Firewall

Xinran Hu, 222996

Harrisburg University

Abstract

Firewalls are network devices that installed between internal and external network to ensure the security of network communication from/to hosts in the internal network. The presence of firewall is ubiquitous in today’s company networks, sometimes even in personal networks. Almost all firewalls functions similarly by blocking or permitting network communications according to predetermined rules. However, firewalls also differ in the network layers they inspect network communication. In this paper I will first describe a four-layer network model, namely the TCP/IP model, and discuss three specific kinds of firewalls that work on three different layers of TCP/IP model. In addition to firewall technologies, I will also discuss related technology such as VPN and SOCKS.

**Introduction**  
Firewalls are widely used by organizations and individuals to control, monitor and protect network communication from/to hosts in private network. The concept of firewalls first appeared in 1993 and popularized as internet soon penetrated into daily applications where privacy and financial interests may be at risk. Understanding how firewall works will help us be more aware of the potential risk involved in those activities and enables us making better decision in all aspects of our lives.

A firewall usually refers to a combination of software and/or hardware devices that are typically installed between an internal network and an external network. The internal network is usually considered secured and external network is considered unsecured. The main purpose of a firewall is to form a protective barrier structure in between the secured and unsecured network. A firewall typically functions by scanning network traffic that flows through it, therefore filtering out some inbound communication such that internal machines cannot be directly contacted by outside computers. The firewall can also shut down outbound traffic on specific ports or IP address such that internal computer cannot access specific data from the outside of the secured network. Some other types of firewall can also block net data based on application level data, such that it can ensure sensitive information will not be distributed outside a secured network. Beside blocking traffic, a firewall may also logging traffic and generating traffic report for administrative purposes.

Firewalls can be categorized based on their positions in a layered network model. Network layer firewalls are usually hardware device that installed at network layer (as shown in figure 1). Network fire walls process network traffic at IP protocol level. This is the lowest layer a firewall is installed. Transportation layer firewall is also likely a hardware device but installed at the transportation layer of a network model. It differs from a network layer firewall by inspecting the traffic base on transport level protocols such as TCP protocols. In many aspects, these two types of firewall are very similar to each other. Another type of firewall is application layer firewall. This type of firewall inspects the traffic at the highest level of abstraction. It can directly inspect the content of application level protocols such as HTTP and FTP, thus it can implement most complicated rules based on application level information.

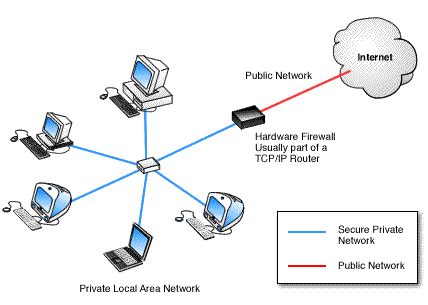
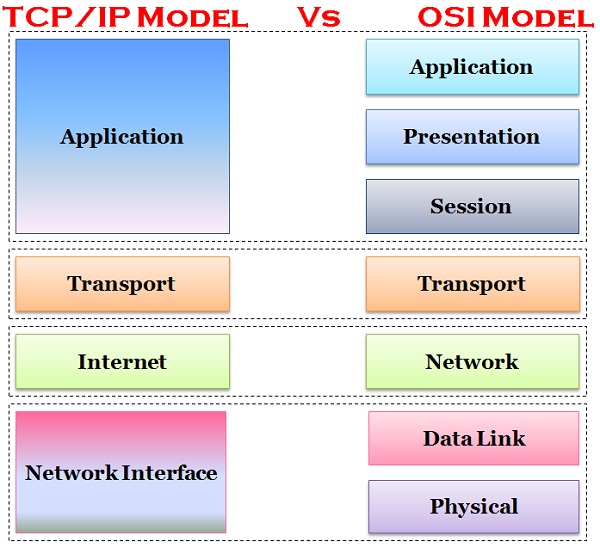


Figure 1 Illustration of the location of a firewall. The most common place a firewall is installed in an organization is at the outset node of the network, even before the router. In this way, it can reduce the amount of traffic a router has to process.

(Source: Internet)

In this paper, I will first describe a new internet layer model named TCP/IP model. This is a four layer model as opposed to the seven layer model of OSI model we studied before. However, main concepts of both models remain similar. The TCP/IP model combined several layers in OSI model and the layers in TCP/IP model have a closer correspondence to the aforementioned three types of firewalls. After discussion of the TCP/IP model, we will discuss the details of how does each type of firewall performs communication filtering. We will then examine some technologies that are closely related to firewall such as proxy servers, secure socket and virtual private network.

