Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 2, No. 2, 2022

Research on firewall technology and its application in computer network security strategy

Peihong Wang

Honghe Hani and Yi Autonomous Prefecture Public Resources Trading Center, Mengzi 661199, Yunnan, China
Email: 501376056@qq.com

Abstract: Computer network is a double-edged sword, which brings convenience to people's life and work, but also brings hidden dangers, and even suffer losses, especially in recent years, the unscrupulous elements use computer network vulnerabilities to steal important data and seek improper benefits, which has caused serious network security problems. Among them, focus on the application of firewall technology can effectively prevent and supervise the existence of network security threats in the computer, control access to the Internet, and ensure the safe operation of computer networks. In this paper, from the importance of firewall, we explore the main functions, technical principles, architecture and use scenarios of cloud firewall, and propose the application in the computer network security strategy for reference.

Keywords: Computer; Firewall; Network security.

1. Introduction

With the vigorous development and wide application of computer technology, the application of information network technology represented by the Internet is becoming increasingly popular, and the application field has gradually expanded from small business systems to large and medium-sized key business systems. The computing model has also undergone a dramatic change from the initial centralized delivery to large processing machines, to network-based distributed task processing, to today's on-demand cloud computing approach, with security increasingly becoming an important factor affecting network effectiveness. According to a report released by the FBI, victims of BEC fraud lost $2.4 billion in 2021, while the average cost of data breach in 2022 has exceeded $4.35 million, a record high, and cybercrime has become the largest type of business crime; in China, cybersecurity is closely related to national security, and huge economic losses are incurred every year due to hacking and virus damage. How to strengthen network security awareness, improve network security skills, build a secure network management system, and efficiently protect the safety of information and property in the network, has become urgent. Among many measures, the most significant is the application of firewall technology, which not only provides a safe and reliable operating environment for computer networks, but also protects against external intrusion and influence, and is gradually recognized by people.

2. The importance of firewall

Firewall is a separator, limiter and analyzer, which has strong anti-attack capability.

2.1. Preventing the leakage of important information

In the current era of big data, people's means of communication and data transmission have been greatly developed, and more and more personal information, enterprise information, government information and other data are flooded into computer networks or stored on the cloud through computer networks, which brings great convenience to people's production, life, work and management, but at the same time poses a greater challenge to computer network security. In this process, firewall becomes a barrier to protect data information and provides a strong guarantee for computer network security. With the development of mobile communication technologies such as 5G, the role of firewalls is reflected in how to prevent a large amount of personal data and private information from being leaked or illegally stolen in the popularization of mobile Internet applications.

2.2. Purify the cyberspace environment

With the use of computers and a large number of mobile devices, people are coupled to computer networks more and more, and at the same time there will be more risks of malicious access to user information and data, there will be many induced malicious invasion of websites or applications, it is difficult for non-professional users to identify their malicious behavior from the surface, such means as this abound in the current computer network environment, seriously disrupting the current computer network environment is seriously disturbed. In this environment, setting up directional firewalls for network use and configuring corresponding filtering policies can largely assist users in scientifically identifying fake websites, inducing malicious network attacks and other behaviors, thus purifying the cyberspace environment.

2.3. Real-time monitoring of network conditions

As people's daily lives become more and more dependent on computer networks, it is extremely insufficient to protect users' important data or private information by simply conducting passive network defense. Therefore, the use of firewalls for real-time detection of network behavior or events during network transmission enables active defense to protect the personal information and private data of network users in a complex network environment. The use of firewalls also allows real-time monitoring of various behaviors in the process of network transmission, so as to make the decision

of allowing or denying access, which largely improves the security level of computer networks and avoids or reduces the losses brought to users by data and information leakage.

