Al-khwarizmi Engineering Journal

Al-Khwarizmi Engineering Journal, Vol.2, No.1,pp 52-69, (2006)

Design and Implementation of a Proposal Network Firewall

Deah J.Kadhim
Electrical Engineering Department
College of Engineering/ University of Baghdad

Walid K.Hussain
Baghdad College for Economic Sciences

(Received 25 September 2005; accepted 4 April 2006)

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 proposal 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. The designed system is constructed using Visual Basic 6.0 Language.

Finally, This proposed 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.

Keywords: Computer Network, Network Security and Firewall

1. Introduction

The firewall imposes restrictions on packets entering or leaving the private network. All traffic from inside to outside, and vice versa, must pass through the firewall, but only authorized traffic will be allowed to pass. Packets are not allowed through unless they conform to a filtering specification, or unless there is negotiation involving some sort of authentication. The firewall itself must be immune to penetration [1].

Firewalls create checkpoints (or choke points) between an internal private network and an untrusted Internet. Once the choke points have been clearly established, the device can monitor, filter and verify all inbound and outbound traffic. The firewall may filter on the basis of IP source and

destination addresses and TCP port number. Firewalls may block packets from the Internet side that claim a source address of a system on the intranet, or they may require the use of an access negotiation and encapsulation protocol like SOCKS to gain access to the intranet [2].

The means by which access is controlled relate to using network layer or transport layer criteria such as IP subnet or TCP port number, but there is no reason that this must always be so. A growing number of firewalls control access at the application layer, using user identification as the criterion. In addition, firewalls for ATM networks may control access based on the data link layer criteria. The firewall also enforces logging, and provides alarm capacities as well. By placing logging services at firewalls, security administrators can monitor all access to and from the Internet. Good logging strategies are one of the most effective tools for proper network security.

Firewalls may block TELNET or RLOGIN connections from the Internet to the intranet. They also block SMTP and FTP connections to the Internet from internal systems not authorized to send e-mail or to move files. The firewall provides protection from various kinds of IP spoofing and routing attacks. It can also serve as the platform for IPsec. Using the tunnel mode capability, the firewall can be used to implement Virtual Private Networks (VPNs). A VPN encapsulates all the encrypted data within an IP packet.

In general, a firewall is placed between the internal trusted network and the external untrusted network. The firewall acts as a choke point that monitors and rejects application-level network traffic (as shown in figure 1.1). Firewalls also can operate at the network and transport layers, in which case they examine the IP and TCP headers of incoming and outgoing packets, and reject or pass packets based on the programmed packet filter rules [1].

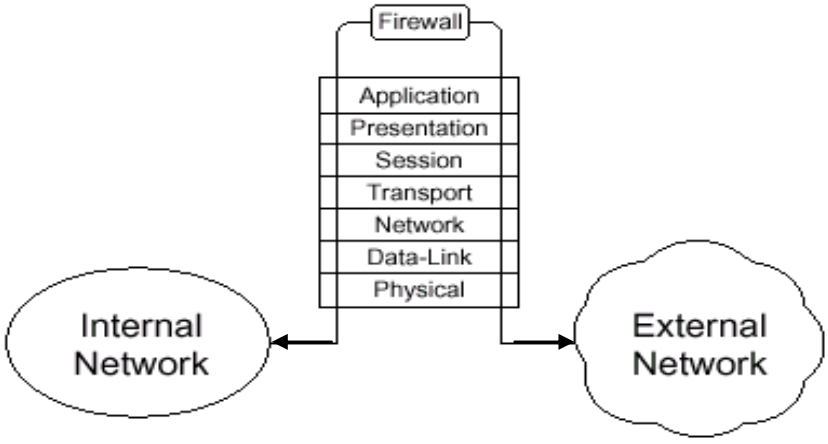

Figure 1: Firewall Operation

2. Firewall Objective

All traffic 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 policy, will be allowed to pass. Various types of firewalls are used, which implement various types of security policies [3]. In general firewall is one of the famous types of intruder detection [4].

Firewall effective against worms because it is much difficult for a worm to authenticate itself to a firewall operating a tight exclusive policy than to a general, widely used system. It is effective against Trojan horse. However, even firewall is not invincible [5].

3. Firewall Conditions

There are some conditions must be considered in the firewalls, the most important conditions are declared in the following points [6]:

- The firewall must be easy to use, has powerful Graphical User Interface (GUI), which simplifies the job of installation, configuration, and management.
- The firewall must be high performance, should be fast enough so users do not feel the screening packets. The volume of data throughput and transmission speed associated with the product should be consistent with the company's bandwidth to the Internet.
- The firewall must be flexible, should be opened enough to accommodate the security policy of the company, as well as to allow for changes in the features. Remember that a security policy should a very seldom change, but security procedures should always be reviewed, especially in light of new Internet and web centric application.

4. Firewall Limitations

Security of firewalls neither provides perfect security nor it free from operational difficulties. The most important limitations of the firewall are interpreted in the following points [7]:

- Firewalls do not protect against malicious insiders.
- Firewalls have no protections against connections that circumvent the firewall (i.e. Modems) attached to computer inside the firewall.
- Firewalls can not protect against the transfer of virus-infected programs or files. Because of the variety of operating systems and applications supported inside the perimeter, it would be impractical and perhaps impossible for the firewall to scan all incoming files, E-mail, and message for viruses.
- Firewalls can not protect against completely new threats, firewalls designed to protect against known threats. No firewall can automatically defend against every new threat arises.

5. Firewalls Favorites Control Positions

A firewall system can be a router, a personal computer, a host, or a collection of hosts, set up specifically to shield a site or subnet from protocols and services that can be abused from hosts outside the subnet. A firewall serves as the gatekeeper to centralized access control between the untrusted Internet and trusted internal network [8]. So due to a firewall behavior, it can be at any of the following levels:

- Between an internal network and Internet. For example a firewall can be implemented on the main server of a country to enforce any security policy to restrict any restricted web sites and monitoring E-mail messages coming in and going out.
- Between subnets inside an internal networks. For example a connection between two organizations related with the same ministry, they are transmitting information between them but each organization enforce its security policy which can be implemented by using a firewall.
- Between a single PC and computers on the same networks or other networks on the Internet. For example if we have

some one wants to isolate his PC from any where, one way to secure his PC is by using a firewall.