**Background of TCP/IP Model**



*Figure 2 Comparison of TCP/IP four layer model with OSI seven layer model*

*Source (Internet)*

Similar to the OSI model, TCP/IP model models the network stacks by layers. There are four layers, network layer, internet layer, transport layer and finally application layer. Each layer is at a different level of abstraction. As shown in figure 2, layers at top are closer to client facing software and layers at the bottom are closer to the physical medium of the network hardware.

**How does a firewall work?**

Different types of firewall works on different layers of the network stack. But they all works based on a common principle. By examine the traffic and utilizing pre-determined rules to allow or disallow communication. With a different layer of abstraction, different firewalls are suited for different use cases. We will now examine the three types of firewall and their working principle in detail

**Internet Layer Firewalls**

The second layer in TCP/IP model is the internet layer. Internet layer corresponds to the Network layer in OSI model. Protocols at this layer manage data transfer between remote computers. The most commonly used protocol in this layer is the internet protocol that allows users and remote computers to establish a packet transmission using a 32 bit IP address. This layer only ensures that packets can correctly reach the destination machines but not ensure the order of packet arrival or packet loss did not occur.

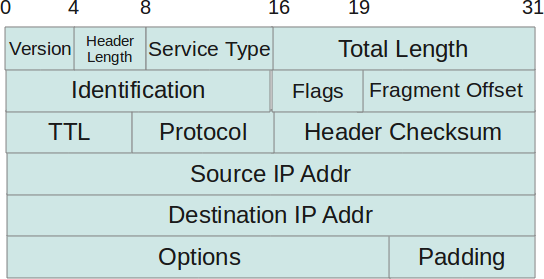


Figure 3. Layout of an IP header

Source: Internet

Encapsulation in network stands for enriching a piece of data payload with additional information that served as metadata. Encapsulation at network layer occurs when transportation layer sends it a piece of data called a segment. Once a segment is received by network layer, an internet protocol header is prepended to the data payload. This header contains necessary information to deliver the data payload to a destination host via its IP address.

Decapsulation, on the other hand, stands for the process of separating of metadata and data payload to inspect metadata to gain knowledge about the data payload. Decapsulation at internet layer occurs when any network device (either a destination host or a router) received a packet from network interface layer. The IP header is first removed from the data payload and being examined carefully. If the device is a router, then it may decide to repackage the packet with a new header and deliver it to the next node that are one step closer to the destination. If the device is host machine, it may compare the destination ip address with its own and decide to either reject or accept this communication. If the device is firewall, it may not perform its due by examine the IP header (as shown in figure 3) and compare against its pre-determined rules to either accept or disregard this packet.

In most cases, the information an internet layer firewall pay attention to is the sender’s IP address. Since IP addresses are usually geographically allocated, IP address provides detail information of the location of the sender. A firewall may have security policies that permit or disallow communications from certain countries so it can effectively block or allow packets send from that country. For example, an online video website may only permitted to provide video streaming services in the United States of America so it can set up its firewall to only accept IP address that are within the United States of America. Or an election website may only allow vote send from IPs within a state border and may not allow online request send from IPs that is not with in a state. Other than IP address, a firewall may also block packet based on protocol type or packet length but those use cases are more rare compare to policies base on IP addresses.

