and can even alter the content. If a VPN is not configured correctly, a hacker might be able to access the user's local LAN directly, which is worse than being exposed to public Wi-Fi. For example, GoGo, a VPN provider was accused of using fake YouTube certificates that could leak users' passwords [23].

- **Man in the Middle Attack (MITM)**. Some VPN providers adopt pre-shared key for their users, and that can lead their users to be caught up in a Man in the Middle attack (MITM). In the MITM attack, there are two endpoints of victims, and the attackers are third-party. The attackers can access the communication channel between two endpoints and manipulate the messages [24]. MITM attack aims to compromise the following three targets [25]:
  - *Confidentiality*: It can be achieved by eavesdropping on the communication.
  - *Integrity*: Attackers can intercept the communication and modify messages.
  - *Availability*: By intercepting and destroying messages or modifying messages, attackers can make one of the party to end communication.

- **Hacking or Eavesdropping**. It includes physical access or listening to the devices that support VPNs. This can happen if someone loses their laptop or mobile device, which supports VPNs. Most VPN applications are not configured for the best security model, and the local license is stored in the device itself. In this case, the hackers can access the VPN channel without entering a password.
- **Unauthorized Access to the VPN Data**. Obtaining secure information from a VPN is a third way in which VPN security may be corrupted. This security information includes IP addresses, configuration parameters and user license certificates for a VPN terminal. Access to this information may come from the insiders who know the specifics of a VPN, such as, people who have left or have been fired from the company. Most networks do not change frequently, and VPN connections remain in the same state for a long time. Therefore, people leaving the company have many opportunities to learn about specific ways to access the VPN. This security information can also be obtained through other social engineering methods, such as phishing or vishing.
- **Exploit Vulnerabilities in the System**. A possible defect in the firmware itself or some other weakness of the authentication system can be exploited, such as, malicious spoofing or redoing SSL authentication. It would even be possible for a hacker to use these well-known vulnerabilities in the VPN concentrator to crash the authentication system to invade the target system [5].

6 The Solutions for the Security Issues of Firewalls and VPN

6.1 The Solutions for the Security Issues of Firewalls

The Immune-Based Firewall System. After an intruder bypasses a firewall, they must control the firewall system or break the work of the firewall system. To achieve this goal, they must destroy the vital information of the firewall. Therefore, the immune-based firewall system security model centers on the critical information files of the firewall and uses the change of these files as a means to determine whether there is an intrusion. Because the intrusion is the "differences" in the firewall system.

The critical information file is the body of the firewall system. If an intruder destroys the body of the firewall system, the firewall will find and resist it to protect the critical files that are on record. It will also record the destruction and control of the network communication. The basic structure of the system security model is shown in Fig. 5 [26], centered on the critical information file of a firewall and file information database. It also uses the immune subsystem as the core to build a relatively perfect firewall system. However, when it comes to the actual application effect, the filtering mechanism of the firewall against these attacks is still not perfect yet, and there is no effective strategy to solve this problem. An ideal firewall filtering mechanism and the security policy model is shown in Fig. 6 [26].

Multi-Stage Filter. The Multi-stage filter uses multilevel filtering in the firewall to filter out all source routing packets and the fake IP sources at the level of packet filtering. The multi-stage filter is a technology that is now widely used by firewalls as

