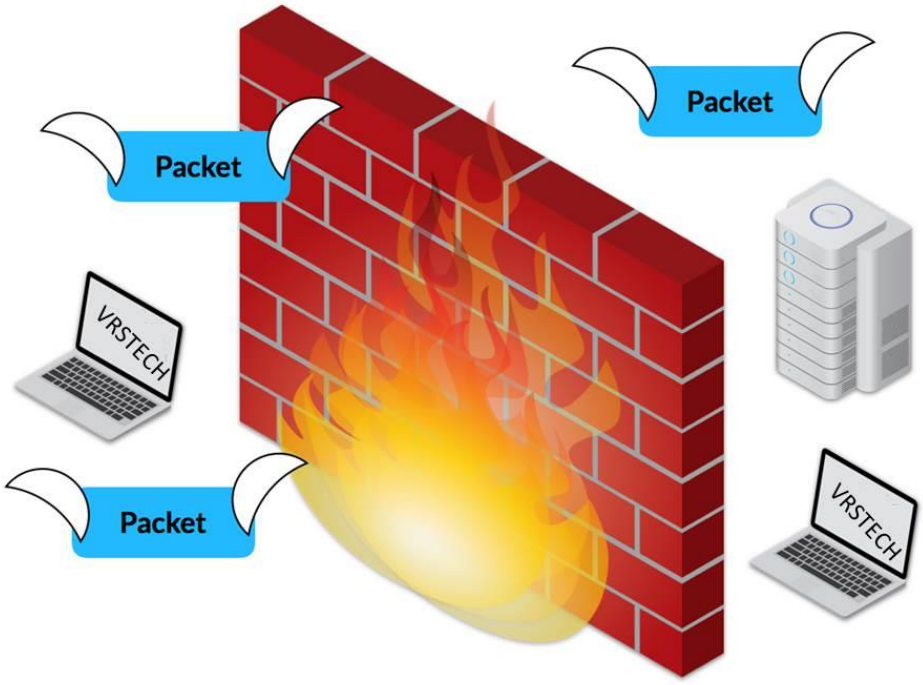
COMP 4108 – COMPUTER SYSTEMS SECURITY

Experience 7 – Network Firewalls



Student Name: Ben Cendana
Student #: 100811212
Date: March 12 2018

Table of Contents

1.0: Introduction

Dr. Somyaji provided the class with four foundational papers to read, among them was the paper *Network Firewalls* by Steven M. Bellovin and William R. Cheswick. This experience will document what was learned from that paper and how the knowledge gained from the paper can be used to build effective network firewalls.

The article makes it clear that there are three distinct types of network firewalls these are:
a) Packet Filters b) Application- Level Gateways c) Circuit Level Gateways and each type of network firewall has a distinct advantage and disadvantage.

But in order to use the three network firewalls effectively its important to understand how to read, interpret what type of network traffic is entering/leaving the network, the overall network behaviour and the protocol of each packet.

1.1: Wireshark

The first step in understanding the networks behaviour is to perform a network audit to perform this task a network analyser tool such as Wireshark can be used.

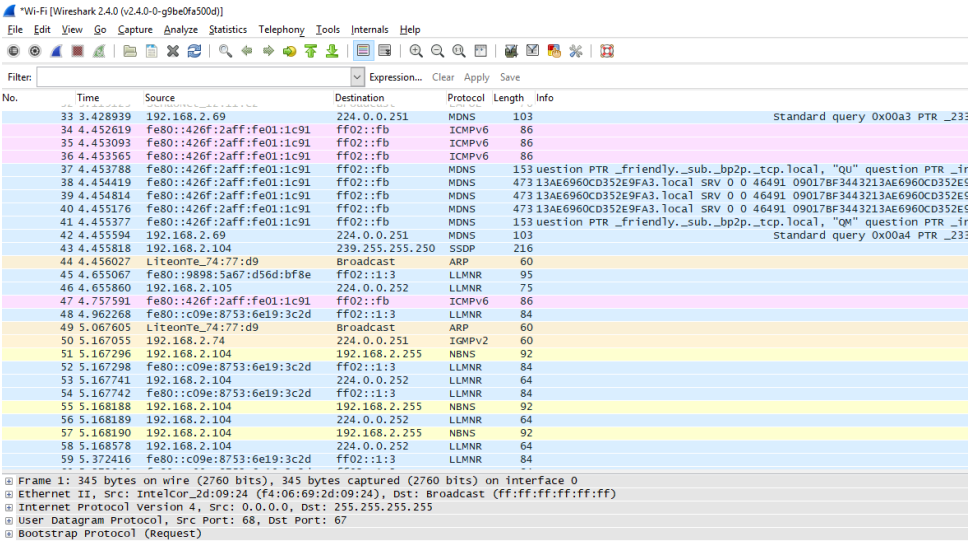


Figure 1: Wireshark Capture

As we can see in Figure 1 the Wireshark capture provides information regarding the time, the source IP, destination IP, protocol and general info about the packets.

