SOFTWARE ENGINEERING 4C03

Computer Networks & Computer Security

Network Firewall

HAO WANG
#0159386
Instructor: Dr. Kartik Krishnan
Mar.29, 2004
Software Engineering
Department of Computing and Software
McMaster University
Hamilton, Ontario, Canada

1. Introduction

A firewall is a virtual wall/gateway, which is located between internal and external networks. Firewalls can be an effective means of protecting an intranet from network-based security threads that come from outside networks while in the mean time providing access to outside world through wide area networks and the Internet. This paper will give a concise discussion about the significance of firewalls and the technical aspects of firewalls.

2. Why are network firewalls necessary?

A huge number of local intranet form the global internet, which allows one to obtain from as well as to provide information to the whole world. Since the internet access provides such benefits to any individuals and organizations, the connection between intranet and internet is essential and absolutely necessary. On the internet it is a virtual world, but it is just like the real world, where be malicious users who snoop on other's valuable information or even some criminals who enjoy bringing down other systems. Security is an important issue, so a virtual firewall needs to be built up around internal network to protect both physical and abstract resources in the intranet.

3. Types of attacks

To help to understand of firewalls implementation, we should better know the most common methods of attacks. Some of them are listed below.

3.1 IP Spoofing Attacks

In this type of attack, an attacker outside the local intranet may pretend to be a trusted computer either by using an IP address that is within the range of IP addresses for the local network or by using an authorized external IP address that has authorized access to specified resources on the local network.

3.2 Denial of Service Attacks

The purpose of these attacks is just to make a service unavailable for normal use by flooding the network with undesired, and often useless, network packets to exhaust the resource limitation on the network or within an operating system or application. Denial-of-service attacks can be implemented using common internet protocols, such as TCP and ICMP.

3.3 Source Routed Traffic

Usually a network packet itself only says where it wants to go, and nothing about how it expects to get there. But sometime the sender of a packet can include information in the packet that tells the route the packet should take to get to its destination. This is called source routing. This can be used to bypass the security measures.

3.4 Tiny fragment attacks

Here an attacker creates extremely small packet fragments by taking advantage of the IP fragmentation option. The attacker hopes that only the first fragment is examined by the security measures and the others can pass through safely.

4. Firewall implementation

Generally, a firewall simply blocks all unauthorized communication between internal and external networks. Basically, there are three basic types of firewalls: packet-filtering firewalls, application-level gateway and circuit-level gateway. We discuss these as follows one by one.

4.1 Packet-Filtering Firewalls (Figure 1)

A Packet Filtering firewalls is normally implemented by configuring a router to filter packets going in both directions. It works at the IP network layer. A packet filtering router usually can filter (i.e. block) IP packets based on some or all of the following fields:

- Source IP address,
- Destination IP address,
- TCP/UDP source port, and
- TCP/UDP destination port.

The packet filter is typically set up as a list of rules based on matches to IP address or TCP/UDP port number to block connections from or to specific hosts or networks, and to block connections to specific ports.

The advantages of packet Filtering Firewalls are as follows:

- Because very little data is analyzed and logged, filtering firewalls take less CPU and create less latency in your network.
- The user does not have to consider blocking rules in their applications, so filtering firewalls are more transparent to the user.

The disadvantages of this type of firewall are as follows:

- If some rules are based on IP numbers and the network is using dynamic IP assignment, this can be a problem, because the dynamic IP is changed sometimes, IP address cannot be specified to be filtered.
- Packet filtering rules are complex to specify and usually no testing facility exists for verifying the correctness of the rules.

4.2 Application-level gateways firewalls (Figure 2)

Application-level gateways firewalls, also called proxy-based firewalls, operate at the application level. They are usually implemented by implementing separate proxy application for each service. They provide all the basic proxy features and also provides extensive packet analysis. The client needs to provide a valid user ID and authentication information to the proxy server in order to communicate with the destination service. In effect, the proxy establishes the connection with the destination behind the firewall and acts on behalf of the client, hiding and protecting individual computers on the network behind the firewall. Since all communication is conducted through the proxy server, computers behind

the firewall are protected. A typical application-level gateway can provide proxy services for applications and protocols like Telnet, FTP (file transfers), HTTP (Web services), and SMTP (e-mail).

Except the disadvantage that they require great memory and processor resources compared to other firewall technologies, application-level gateways have a number of general advantages over the default mode of permitting application traffic directly to internal hosts. Below are some:

- Information hiding, in which the names of internal systems need not necessarily be made known to outside systems, since the application gateway is the only host whose name has to be known to outside systems.
- Robust authentication and logging, in which the application traffic can be pre-authenticated before it reaches internal hosts and can be logged more effectively than if logged with standard host logging,
- Less-complex filtering rules, in which the rules at the packet filtering router will be less complex than they would be. The router need only direct application traffic to the application gateway and reject the rest.

4.3 Circuit-level gateway (Figure 3)

It is basically used for TCP connections. It examines each connection setup to ensure that it follows a legitimate handshake for the transport layer protocol being used. Circuit level gateways do not examine each packet rather they monitor each connection at first. Once a connection (with a unique session identifier) is established, all other packets in that session are allowed to cross the gateway.

Generally, circuit-level gateway is faster than application-level gateway because of fewer evaluations, and it can secure the entire network by prohibiting connections between specific internet sources and internal hosts. One of the biggest disadvantages is that it cannot restrict access to protocol subsets other than TCP.

