Implement the packet filtering mechanism using the Dual-homed host architecture

Mustafa Sabah Mustafa
Al-Mansour University College
Computer science department
Abstract

In today's world, most business, regardless of size, believe that access to Internet is imperative if they are going to complete effectively. Yet connecting a private computer (or a network) to the Internet can expose critical or confidential data to malicious attack from anywhere in the world since unprotected connections to the Internet (or any network topology) leaves the user computer vulnerable to hacker attacks and other Internet threats. Therefore, to provide high degree of protection to the network and network's user, **Firewall** need to be used.

**Firewall** provides a barrier between the user computer and the Internet (i.e. it prevents unauthorized Internet users from accessing private computers and networks connected to the Internet).

This paper concerned with the design and implementation of a firewall system which is used to protect both individual computers and corporate networks from hostile intrusion coming through Internet.

The Dual-homed host architecture has been used to implement the proposed firewall system. Finally, This system is built depending on the packet filtering mechanism to regulate all the packets entering and leaving the protected site using IP address and port number of the TCP packet. Also this system deals with application level and monitors all packet data (content) and maintains the firewall activity with Internet connection.
نتائج التطور والنمو السريع في شبكات المعلومات و الإنترنت نظرا لأهمية الإنترنت

في عالم اليوم لما يوفره من خدمات للمستخدمين من سهولة الحصول على المعلومات المختلفة بسرعة عالية وقابل جهد يمكن، كل هذه الفوائد وغيرها يمكن أن تكون إلى ضياع خطيرة، إذ إن ارتباط الحاسبة الخاصة (LAN) أو الشبكات المحلية (Private Computer) وال точки (Intruders) الذين يحاولون بطريقة ما إيجاد نقطة ضعف أو منفذ للدخول عبر الإنترنت إلى هذه الحاسبات لأغراض التجسس أو سرقة معلومات (التلاعب بالحاسبات المصرفية أو معرفة كلمة سر وغيرها) أو في بعض الأحيان لاغراض التخريب ليس إلا. لذلك أصبح من المهم جدا إيجاد طريقة لحماية الشبكات ومستخدميها من مثل هذه التهديدات. واحدة من أهم طرق الحماية التي توفر درجة عالية من الأمنية هي استخدام جدار النار (Firewall).

يفتح المجال أمام هجمات القراصنة (Hackers) والدخلاء (Intruders) الذين يحاولون بطريقة ما إيجاد أي نقطة ضعف أو منفذ للدخول عبر الإنترنت إلى هذه الحاسبات لأغراض التجسس أو سرقة معلومات (التلاعب بالحاسبات المصرفية أو معرفة كلمة سر وغيرها) أو في بعض الأحيان لاغراض التخريب ليس إلا. لذلك أصبح من المهم جدا إيجاد طريقة لحماية الشبكات ومستخدميها من مثل هذه التهديدات. واحدة من أهم طرق الحماية التي توفر درجة عالية من الأمنية هي استخدام جدار النار (Firewall).

1.1 Introduction:

The Internet has made large amounts of information available to the average computer user at home, in business and in education. For many people, having access to this information is no longer just an advantage, it is essential. Yet connecting a private network to the Internet can expose critical or confidential data to malicious attack from anywhere in the world. Users who connect their computers to the Internet must be aware of these dangers, their implications and how to protect their data and their critical systems. Firewalls can protect both individual computers and corporate networks from hostile intrusion from the Internet, but must be understood to be used correctly [14].

A firewall examines all traffic routed between the two networks to see if it meets certain criteria. If it does, it is routed between the networks, otherwise it is stopped. A firewall filters both inbound and outbound traffic. It can also manage public access to private networked resources such as host applications. It can be used to log all attempts to enter the private
network and trigger alarms when hostile or unauthorized entry is attempted. Firewalls can filter packets based on their source and destination addresses and port numbers. This is known as address filtering. Firewalls can also filter specific types of network traffic. This is also known as protocol filtering because the decision to forward or reject traffic is dependant upon the protocol used, for example HTTP, FTP or Telnet. Firewalls can also filter traffic by packet attribute or state [14].

