A Proposed Firewall For Viruses

Hillal Mohammad Yousif*
Mohammad Ala'a AL-Hamami* Soukaena Hassan Hashem*

Abstract:

The open communication network, Internet, has problems surrounding the security of the **Internet sites.** Such as hacker intrusion costing organizations a large amount of money and untold losses in productivity; hate groups using the Internet to distribute their malicious works to these sites, and many other types of attacks. A firewalls strategies protect Internet sites from intentional hostile intrusion that could compromise confidentiality or results in data corruption or denial of service.

This research would build a firewall against the unauthorized intruders, viruses which have specified signatures, worms and Trojan horse. Depending on the dual bastion host configuration for the web hardware, packet filtering firewall, detect the IP impersonate attack (by both worm and Trojan horse to enter the web as authorized IP) by the proposed SYN/ACK checkup procedure and last install a virus scanner for the data in all packets of the session by the proposed procedure which is three handshaking proxy procedure.

Keywords:
Firewalls, anti-virus, internet site, intrusion, worms, Trojan horse.

---

* AL-Rafidian University College, Baghdad, Iraq.

1- Introduction [1]:

When you send information through the Internet, the information is broken down into small pieces, called packets. Each packet travels independently through the Internet and may take different path to arrive at the intended destination. All the protocols encapsulate data into envelopes referred to as Protocol Data Units (PDU s). There are many different labels used for this (PDU s) at various layers. As shown in figure (1) .

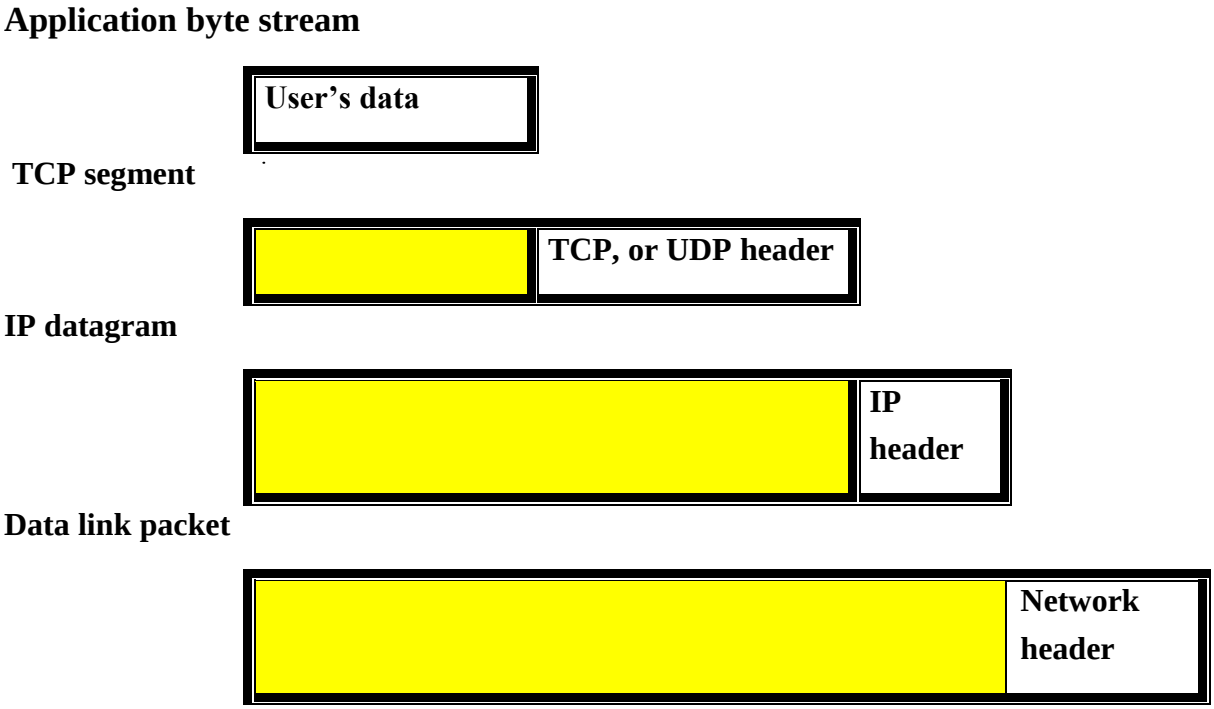


Figure (1) protocol data units in the TCP/IP model.