5. Firewall design principles

To design a firewall for a network, briefly there are several aspects needed to be considered:

1. The attacks you intend to deal with.
2. The services you intend to offer to external networks from your protected network.
3. The services you intend to request from external networks via your protected network.
4. Evaluate the available firewall products

Generally, if cost, speed, flexibility, and ease of use are strong motivators, a packet-filtering firewall is the best choice. But because each type of implementation has its own disadvantage and advantage, so if you can afford it, it is better to have multi-level firewall architecture to achieve the securest network.

6. Conclusion

In conclusion, to prevent your internal network from exposing to malicious attacks, a firewall is absolute necessary. Based on the knowledge about the attacks and the features of each type of firewall, network security can be realized as much as possible.

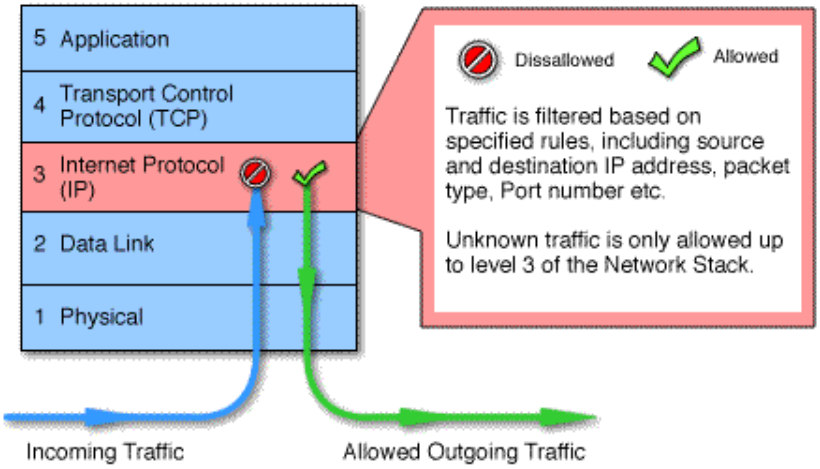

Figure 1. Packet-Filtering Firewall

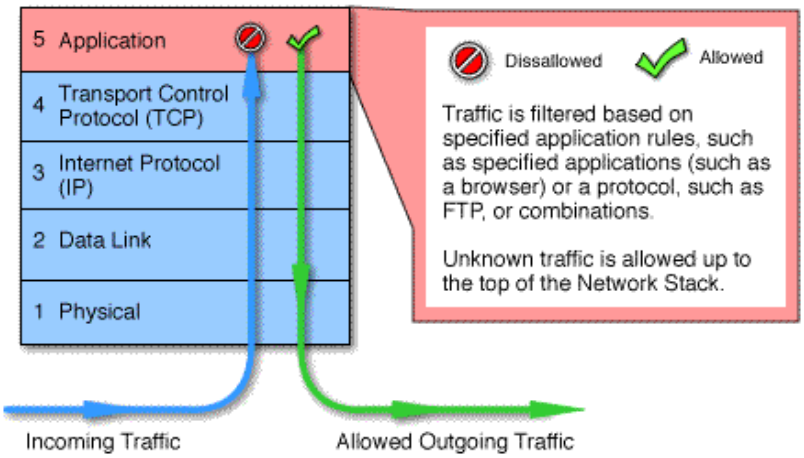

Figure 2. Application-level gateways firewall

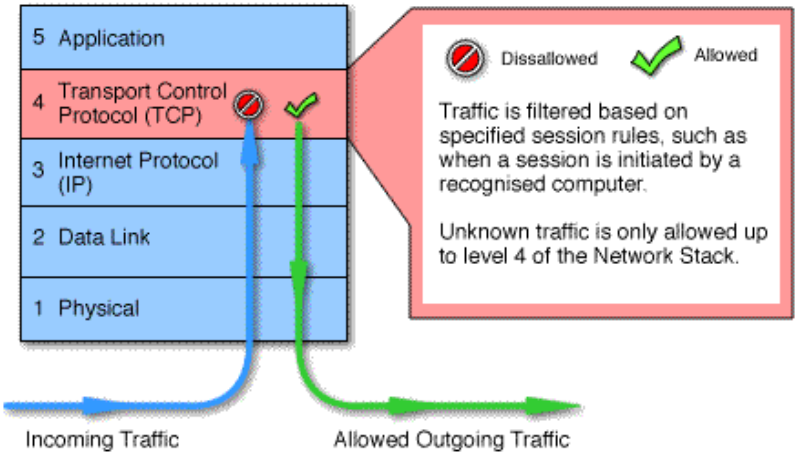

Figure 3. Circuit-level gateway

(Note: All figures are cited from Vicomsoft Ltd's website http://www.firewall-software.com/firewall_faqs/types_of_firewall.html)

Reference

1. D.E. Comer, *Internetworking with TCP/IP: Principles, Protocols, and Architectures*, 4th edition, Prentice Hall, NJ, 2000.
2. W. Stallings, Cryptography and Network Security, 2nd edition, Prentice Hall, 1999.
3. Vicomsoft Ltd website: http://www.firewall-software.com/firewall_faqs/firewallqa.pdf
4. Hany Abadir's website: http://www.cas.mcmaster.ca/~wmfarmer/SE-4C03-01/papers/Abadir-Firewall-1.html
5. Ran Pang's website: http://www.cas.mcmaster.ca/~wmfarmer/SE-4C03-02/projects/student_work/pangr.html
6. Dana El-kaissi's paper: http://www.cas.mcmaster.ca/~wmfarmer/SE-4C03-03/projects/papers/firewalls_in_a_nutshell.pdf
7. CISCO's website: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/centri4/user/scf4ch2.htm
8. CERT/CC's website: http://www.cert.org/security-improvement/practices/p053.html