6. Types of Firewalls [1]

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. These types are described and explained with its configurations and its advantages vs. disadvantages in details in above reference and it can here list them as follows:

- Packet Filtering Firewall
- Circuit Level Firewall
- Application Layer Firewall
- Dynamic Packet Filter Firewall

The proposed 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.

7. Firewall Architecture (Configuration) [1]

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. The Dual-homed host architecture has been used to implement the proposed firewall system.

8. Proposed Firewall System

The following sections will give the design and software implementation processes of the proposed firewall system and show all the main points that used in design and software implementation processes.

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 (2) and (3) represent the mechanism of the proposed firewall system.

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

9. 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.

Send/Received Packet from LAN Card

Input: Packets
Output: Scan packet for passing.
Step 1: Get packet from LAN card.
Step 2: Store incoming packet in a buffer.
Step 3: Check the IP address and port number of the sender.
Step 4: Check the IP address and port number of the receiver.
Step 5: If the IP address and port number are authorized,
Then allow packet to Send/Receive
Else block the connection
Step 6: End

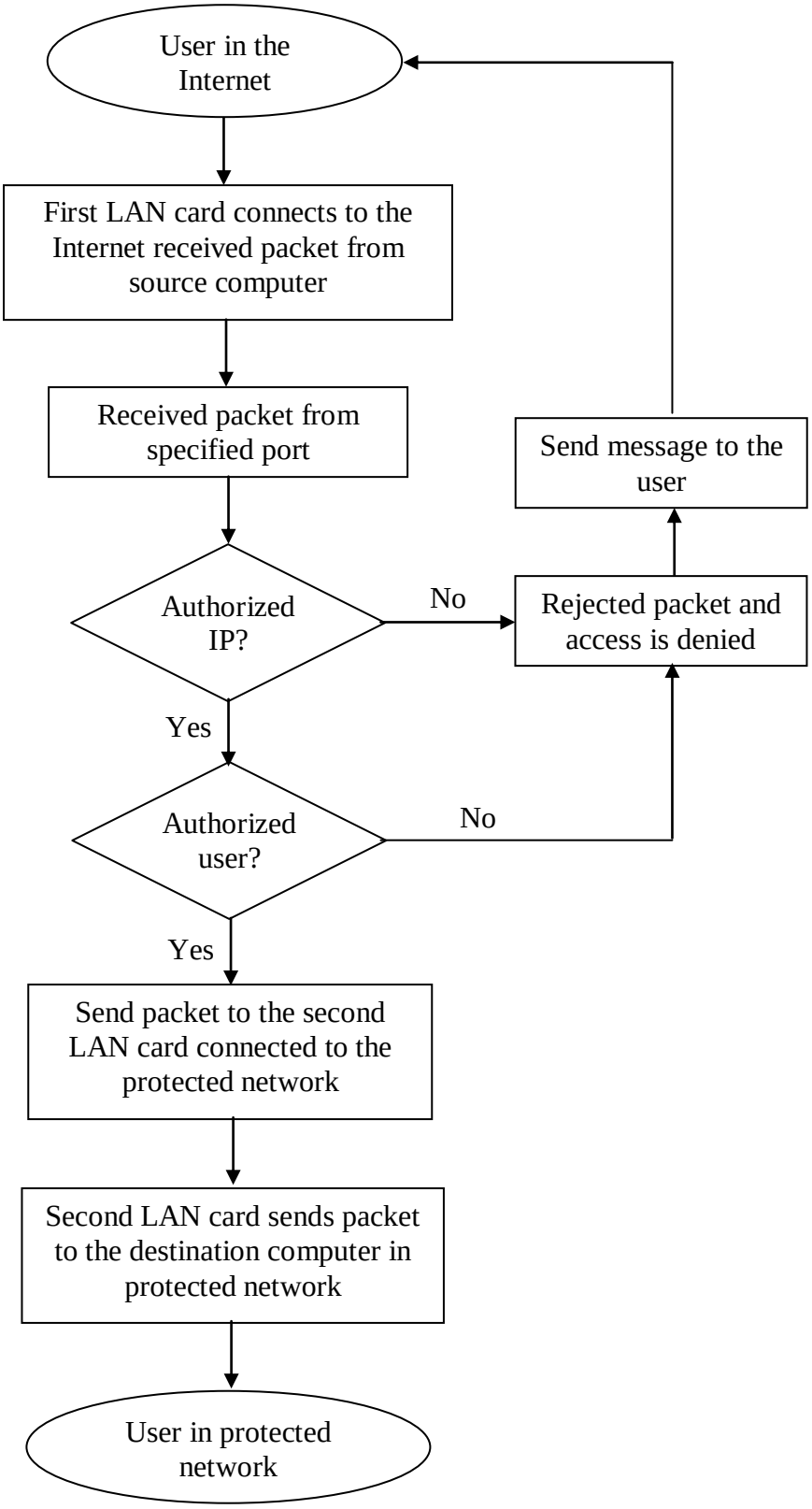

Figure (2): Incoming packets to the firewall system from the Internet

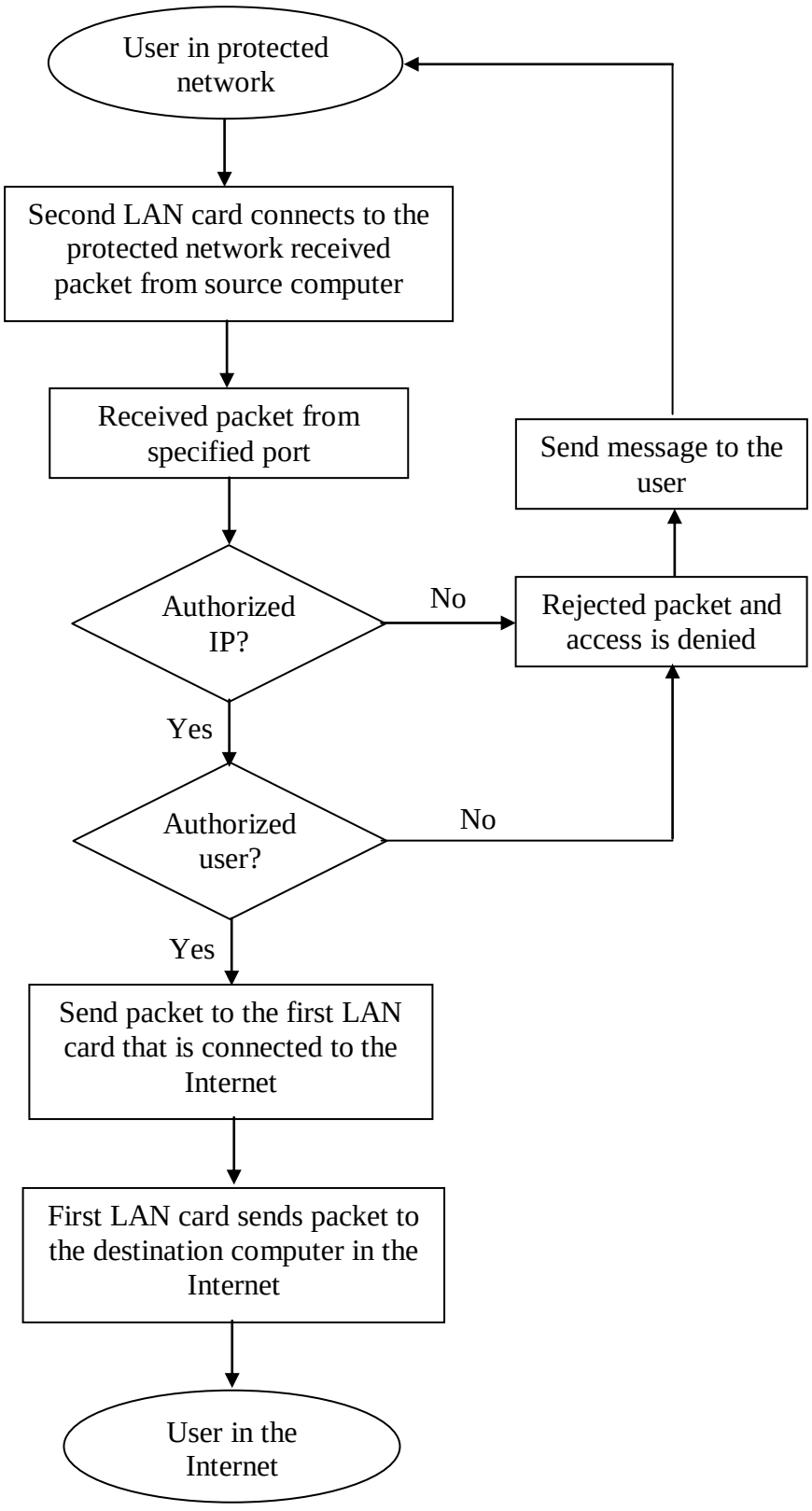

Figure (3): Incoming packets to the firewall system from protected network

8.1 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.

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

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).

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

8.2 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
Then display message "The port number is found"
Else store the port number in database
Step 3: End

8.3 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, and the administrator will choose the ort number of specified computer and removed it.

Remove Port Number

Input: Port number
Output: Port number removed from database.