3. Firewall technology

Firewall is a control device for two different networks to realize mutual access, and it is an important security device for network security to realize access control of private network and public network according to the artificially formulated control policy. The main role of firewall is to shield the internal information, structure and operation of the protected network, and to monitor and restrict the data flow across the network. Firewall technology is an applied security technology based on modern communication network technology and information security technology, which is the most recognized and widely used in the current network security field. As shown in Figure 1

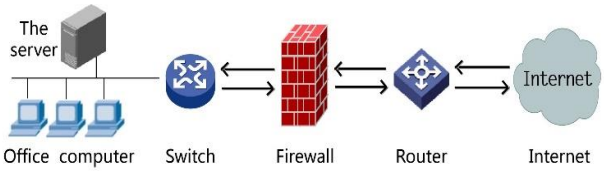

Figure 1. Diagram of the location of the firewall in the network

3.1. The main functions of firewall

The technology of firewall is very mature, and there are many kinds of products, but the role is basically the same. The overall function is to achieve isolation and security control between two connected networks, and the main functions are six points.

3.1.1. Monitor and restrict access

In response to the insecurity of network attacks, the firewall takes control of packets entering and leaving the internal network and external network, monitors the status of packets on the network in real time, and analyzes and processes these states to detect abnormal behavior and take linked preventive measures in a timely manner to ensure the security of the network system.

3.1.2. Control protocols and services

In response to the insecurity of the network itself, control measures are taken for relevant protocols and services, allowing authorized protocols and services to pass through the firewall, while unauthorized protocols and services are refused to pass through the firewall, effectively shielding insecure services.

3.1.3. Protection of internal network

In order to prevent the security impact caused by system vulnerabilities, etc., the firewall adopts its own security system, and also detects system vulnerabilities and network intrusions inside the network in a timely manner through technologies such as vulnerability scanning and intrusion detection, and protects the application service systems in the internal network through restrictions on abnormal access.

3.1.4. Network Address Translation

In network interconnection, since different addresses are used, it is necessary to implement address conversion on the firewall to convert the own address of the internal network to the public address of the external network. After implementing address translation, the internal structure of the protected network can be hidden and network security can be improved to some extent.

3.1.5. VPN function

Through VPN (Virtual Private Network), LANs or private subnets distributed in a certain unit can be organically connected into a whole through the Internet, which not only saves dedicated communication costs, but also provides security for information sharing.

3.1.6. Logging and Auditing

Firewall provides reference for the operation optimization of network management, important intelligence information for the development of attack prevention strategy, and an important basis for tracing the occurrence of abnormal things by logging all the requests for access.

3.2. Technical principle of firewall

There are two main technologies used in firewalls, one is a firewall working at the application layer and the other is a firewall working at the network and transport layers. Firewalls working at the application layer implement access control for applications, for example, allowing access to some applications (e.g. HTTP) and blocking access to others (e.g. FTP); firewalls working at the network and transport layers implement control over packets passing through the network, for example, allowing some packets to pass and disallowing others.

3.2.1. Packet filtering firewalls

The packet filtering firewall works at the network and transport layers and is installed between the two networks that need to be controlled. The packet filtering module checks items such as source IP address, source port number, protocol type, TCP header flag bits, etc. It inspects the packets passing through at the entrance and exit of the network and decides whether the packets are allowed to pass or not according to the pre-set security access control policy (Access Control List - ACL) rules. The filtering of packets is bidirectional, handling both packets from the external network to the internal network and packets from the internal network to the external network. When configuring the firewall, filtering rules must be manually formulated in advance to determine your own security policy. The packet filtering firewall can also make judgments based on flag bits in TCP, for example, the extended ACL of Cisco routers supports the established keyword to determine if the ACK or RST is set in TCP packets, and thus whether to respond to internally initiated session messages.

3.2.2. Stateful Inspection Firewall

The stateful inspection firewall, also known as the dynamic packet filtering firewall, has a stateful inspection module that creates a stateful inspection table consisting of two parts: a filtering rules table and a connection status table. If a packet enters, the stateful inspection firewall first analyzes it according to the filter rule table to decide whether to allow it to pass. According to the relevant information in the filtering rule table, if it is allowed to pass, the stateful firewall lets it pass and analyzes the relevant information of the packet to establish a connection in the connection status table for that communication process. After that, when subsequent packets in the same communication process enter the firewall, the stateful firewall will no longer detect them, but match them directly through the stateful connection table, and since subsequent packets have the same status as those already Since the subsequent packets have the same connection information as the packets already allowed through the firewall, they will be allowed to pass directly. As you can see,

this type of firewall is very useful for preventing "IP spoofing" attacks.

