Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/5/20230688

Network security and computer program

Xinyang Qian

Carmel Catholic High School, Vernon Hills, IL, United States 60061

xqian.2024@carmelhs.org

Abstract. In this era of rapid development of network and computer technology, the potential dangers become more and more numerous. There are many security issues that are hidden and unobtrusive. Creating a computer firewall to defend against network security leaks is a necessity. Firewalls can be personal and make a match that is more in line with what is in mind. Firewalls must allow any necessary connections from application business and technical expertise through the firewall to ensure the integrity of the data network. For firewall pairings, Border network, Perimeter Network, and Internal Network are also necessary for impact. The firewall construction can also be made more secure by implementing it through WIFI IP address. Dynamic NAT, Static NAT and PAT are essential in firewall building, and they all aim at network address translation. When building a firewall, changing a specific IP address can monitor the own network and control the message delivery in terms of security.

Keyword: Firewall, Network Security, Firewall Construction, IP Address.

1. Introduction

With the gradual development of computer networking, the popularity of computers is becoming more and more widespread, and people are becoming more and more dependent on computers, which also brings great convenience to people's lives [1-2]. There are still some security vulnerabilities in the complex Internet that may allow users to lose their data or even have their private information or privacy stolen. Even though computer technology is very advanced nowadays, there are still some hidden dangers [3-4]. The uncertainty of computer security has increased the complexity of computer network management. Burns J, Cheng A, Gurung P, Rajagopalan S, Rao P, Martin D.M., " (2001) "Automated Management of Cyber Security Policies," Proceedings of the DARPA Information Survivability Conference and Exposition II [5-6].

Computer security is everywhere, even in the most inadvertent way. For example, when people shop online, websites will need a person's identity information and record transaction history. At this point, some illegal websites may use hacking methods to leak information and steal users' personal information, which can harm users' personal interests. Therefore, more attention must be paid to the importance of network security to ensure that the user's personal information is secure and not cut by the minions. The requirements for network information security continue to increase and promote the stable development of computer networks. If a person aims to damage the system, he or she will keep making breakthroughs to the system, and it is easy to find the loopholes of the system and launch attacks on the computer network, user information and data and other issues, which is very unfavorable to maintain the security of the computer network. Viruses have many characteristics, such as fast infection, widespread, complex and diverse forms of transmission, difficult to remove completely, destructive, easy to excite, and have potential [7-8]. Firewall is the protective barrier of

DOI: 10.54254/2755-2721/5/20230688

the world that people see when using the Internet. The three most used ports, the World Wide Web (port 80), email in (port 110), and email out (port 25). Paunet H, a security expert at the cyber security firm Untangle, testified in an email interview that cyber threats have proven that access to the Internet from home has increased in the last year. Kirkham T, CEO of cybersecurity firm Iron Tech Security testified that one of the most common attacks that firewalls help prevent is denial of service (DDoS) attacks, which are attacks on websites that offer online services. The firewall helps to close any unused ports. Finally, it blocks access from particularly insecure websites, thus preventing all communication from unknown intruders. A website crash can be considered a malicious attack, where cybercriminals disable a website to attack a specific online service, and hackers bombard the website with large amounts of online traffic that the server or network can no longer handle. Firewalls are certainly a very important and useful solution when people encounter these insecure network problems [9-10].

2. Method

2.1. Computer firewall

If a computer needs a way to avoid intrusion into a networked system, a firewall would be a good choice. Shwed G, one the fathers of the modern Internet based security, invented the first firewall that used " state detection" - the widely used second generation firewall technology available today. This allows it to sit like a door at the entrance to an organization, and people block who comes in or goes out. It knows how to analyze traffic and basically classify each type of connection. Firewall is mainly used to create a barrier of protection between the inner and outer network surroundings with the help from hardware and software, thus realizing the blockage of insecure computer network elements. Schuba C.L. and Spafford E.H. COAST Laboratory, Purdue University, Computer Science Department, West Lafayette, Indiana, USA. The fundamental components of the reference model are certification, integrity guarantees, accessibility control, assurance, and implementation. All components are managed by a focused security policy and can be deployed in a decentralized fashion for scalability. Schuba C.L. and Spafford E, Purdue University, 1998 The basic components of the reference model are authentication, integrity guarantees, access control, auditing, and their enforcement. All components are managed by a centralized security policy and can be distributed and deployable in a distributed manner to achieve scalability. Users can only access a computer if the firewall agrees, and if they don't, they are blocked. Firewall technology has very powerful alarming features. When an external user wants to access the computer, the firewall will quickly issue the appropriate alarm and alert the user's behavior, and make a self-judgment to decide whether to allow the external user to enter the internal, as long as it is within the network environment, the firewall can effectively query the user and display the query information to the user, the user then needs to set the firewall accordingly to block any impermissible user behavior. The firewall also provides an effective view of the flow of information and data, as well as the speed of uploading and downloading of those data and information, giving the user good command over the use of the computer. Through this firewall it is also possible to view the internal situation of the computer and also to start and shut down programs. The firewall is a separator, restrictor and parser that can be effectively used to monitor any activity between the intranet and the Internet to ensure the security of the internal network.