Step 1: Get port number from field of deny access from/to ports.
Step 2: Search in database for ports, if found
Then delete port number
Else display message "Port not found"
Step 3: End

8.4 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.

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

8.5 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

8.6 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.

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 it will be routed to the second server and so on. To successfully block an address that need to know all the IP addresses that are registered to the primary web address.

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

The unload this IP address or port number

Else display message "The IP address and port number are found"
Step 3: End

8.7 Try 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. 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.

Try to connect to address

Input: physical address or IP address.
Output: Connected to physical address or IP address.
Step 1: Get IP address or address from administrator.
Step 2: If received request
Then check the socket is not busy
Step 3: If socket is busy
Then send wait to user
Else accepted request
Step 4: Send "Identify" command to user request connection
Step 5: End

9. Software Implementation of the Proposal Firewall System

This section presents the software implementation of the proposed firewall system that had been built from algorithms discussed in previous sections. Like any firewall system, the proposed firewall system consists from many parts, this section presents and explains the works of proposed firewall system's windows and the relationship between these windows.

The proposed firewall system contains more than one window to display the parts of the system; the following sections will describe these parts with its job in firewall system work.

9.1 The Main Window of Firewall System

Figure (4) shows the main window of proposed firewall system, that displays the public parts of this system. This main form of the network firewall program, which has a screen monitoring of all the connections associated with the computer that this program is working on , and also have a filter screen that represents the filter contents preventing any incoming packets by blocking three types of locations (Address , Local port and Remote port) .