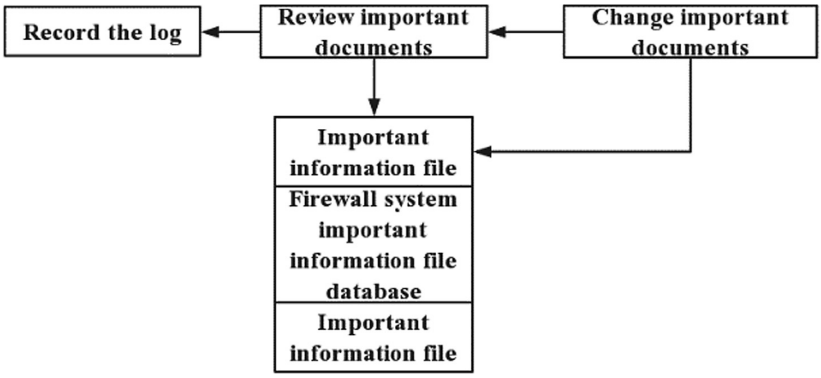

Fig. 5. The model of immune-based security firewall

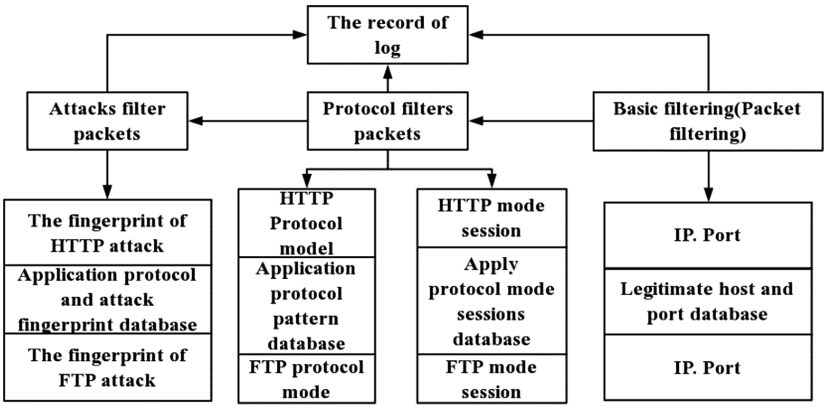

Fig. 6. Protocol-based firewall security policy model

packet filtering to efficiently help the protection of firewalls. This method is evident in the layer and can expand many new contents from this concept.

Next Generation Firewall. Next-Generation Firewall (NGFW) is the latest buzz in the firewall market at present. Through in-depth insight into users, applications, and content in network traffic, and with the help of a new high-performance single-path heterogeneous parallel processing engine, NGFW can provide users with active application layer integrated security protection. It can help users to conduct business safely and simplify their network security architecture. Application recognition is the most critical technology in the route. The technical route of NGFW is shown in Fig. 7 [27].

Secure Web Gateway. Secure Web Gateway (SWG) is a kind of product solution for Internet exploitation. It has the functions like URL filtering, malicious code protection, control functions, and the application control functions including the Web functions. This means it can enforce the enterprise's Internet access strategy while protecting it from the security threats. Most of the mainstream SWG products also

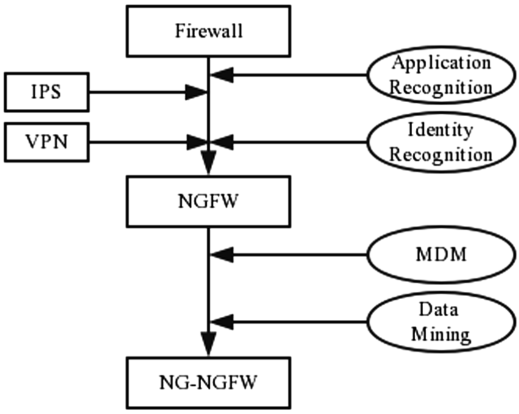

Fig. 7. Technical route of NGFW

provide the user identification and the DLP (Data Leakage Protection) function on this basis. Some company such as Intel uses SWG to protect their company's security. Figures 8 and 9 shows the structure of SWG firewall [28].