2.2. Firewall capabilities

Firewall is an essential part of contemporary network security protection technology; it can effectively defend against external invasion and impact. As the network technology means to improve, the firewall technology is also improving its features, which can realize the filtering of information and ensure the security of information. Elizabeth D. Zwicky, Simon C, Chapman B. D., published an article in June 2000, which proposed cryptographic attacks and exploitation of known security vulnerabilities that existed early in the network. Firewall is a prevention system that works in the intermediate process of internal and external networks and has the security protecting value. The firewall provides effective flow of inner and outer sources and timely handling of various security issues, thus improving the security of information and data materials. The firewall technology has the ability to fight against certain attacks and self-protection against external attacks, and with the

DOI: 10.54254/2755-2721/5/20230688

progress of computer technology firewall technology is constantly developing. A firewall performs a scan of the network traffic flowing through it and can screen out some attacks before they are implemented on the destination computer. A firewall may also close ports not being used. And it can also stop outbound traffic on particular portions of the port and stop the launch of some viruses.Sokolov V, Alekseev I, Nikitinskiy M and Mazilov D, "Modern Networking Technologies", A network analytics system in the SDN // SDN &NFV: The Next Generation of Computational Infrastructure.

2.3. Classification of firewalls

Firewalls can be divided into hardware firewalls and software firewalls. A hardware firewall is a system that is independent of the computer it protects, as it filters information from the Internet into the system. If people have a broadband Internet router, it may have its own firewall. A software firewall is a program that a computer uses to check data coming in and out of the device. Users can customize it to meet their needs. Like hardware firewalls, software firewalls filter data by examining it or its behavior to see if it matches a malicious code profile. Software firewalls can also monitor traffic trying to leave a computer to prevent it from being used to attack other networks or devices. A software firewall must be installed on every computer in the network. Therefore, the software firewall can only protect one computer at a time.

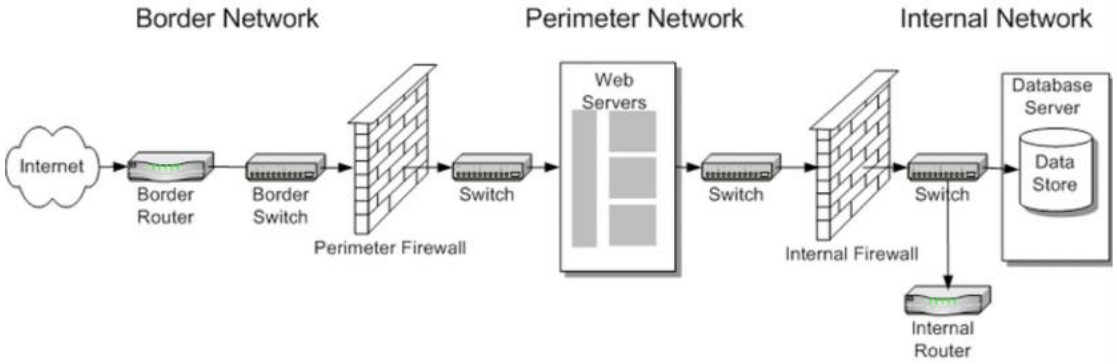

Figure 1. Components of Firewall are shown here.

As Figure 1 shows, Border Network is established through manual configuration between routers and is unique as far as its transport protocol is concerned. Perimeter Network is a secure border that provides the primary defense for private networks and other public networks such as the Internet. A firewall detects and protects the network from unwanted traffic, potentially dangerous code and intrusion attempts. internal Network is a network of computers within an organization used for sharing information, easier communication, collaboration tools, operating systems and other computing services, usually excluding access by outsiders. The composition of these three can be paired with a firewall that is extremely secure and protects the internal exchange of information.

3. Result

People can implement the firewall construction by looking at our WIFI IP address, also can make it more secure. Secure the internal network and prohibit external users from connecting to the internal network. Secure the hosts that act as firewalls and prohibit external users from using the hosts of the firewall. telnet is the standard protocol and primary method for Internet remote login services. FTP is a file transfer standard developed to enable us to transfer files to and from each other on the Internet, and it defines how files are transferred on the Internet. People can choose to use Telnet to manage the firewall. The internal network structure is concealed to ensure that internal users can connect to the network through only one legitimate IP address. Now it gets an internal port and an external port. After booting it up and changing Forward Chains to DENY prohibiting unfamiliar information theft or forwarding. NAT stands for Network Address Translation, and its main function is to convert a private network IP address in an IP header to another IP address that is recognized by the public network. It

DOI: 10.54254/2755-2721/5/20230688

can successfully address the function of private network access to the public network, usually in this case by converting multiple private network-specific addresses within the enterprise to one public IP address at the enterprise egress gateway to access the Internet. This solution, by using a small number of public IP addresses to represent a larger number of private network-specific IP addresses, helps to alleviate the available IP address space depletion of the available IP address space. The NAT format is divided into three typical applications. Static NAT, Dynamic NAT, and PAT.