1.2 Types of Firewalls:

There are many types of firewall, they tend to differ in their approach but can be characterized as firewalls, which block traffic, and firewall which permit traffic. Then each one of them differ than the other in behaves but they are all share the same point that they do as a shield to protect the private network users.

1.2.1 Packet Filtering Firewall:

A packet filter firewall is a first-generation firewall technology that analyzes network traffic at the transport protocol layer. Each IP network packet is examined to see if it matches one of a set of rules defining what data flows are allowed. These rules identify whether communication is allowed based upon information contained within the Internet and transport layer headers and the direction in which the packet is headed (internal to external network or vice-versa), see figure 1.1.

Packet filters typically enable you to manipulate (that is, permit or prohibit) the transfer of data based on the following controls [1]:

1. The physical network interface that the packet arrives on
2. The address the data is (supposedly) coming from (source IP address)
3. The address the data is going to (destination IP address)
4. The type of transport layer (TCP, UDP, ICMP)
5. The transport layer source port
6. The transport layer destination port

Packet filters generally do not understand the application layer protocols used in the Communication packets. Instead, they work by applying a rule set that is maintained in the TCP/IP kernel. This rule set contains an associated action that will be applied to any packets matching the criteria mentioned above.
Figure 1.1: Depicts The Network Packet Evaluation Process Used By a Packet Filter Firewall.

Packet filters typically implement command sets that allow the checking of the source and destination port numbers on the TCP and UDP transport layer protocols. This check determines whether an applicable permit or deny rule exists for that specific port and protocol combination. Due to the fact that the ICMP protocol layer does not utilize port numbers for its communications protocol, it is difficult for packet filters to apply any security policy to this form of network traffic. In order to apply an effective security policy to Impute packet filter must maintain state tables to ensure that an ICMP reply message was recently requested from an internal host.
This ability to track communications state is one of the primary differences between simple packet filters and dynamic packet filters.

Because packet filters are implemented in the network layer, they generally do not understand how to process state information in the high-level protocols, such as FTP. The more sophisticated packet filters are able to detect IP, TCP, UDP, and ICMP. Using a packet filter that includes the TCP/UDP port filtering capability, you can permit certain types of connections to be made to specific computers while prohibiting other types of connections to those computers and similar connections to other computers.

The complete network packet inspection adheres to the following general algorithm [1]:
1. If no matching rule is found, then drop the network packet.
2. If a matching rule is found that permits the communication, then allow peer-to-peer communication.
3. If a matching rule is found that denies the communication, then drop the network packet. Because this type of firewall does not inspect the network packet’s application layer data and does not track the state of connections, this solution is the least secure of the firewall technologies. It allows access through the firewall with a minimal amount of scrutiny. In other words, if the checks succeed, the network packet is allowed to be routed through the firewall as defined by the rules in the firewall’s routing table. However, because it does less processing than the other technologies, it is the fastest firewall technology available and is often implemented in hardware solutions, such as IP routers.

1.2.2 Circuit Level Firewall:
A circuit level firewall is a second-generation firewall technology that validates the fact that a packet is either a connection request or a data packet belonging to a connection, or virtual circuit, between two-peer transport layers. To validate a session, a circuit level firewall examines each connection setup to ensure that it follows a legitimate handshake for the transport layer protocol being used (the only widely used transport protocol that uses a handshake is TCP), see figure 1.2.
In addition, data packets are not forwarded until the handshake is complete. The firewall maintains a table of valid connections (which includes complete session state and sequencing information) and lets network packets containing data pass through when network packet information matches an entry in the virtual circuit table. Once a connection is terminated, its table entry is removed, and that virtual circuit between the two peer transport layers is closed.