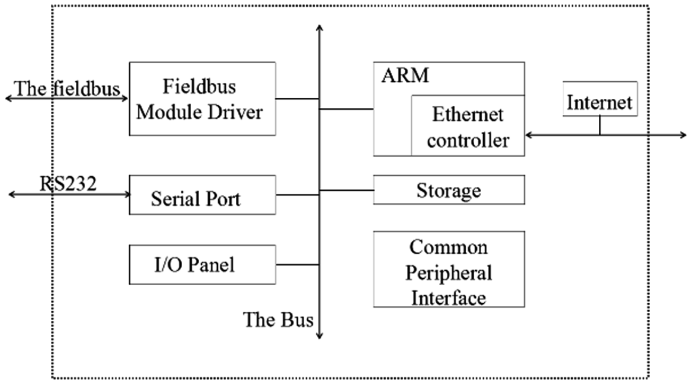

Fig. 8. The hardware structure of embedded gateway

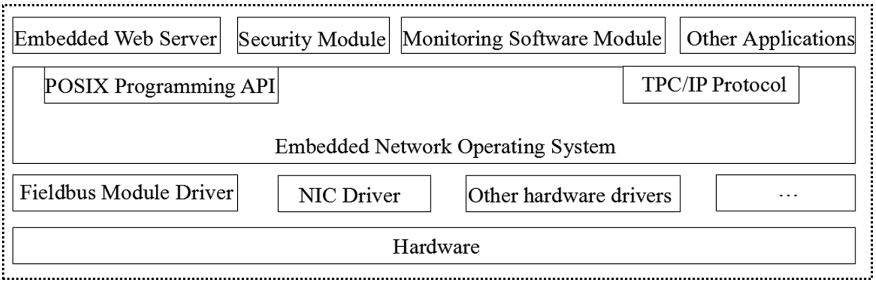

Fig. 9. The overall structure of gateway software

Web Application Firewall. Web Application Firewall (WAF) is mainly used to strengthen protection against web-specific intrusion methods such as DDoS attacks, SQL injection, XML injection, XSS, etc. WAF can be divided into front-end capture, rule setting and monitoring (brain), regulation action (monitoring or blocking), log storage/monitoring display, and corresponding processing unit as shown in Fig. 10 [29]. Currently, there are three types of WAFs in the market, namely: Hardware Web firewall, Web protection software and Cloud WAF.

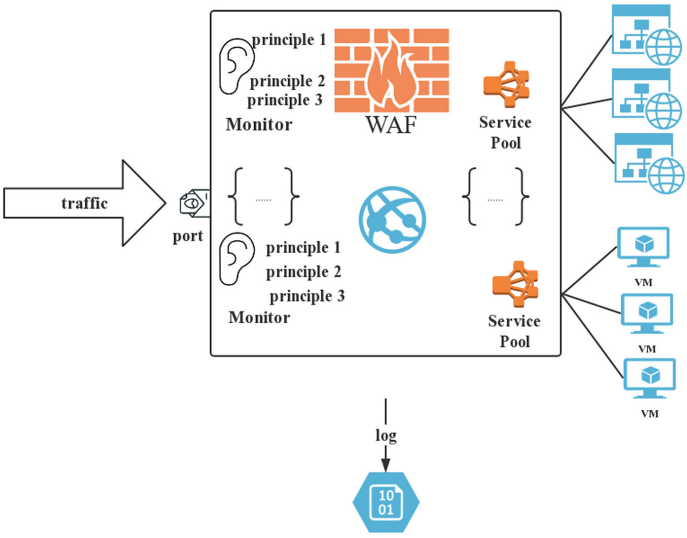

Fig. 10. WAF working principle

6.2 The Solutions for the Security Issues of VPNs

Wi-Fi wall. It is a useful technology to protect the VPNs when the user connects to the Wi-Fi. This technology can monitor the Wi-Fi traffic, and it can constantly check if there are attacks. The Wi-Fi wall will disconnect the Wi-Fi once an attack is detected.

Authentication service. The VPN service providers need the authentication service to help them to protect the identity information about the potential end-users [30].

Access control. This service can maintain the security and prevent the use of unauthorized VPN service features and access to the unauthorized resources [30].

Data integrity and confidentiality. This service can keep the integrity of information, prevent the leakage of information, and counter threats. The cryptographic hardware can protect the integrity and confidentiality of management data [30].

VPN audit requirement. The suitable auditing system is necessary to detect potential abuse, since the present security service and security mechanisms may be compromised or bypassed. Therefore, the hackers may gain the unauthorized access

and damage the VPN protected by them. Enumerating and understanding the VPN service behavior is necessary for providing enough information for studying the VPN auditing requirements [30].

VPN firewall. VPN Firewall is a kind of firewall that is installed at the server end or the front of a VPN server. It is configured with the filters only to let the VPN specific packets to access the network when installed at the server end of the VPN. However, when it is installed at the front of a VPN, it will only allow the tunnel data on its Internet interface to access the server [31].