With static NAT, the private IP is usually in a one-to-one relationship with the public IP. It only hides the real private IP address externally, which satisfies the possibility of Internet users to access the internal server and improves the security to some extent.

Dynamic NAT requires defining a pool of addresses on the NAT router for the public network. In dynamic NAT, numerous hosts with private IP addresses can share the same or fewer public IP addresses. It may look very similar to dynamic PAT, but the main difference is that it is a NAT - the port number does not change, only the IP address. This means that a single public IP address cannot be shared between multiple internal hosts at the same time.

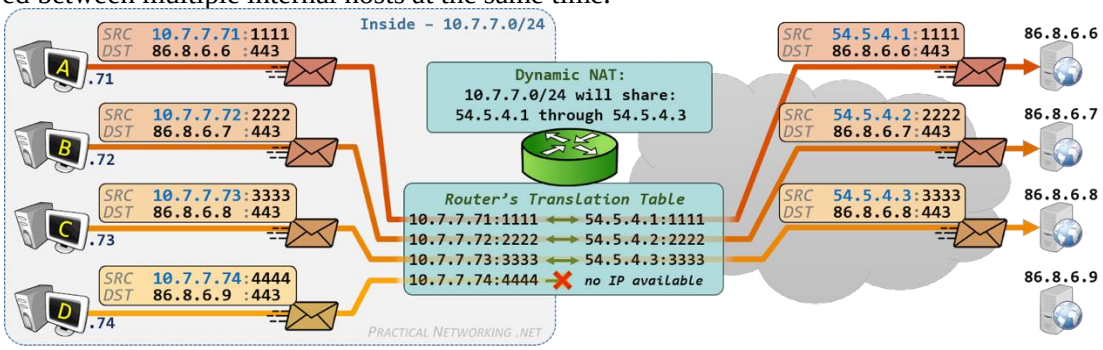

Figure 2. Dynamic NAT Connection is shown here.

As shown in Figure 2, here there is a router with an internal network with four hosts. The router is configured with dynamic NAT, which declares that hosts on the internal network can share three public IP addresses and that the hosts are all connected. This means that the hosts communicate in both directions. However, 10.7.7.74 is not connectable, so the information is all transmitted only to 1, 2, and 3. If multiple internal hosts share fewer public IP addresses, it is possible for the dynamic NAT to save the IP addresses. If they are kept in series, the connection problem will be intermittent. It is because nothing is perfect in each thing that so many conditions as well as ways are derived.

PAT (port address Translation) is a type of NAT, strictly speaking, it is a type of dynamic NAT, which is created to proxy the hosts in a large number of enterprise networks that use private network private addresses to access the public network, for example, to access the Internet. Its biggest advantage is that it converts all private network private addresses used internally into a public IP address, usually the IP address of the NAT router's external interface, and then proxies them to access the Internet, thus maximizing the address cost of accessing the Internet, since only one public IP address is required for the entire enterprise to access the public network when using PAT.

Static NAT becomes particularly useful when a device requires access from outside the network. This method is not often used because it does not store registered IP addresses and because this kind of transformation causes IP addresses not to be used for anything else. There are two cases where dynamic NAT can be used, the first one of which is a protocol that permits the creation of a minor dynamic connection is made back to the customer. The other one is in the case of a private-to-public IP is mapped in both directions, but not specifically focused on an unambiguous migration from one to the other. PAT is one of the most prevalent forms of network address translation. PAT should be used if the Internet needs to be used by all hosts at the same time. Within this approach, a common IP address is sufficient to connect thousands of servers to the Internet, and Newar Virtual Carrier Grade NAT supports all kinds of network addressing translations, including dynamic, static and PAT, to meet any requirement, regardless of which type of NAT the carrier chooses. In addition, it offers NAT64 in parallel to NAT44 mode, allowing operators to smoothly migrate to IPv6 infrastructure. It

DOI: 10.54254/2755-2721/5/20230688

changes private network addresses to public IPv4 addresses using a translation device embedded in the carrier's network. This allows a small pool of public addresses to be shared across multiple end sites, greatly extending the capabilities of existing networks. the most common format for IPv4 addresses, called dashed four or dashed ten, e.g., 192.0.2.146 IPv6 addresses are four hexadecimal digits delimited by colons (e.g., 2002:db8::8a3f:362:7897) IPv6 also offers some additional benefits that make the migration a good idea. ipv4 provides a larger address space, eliminates complexity, and is faster than IPv6. IPv6 was created to be more robust than IPv4, but every object has an enemy, and all new things bring new risks. The right approach to network fragmentation and blocking particular flows to control network aggression during remediation.

