How to bypass a firewall

Pei Guo

Master Media Informatics

Matr. Nr.: 268643

Title of Seminar: Computer Security

Prof. Dr. Joachim von zur Gathen

Tutor: Michael Nüsken
Daniel Loebenberger

Bonn-Aachen International Center for Information Technology

06.11.2006

1. Abstract

Nowadays, the Internet users are traditionally relied on the firewalls to enforce their security policy by protecting their local network systems from the network-based security threat and illegal data access. However, these controls do not provide a comprehensive solution to secure a private network connected to the Internet. The purpose of this paper is focused on the origin, definition, functionalities and characteristics of the various firewalls. Then, this paper also describes some methods to bypass the firewall.

2. Introduction

As we all know, the Internet has experienced a rapid and triumphant improvement in the last decade. [Rolf(1997.5)] indicates that there have had over one million computer networks and well over one billion users by the end of the last century. The Internet is penetrating every field all over the world. At the beginning, the Internet was built only as research-oriented and its communication protocols were designed for a more non-malignant environment than now exists. But when the time went on, the Internet is twisted steadily from the initial one and its environment is much less reliable. It has all dangerous and risky situations, intended and malignant attacks and nasty people that we can find in the real life society as a whole. Today, when the users are connected to the Internet, they are enabled to reach and communicate with the outside world through the Internet. But at the same time, however, the outside world can reach and interact with the premises network by the same way. Therefore, it is very important for the users to protect their local systems from the spiteful attacks from the outside.

3. The types of firewall

As stated in [Wikipedia(2006.10)], the technology of firewall first emerged in the late 1980s and the first paper of this technology was published in 1988.

[Tom(2001)] writes that the firewall (as shown in Figure 1) is a kind of gateway that limits and controls the flow of traffic load between networks, typically between an internal Ethernet network and the Internet. It is built up to establish a restrained link and an outer security wall. The firewall examines all the exchanged messages going in or out the intranet and blocks these packets that do not meet the specified security criteria and therefore, it should be designed to meet the following characteristics stated in book of [Stallings]:

- All the traffics, which try to go in or out the network, must pass through the firewall.
- Only the authorized traffic that defined by the local security policy will be permitted to pass the firewall.
- The firewall itself is immune to be penetrated, which means that operating system is secure.

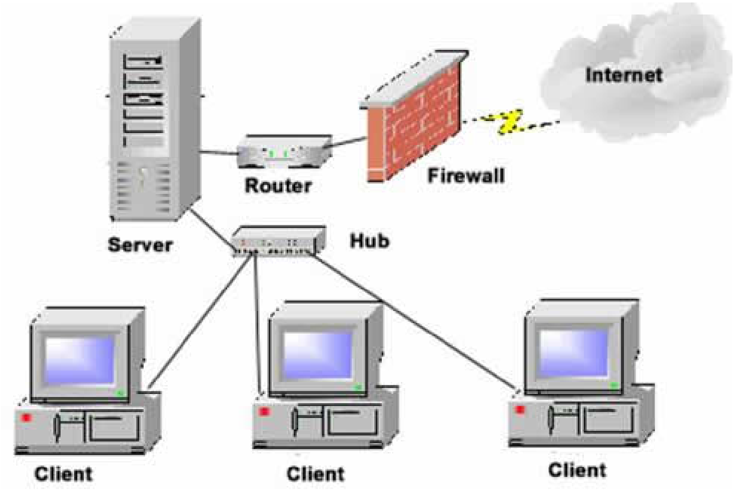


Figure 1 Firewall Infrastructure

To build up a specific firewall, each user has his/her different way. The firewall can be implemented in both hardware and software, or a combination of both. Normally, there are three common types of firewalls:

(1). Packet-filtering Router: This type of firewall (as shown as Figure 2) is checking all the packets entering or leaving the network and accepts or rejects it based on user-defined rules. Packet-filtering router is working on the packets at TCP/IP network layer. The designing of the filtering rules are based on the information contained in the network packet: source IP address, destination IP address, source and destination transport-level address, IP protocol field and interface. The internal network is directly connected with the outside network.