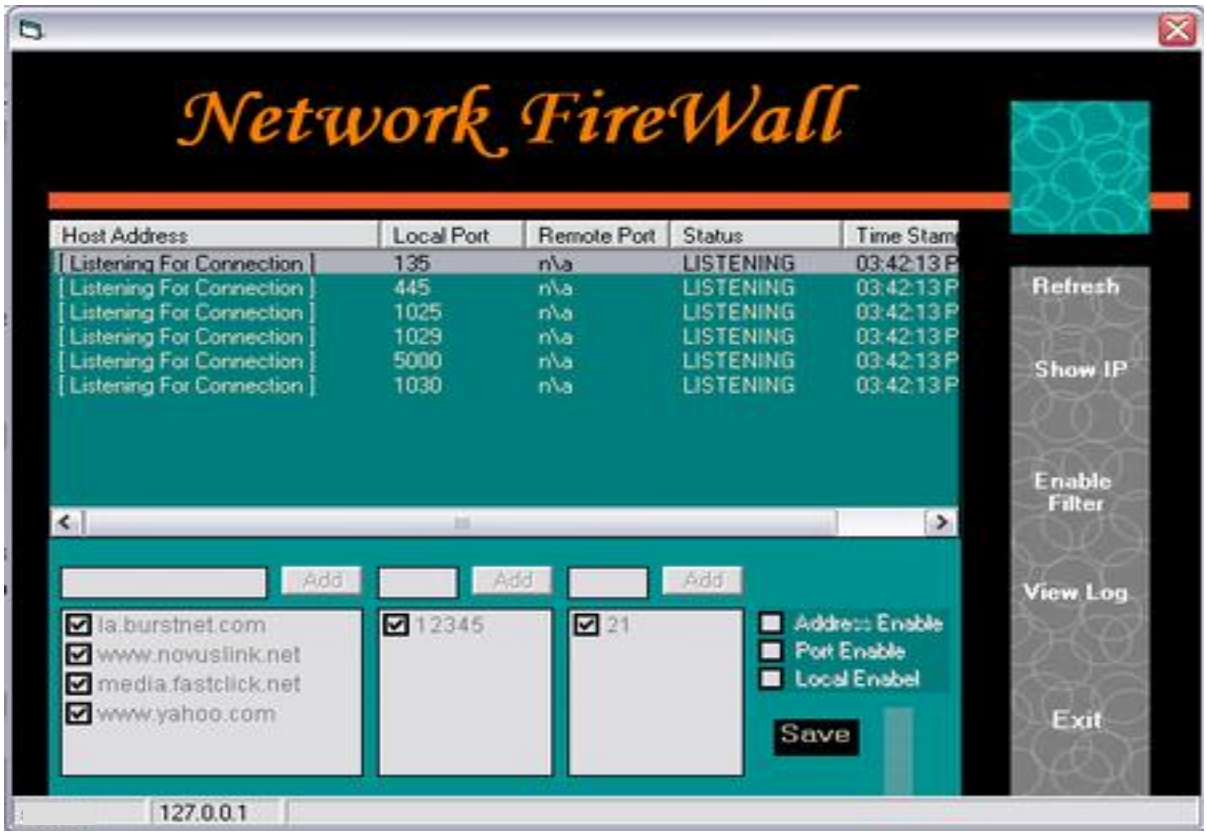

Figure (4): The Main Window of Proposed Firewall System

9.2 Enabling Packets Filtering

It can start work this proposed firewall system by adding some addresses (preferred IP Addresses) or it can add a remote port or Local port, it can retrieve the information about these setting from the listening screen.

Note that the filter can be enabled and disabled by clicking on enable, disable Filter button on the right of the main window as shown in figure (5). So public address or IP address, local port and remote port can be added to filter them from accessing through the Internet.

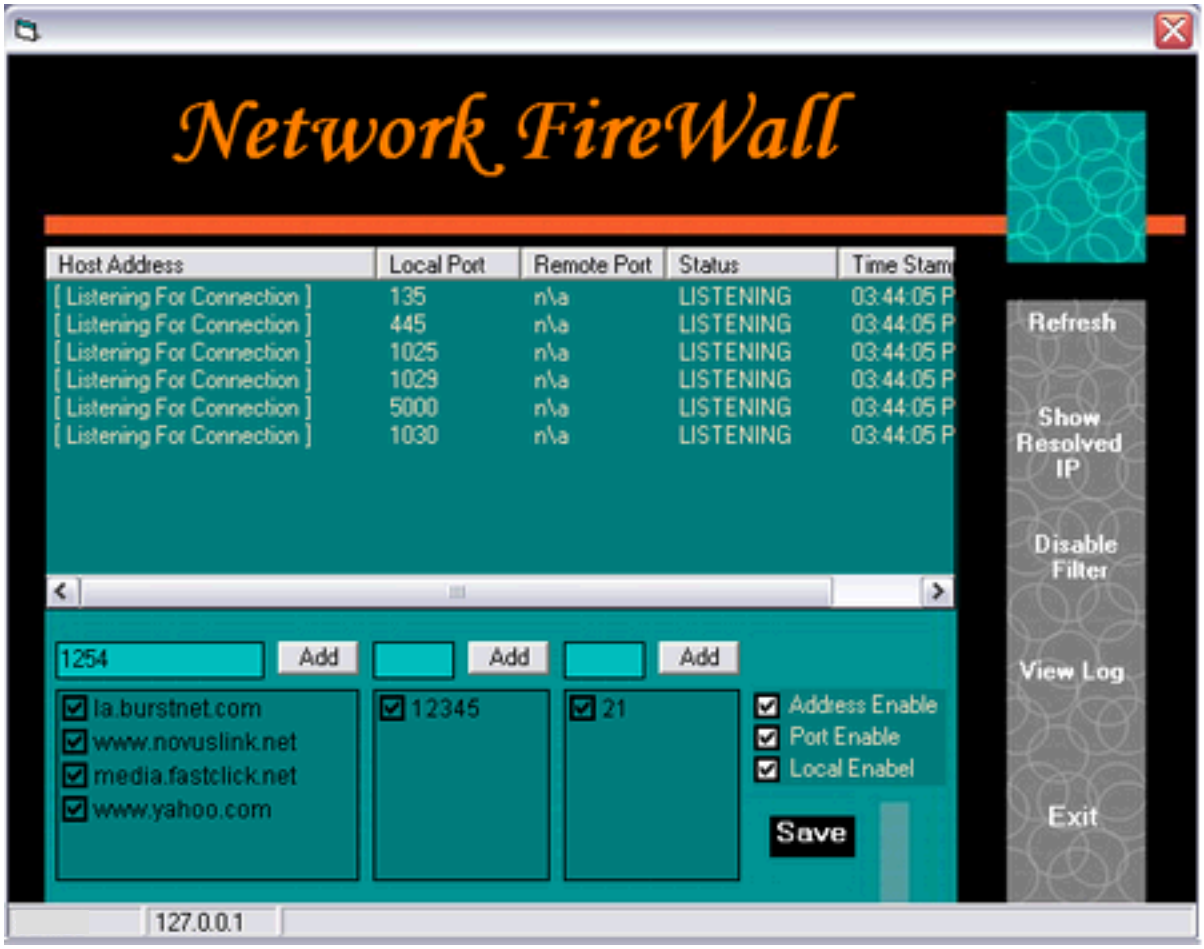

Figure (5): Enabling or Disabling Packets Filtering

9.3 Log View File Window

This file is used to enable the administrator to show all information about each connection established when the proposed firewall system is running. When button "View Log" is pressed, the system will display the content of log file as shown in figure (6), and then the details of all connection can be shown with time and date. So it can say that this file displays the status of the firewall system and on line status of the connection over the firewall system.