First of all we have user's data in application layer represented as byte stream. Data user transmitted to the transport layer. According to the protocol used in this layer (either TCP or UDP) data user encapsulation is accomplished. TCP may break the blocks of data user into smaller pieces to make it more manageable. To each piece, TCP appends control information in the TCP header, forming TCP segment.

1.1- Security Attacks [2, 4]:

Internet makes the world as a global village, and all the doors are unlocked. In the past, people in small villages left their doors unlocked because they trusted everyone else, and knew that nothing bad was going to come of their lack of security. In case of the Internet, however, people know that something bad is likely to happen to them if they do not lock their doors.

They know that there are a number of individuals out there who have nothing better to do than to attempt to break into their computer systems just for hell of it. From that the administrators of the sensitive sites considers the security is a wide and important issue in computer networks. A security policy must attempt to protect the privacy of users and their data, control access to restricted data and resource and prevent fraudulent transactions. Because of the previous reasons many protections systems are appear to protect the sensitive sites on the Internet from many and different types of penetrations and attacks. Any action that compromises the security of information owned by an organization. *These attacks may be:* ***Interruption*****:** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. ***Interception*****:** An unauthorized part gains access to an asset. This is an attack on confidentiality. ***Modification*****:** An unauthorized party not gains access to but tampers with an asset. This is attack on integrity. ***Fabrication*****:** An unauthorized party inserts counter fiet objects into the system. this is an attack on authenticity.

Computer viruses are programs which replicate themselves, attach themselves to other programs, and perform unsolicited and often malicious actions. Self-replication is the key trait that distinguishes viruses from other destructive programs. For instance, a Trojan Horse is a program which performs unsolicited actions, but it cannot replicate and spread on its own. A payload is an action performed by a virus - usually, but not always, the action that reveals the virus' presence. Examples of payloads include:

- "Amusing" or political messages (such as the Nuclear macro virus which asks for a ban on the French nuclear testing).
- Prevention of access to one's disk drives (the Monkey virus).
- A stealth boot virus overwriting data as it attempts to write pre-infected boot information to another part of the disk.
- Inconspicuous activity and minute data damage spread out over a long period of time - probably the most lethal type of virus effect (the Ripper virus).

Typical Signs that a Virus May Be Present:

- Unusual messages displayed
- Files are missing or have increased in size
- System operates slower
- Sudden lack of disk space
- Cannot access disk

Worms

Network worm programs use network connections to spread from system to system, thus network worms attack systems that are linked via communications lines. Once active within a system, a network worm can behave as a computer virus, or it could implant Trojan horse programs or perform any number of disruptive or destructive actions. In a sense, network worms are like computer viruses with the ability to infect other systems as well as other programs. Some people use the term virus to include both cases.

To replicate themselves, network worms use some sort of network vehicle, depending on the type of network and systems. Examples of network vehicles include:

- a network mail facility, in which a worm can mail a copy of itself to other systems,
- a remote execution capability, in which a worm can execute a copy of itself on another system,

- a remote login capability, whereby a worm can log into a remote system as a user and then use commands to copy itself from one system to the other.

The new copy of the network worm is then run on the remote system, where it may continue to spread to more systems in a like manner. Depending on the size of a network, a network worm can spread to many systems in a relatively short amount of time, thus the damage it can cause to one system is multiplied by the number of systems to which it can spread. A network worm exhibits the same characteristics as a computer virus: a replication mechanism, possibly an activation mechanism, and an objective. The replication mechanism generally performs the following functions:

- searches for other systems to infect by examining host tables or similar repositories of remote system addresses
- establishes a connection with a remote system, possibly by logging in as a user or using a mail facility or remote execution capability
- copies itself to the remote system and causes the copy to be run The network worm may also attempt to determine whether a system has previously been infected before copying itself to the system. In a multi-tasking computer, it may also disguise its presence by naming itself as a system process or using some other name that may not be noticed by a system operator.