The main advantage of the packet-filtering router is its simplicity. It is fairly easy-installed, effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to security breaches caused by improper configurations, such as IP spoofing.

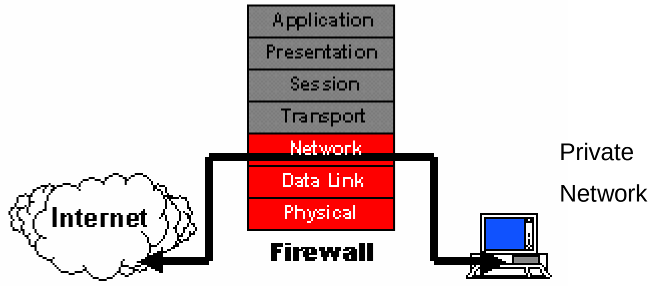


Figure 2 Packing-Filtering Router

This traditional packet-filtering makes filtering decisions on the information in an individual packet and does not consider of any high layer context. Normally, this traditional technology only filters the low-numbered port from 1 to 1024. It must allow the occurrence of internal network traffic on all the high-numbered port from 1024 to 16383. Therefore, an improved way named stateful inspection packet filter

(As shown in Figure 3) adds stateful inspection modules between the date-link layer and network layer. There is an entry for each currently established connection. It will enable the incoming traffic to high-numbered ports only when the packets fit the profile of one of the entries in the directory.

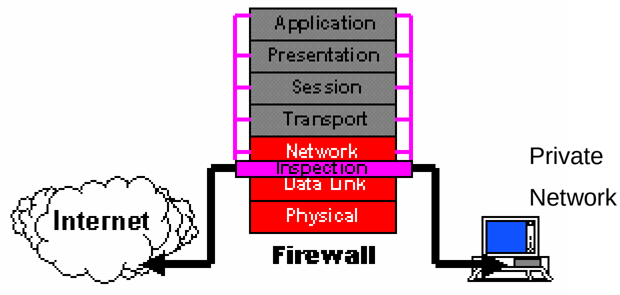


Figure 3 Stateful Inspection Packing-filtering

(2). Circuit-Level Gateway: Circuit-level gateway (as shown in Figure 4), which is described in [Tom(2001)], offers a controlled network connection between the internal and external systems. It works on the Transport Layer. This kind of firewall applies security mechanisms when a TCP or UDP connection is established. A virtual "circuit" is built up between the internal client and the proxy server. The internal client’s requests are sent to the proxy server through the circuit, and the proxy server sends these requests to the Internet after changing the IP address. The external users can only see the proxy server’s IP address. When the proxy server receives the responses and then sends them back to the client through the circuit. Although the traffic is allowed to go through, the external users never know the internal systems. This type of connection is often used to connect "trusted" internal clients to the Internet. As soon as the connection has been constructed, these data packets can flow between the hosts without the further checking.

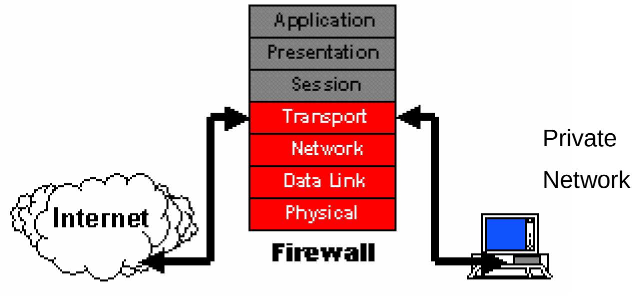


Figure 4 Circuit-Level Gateway

(3). Application-Level Gateway: As indicated in [Tom(2001)], the application level gateway (as shown in Figure 5) can provide all the basic features of proxy and an extensive packet analysis. It applies security mechanism to some particular applications, such as FTP and Telnet services, and can also interoperate through this gateway and fully manage the traffic from both of the inbound and outbound at the application layer which is defined in OSI model. When the packets arrive at the gateway from the external network, they are examined and evaluated by the gateway to determine if they are allowed to enter the internal network according to the security policy. The server not only checks the IP address of these packets, but also verifies if the data in these packets is from a trusted user or a malignant hacker. The disadvantage of this kind of firewall is that might cause performance degradation, but it is the most effective and popular one.