When a connection is set up, the circuit level firewall typically stores the following information about the connection [1]:
1. A unique session identifier for the connection, which is used for tracking purposes.
2. The state of the connection: handshake, established, or closing.
3. The sequencing information.
4. The source IP address, which is the address from which the data is being delivered.
5. The destination IP address, which is the address to which the data is being delivered.
6. The physical network interface through with the packet arrives.
7. The physical network interface through which the packet goes out.

Using this information, the circuit level firewall checks the header information contained within each network packet to determine whether the transmitting computer has permission to send data to the receiving computer and whether the receiving computer has permission to receive that data.

Circuit level firewalls have only limited understanding of the protocols used in the network packets. They can only detect one transport layer protocol, TCP. Like packet filters, circuit level firewalls work by applying a rule set that is maintained in the TCP/IP kernel. Circuit level firewalls allow access through the firewall with a minimal amount of scrutiny by building a limited form of connection state. Only those network packets that are associated with an existing connection are allowed through the firewall. When a connection establishment packet is received, the circuit level firewall checks its rule bases to determine whether that connection should be allowed. If the connection is allowed, all network packets associated with that connection are routed through the firewall as defined in the firewall server’s routing table with no further security checks. This method is very fast and provides a limited amount of state checking [15].

1.2.3 Application Layer Firewall:

An application layer firewall is third-generation firewall technologies that evaluate Network packets for valid data at the application layer before allowing a connection. It examines the data in all network packets at the application layer and maintains complete connection state and sequencing information. In addition, an application layer firewall can validate other security items that only appear within the application layer data, such as user passwords and service requests, see figure 1.3.

Each application proxy requires two components that are typically implemented as a single executable: a proxy server and a proxy client. A proxy server acts as the end server for all connection requests originated on a trusted network by a real client. That is, all communication between internal users and the Internet passes through the proxy server rather than allowing users to communicate directly with other servers on the Internet.
An internal user, or client, sends a request to the proxy server for connecting to an external service, such as FTP or Telnet. The proxy server evaluates the request and decides to permit or deny the request based on a set of rules that are managed for the individual network service [1].

![Application Layer Firewall Architecture](image)

Figure 1.3: Depicts the Network Packet Evaluation Process Used By a Application Layer Firewall

Proxy servers understand the protocol of the service that they are evaluating, and therefore, they only allow those packets through that comply with the protocol definitions. They also enable additional benefits, such as detailed audit records of session information, user authentication, and caching. A proxy client is part of a user application that talks to the real server on the external network on behalf of the real client. When a real client requests a service, the proxy server evaluates that request against the policy rules defined for that proxy and determines whether to approve it. If it approves the request, the proxy server forwards that request to the proxy...
Implement the packet filtering mechanism

Mustafa Sabah Mustafa

client. The proxy client then contacts the real server on behalf of the client (thus the term “proxy”) and proceeds to relay requests from the proxy server to the real server and to relay responses from the real server to the proxy server. Likewise, the proxy server relays requests and responses between the proxy client and the real client, see figure 1.4. Proxy services are implemented on top of the firewall host’s network stack and operate only in the application space of the operating system. Consequently, each packet must pass through the low-level protocols in the kernel before being passed up the stack to application space for a thorough inspection of the packet headers and packet data by the proxies. Then, the packet must travel back down to the kernel, and then back down the stack for distribution. Because each packet in a session is subject to this process, proxy services are notoriously slow [15]. Like circuit level firewalls, application layer firewalls can perform additional checks to ensure that a network packet has not been spoofed, and they often perform network address translation.

Figure 1.4: Depicts the Flow of Communications between a Real Client and a Network Server When the Communications Pass Through a Proxy Server.
1.2.4 Dynamic Packet Filter Firewall:

A dynamic packet filter firewall is a fourth-generation firewall technology that allows modification of the security rule base on the fly. This type of technology is most useful for providing limited support for the UDP transport protocol. The UDP transport protocol is typically used for limited information requests and queries in application layer protocol exchanges see figure 1.5.