Based on the protocol we can then determine what the network traffic is and to a lesser extent if its malicious.

1.2: Network Protocols

Knowing each protocol and what type of network traffic is associated with that type of protocol can give us clues what that packets primary function is. If we know what the packet is trying to do we can make an inform decision if that packet is malicious or not.

Its almost impossible to know every protocol but by knowing where the protocol belongs according to the OSI Model or TCP/IP Protocol Architecture Model we can understanding what it is trying to do.

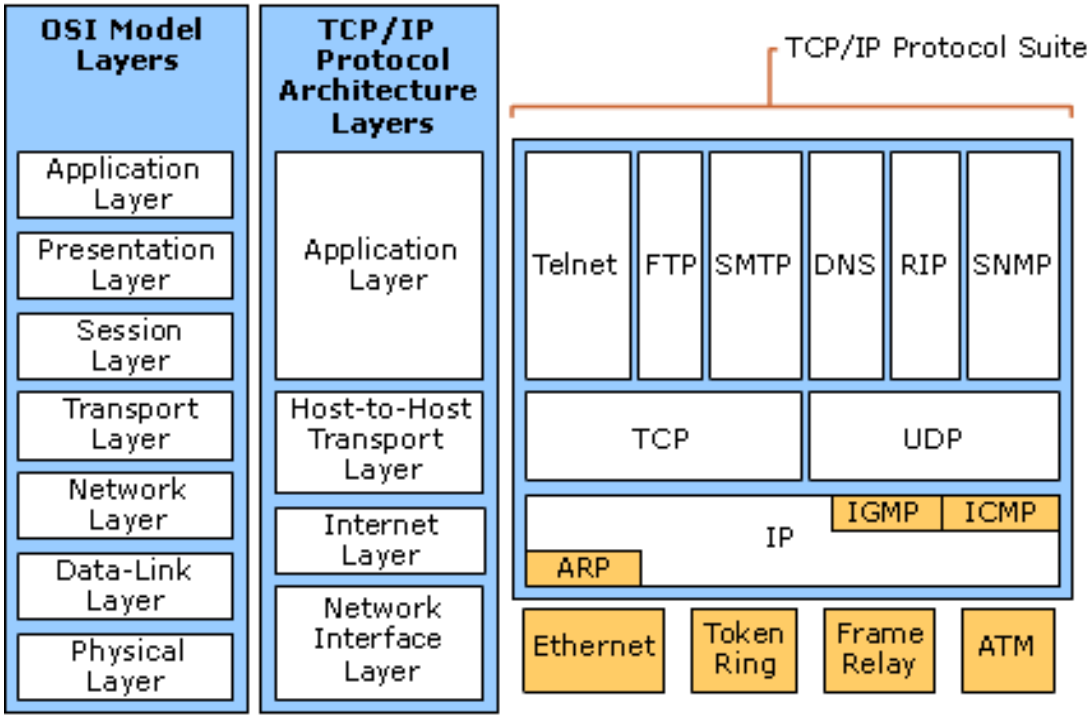


Figure 2: The TCP/ IP Protocols and The Corresponding Protocols Of Each Layer

Each of the layers performs the functions as listed below:

Application Layer: Provides services to lower level layers
Host-to-host Transport Layer: Provides Network Communication
Internet Layer: Datagram Transportation
Network Interface Layer: Network Hardware

2.0: The Network Firewalls

2.1: Packet Filters

As the name suggests packet filters are firewalls that filter incoming packets based on predefined rules. These rules are normally based on any of the following or a combination of them:

1) Source IP
2) Destination IP
3) Source IP
4) Source Port
5) Destination Port.