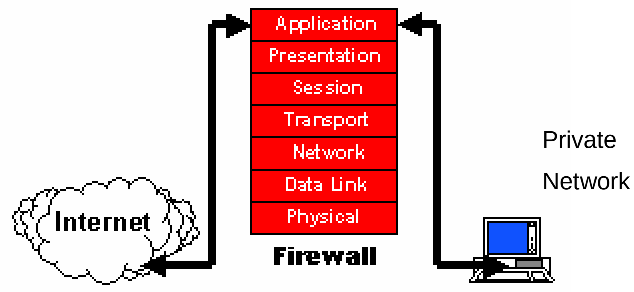


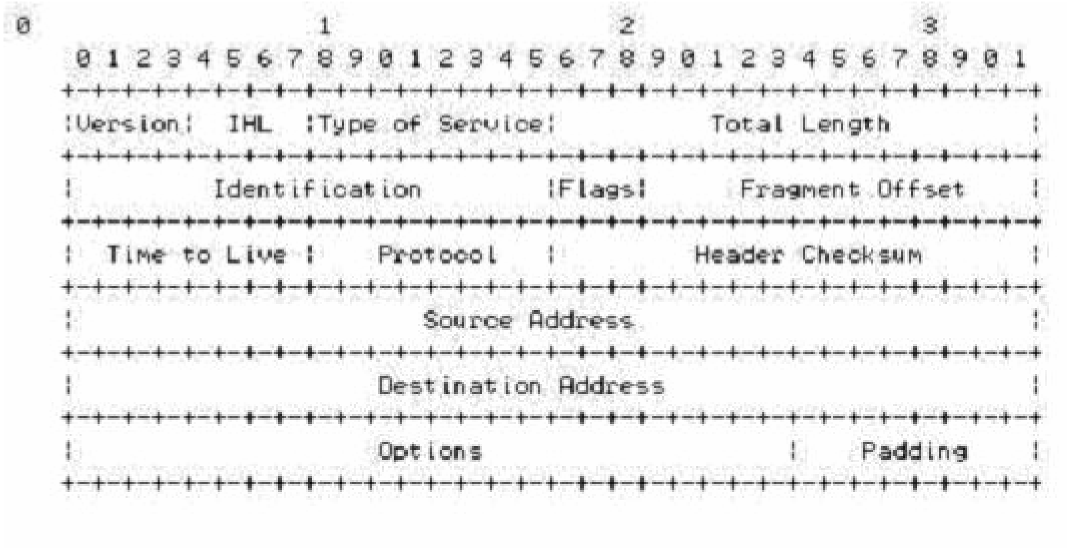
Figure 5 Application-Level Gateway

Both of these gateways can provide more opportunities for monitoring and restraining access between different networks as they work on the higher layers. The gateways work as a middle-man and they fetch the data packets from internal clients to external services. The proxy service hides the client to the Internet by changing the IP address of the data packets. And at the other hand, it also acts as an agent for the client on the Internet.

4. How to bypass the firewall

As stated above, there are different types of firewall and each of them has its advantage and disadvantage. In the following section, we will talk about some certain methods to bypass the firewall.