This firewall accomplishes its functional requirements by associating all UDP packets that cross the security perimeter with a virtual connection. The information associated with a virtual connection is typically remembered for a short period of time, and if no response packet is received within this time period, the virtual connection is invalidated. Dynamic packet filter firewalls have the same advantages and disadvantages associated with first-generation packet filter firewalls with one notable exception: the advantage of not allowing unsolicited UDP packets onto your internal network. As long as a UDP request packet originated on your internal network and is delivered to an untrusted host, the firewall server allows what appears to be a response packet to be delivered to the originating host. The response packet that is allowed back must contain a destination address that matches the original source address, a transport layer destination port that matches the original source port, and the same transport layer protocol type [1].
Implement the packet filtering mechanism

Mustafa Sabah Mustafa

1.3 Firewall Reference Model [12]:

Firewall reference model is generic model of network security services of authentication, connection authentication, data integrity, data confidentiality, call admission control, and accountability through the application of combination of security functions, such as authentication and auditing shown in figure 1.6 below.

Figure 1.5: Depicts the Network Packet Evaluation Process Used By a Dynamic Packet Filter

Figure 1.6: Reference Model for Firewall Technology
Confidentiality Function (CF):
Provides the confidentiality and secrecy this accomplished by cryptography.

Authentication Function (AF):
Provides the entity authentication.

Connection Authentication Function (CAF):
Provides assurance about the authenticity of sender of data in a connection and the integrity of the transmitted data.

Admission Control Decision Function (ACDF):
Call admission control decisions are based on explicit policies that act on the security domain membership of connection endpoint identity (Initiator and Target).

Audit Function (AF):
All components of system need the opportunity to record information in a consistent manner for use by notification utilities, audit trial analysis, intrusion detection engines, and billing agents.

Access Enforcement Function (Access Control):
Access controls ensures that all direct access to objects are authorized. By regulating the reading, changing, and detection of data and programs, access control protect against accidental and malicious threats to secrecy, authenticity, and system availability.

The work of the reference model for firewall can be summarized in the following points:
Implement the packet filtering mechanism

1. **A** Initiates a connection to destination **B**, they are located in different sides. The originator **A** creates its credentials for the authentication call setup. After connection request arrives at the destination's network boundary the authentication module located at that virtual boundary verifies the authenticity of **A**.

2. Call admission control decision between authentication module and **B** calculate and enforce its access control decision.

3. A positive access control decision might call for further actions, such as the validation of the functionality of an enforcement module at **B** or something else according firewall's technology.

4. Once the connection is established; **A** and **B** can communicate. If so desired connection authentication is provided on data stream on an end-to-end basis.

1.4 Firewall Architecture (Configuration):
Firewalls are configured in different ways, depending on how your company decides to balance the cost versus security. The most secure firewalls often use combination of security layers to offer the most protection. There are three types of basic firewall configurations (architectures) in use today. They are:

- Dual Homed Host Architecture
- Screened-Host Architecture
- Screened-Subnet Architecture

Each configuration has a different tradeoff among between security, cost, and performance. For example, dual homed firewalls are easier to configure and set up than screened hosts, but at a slight loss in security.

1.5 Dual-Homed Host Architecture:

**Dual-homed host architecture** is built around the dual-homed host computer, a computer that has at least two network interfaces. Such a host could act as a router between the networks these interfaces are attached to; it is capable of routing IP packets from one network to another. However, to implement a dual-homed host type of firewalls architecture, it must disable this routing function. Thus, IP packets from one network (e.g., the Internet) are not directly routed to the other network (e.g., the internal, protected network). Systems inside the firewall can communicate with the
dual-homed host, and systems outside the firewall (on the Internet) can communicate with the dual-homed host, but these systems can't communicate directly with each other. IP traffic between them is completely blocked. The network architecture for a dual-homed host firewall is pretty simple: the dual homed host sits between, and is connected to, the Internet and the internal network. Figure 1.7 shows this architecture.