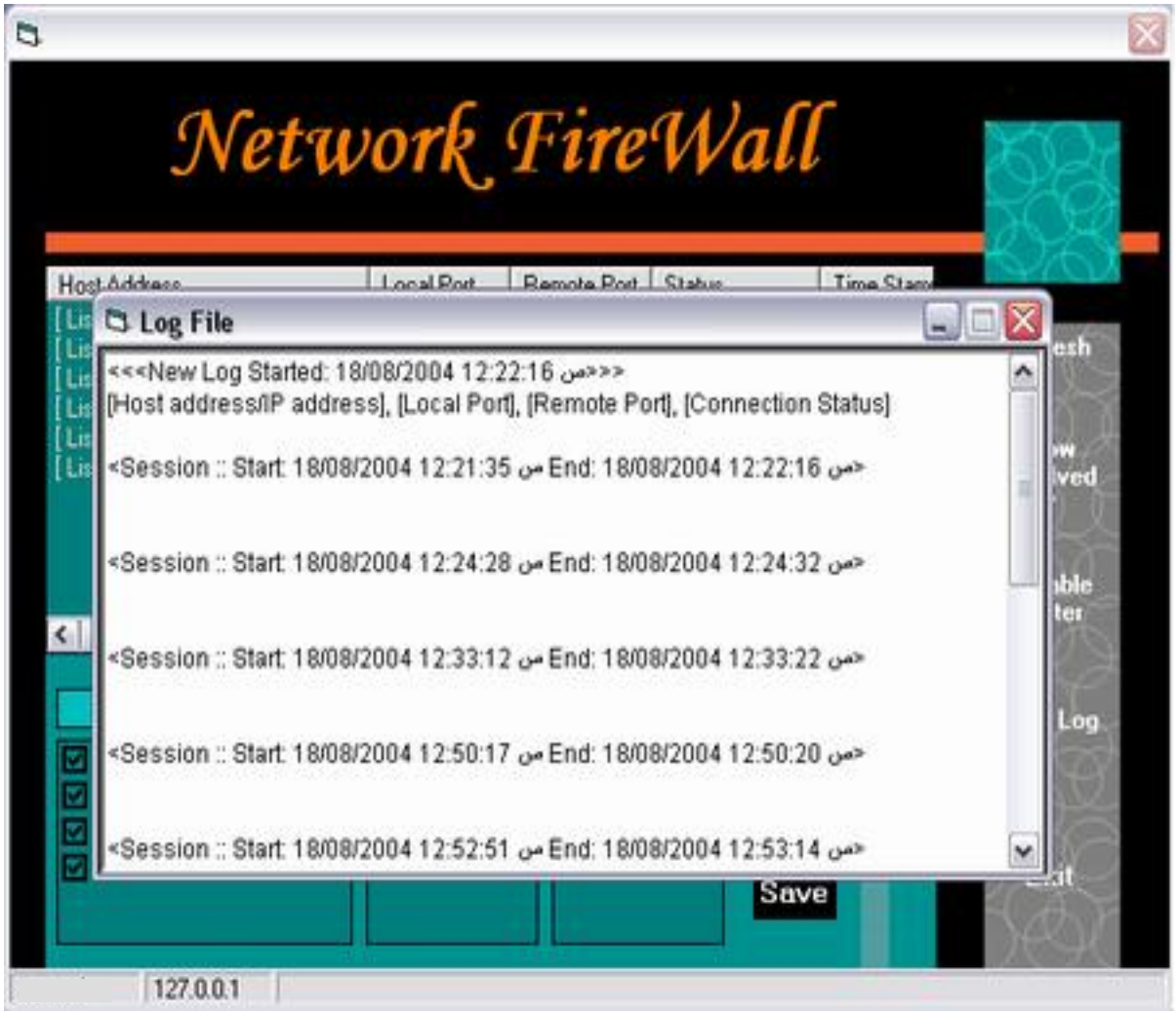

Figure (6): View Log File Window

9.4 Blocking and Connection Functions

The power of this program is presented by Right clicking on any connection, then it see in the Listening Screen (main program window); then you will see three options:

1. Block: Just for blocking the connection but not ending it.
2. Connect: for trying to connect to this connection and deal with it.
3. End the connection.

Figure (7) shows these three options.