The successful method is to add the licensed user to the forwarding chain that has been set to DENY on the computer. The IP address is changed to a specific one, depending on the location of the network digitization. At the same time, the IP packet forwarding function of the system must be activated. For security reasons, it is recommended to set the Forward Chains policy to DENY disabling all end-permitted packet forwarding before turning on the forwarding function. The overall setting is single transformation to determine security. Regarding the prevention of IP address theft, in this network topology, it is visible that all users are connected to the firewall through two routers, so it is only necessary to establish a static mapping table of authorized IP addresses to MAC addresses in the routers. If there are clients connected directly to the firewall host, so it is necessary to create a static mapping table of IP addresses to MAC addresses in the firewall host using the ARP command. After completing the above steps, simply set IP address confirmation on the ingress port and discard packets that are unlikely to come from that port. At this point, a more secure firewall is basically set up and then run After debugging, one can save the configuration with the IP-chains-save command. After debugging, the configuration can be saved with the IP-chains-save command. When it needs to be used again, the IP-chains-restore command can be used.

4. Conclusion

When having a personal firewall was new and exciting, most of us connected a single home computer to a cable modem, an IDSN box, or the phone line that brought us our Internet connection. In the modern world, the very fact that everyone has a home network is a defense against online attacks. Overall, all other packet filtering firewalls operate on a similar principle to IP-chains, and the configuration commands are similar. Commercially available firewalls can be pre-configured with some basic elements, but since end-user requirements and environments vary, it is inevitable that the configuration will have to be done by itself. Firewalls are a key component in protecting against unexpected activity and malicious attacks on this part of one' s equipment and network. Rather, they protect the average computer user from attacks via online applications, monitor incoming and outgoing data, and do not allow the computer to connect to insecure or unrecognizable programs.

References

[1] Lutkevich B, US. (2021) Network Security. This article introduces the firewall in terms of software and firmware and checks incoming and outgoing traffic with a set of rules. https://www.techtarget.com/searchsecurity/definition/firewall

[2] Brodsky S, US. (2021) How Firewalls Can Protect You From Security Risks. This article focuses on the role of the firewall and its advantages. https://www.lifewire.com/how-firewalls-can-protect-you-from-security-risks-5180818

[3] Harmoush E, US. (2019) Dynamic NAT. This article introduces NAT and suggests that a single public IP address cannot be shared among multiple internal hosts at the same time. https://www.practicalnetworking.net/series/nat/dynamic-nat/

[4] Rubenking N J, US. (2022) Do You Need a Personal Firewall? This article presents a personal firewall that involves allowing all valid network traffic and blocking suspicious or malicious traffic. It can be built and enforced according to the individual's whims. https://www.pcmag.com/how-to/do-you-need-a-personal-firewall

[5] Schuba C.L. and Spafford E.H, US. (2002) Model for firewall technology. This article illustrates that firewall technology is a specialized engineering solution, not a science-based

DOI: 10.54254/2755-2721/5/20230688

solution. The formations in a firewall are constrained by a secure set to enable deployment and scaling in a distributed manner. https://ieeexplore.ieee.org/document/646183/authors#authors.

[6] Taylor R, US. (2021) IPv4 vs IPv6: What's the difference? This article explains the differences and excesses between IPv4 and IPv6. IPv6 can be a more secure form. https://bluecatnetworks.com/blog/ipv4-vs-ipv6-whats-the-difference/.

[7] Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, US. (2000) Building Internet Firewalls. This article describes cybersecurity issues. https://www.oreilly.com/library/view/building-internet-firewalls/1565928717/.

[8] Schuba C.L. and Spafford E, US. (1998) Computer Security Applications. I t describes a model of existing firewall technology. https://www.researchgate.net/publication/3728380_A_reference_model_for_firewall_technology.

[9] Burns J, Cheng A, Gurung P, Rajagopalan S, Rao Rosenbluth D, Surendran A.V., Martin D.M., Us. (1997) Firewalls: an expert roundtable. This article describes how firewall works. https://ieeexplore.ieee.org/document/605932/citations#citations.

[10] Sokolov V, Alekseev I, Nikitenko M, and Mazilov D, US. (2014) Firewall application for Floodlight SDN controller. This article describes the renewal of firewalls. https://ieeexplore.ieee.org/abstract/document/7491821/references#references.