3.2.3. Proxy firewalls

Proxy firewalls are proxy servers and application gateways that work at the application layer and are controlled by the application, allowing access to one application and preventing others from passing through. Proxy servers are implemented using hosts with dual NICs, usually running between two networks, and are intermediaries between clients and real servers, isolating direct communication between internal and external networks. Access to external network servers by clients of internal networks becomes access to external network servers by proxy servers, which are then forwarded to internal clients by proxy servers. The proxy server is like a server to the internal client, and it is like a client to the external network server, which successfully achieves the isolation of computer systems inside and outside the firewall, and reduces the possibility of being attacked because the external network cannot directly contact the internal network to be accessed.

In addition, adaptive proxy technology is a revolutionary technology implemented in recent years in firewalls for commercial applications, combining the security of proxy firewalls and the high speed of packet filtering firewalls, etc. It can increase performance by at least 10 times without losing security, and has two basic elements: adaptive proxy server and dynamic packet filter. The initial security checks of an adaptive proxy firewall still occur at the application layer, and once the trusted identity is authenticated, a secure channel is established and packets can pass directly and quickly through the network layer.

3.3. Firewall architecture

The architecture of a firewall refers to the physical location of the firewall in the network and its relationship with other devices in the network. Only by choosing and configuring the firewall topology reasonably can it have the best security performance. There are four common architectures of firewalls as follows.

3.3.1. Dual-homed architecture

This architecture is actually a firewall configured with two network port host systems, where one network port is connected to the internal network and the other port is connected to the external network, and the host controls whether packets can pass through the port between the two networks through control policies. Since the dual-homed host is the transmission channel for communication between the two networks, the dual-homed host may become a bottleneck for communication when the network communication volume is large, so the dual-homed host should be selected with good performance. As shown in Figure 2

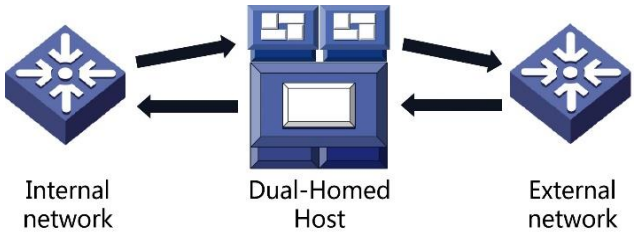

Figure 2. Schematic diagram of dual-homed host structure

3.3.2. Single-segment firewall architecture with a shielded router

This architecture consists of a shielded router and a bastion host. The bastion host has only one NIC connected to the internal network and becomes the only site accessible to the external network. The shield router makes all incoming information must be sent to the bastion host first and only accepts information from the output of the bastion host. All hosts on the internal network can also only access the bastion host, and the bastion host becomes the bridge between the hosts on the external network and the hosts on the internal network. The blocking router denies the internal network hosts direct access to the external network, and requests from the internal network hosts to access the external network must be proxied through the bastion host. To ensure that the above fixed packet path is not changed, the shield router should perform the necessary configuration, such as setting up static routes.

3.3.3. Single DMZ firewall architecture

DMZ is the abbreviation of "demilitarized zone", the Chinese name is "isolation zone", also known as "demilitarized zone". It is a buffer zone between the non-security system and the security system to solve the problem that the external network cannot access the internal network server after installing the firewall, which is not conducive to the deployment of Web, E-mail and other network services. This buffer zone is located in a small network area between the internal network and the external network, in which some server facilities that must be made public can be placed, such as corporate Web servers, FTP servers and forums. With such a DMZ zone, the internal network is more effectively protected, as this network deployment provides an additional barrier similar to a security gate to attackers than a typical firewall solution.