1.2 Firewall mechanisms [3]:

The common types of the firewalls according to the levels of TCP/IP and OSI stacks are:

a- Network Level Firewall (Packet Filtering Firewall):

A packet filtering is an access control mechanism for network traffic. Instead of processing or forwarding all packets that leave and arrive on the node's network adapters, the packet filters consults its access control rules before handling each packet. Work at the network layer of TCP/IP stack and OSI stack in the same principle. A filter is a program

that, in general examines the IP addresses (source and destination addresses), ports numbers, protocol type , and service type fields of every incoming specified access control mechanism.

b- Application Level Firewall (Application Proxy):

These firewalls work a bit differently from packet filtering firewalls. Application gateway firewalls are software-based when a remote user from the void contacts a network running an application gateway, the gateway blocks the remote connection. Instead of passing the connection along, the gateway examines various fields in the request, if these meet a set of predefined rules, the gateway create abridge between the remote host and the internal host (in common called proxy).

c- Circuit Level Firewall (Circuit Proxy):

A circuit level gateway firewall is a generic proxy that does not know the specifies of the application but performs a more generic set of capabilities. Circuit level gateways work at transport layer of TCP/IP stack and OSI stack in same principle. The circuit level firewalls monitor TCP three handshaking in the TCP connection (session) between packets to determine whether a requested session is legitimate.

1.3- Anti-virus Techniques [5]:

Without anti-virus software, there is no conclusive way to rule out viruses as the source of such problems and then arrive at solutions.

Effective anti-virus software must be capable of performing three main tasks: Virus Detection, Virus Removal (File Cleaning) and Preventive Protection. Of course, detection is the primary task ad the anti-virus software industry has developed a number of different detection methods, as follows.

Five Major Virus Detection Methods:

- **Integrity Checking (aka Checksumming)** - Based on determining, by comparison, whether virus-attacked code modified a program's file characteristics. As it is not dependent on virus signatures, this method does not require software updates at specific intervals. ***Limitations*** - Does require maintenance of a

virus-free Checksum database; allows the possibility of registering infected files; Unable to detect passive and active stealth viruses; Cannot identify detected viruses by type or name.

- **Interrupt Monitoring** - Attempts to locate and prevent a virus "interrupt calls" (function requests through the system's interrupts). ***Limitations*** - Negative effect on system resource utilization; May flag "legal" system calls and therefore be obtrusive; Limited success facing the gamut of virus types and legal function calls.
- **Memory Detection** - Depends on recognition of a known virus' location and code while in memory; Generally successful. ***Limitations*** - As in Interrupt Monitoring, can impose impractical resource requirements; Can interfere with valid operations.
- **Signature Scanning** - Recognizes a virus' unique "signature," a pre-identified set of hexadecimal code, making it highly successful at virus identification. ***Limitations*** - Totally dependent on maintaining current signature files (as software updates from vendor) and scanning engine refinements; May make false positive detection in valid file.
- **Heuristic/Rules-based Scanning** - Faster than traditional scanners, method uses a set of rules to efficiently parse through files and quickly identify suspect code (aka Expert Systems, Neural Nets, etc.). ***Limitations*** - Can be obtrusive; May cause false alarms; Dependent on the currency of the rules set.

2- The Proposed Protection System:

All traffics from inside to outside, and vice versa through the main entry, must pass through the firewall. This is achieved by physically blocking all access to the site except via the firewall. Various configurations are possible. Only authorized traffic, as defined by the local security policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies. In general Firewall is one of the famous types of intruder detection. Security of firewalls neither provides perfect security nor is free of operational

difficulties. The most important limitations of the firewall are interpreted in the following points:

- Firewalls can not protect against the transfer of virus-infected programs or files**.**
- Firewall not effective against worms andTrojan horse because it is authenticate itself to a firewall after impersonate an authorized packets by IP spoofing.