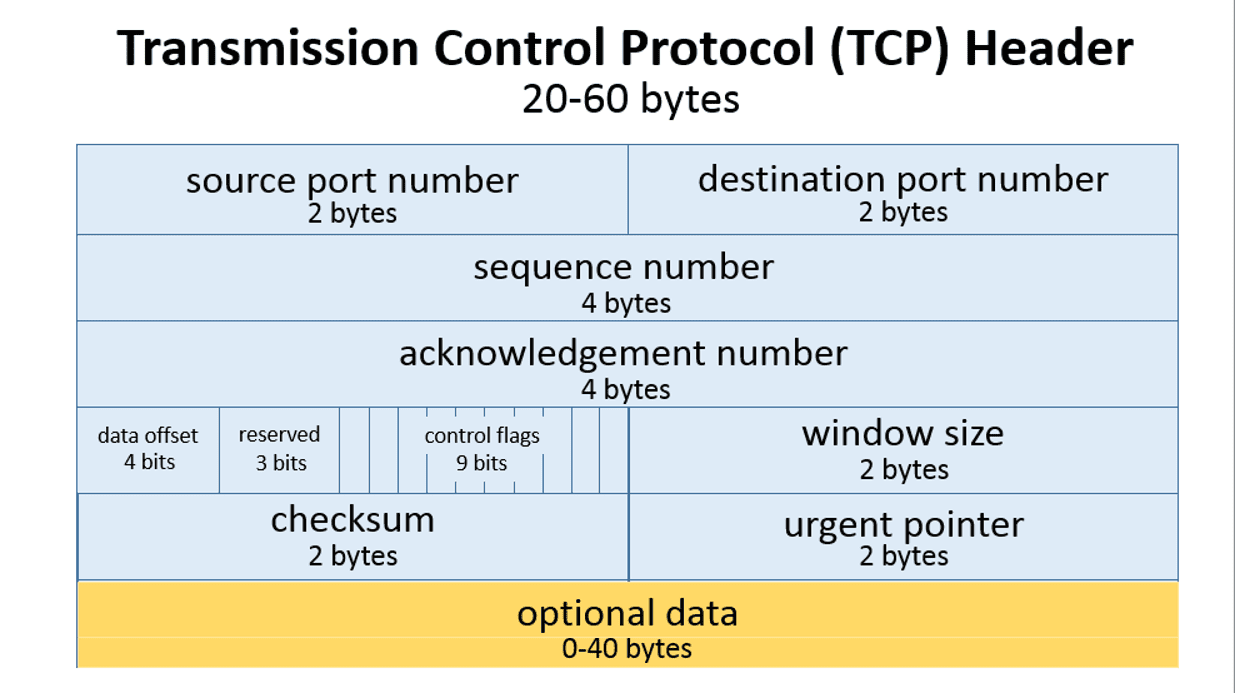
**Transport layer Firewall** 

Figure 4. Layout of a Transmission Control Protocol Header

Source: Internet

The transport layer in TCP/IP model corresponds to the transport layer of the OSI model. The transport layer provides reliable communication between processes on different hosts. Other features that are included in transport layer are: error checking and flow control. In order to achieve reliable communication, the transport layer protocol stipulates that the receiving end must send back a confirmation message, and if the packet is lost, it must be sent again. The transport layer includes Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), which are the most important protocols in the transport layer. TCP is based on IP and defines the format and rules of data transmission from program to program on the network. It provides the transmission confirmation of IP data packets, re-requests of lost data packets, reassembled received data packets according to their sending order Mechanisms. TCP protocol is connection-oriented protocol, similar to making a call, before you start to transfer data, you must first establish a clear connection. UDP is also built on top of IP, but it's a connectionless protocol. The transfer between two computers is similar to delivering a message: a message is sent from one computer to another without an explicit connection between the two. UDP does not guarantee the transmission of data nor does it provide the ability to rearrange or re-request, so it is not reliable. Although UDP's unreliability limits its application, it has better transmission efficiency than TCP.

Similarly to internet layer, transportation layer also has encapsulation and decapsulation (as shown in figure 4). Encapsulation at transportation layer adds important information to a data payload to distinguish processes in a host. For example, Transportation Control Protocol (TCP) adds port number to its data payload. A port number is like an apartment number with in a street number (IP). Each process in a host shared an IP address but can establish its own connection using a different Port number.

Port numbers turn out to be a useful indicator of the purpose of a communication. For example, port number 80 is for HTTP requests that are most likely are webserver. Port number 20/25 is for FTP to download or upload files. Port number 25 is usually for email server.

Therefore, during decapsulation of TCP header, a firewall can implement network security policies that are set based on transportation layer headers. For example, a company wants to block port 80 such that employees cannot visit websites from company. A company may also want to ban FTP such that download from internet is not possible.

**Application Layer Firewall**

The highest layer in TCP/IP model is the application layer. The application layer in TCP/IP model equals the application layer, presentation layer, and session layer combined in OSI model. Its main task is to provide human users an easy to use way of sending and receiving data. Examples of protocols in application layer include HTTP, FTP, Telnet, SMTP and Gopher.

As in previous two sections, firewalls can blocks based on IP or port but this kind of blocking can sometimes be too restrictive and not suitable for certain use cases. For example, blocking port 25 will render no one can send any email which can be very undesirable for most people. One the other hand, letting everyone send email also carries significant risk of leaking sensitive information thru email. This is because firewall at transport layer and internet layer will never look at that kind of data is in the application payload.

Application layer firewall, on the other hand, has the ability to inspect the content at application level, i.e., it may be able to read the email address and contents. It can block packets send to/from port 25 only if the email addresses is from a certain organization or the email body contains keywords such as “password”. Application ley firewall technology has greatly extended the   
  
 This is the most powerful form of firewall because it has the highest level of understanding of the communication.