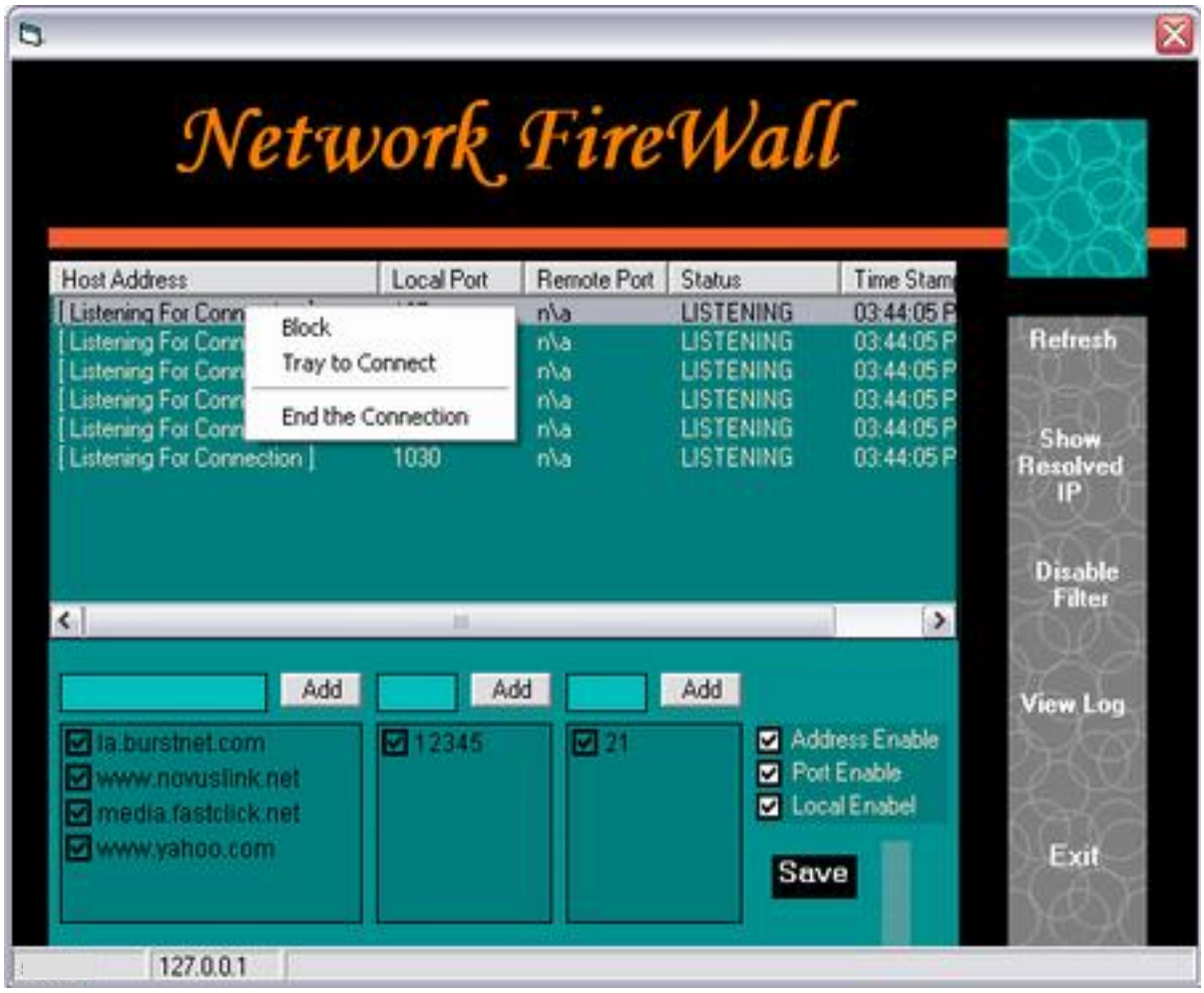

Figure (7): Blocking and Connection Functions

9.5 Blocking Function Window

This window is used to block (cannot open) any specified IP address or port number. The blocking process is done using by either IP address or remote port number or local port number.

Figure (8) shows how this operation is done by clicking on (Block) the form Block will appeare conaining three Options , By address or by remote port or by Local port, Click (Block) to block the desired option or click (Cancel) to unload the form and return to the main form. To successfully block an address you need to know all the IP addresses that are registered to the primary web address.

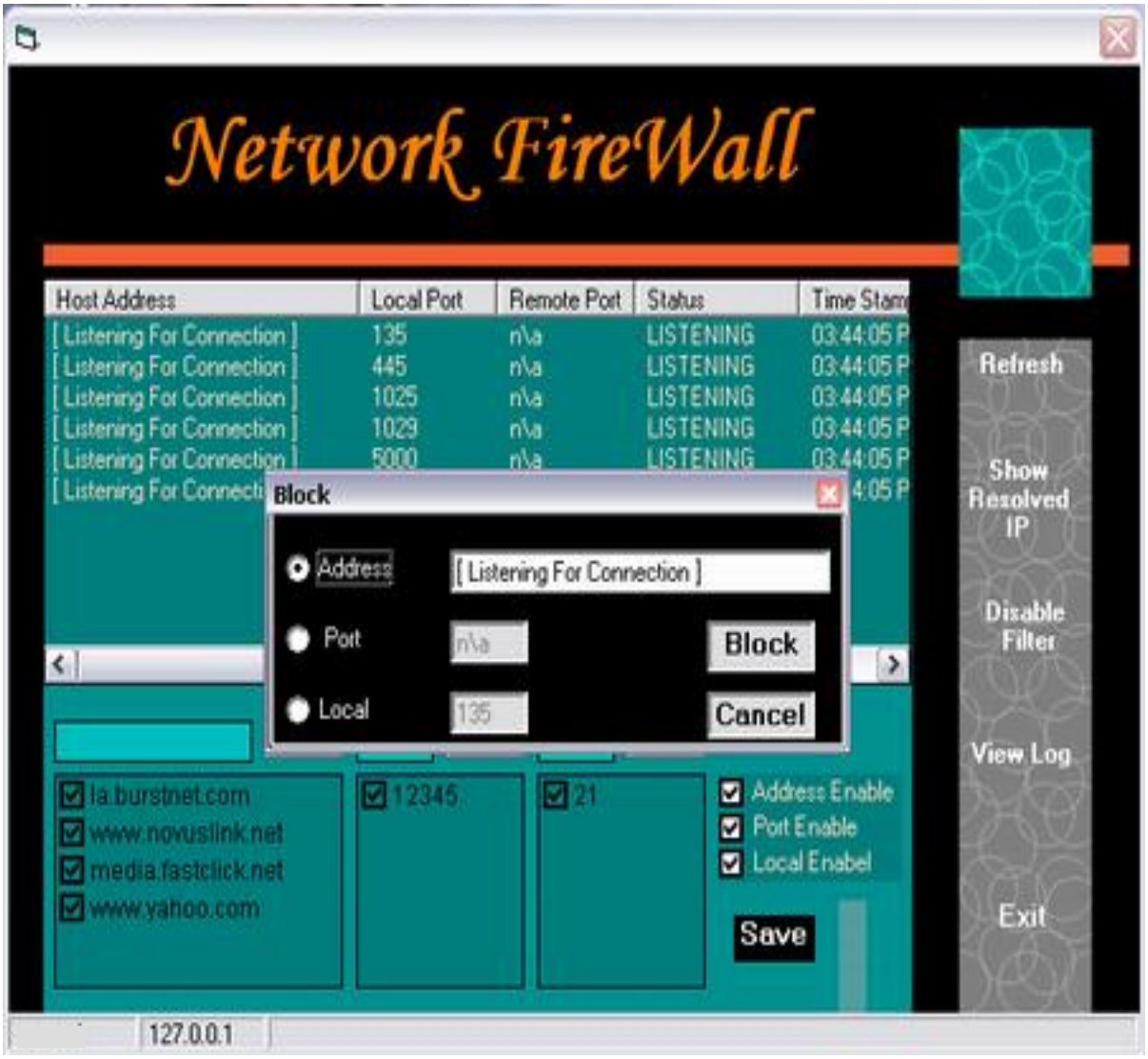

Figure (8): Blocking Function

9.6 Connection Function Window

This window is used to try connecting to address in order to show data viewer. 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. Finally it can also disconnect this connection through enabling the administrator this feature by its opinion.