(1). IP Address Spoofing: IP address spoofing is one effective method to bypass the firewall. As mentioned in [Matthew(2003.3)], the users gain an unauthorized access to a computer or a network by making it appear that the message comes from a trusted machine by “spoofing” the IP address of that machine. To completely understand how it works, we should review the structure of the TCP/IP protocol suite. A basic understanding of these headers and network exchanges is essential to the whole process. Internet protocol (IP) is a network protocol operating at the network layer of the OSI model. This protocol is connectionless and has no information regarding transaction state, which is used to route data packets on a network.



```
0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|  IHL  |Type of Service|          Total Length         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Identification        |Flags|      Fragment Offset    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|  Time to Live |    Protocol   |         Header Checksum       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                       Source Address                          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Destination Address                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                    Options                    |    Padding    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 6 IP Packet Header

As shown in Figure 6, the first 12 bytes in IP packet header contain the multifarious information of the packet. However, the next 8 bytes contain the source and destination IP addresses. Using some kinds of tools, the users can easily modify these address information in IP packet header, specifically the source address bits field, to make them to bypass the firewall.

For example, suppose that we have three hosts A, B and C. Host C is a trusted machine of host B. Now, host A wants to send some packets to host B and A impersonates itself to be C by changing the IP address of these packets (shown in Figure 7). When these packets are received, B thinks that these packets are from C, but actually they are from A.

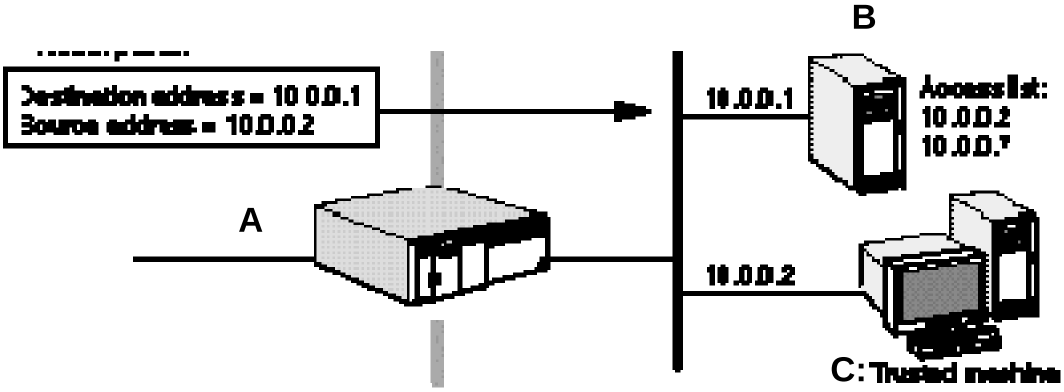


Figure 7 IP Address Spoofing

(2). Source Routing: As introduced in [ISS], source routing is another method to bypass the firewall and the packets sender can designate the route that a packet should take through the network. When these packets travel among the nodes in the network, each router will check IP address of the destination in these packets and choose the next node to forward them. In source routing, the sender makes some or all of these decisions on the router. In the Figure 8, it shows the principle of the source routing but it is an optimal way, which makes all the decision of the next hop.

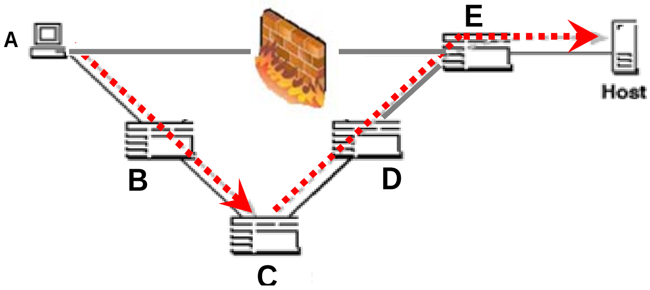
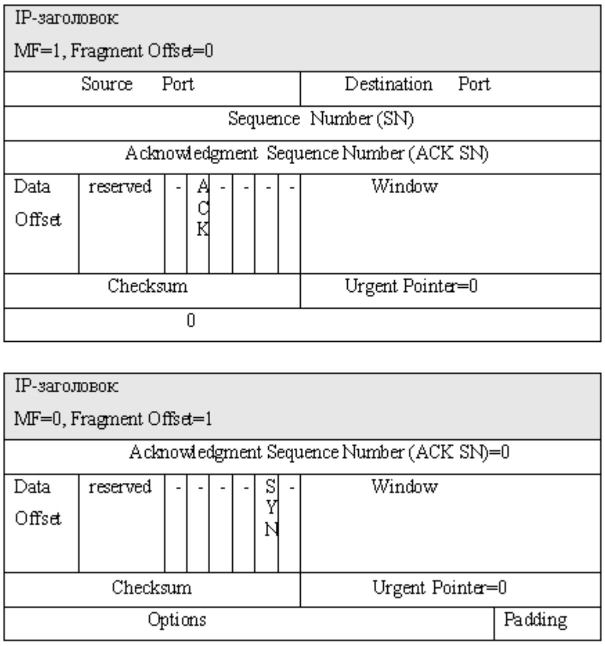


Figure 8 Source Routing