Dual-homed hosts can provide a very high level of control. If you aren't allowing packets to go between external and internal networks at all, you can be sure that any packet on the internal network that has an external source is evidence of some kind of security problem. In some cases, a dual-homed host will allow you to reject connections that claim to be for a particular service but that don't actually contain the right kind of data. (A packet filtering system, on the other hand, has difficulty with this level of control.) However, it takes considerable work to consistently take advantage of the potential advantages of dual-homed hosts. A dual-homed host can only provide services by proxying them, or by having users log into the dual-homed host directly. Proxying is much less problematic, but may not be available for all services. The screened subnet architecture we describe in the next section offers some extra options for providing new and/or untrusted services (e.g., it can be added to the screened subnet a worthless machine that provides only an untrusted service)
1.5.1 Advantages of Dual-Homed Host Architecture:

Dual-homed host architecture has some advantages can be listed in the following points [13]:

1. It implements authentication and proxy functions.
2. It affords flexibility in providing direct Internet access. For example public information web server, for whom a high level of security is not required.
3. It has physical configuration prevent direct flow through router between the Internet and other host on private network if the packet filter router is completely comprised.

1.5.2 Implementation of Dual-Homed Host Firewall:

The dual-homed host can be used to isolate an internal network from an external untrusted network as shown in figure 1.8. Because the dual-homed host does not forward any TCP/IP traffic, it completely blocks any IP traffic between the internal and external untrusted network. Internet services such as mail and news are essentially store-and-forward services. The World Wide Web also can be considered store and forward, but the terms “caching” and “proxy” are more commonly used in Web vocabulary. If these services run on the dual-homed host, they can be configured to transmit application services from one network to the other. If application data must cross the firewall, application forwarder agents can be set up to run on the dual-homed host. Application forwarder agents are special software used to forward application requests between two connected networks. Another approach is to allow the users to log in to the dual-homed host, and then access external services from the external network interface of the dual-homed host as shown
If application forwarders are used, the application traffic cannot cross the dual-homed firewall unless the application forwarder is running and configured on the firewall machine. This is an implementation of the policy “That which is not expressly permitted is prohibited.” If users are allowed to log in to the firewall directly as shown in figure 1.9, the firewall security can be compromised. This is because the dual-homed firewall is a central point of connection between the external network and the internal network. By definition, the dual-homed firewall is in the zone of risk. If the user selects a weak password, or allows his user account to be compromised (such as by giving away passwords), the zone of risk could extend to the internal network, thus defeating the purpose of the dual-homed firewall.
Implement the packet filtering mechanism

Mustafa Sabah Mustafa

If proper logs are kept of user logins, it is possible to trace unauthorized logins to the firewall when a security breach is discovered. If users are not permitted direct login to the dual-homed firewall, however, any attempt at a direct user login will be registered as a noteworthy event and a potential security breach. Examples of store-and-forward services are SMTP (mail) and NNTP (news). Figure 1.10 shows a situation where the dual-homed host is configured to provide discretionary forwarding of mail messages between an external untrusted network and an internal network.

![Figure 1.10 A Dual-Homed Host As A Mail Forwarder](image)

Figure 1.10 A Dual-Homed Host As A Mail Forwarder

Figure 1.11 shows a situation where the dual-homed host is configured to provide discretionary forwarding of news messages between news servers on the external untrusted network and the internal network. The dual-homed host is the basic configuration used in firewalls. The critical aspect of dual-homed firewall hosts is that routing is disabled, and that the only path between the network segments is through an application layer function. If the routing is accidentally (or by design) misconfigured so IP forwarding is enabled, it is possible that the application layer functions of the dual-homed firewalls are bypassed as shown in figure 1.12.
1.5.3 Services on A Dual-Homed Firewall:

Besides disabling IP forwarding, it should be removed from the dual-homed firewall all programs, utilities, and services that could be dangerous in the hands of an intruder. The following is a partial list of some useful checkpoints for UNIX dual-homed firewalls:

1. Remove programming tools: compilers, linkers, and so forth.
2. Remove programs with SUID and SGID permissions that it does not need or does not understand. If things do not work, it can be always put back essential programs. If we have the experience, build a disk
Implement the packet filtering mechanism

Mustafa Sabah Mustafa

space monitor that will shut down the dual-homed host should a critical disk partition become full.