Provided with the Linux operating system is a packet filter called IP Tables which can accessed by the command **iptables -L.**

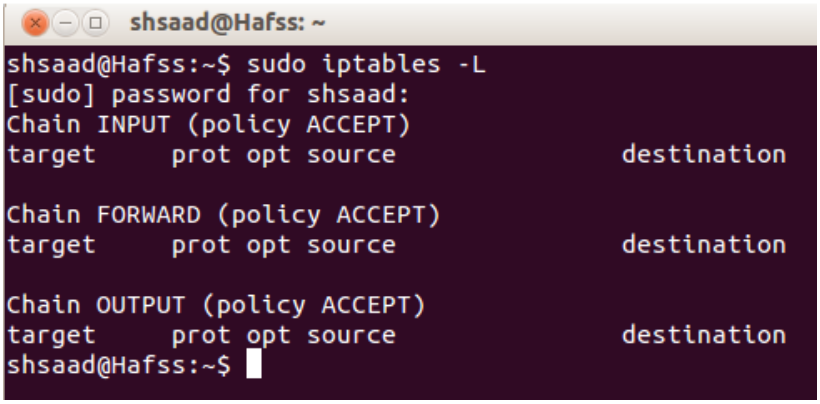


Figure 3: IP Tables

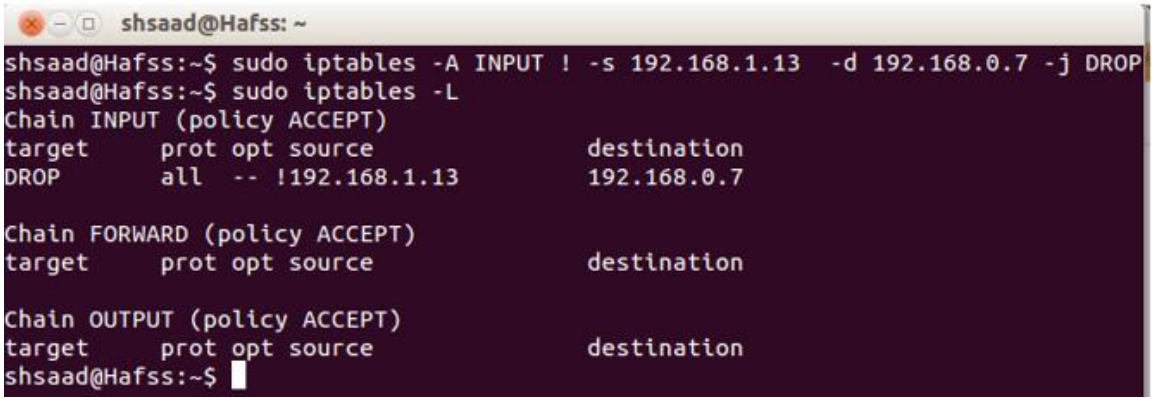


Figure 4: IP Tables With A Blocked IP

As we can see in Figure 4 all packets from the source IP 192.168.1.13 are blocked from entering the destination IP 192.168.0.7.

2.1.1: Packet Filters Advantages

The main advantage to using a packet filter is the speed in which it processes incoming/outgoing packets this is because packet filters operate on the transport and network layers.

2.1.2: Packet Filters Disadvantages

The primary disadvantage as highlighted in the article is a dedicated attacker could simply spoof there source IP and enter the network by spoofing or the administrator will detect the intruder but will be forced to create a new rule blocking another source IP.

2.2: Application Gateways

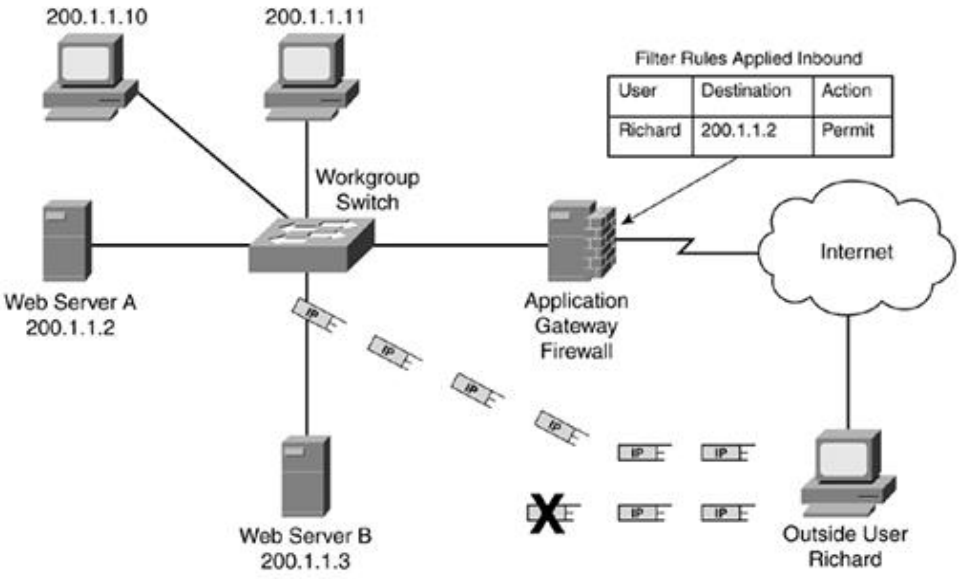


Figure 5: An Example Of An Application Gateway

In contrast to packet filters an application gateway works by having a layer of authentication that checks to ensure anyone accessing the network is valid. For that reason Application Gateways are popular among email and webservers were the user requesting the service can be authenticated.