In this research we would describe how to build secure web against many types of attacks. The following sections describe all the basics to develop the proposed system.

2.1- The Web Hardware to Build the Firewall:

We propose to make the web hardware as a Dual homed bastion is a bastion hosts configuration to support two network interfaces one face in toward the secure site and one face out toward the Internet. Screened host firewall, dual-homed bastion has physical configuration prevent direct flow through router between the Internet and other host on private network if the packet filter router is completely compromised. As shown in figure (2).

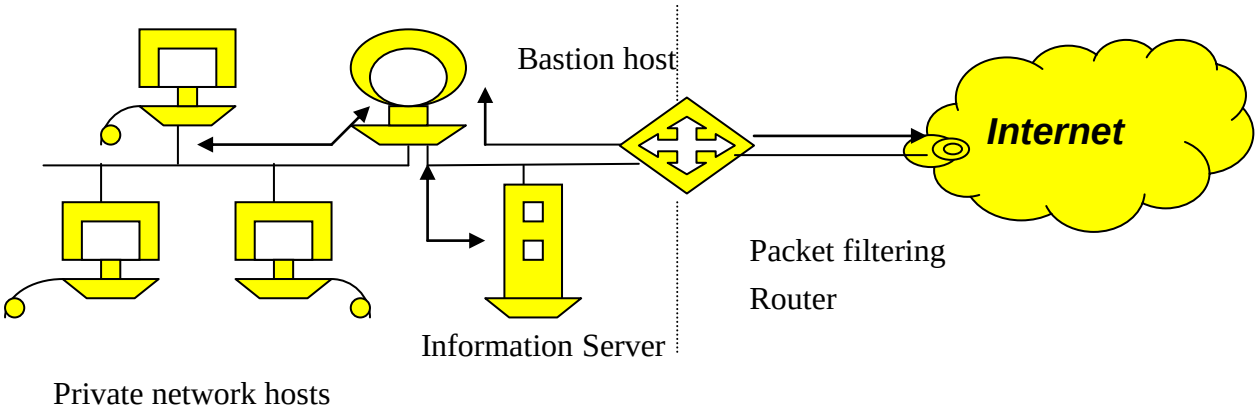


Figure (2) Screened Host Firewall, Dual-Homed bastion Architecture:

External Router:

The external router response to direct connect the protected site with the Internet, so the external router controls all the connections deals with

the site. And this is the basic and unique operation do it. ***It is operations are the IP header filtering firewall.***

Bastion Host:

Bastion host represents the basic element in any proposed protection system for the Internet site, because it response to connect the protected site with the Internet by the modems, so the bastion host controls all the dial up connections deal with the site. By using this proposed configuration all the packets even were secure authorized packets to secure server or normal authorized packets to normal users communicates with the protected site by the Bastion host address (advertise address). ***It is operations are the IP header filtering and anti-virus scanners.***

Information Server:

The information server response only to provide public information for normal authorized users. And this is the basic and unique operation do it.

Secure Network:

The secure network response to receive and send secure and sensitive information for secure authorized users. Remember that no one know the address of the secure server only the administrator of the site. ***It is operations are the Syn/Ack check up to detect the worms and Trojan horse.***

2.2- Packet Filtering Firewall:

This procedure is a traditional type of firewall but it provides good **access control mechanism** at IP layer and TCP layer and either accept or reject packets based mainly on the following fields in common. They are Source IP address at IP layer, Destination IP address at IP layer, Protocol number at IP layer, Source port number at TCP layer, and Destination port number at TCP layer. Figure (3) explain the packets captured from the adapter immediately and stored in a buffer before they accessed to the network and upper layers.