**Stateful and Stateless Firewall**

A network firewall can make decision immediately for a single traffic based on per-determined rules. This key of firewall is called stateless firewall. One the other hand, a new type of firewall technology can temperately hold packets, not allowing them to go through but neither discarding them immediately. This type of firewall can keep track of packets as a session and wait until enough packets have arrived then make decisions for all packets that belongs to the same session. This type of firewall is called a stateful firewall. Compare to a stateless firewall, a stateful firewall usually requires a certain amount of memory device to store the retained packets. Therefore the price of a stateful firewall is usually higher than a stateless firewall. A person who would like to attach a stateful firewall may also send a great amount of packets to a stateful firewall in hope to overflow its memory.

**Gateway proxy servers**

Proxy servers are network devices that received traffic from a machine and then send out the traffic on behalf of that machine to a destination. Proxy servers may also perform additional modification to the traffic such as encryption or logging. Gateway proxy servers are simple proxy servers that only pass unmodified traffic. The purpose of using a gateway can be different. For example, a gateway can be used to hide an internal LAN from being seen by outside networks. Or a gateway can be used to do load balancing for a group of servers.

However, the most straightforward the use case of a gateway is to hide a machine’s IP. Since a gateway send out your packet on behalf of you, your packet will have the gateway’s IP instead of yours. This can bypass a network layer firewall’s block based on IP. For example, if a website only allows traffic from the United States of America, a user in Germany will not be able to connect to this website normally. But if he/she choose to use a gateway that is located in the United States of America and has a American IP address, he/she can use this gateway to relay his/her requests and the website firewall will allow this request base on the gateway’s IP is valid. Than the gateway can send the user in Germany the web page he/she requested. This is also a weakness of internet layer firewall.

**Virtual Private Network**

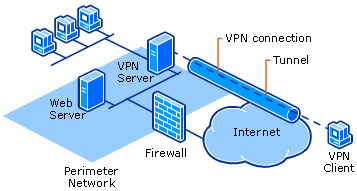


Figure 5, Illustration of a Virtual Private Network (VPN)

Source (Internet)

Virtual Private Network (VPN) is a technology that allows secure communication over a public network (as shown in figure 5). In 1996, engineers at Microsoft developed a secured peer-to-peer tunneling protocol named PPTP. PPTP is a predecer of VPN technology and it represented a need of highly secured way of communicating over unsecure network. As the Internet continues to develop, VPN eventually emerged as the standard method to solve such question. VPN works by sending up a list of VPN servers and uses software to establish a secured and encrypted connection between users over a public network. Once a VPN is established, client can bypass almost all kind of firewalls to access a piece of information. In addition, because all the communication between VPN server and client is always encrypted, we can consider this communication is transmitted via a private tunnel, although the actual network traffic is carried by a public network infrastructure.

**Secure Socket**

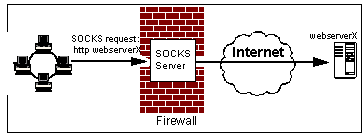


Figure 6. Diagram of how SOCKS works

(Source: Internet)

Sometimes a user behind a firewall has the needs to establish a connection with a remote host from an external network. But such connection is disallowed by the firewall policy. Secure Socket (SOCKS), shown in figure 6, is a protocol that allows authorized users to bypass a firewall policy to establish such connection via a proxy server. For example, a company blocked access to youtube.com to disallow video watching at office. Therefore any packet that has youtube.com’s IP address will be blocked by the firewall. However, the firewall will allow packet send to other IP. An employee who has a home desktop computer with its own IP can be used as a Secured Socket Server. He can send packet to his home computer, which is allowed by the firewall, and let the home computer to retrieve the video from youtube.com and send back to the computer at office. In that way, the firewall thinks the packet is from the home computer’s IP.

**Reference**

Figure 1, *https://www.myfastpc.com/blog/understanding-firewalls/*

Figure 2, *https://*techdifferences*.com/difference-between-tcp-ip-and-osi-model.html*

Figure 3, *https://www.thegeekstuff.com/2012/03/ip-protocol-header/*  
Figure 4, *https://www.lifewire.com/tcp-headers-and-udp-headers-explained-817970*  
Figure 5, *https://www.stupidtechlife.com/setting-up-a-vpn-connection-on-windows-10/*Figure 6, *http://medialab.di.unipi.it/web/doc/JNetSec/jns\_ch12.htm*