3. Use disk partitions so that an intrusion to fill all disk space on the partition will be confined to that partition.

4. Remove unneeded system and special accounts.

5. Delete network services that are not needed.

6. Alter the system startup scripts to prevent the initialization of unneeded programs such as routed/gated and any routing support programs.

1.6 Software Design Process:

The proposed system contains packet filtering mechanism and application level monitor. The first part of firewall is constructed using packet filtering mechanism by applying the single box architecture (Dual-homed host) because this architecture provides the best isolate between Internet and protected network. The packet filtering is used because it is the basic rule to construct all types of firewall mechanisms are using the packets in it work.

The second part of firewall uses other security mechanisms like log file, authentication and auditing to the user. This part is used to identify the manager or employee and to display the private information that specified to manager or employee. The proposed firewall system works by receiving packet from the first LAN card that connects to the Internet and from the ports that the system scans it. Then it sends the packet to a buffer, the system will be examining each packet in the buffer by compare the IP address of the source computer and destination computer of packet with authorized IPs table. Therefore, the number of ports and the IP of source and destination computer determine the level of security. Whereas the IP of the source or destination computer is unauthorized the packet is rejected, access is denied and sends message to the request owner (source computer) about this situation. When the IP of the source and destination address is authorized, the firewall system will ask the user about his name and password to login inside the protected network. If the name and password is not true the firewall system will reject his request until the user enter the true name and password or cut the connection. But when the user enters the true name and password, the firewall system sends the packet to the second LAN card connected to the protected network. The flowcharts of figures 1.13 and 1.14 represent the mechanism of the proposed firewall system.
Figure 1.13 Incoming packets to the firewall system from the Internet

User in the Internet

First LAN card connects to the Internet received packet from source computer

Received packet from specified port

Authorized IP?

Yes

Authorized user?

Yes

Send packet to the second LAN card connected to the protected network

Second LAN card sends packet to the destination computer in protected network

User in protected network

Send message to the user

Rejected packet and access is denied

No

No

Yes

No

Yes

Implement the packet filtering mechanism

User in protected network

Second LAN card connects to the protected network received packet from source computer

Received packet from specified port

Authorize d IP?

Authorize d user?

Send packet to the first LAN card that is connected to the Internet

First LAN card sends packet to the destination computer in the Internet

User in the Internet

Send message to the user

Rejected packet and access is

No

Yes

Yes

No

Figure 1.14 Incoming packets to the firewall system from protected network
1.7 The Proposed Firewall System Algorithms:

The proposed firewall system uses many algorithms to complete his work; the following sections will provide the outline of these algorithms:

1.7.1 Send/Received Packet from LAN Card:

The following algorithm is used when received packet from LAN card, this algorithm explains the operation of send packet after check the IP address and port number. The firewall program will check the IP's and ports that come from a packet. If the received packet comes from an authorized IP and port is authorized, then allow packet to transfer normally if it is unauthorized then block the connection.

<table>
<thead>
<tr>
<th>Send/Received Packet from LAN Card</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong> Packets</td>
</tr>
<tr>
<td><strong>Output:</strong> Scan packet for passing</td>
</tr>
<tr>
<td><strong>Step 1:</strong> Get packet from LAN card</td>
</tr>
<tr>
<td><strong>Step 2:</strong> Store incoming packet in a buffer</td>
</tr>
<tr>
<td><strong>Step 3:</strong> Check the IP address and port number of the sender</td>
</tr>
<tr>
<td><strong>Step 4:</strong> Check the IP address and port number of the receiver</td>
</tr>
<tr>
<td><strong>Step 5:</strong> If the IP address and port number are authorized, Then</td>
</tr>
<tr>
<td>Allow packet to Send/Receive</td>
</tr>
<tr>
<td>Else</td>
</tr>
<tr>
<td>Block the connection</td>
</tr>
<tr>
<td><strong>Step 6:</strong> End</td>
</tr>
</tbody>
</table>