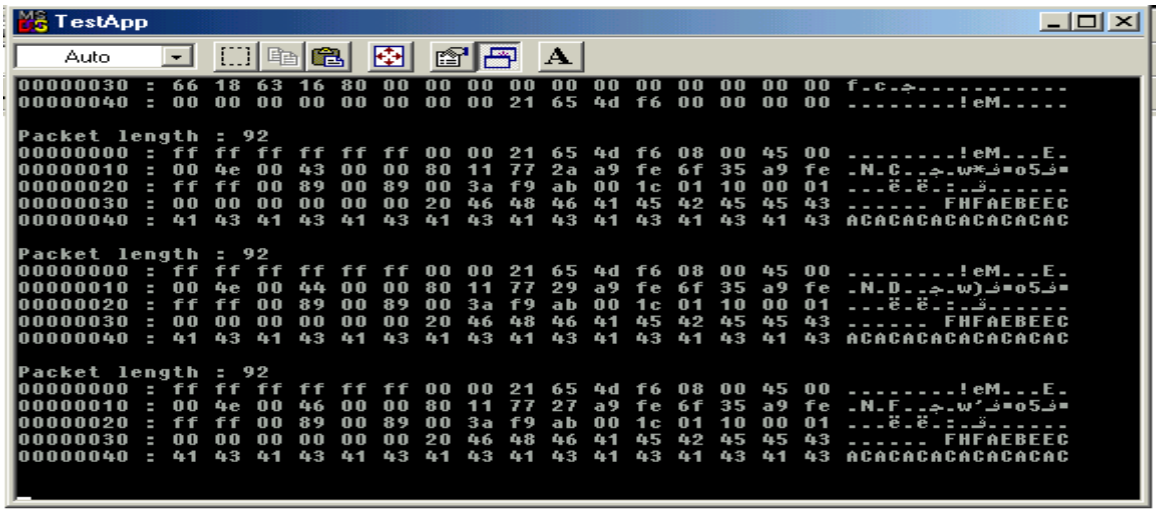


Figure (3) packets captured from adapter by packet capture software.

2.3- Three Handshaking proxy procedure (virus detection):

In normal case when packets pass the protected site to secure network these packets must pass through a Bastion host and these packets submitted to a specific procedure.

We would propose a protection procedure for secure network is an approach for defending against all the viruses which have signatures. The three handshaking proxy counters the virus by collect the data of all the packets of the session in a buffer by making sure that the three-way handshaking is actually completed between the secure authorized site and bastion host before sending a SYN packet to the secure network, destination of connection. To declare this procedure let secure network be S, let Bastion host be B, let author site be A. and note the following points:

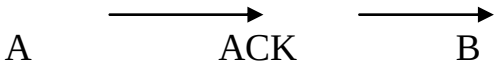
1. Suppose A request connection to secure server, at first A send SYN packet to B.

A ⟶ SYN ⟶ B

2. B receive the SYN packet but it does not pass the SYN packet to S but rather B send SYN/ACK to A directly.

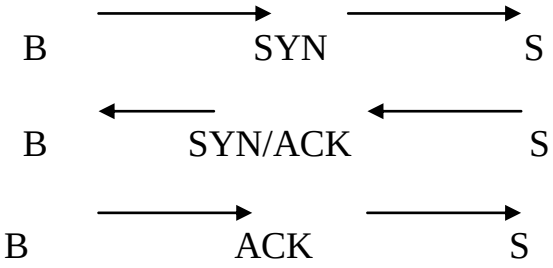
A ⟵ SYN/ACK ⟵ B

3. If A send ACK packet to B then the connection is established between A and B.



4- Get the data of all the packets of that session and store it in a buffer. Then that buffer would submitted to **Signature Scanning** - Recognizes a virus' unique "signature," a pre-identified set of hexadecimal code, making it highly successful at virus identification. to detect if the data has virus or not this depend if there is a signature of a virus in the data, then the session destroyed and assign that session as malicious one then put all the information related to it (such as source and destination IP addresses, ports, protocol type and statues) as unauthorized packets that would be as updating for firewall rules. But if there is no virus the session would be established with the secure network as in the following step.