(3). Tiny Fragments: The way of tiny fragments is also an effective method to bypass the firewall and in this means, the user uses the IP fragmentation to create extremely small fragments and force the TCP header information into separated packet fragments. This way is designed to bypass the filtering rules that depend on TCP header information. The users hope that only the first fragment is examined by the filtering router and the remaining fragments are passed through. The way of working of Tiny Fragments is defined and explained in [Ziemba(1995.10)].



IP-заголовок MF=1, Fragment Offset=0								
Source Port								Destination Port
Sequence Number (SN)								
Acknowledgment Sequence Number (ACK SN)								
Data Offset	reserved	-	ACK	-	-	-	-	Window
Checksum								Urgent Pointer=0
0								

IP-заголовок MF=0, Fragment Offset=1								
Acknowledgment Sequence Number (ACK SN)=0								
Data Offset	reserved	-	-	-	-	SYN	-	Window
Checksum								Urgent Pointer=0
Options								Padding

Figure 9 TCP Packet Header

As shown in Figure 9, the TCP header is very different from the IP header. We are interested with the first 12 bytes of the TCP packet, which contain information of the ports and sequence number. As the same with IP packets, TCP packets can also be manipulated by some tools or software. The ports of source and destination hosts normally rely on the network application, for instance, FTP via port 21 and SSH via port 22.

The functionality of tiny fragment method is to segment TCP header packets into the extremely small sections, which are even smaller than the minimum fragment size defined in filter rules. Therefore, these packets are free to be examined by the firewall. For example, all the Internet modules should be able to forward a datagram of 68 octets without further fragmentation. It is because that the size of the Internet headers should be up to 60 octets, and the minimum fragment is 8 octets.

Last but not least, there are also some other "illegal" ways to bypass the firewall, such as Rootkit and Trojan. They are not only using some tricks to bypass the firewall, but also changing the rule or destroying the firewall in some certain way.

References

[Rolf(1997.5)]. Rolf Oppliger. Internet security: firewalls and beyond. *Communications of the ACM*, Vol. 40, Issue 5, pp. 92-102.

[Tom(2001)]. Tom Sheldon. "The Encyclopedia of Networking and Telecommunications". http://www.linktionary.com/f/firewall.html

[Wikipedia(2006.10)]. Firewall. http://en.wikipedia.org/wiki/Firewall_%28networking%29

[Stallings]. "Cryptography and Network Security". Chapter 20, ISBN 0-13-111-502-2

[Matthew(2003.3)]. IP Spoofing: An Introduction. http://www.securityfocus.com/infocus/1674

[ISS]. Source Routing. http://www.iss.net/security_center/advice/Underground/Hacking/Methods/Technical/Source_Routing/default.htm

[Ziemba(1995.10)]. G. Ziemba, Alantec, D. Reed, etal. Security Considerations for IP Fragment Filtering. http://www.ietf.org/rfc/rfc1858.txt, RFC1858