Figure (9) shows how this function is operated by clicking on (try to connect), the form (Test Connection) will appear containing the address or the address that want to connect to, and when it choose the (connect to) part of the form will be enabled asking about the text that want to send to that connection. it can verify the type of Emulation by enabling it and choosing any type of windows that is wanted.

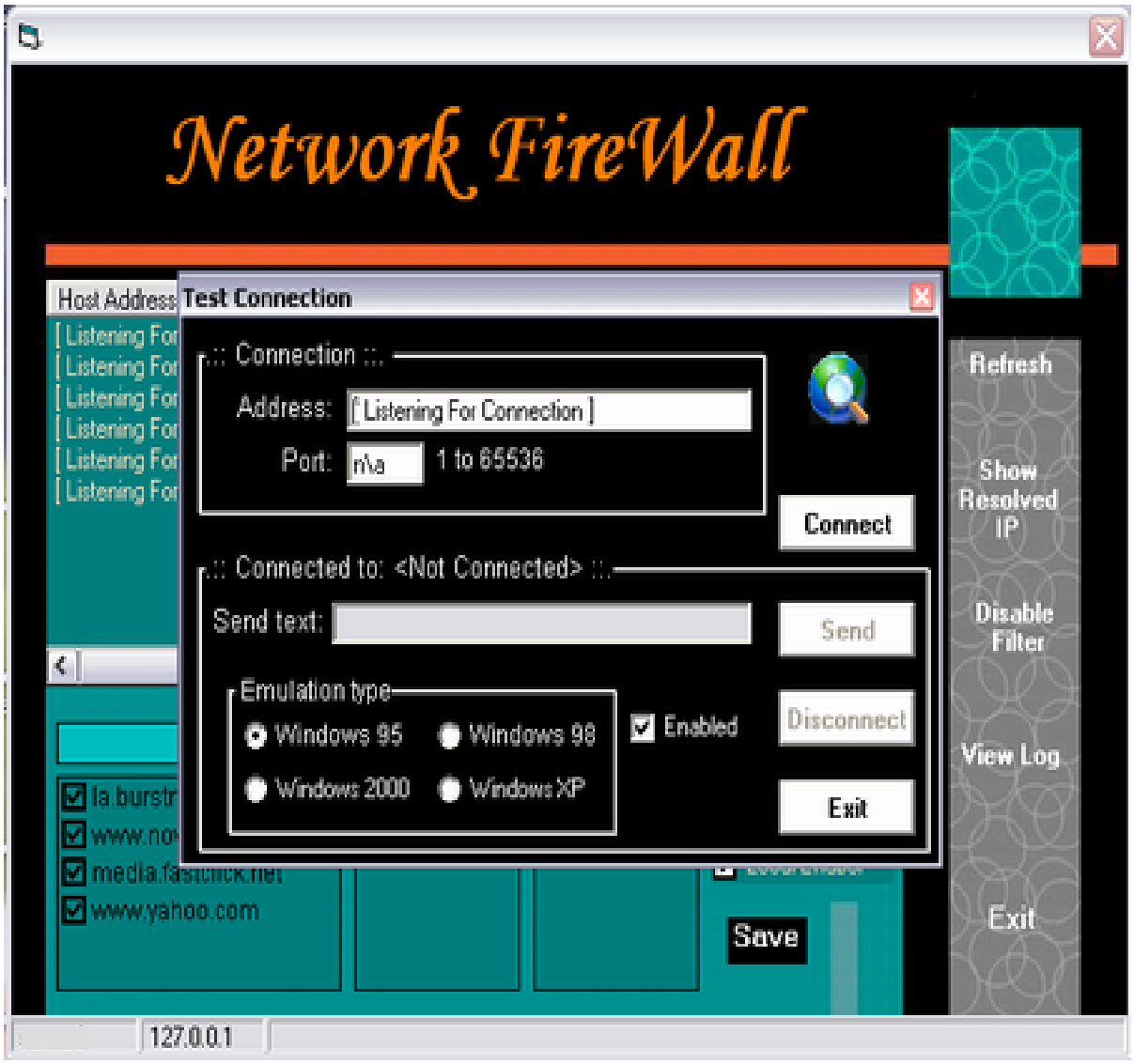

Figure (9): Connection Function

9.7 Error Windows

There are error labels in this program and one of them can be shown in figure (10), this error label is caused by trying to end a connection without a connection to a remote port.