5- Now B would make a connection establishment between B and S but it would use the SYN and ACK of A.



The best anti-virus software in the world cannot protect you if it is not deployed systematically throughout the enterprise (even if "the enterprise" is a single homebased computer!).

2.4- SYN/ACK Check Up Procedure:

Worms and Trojan horse are malicious code they are have unauthorized addresses but to pass the firewall they would impersonate an authorized IP address then they enter to the firewall and pass it. This

impersonation would be done by the IP address spoofing attack. To detect that impersonation we suggest the following procedure:

As known TCP is a connection-oriented and reliable transport protocol. When the authorized host communicate with the secure network at first establish a connection by three handshaking and then exchange data and at the last finish the connection by, finished the three handshaking. TCP header contain the SYN field which identify the number of bytes in the TCP segment and ACK field which detect that the recipient receive these bytes and expect the next byte. This point would be very important in security as declared in the following points:

1- SYN/ACK checkup in the connection establishment three handshaking. The legitimate and secure three handshaking depend on checking the ACK found in the received packet by the secure server during connection establishment:

IF (ACK (in received packet by secure server) = SYN (previous packet sent by secure server) + 1) THEN it legitimate and secure three handshaking.

The intruders whose stay in the middle between authorized client and secure server could not know any thing about the SYN/ACK of three handshaking for connection establishment because the entire packet is encrypted when send from or to secure server. This point in this procedure represents the **circuit gateway scheme**.

2-For data exchange after connection establishment three handshaking , the SYN/ACK must be checked up by the secure server to guarantee the intruders could not sent their packets after three handshaking because the SYN/ACK in the packets transmitted between the two hosts aren't checked. The check up for data exchange detected by the following equation :

IF (ACK (in received packet by secure server) = SYN (previous packet sent by secure server) + BUFFER (previous packet received by the secure server)) .

This procedure provide good protection against the, IP Impersonation Attack, this by make assurance that the session is a legitimate.

3- Conclusions:

In this research we conclude the following:

1. There is no perfect firewall because always there are intruders and new types of different attacks and malicious code. But since all the attacks can be pass the firewall as packets, so the proposed firewall protection system could be strong since it intend to analyze all the components of the packet headers and data.
2. Analyze the headers for recognizing the unauthorized intruders, worms, Trojan horse by packet filtering and syn/ack checkup procedure. And data by collect all the data of the packets for one session by three handshaking procedure and store them in a buffer would be submitted to a virus scanner to detect if this session is infected or not.
3. The SYN/ACK check up procedure represent the basic procedure in the proposed system, because it protect both the secure server and bastion host from IP Spoofing (IP Impersonation) Attack. This by checking up the SYN/ACK to all the packets enter and leave the protected site along the session (not only in the three handshaking).
4. The Three-Handshaking Proxy procedure represent the most important element in the firewall to protect the secure server from IP Spoofing (IP Impersonation) Attack. This by make the bastion host as a buffer for all the data in all the session's packet. If the malicious attack (viruses) has known signature then this attack would be prevented, but if has not known signature then the damage would be on the bastion host only.

References:

1. Russell .T .,**" Telecommunication Protocols"** , Second Edition , Mc-Graw Hill Companies ,Inc.,2000.
2. Mcnulty .F .L . , Associate Director For Computer Security National Institute of Standards and Technology U.S. Department of Commerce, **" Security on The Internet "**, Before the Subcommittee on Science, Space, and Technology U.S. House of Representative, March 22, 1994.
3. Zwicky .E .D ., Cooper .S ., and Chapman .D .B ., **" Building Internet Firewalls"**, Second Edition, O'Relly & Association, June 2000.
4. Bug Killers **" A new Generation of Antivirus Softwrae offer Maximum Protection "**, Pc Magazine , February, vol. 4, issue 2, 2004. **www.Pcmag.mideast.com.**
5. Wolder .B ., **" Internet/Intranet Security "**,NSS Group , 2004.

Email: web master@Nss.co.uk.