Typical methods of authentication involve having a separate browser with logins similar to an SSH connection or the client can be authenticated when it sends a TCP request to access the network.

2.2.1: Application Gateways Advantages

The main advantage of this type of firewall is users are authenticated rather then the device which makes spoofing an IP extremely difficult.

2.2.2: Application Gateways Disadvantages

Due to the authentication process, application gateways are slower and offer very few services. This is because this type of firewall require more processing power and all the processing power will be dedicated to authentication.

2.3: Circuit Level Gateways

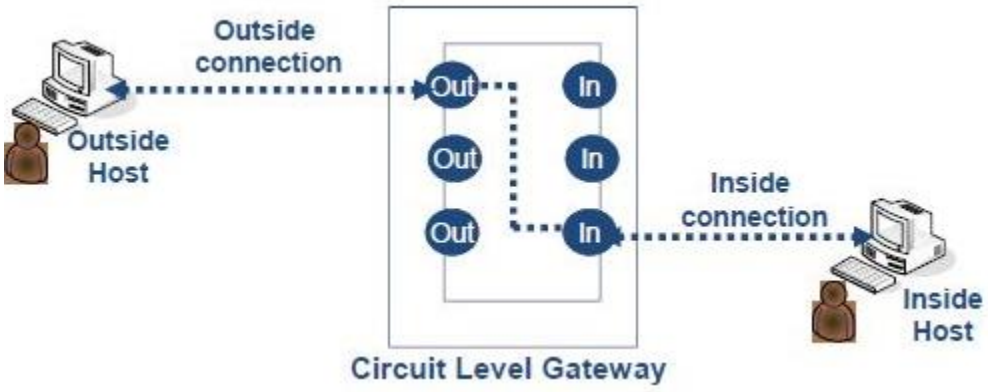


Figure 6: An Example Of A Circuit Gateway

Circuit level gateways operate by checking the connections between the host and the server, if a successful handshake occurs such as a TLS handshake then it know the connection is secure and should therefore allow the packet to enter the network.

2.3.1: Circuit Level Gateways Advantages

Since sniffers and network topology scanners are not secure connections and do not offer a TLS handshake it can be difficult for an attacker to test the network for vulnerabilities.

2.3.2: Circuit Level Gateways disadvantages

Since most of the emphasis is concerned with building a secure connection, circuit level gateways do not sanitise incoming packets and there contents. Therefore a connection maybe secure but the packets may not be.

3.0: Putting It All Together

3.1: Performing An Network Audit

Putting together what we know about protocols and how to use Wireshark we can determine the network behaviour in Figure 3. We can tell that the TCP protocol was in use since the TCP protocols ar used to initiate communication. We can also tell the client at IP 192.168.2.94 was attempting to communicate to the server at 40.117.145.132.