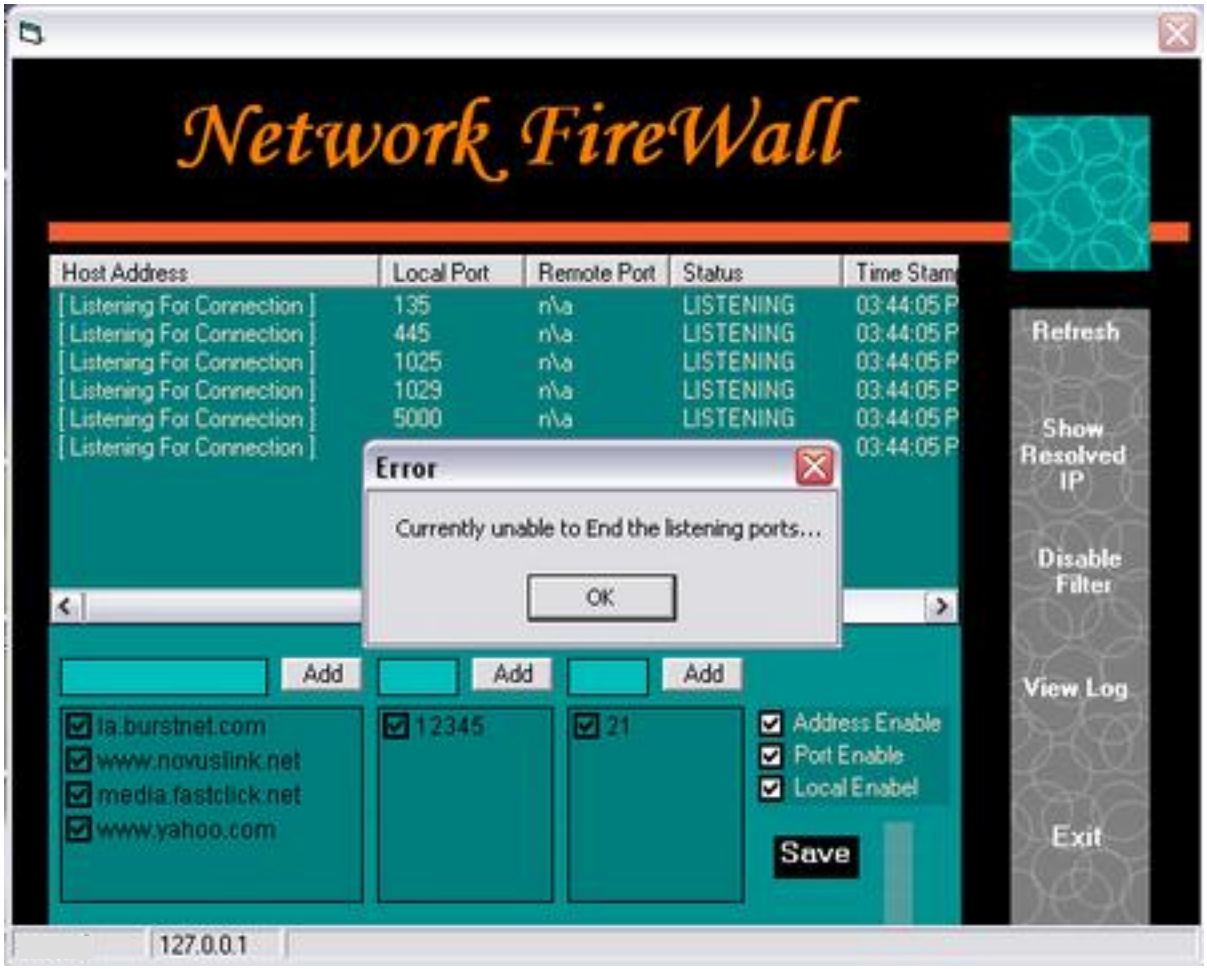

Figure (10): One of Errors Windows

10. Conclusions

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

- 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.
- 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.
- 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.
- 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 though this host.

- 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.

11. References

[1] E. Zwiky, S. Copper, and D. Chapman, **"Building Internet Firewalls"**, Second Edition, O'relly & Association, 2000.

[2] J. Bryan Lyles & Christoph L. Schuba, **"A Reference Model for Firewall Technology and its Implications for Connection Signaling",** 1996.

[3] Kent P., **"10 Minute Guide to the Internet"**, Prentice-Hall of India, 1998.

[4] Kent P., **"The Complete Idiot's Guide to the Internet"**, Second Edition, Que, Adivision of Macmillan Computer Publishing, 1994.

[5] Crumlish C., **"The ABCs of the Internet"**, SYBEX Inc., USA, 1996.

[6] Escamilla T., **"Intrusion Detection Network Security Beyond the Firewall"**, John Wiley & Sons Inc., 1998.

[7] Stallings W., **"High-Speed Networks: TCP/IP and ATM Design Principle",** Prentice-Hall Inc., 1998.

[8] K. Parner & N. Cowchan Duncan**, "An Introduction to Security",** Security Manual, Canada, 1999.

ضياء جاسم كاظم
كلية الهندسة – جامعة بغداد

وليد خالد حسين
كلية بغداد للعلوم الاقتصادية

الخلاصة:

نتيجة التطور و النمو السريع في شبكات المعلومات و الانترنيت نظرا لأهمية الانترنيت في عالم اليوم لما يوفره من خدمات للمستخدمين من سهولة الحصول على المعلومات المختلفة بسرعة عالية وبأقل جهد ممكن ، كل هذه الفوائد وغيرها ممكن ان تنقلب الى مضار خطيرة ، اذ ان ارتباط الحاسبة الخاصة (Private Computer) او الشبكات المحلية (LAN) بالأنترنيت يفتح المجال امام هجمات القراصنة (Hackers) والدخلاء (Intruders) الذين يحاولون بطريقة ما ايجاد اي نقطة ضعف او منفذ للدخول عبر الانترنيت الى هذه الحاسبات لاغراض التجسس او لسرقة معلومات (كالتلاعب بالحاسبات المصرفية او معرفة كلمة سر وغيرها) او في بعض الاحيان لاغراض التخريب ليس الا . لذلك اصبح من المهم جدا ايجاد طريقة لحماية الشبكات ومستخدميها من مثل هذه التهديدات . واحدة من اهم طرق الحماية التي توفر درجة عالية من الامنية هي استخدام جدار النار (Firewal).

يهدف هذا البحث الى تصميم وتنفيذ جدار ناري (Firewall) مفترض يستخدم لحماية الحاسبات الخاصة (Private Computer) والشبكات المحلية (LAN) من الاعداء المتطفلين خلال الانترنت.تم أستخدام معمارية الموطن المضيف المزدوج (Dual-homed host) في تصميم نظام الجدار الناري المقترح. النظام المقترح تم بناءه بأستخدام لغة الفيجول بيسك6.

أخيراً تم بناء هذا النظام المفترض بالاعتماد على استخدام ميكانيكية مرشح الحزم لتنظيم دخول وخروج جميع الحزم للموقع المحمي وذلك باستخدام عنوان الانترنت برتوكول (IP) ورقم البوابة (Port Number). وكذلك يتعامل هذا النظام مع مستوى التطبيق (Application Level) لمرقبة جميع محتوى حزم البيانات الداخلة من خلال تفعيل دور الجدار الناري عند الاتصال بالانترنت.