HAIPE security gateway. In this model, VPN client edge device is intended to use network hardware encryption device HAIPE as a security gateway to protect the communication between VPN client sites. It is shown in Fig. 11 [32] that the VPN user network consists of A and B stations. The edge of station A is deployed with the HAIPE_A security gateway, and the edge of station B is deployed with the HAIPE_B security gateway. HAIPE_A and HAIPE_B are equal and establish ESP (Encapsulating Security Payload) encrypted tunnel between them, which let any information stream between station A and station B be protected by the ESP encrypted tunnel. Only the flow of the network to peer protection or the flow of the network from the peer protection network will pass through the gateway, and the rest of the traffic is stopped by the secure gateway of ESP encrypted tunnel.

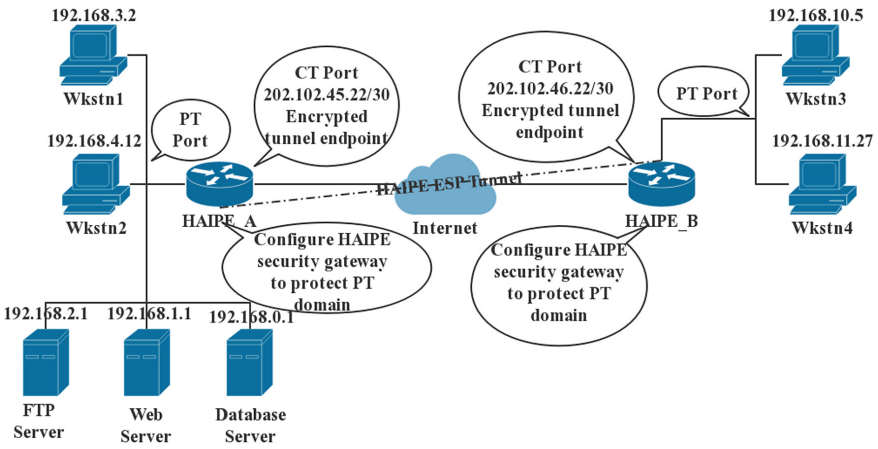

Fig. 11. Diagram of HAIPE security gateway protecting plain text (PT) domain communication

7 Conclusion and Future Work

As a result of this study, we have concluded that the potential threats and risks to the Internet and Intranet will keep growing and so does the development of firewalls and VPNs. With the increased implementation of technology in almost all possible domains of cyberspace, the security and protection of a network will need more attention with time. We also realized that the gap between the potential threats and the risks to these

systems are growing exponentially and the present-day firewalls and VPNs are not full proof yet. This results in defeating their purpose sometimes.

We also concluded that it is not easy to judge firewall or VPN against each other because there are many types of firewalls and VPNs available in the market and each one of them has its advantages and disadvantages. The kind of users and their demands regarding how much safety they want in their network and how much budget do they have to get what they need in a firewall or VPN is also the key in its implementation. A combination of firewalls and VPNs can always provide more security to a network than using them individually. The users also need to keep in mind that both VPNs and firewalls have quite a few security flaws and there are various solutions available to avoid these loopholes. Our advice is to consider the application environment and the user's expectation of performance carefully when choosing a firewall or a VPN or both for creating a secure network system. However, there are still some parts that we did not cover in this paper. Our following plan for this topic is to study some methods that can deal with the security issues both related to firewalls and VPNs since we have already researched the security threats, risks, and issues that both firewalls and VPNs have.

In all, we hope that our work can be used as a reference by the organizations and individuals when it comes to the solutions for the loopholes, threats, and risks related to a firewall and a VPN. Further study needs to be done to make a unified model of a secure firewall and VPN to fight the attacks and the attackers and save the data and the network from being destroyed or breached.