Single DMZ firewall structure of the shield router and the bastion host connection to be on the same network segment, to ensure that data across the firewall must first pass through the shield router and the bastion host these two security units, single DMZ firewall structure of the bastion host is a dual-homed host, and the DMZ zone becomes an additional layer of security between the external network and the internal network. The bastion host can act as an application gateway or as a proxy server. Since the bastion host is the only host that can access the internal network directly from the external network, it makes the internal host protected.

3.3.4. Dual DMZ firewall architecture

If there is a requirement in the internal network that some information can be shared by providing direct access to the outside, this can be solved by creating two DMZ zones in the firewall. One for the outer DMZ zone and one for the inner DMZ zone. Place some public information servers like Web and FTP in the outer DMZ zone, and these server systems themselves act as outer bastion hosts. For packets coming from the external network, the outer shield router is used to prevent external attacks and manage access to the outer DMZ, while the inner shield router allows only packets whose destination address is the bastion host to be accepted, and is responsible for access from the inner DMZ to the internal network. For packets to be sent to the external network, the internal shield router manages access from the bastion host to the DMZ network. The firewall system allows sites on the internal network to access only the bastion host, and the shield router only accepts packets from the bastion host going to the external network.

The advantage of deploying a firewall with DMZ is that an intruder must break through several different devices, such as external shield router, internal shield router, and bastion host,

in order to attack the internal network, which makes it much more difficult to attack, and accordingly the security of the internal network is greatly enhanced, but the construction cost is correspondingly the highest.

3.4. Usage scenarios of cloud firewall

Cloud firewall is a security product that supports network-wide traffic identification and unified policy control, and can filter out potentially malicious network traffic. It is a collective name for Internet border firewall, VPC border firewall, and host border firewall, providing users with three kinds of border protection and traffic visualization for Internet, virtual network, and host. The cloud firewall is hosted in the cloud, and there are three main usage scenarios.

3.4.1. Internet service protection

It controls access traffic to and from the Internet and intercepts attacks and threats from the Internet, including mining, malicious traffic and hacking. For example, if a financial user has other types of business exposed to the Internet in addition to HTTP business, the user needs to use an intrusion detection module (IPS) for protection.

3.4.2. Active outreach protection

The active outreach behavior of cloud assets is detected and analyzed to help users understand network traffic dynamics in real time and implement protection. For example, a government department user, in addition to focusing on defense from the Internet to the business, also focuses on active outreach to the business to determine which hosts are already at risk and to block these abnormal behaviors in real time to avoid potential risks.

3.4.3. Micro-isolation Protection

Access traffic between ECS servers in the intranet is controlled so that different businesses can be safely isolated. For example, an e-commerce customer, although all HTTP services are protected by a Web application firewall, expects security isolation of different services to enhance the overall network control and avoid security threats to the entire business on the cloud due to the existence of security risks in one ECS.

4. Application of firewall technology in computer network security policy

Network security policy refers to the sum of a series of preventive measures taken in a specific environment to protect the network from hazards. In addition to strict management, legal constraints and security education, advanced technologies like firewalls are relied upon to ensure system security, mainly including two aspects of technical means and management measures. Firewall can achieve access permission, denial, monitoring, by filtering insecure services, allowing or denying access to certain hosts in the network, providing access logs, monitoring access, and achieving centralized security management for the internal network without the need to set up separate security policies on each computer, and its application mainly has the following six points.

4.1. Composite technology applications

Composite technology combines the advantages of both proxy and packet filtering firewalls, incorporating a number of security technologies such as IDS and log monitoring, combined with the actual situation of network security operations, to ensure that the computer network can respond quickly when attacked, provide defense services, effectively stop external attacks, and proactively monitor internal network information security. Its defense mechanism is the network security in the form of authentication, using dynamic filtering to achieve the security of information exchange.

4.2. Monitoring log application

In the process of defending against external network attacks, the firewall opens full logs and obtains relevant threat information, categorizes various viruses and Trojans that may threaten the security of computer networks, and stores them in the database. Through configuration log, management log, connection log and view log, analyze the error interception information in the monitoring log, set default log options, reset and upgrade the firewall, and intelligently enhance the interception behavior of the firewall to further improve the security performance of the computer network.