1.7.2 Check/Add IP Address:

The following algorithm is used to check the IP address for database when the administrator of the proposed firewall system insert IP address, examine the database if it is found or not. The first step in this algorithm is used if the administrator adds new IP address to the database. The second step check if this IP address found in the database, if found then message "IP is found" will be displayed, if not then store IP address in the database.
Implement the packet filtering mechanism

1.7.3 Remove IP Address:
This algorithm explains how to delete IP address from the database, the program will open database that contains all the IPs, the administrator will choose the IP of specified computer and removed it. This program has the same function of remove the address of this specified computer (i.e. the real address web page address in the Internet of this specified computer).

**Check IP Address**
*Input:* IP Address
*Output:* Scan IP address
*Step 1:* Get IP address from administrator
*Step 2:* Search the IP value in database, if found
  - Then
  - Display message "IP address is found"
  - Else
  - Store the IP address in database
*Step 3:* End

**Remove IP Address**
*Input:* IP Address
*Output:* IP address remove from database
*Step 1:* Get IP address from field of deny access from/to IP's
*Step 2:* Search in database for IP, if found
  - Then
  - Delete the IP address
  - Else
  - Display message "IP not found"
*Step 3:* End

1.7.4 Check/Add Port Number:
This algorithm is used to check port number for database when the administrator of the proposed firewall system insert port number, examine the database if it is found or not. The first step is used if the administrator adds new port number to the database. The second step check if this port number is found in the database, if found then message appear the "Port is found" of if not then store port number in the database.

**Check Port Number**
*Input:* Port number
*Output:* Scan port number
*Step 1:* Get port number from administrator
*Step 2:* Search the port number value in database, if found...
1.7.5 Remove Port Number:

This algorithm is used to show how to delete port number from database, the algorithm will open database that contains all port numbers, the administrator will choose the port number of specified computer and removed it.

<table>
<thead>
<tr>
<th><strong>Remove Port Number</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong> Port number</td>
</tr>
<tr>
<td><strong>Output:</strong> Port number removed from database</td>
</tr>
<tr>
<td><strong>Step 1:</strong> Get port number from field of deny access from/to ports</td>
</tr>
<tr>
<td><strong>Step 2:</strong> Search in database for ports, if found</td>
</tr>
<tr>
<td>Then</td>
</tr>
<tr>
<td>Delete port number</td>
</tr>
<tr>
<td>Else</td>
</tr>
<tr>
<td>Display message &quot;Port not found&quot;</td>
</tr>
<tr>
<td><strong>Step 3:</strong> End</td>
</tr>
</tbody>
</table>

1.7.6 Check/Add Address and Port Number:

This algorithm is used to check the IP address and port number for database when the administrator of the proposed firewall system insert IP address and port number, examine the database if it is found or not. The first step is used, if the administrator adds new IP address and port number to the database. The second step check if this IP address and port number found in database, if found then message appear the IP and port number are found or if not then store IP address and port number in the database.
Implement the packet filtering mechanism

Check/Add Address and Port Number

**Input:** IP address and port number  
**Output:** Scan IP address and port number  
**Step 1:** Get IP address and port number from administrator  
**Step 2:** Search the IP and port value in database, if found
   Then  
   Display message "The IP address and port number are found"  
   Else  
   Store the IP address and port number in database  
**Step 3:** End

1.7.7 Remove IP Address and Port Number:
This algorithm is used to show how to delete IP address and port number from the database.

Remove IP Address and Port Number

**Input:** IP address and port number  
**Output:** IP address and port number are removed from database  
**Step 1:** Get IP address and port number from field of deny access  
**Step 2:** Search in database for the IP and port number, if found
   Then  
   Delete the IP address and port number  
   Else  
   Display message "IP and port number are not found"  
**Step 3:** End

1.7.8 Block IP Address and Port Number:
This algorithm is used to block (cannot open) any specified IP address or port number. The blocking process is done using by either IP address or port number.