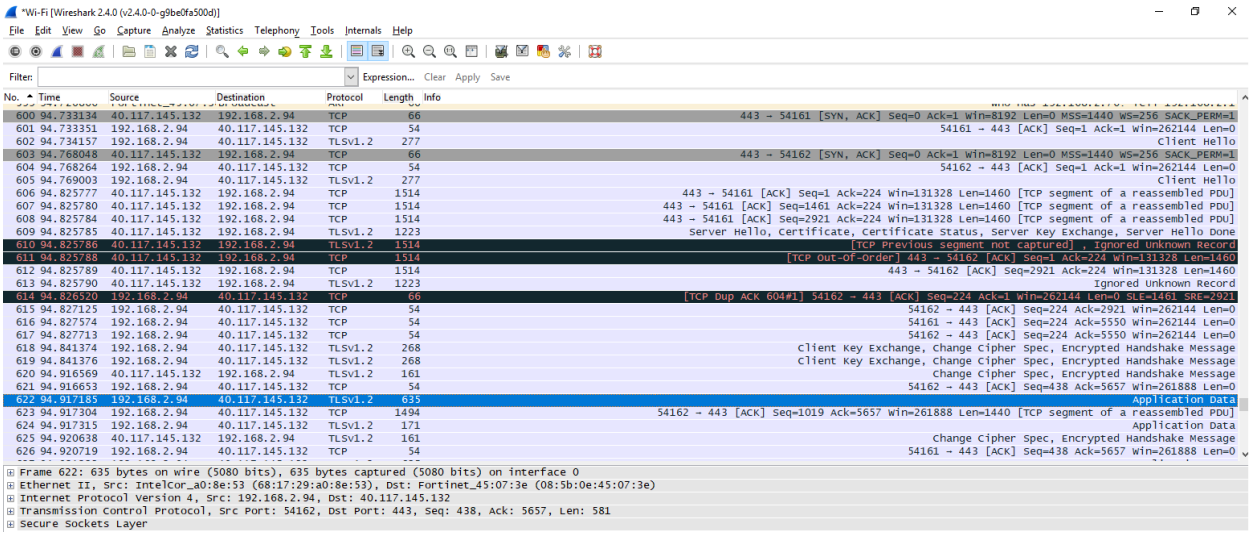


Figure 7: TCP ACK Sequence Captured

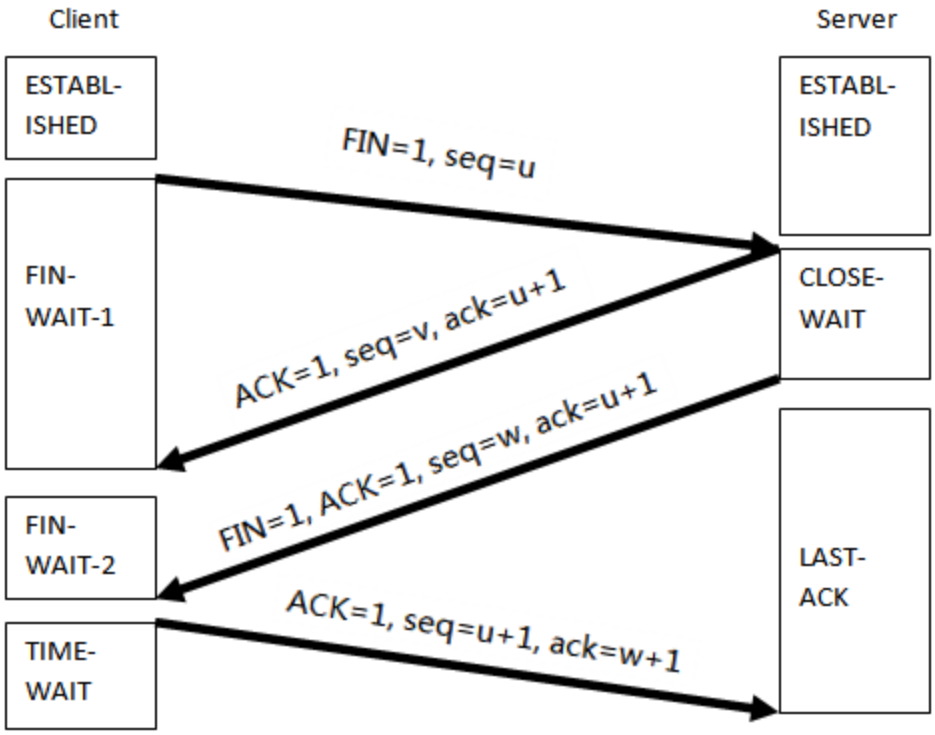


Figure 8: TCP ACK Sequence

The communication between the client at 192.168.2.94 and the server is not much different then the communication modeled in Figure 4. If we look closely at Figure 3 we can tell that the packets are ACK packets indicating that the client was successful *Acknowledged* by the server.

However, an error occurred which was highlighted indicating that the packets being sent back to the client arrived out of order and the client failed to receive the last ack packet from the server.

Based on this information we can get some idea of what kind of network behaviour is occurring, what type of firewall should be used and is the existing firewall working properly?

3.2: Which Type Of Firewall Should be Used?

In all likelihood a packet filter was most likely the cause of the ACK sequence failing as it can block the client/server from receiving packets and establishing some form of communication.

For the example listed above all the firewalls should be able to work fine. But depending on what type of service your network provides the decision should be based on the pros/cons described in section 2.0.

The best type of defense is essential any firewall with every packet being blocked. A dedicated administrator should then be present to perform an network audit and once the checks are completed allow the incoming packet.