4.3. Proxy server application

Through the proxy server to provide network proxy for the computer, so that the real network address is not discovered, and smoothly complete the information interaction. The leakage of computer IP information often occurs during the dialogue between the internal network and the external network, and once the IP address is resolved and tracked by network hackers, the computer's data information can be easily stolen. By using a proxy server, network hackers can only resolve virtual IPs and will not obtain any real information, thus protecting the data security of the internal network. The proxy server plays a transit role in controlling the interaction process of internal and external network information, and also has obvious advantages in account management and information verification. In addition, SSL access information from internal network users to external network is first transferred to the internal proxy server for analysis and confirmation of security before forwarding outward, and the encrypted packets are audited and analyzed internally, which can prevent hackers from using SSL encryption to take away internal data while satisfying users' access needs.

4.4. Packet Filtering Technology Application

Packet filtering technology is a firewall with information selection qualities. After the computer obtains the transmission information and the destination IP, it has to parse the destination IP data first, compare the packet with the user security registry, identify whether the data contains threat information, and confirm the security before transmitting the packet to the computer. Transmission from inside to outside restricts dangerous information from being transmitted; transmission from outside to inside restricts illegal information flow into the computer and internal network. In practice, packet filtering is usually installed on routers and used in conjunction with devices such as bastion hosts to provide security by examining the IP header, TCP header, or UDP header of packets.

4.5. Configuring the security module

We know that the firewall divides the network into several different areas, including the DMZ. we then use firewall technology to modularize these one by one areas as a unit for protection, and build up one by one security isolation zones by configuring the firewall, so as to protect the internal network information security.

4.6. Configuring access policies

In general, when setting up the firewall, it is necessary to fully understand the internal and external applications of the computer, classify and analyze the original address, IP address and other information, scientifically and reasonably configure the policy, adopt different policies for different types of information, take corresponding measures, and apply the firewall technology to automatically detect the vulnerabilities generated during operation and remind users to solve them in time, effectively reducing the information in the transmission process This can effectively reduce the risks that may arise during the transmission of information.

5. Conclusion

Computer network security is a complex and relatively large system project, and the firewall is in the key channel of the network, which is the most basic security mechanism in protecting the network security, and its role is pivotal to the information system and data security. Due to the increasing scale of computer network applications, especially the rise of the meta-universe, various network attacks have become endless, new network viruses to covert, diversified, industrial development, hacking techniques also continue to evolve, the firewall technology based on network security has put forward higher requirements, only to continue to develop in the direction of intelligent and active, do a good job of network security system risk assessment, develop Network security strategy, network security protection system, in order to more effectively maintain and protect network security, to meet the hundreds of millions of Internet users to a better life of cloud aspirations.

Restricted by the level, my views have certain limitations, and hope that experts and scholars and peer's criticism and correction.

References.

[1] Deng Shikun. Computer network engineering and planning design [M]. Yunnan University Press. 2014.09.

[2] Zheng Kaiyuan. Computer network security and enterprise network security application research [J]. Network Security Technology and Application,2017(03):3-4.

[3] Tan Xiongsheng,Huang He. Research on the application of firewall technology in computer network security [J]. Digital Technology and Applications,2019,37(01):211+213.DOI:10.19695/j.cnki.cn12-1369.2019.01.109.

[4] Wang J. Computer network management and security technology research ideas framing practice [J]. Digital design,2019(8):14.

[5] He, Tonghui Xu, Dongsheng Zhang, Qi. Computer network security and defense research [M]. Beijing University of Technology Press.2019.05.

[6] Wang Yijia. Analysis of the application of firewall technology in computer network security [J]. Computer products and circulation,2020(06):69.

[7] Pan Ye, Liu Yuan. Research on the security protection of computer networks based on firewall technology [J]. Network security technology and application,2022(08):6-8.