Block IP Address and Port Number

**Input:** IP address or port number  
**Output:** IP address and port number are blocked  
**Step 1:** Edit IP address or port number from field of deny access  
**Step 2:** Search for IP address or port number that is edited, if found
   Then  
   Unload this IP address or port number  
   Else  
   Display message "The IP address and port number are found"  
**Step 3:** End
Blocking addresses does not always work. Some web sites have multiple servers baking up the primary site. If connection to the first server does not work then you will be routed to the second server and so on. To successfully block an address you need to know all the IP addresses that are registered to the primary web address.

1.7.9 Tray to Connect Address and Send Text:

This algorithm is used to try connecting to address in order to show data viewer. This algorithm used network Winsock object to connect and get data through network. The trying to connect is limited through timer and gives specified time to try connecting. After the connection is established, then it can send any text to this address, note that the emulation taking any chosen operating system like windows-95, windows-98, windows-2000, and windows-XP. And finally it can also disconnect this connection through enabling the administrator this feature by its opinion.

<table>
<thead>
<tr>
<th>Try to connect to address</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong> physical address or IP address</td>
</tr>
<tr>
<td><strong>Output:</strong> Connected to physical address or IP address</td>
</tr>
<tr>
<td><strong>Step 1:</strong> Get IP address or address from administrator</td>
</tr>
<tr>
<td><strong>Step 2:</strong> If received request</td>
</tr>
<tr>
<td>Then</td>
</tr>
<tr>
<td>Check the socket is not busy</td>
</tr>
<tr>
<td><strong>Step 3:</strong> If socket is busy</td>
</tr>
<tr>
<td>Then</td>
</tr>
<tr>
<td>Send wait to user</td>
</tr>
<tr>
<td>Else</td>
</tr>
<tr>
<td>Accepted request</td>
</tr>
<tr>
<td><strong>Step 4:</strong> Send &quot;Identify&quot; command to user request connection</td>
</tr>
<tr>
<td><strong>Step 5:</strong> End</td>
</tr>
</tbody>
</table>

1.8 Conclusions:

1. Many conclusions can be noticed in this paper, they are:

2. The proposed firewall system can be used to protect one computer (personal computer PC) from the attacker when connecting to a LAN and also can be used to protect many computers that connected together in LAN from the outside attack in the Internet.

3. From functional point view, the proposed system can be used in two ways: first as security tool, where the system prevents the hacker from entering the protected computer or network. Second as monitoring tool which can be used in many applications by using IP address and port number.
4. All types of firewall depend on packet capture processing. When we need to build any type of firewall, we must process the packet of connection to make firewall work in the right place. For this reason, this research depends on packet filtering firewall.

5. Using dual-homed host architecture helped us in increasing the protection because it isolate the protected network from the Internet and all traffic must pass through this host.

6. There are basic firewall types, but they can typically be grouped into (Packet filtering, Application level, and Circuit level) with each approach having strength. However, all firewalls share a common attribute, either allowing or deny access to the packet coming from Internet.

1.9 Future Works:

1. The following are some suggestions for future works especially in areas that are not covered in this paper:

2. Add the Virtual Private Network (VPN) is a technology that allows two or more locations to communicate securely over a public network (like Internet) while maintaining the security and privacy of private network encryption, authentication, and packet integrity checks are enablers of VPNs as they ensure that the data is private and the integrity of data is maintained.

3. Build a firewall as a search engine, which searches for the permitted sites and return the IP of these sites.

4. Convert the firewall from software to hardware to increase the speed of processing and make it more efficient.

5. It is preferable to develop programs with a whole control over the traffic, firewalls in some cases must have the ability to perform the content filtering depending on text, images, sound …etc. with the ability to pass or deny the traffic according to our security policy.
References