References

1. Ma, L., Liang, H.: Application of firewall technology in computer network security. Comput. Knowl. Technol. **10**, 3743–3745 (2014). Print
2. Jiang, C.: Research on computer network security technology and firewall technology. Ability Wisdom 235 (2017). Print
3. Su, J., Yuan, J.: Firewall technology and its development. Comput. Eng. Appl. 147–149 (2004)
4. Zhang, Z., et al.: VPN: boon or trap? A comparative study of MPLS, IPSec, and SSL virtual private network. In: ICCMC 2018 (In Press)
5. Sun, J., Wei, J.: Computer Network Technology and Application. Xi'an University of Electronic Science and Technology, Xi'an, China (2010)
6. Stateful-inspection firewall: the Netscreen way. http://www.netscreen.com/products/firewallwpaper.html
7. Li, S., Tørresen, J., Sorensen, O.: Exploiting Stateful Inspection of Network Security in Re-Configurable Hardware
8. Suehring, S.: Linux Firewalls: Enhancing Security with Nftables and Beyond, Illustrated edn, p. 25. Pearson Education (2015). ISBN 0134000021
9. Successful case: Hanbo firewall to build a safe and efficient enterprise Intranet. Network World 2011-12-12 (021) (2011)
10. Qing, Y.: Shortcomings and improvements in firewall security. Sci. Technol. Eng. **14**, 1009–1012 (2005)

11. Sun, K.: Concrete application of firewall technology in computer network security. Sci. Technol. Econ. Guide **17**, 38 (2017)
12. Wang, D.: Research on Deep Packet Inspection Technology of Firewall. Xi'an University of Electronic Science and Technology (2005)
13. Zhang, T.: Design and Implementation of Firewall Based on Content Filtering Software. University of Electronic Science and Technology (2012)
14. Security analysis of VPN technology, 19 Sept 2014. Web. http://sec.chinabyte.com/368/13082868.shtml
15. Comparison between professional VPN and firewall with VPN. Web. https://wenku.baidu.com/view/6e89ab1055270722192ef791.html
16. Network security: a simple guide to firewalls. In: Network Security, pp. 2–3 (2000)
17. Yadav, A.S.S., et al.: Prevention of spoofing attacks in wireless networks. In: International Conference on Computing Communication Control and Automation, pp. 164–171. IEEE (2015)
18. Hollis, K.: The Rose Attack Explained. Retrieved on 2013-11-25
19. Sakurai, S., Ushirozawa, S.: Input method against Trojan horse and replay attack. In: IEEE International Conference on Information Theory and Information Security, pp. 384–389. IEEE (2010)
20. Chen, D., Wang, P.: Study and implementation of tunnel attack in MANET. Comput. Eng. **33**(9), pp. 140–141 (2007)
21. What is PASV FTP (passive FTP)? 13 Jun 2018. Web. https://www.lifewire.com/definition-of-passive-mode-ftp-816441
22. Zhao, T.F., et al.: Detecting rebound port Trojan based on network behavior analysis. Netinfo Secur. (2011)
23. VPN helps you scale the wall? Let's put our privacy first, 6 Jun 2016. Web. https://www.jb51.net/hack/471867.html
24. Conti, M., Dragoni, N., Lesyk, V.: A survey of man in the middle attacks. IEEE Commun. Surv. Tutor. **18**, 2027–2051 (2016)
25. Khan, M.M., Bakhtiari, M., Bakhtiari, S.: An HTTPS approach to resist man in the middle attack in secure SMS using ECC and RSA. In: 2013 13th International Conference on Intelligent Systems Design and Applications, pp. 115–120, Dec 2013
26. Yang, Z., Cheng, Q.: Research of immune-based technology for the firewall system security. Microcomput. Inf. **21**, 9-3
27. Network behavior management and the next generation of firewalls, SWG relations. Web. https://jingyan.baidu.com/article/cbf0e50095f63a2eaa2893cc.html
28. Zhao, Y., Du, Y.: Design and implementation of embedded secure web gateway. Comput. Eng. Des. **27**(4) (2006)
29. Sahin, M., Sogukpınar, I.: An efficient firewall for web applications (EFWA). In: 2017 International Conference on Computer Science and Engineering (UBMK), pp. 1150–1155 (2017)
30. Boukari, N., Aljane, A.: Security and auditing of VPN. In: Proceedings of Third International Workshop on Services in Distributed and Networked Environments, pp. 132–138, 6 Aug 1996
31. VPN firewall. Techopedia. 28 Jun 2017. Web. https://www.techopedia.com/definition/30753/vpn-firewall
32. Dian, A.: Security research and improvement of mainstream VPN technology (2009)