A Study of Network Security Systems

Ramy K. Khalil, Fayez W. Zaki , Mohamed M. Ashour, Mohamed A. Mohamed
Department of Communication and Electronics
Mansoura University
El Gomhorya Street, Mansora ,Dakahlya
Egypt
Ramykamal2005@hotmail.com

Abstract: - Firewalls provide security by applying a security policy to arriving packets these policy called security rules and also firewalls can perform other functions like Gateway Antivirus, Gateway Monitor Program to monitor the traffic which pass through the firewall and also the firewall can have the responsibility to establish VPN connections. The complexity of these functions can cause significant delays in the processing of packets, resulting in degraded performance, traffic bottlenecks, and ultimately violating Quality of Service constraints. As network capacities continue to increase, the improvement of firewall performance is a main concern. One technique that dramatically reduces required processing is using Network Load Balance Technique. This paper describes how the performance can be effected because of using a Microsoft firewall. in this paper lots of situations and designs will be tested and results will be shown to determine the effect of using firewall in performance. Also in this paper a new technique to increase firewall performance will be discussed and the performance results will be shown.

Key-Words: - Security, firewalls, parallel, policy, management

1. Introduction

Firewalls provide security by applying a security policy to arriving packets. A policy is a list of rules which define an action to perform on matching packets, such as accept or deny [11]. Determining the appropriate action is typically done in a first-match fashion, dictated by the first matching rule appearing in the policy and the time required to process packets increases as policies grow larger and more complex So Network firewalls must continually improve their performance to meet increasing network speeds, traffic volumes, and Quality of Service (QoS) demands. Unfortunately, firewalls often have more capabilities than standard networking devices, and as a result the performance of these security devices lags behind [1], [2], [3]. Furthermore, computer networks grow not only in speed, but also in size, resulting in convoluted security policies that take longer to apply to each packet [4], [5].

When a security solution cannot keep pace with the speed of incoming data, it either allows packets through without inspection or places incoming packets into a growing queue, thus becoming vulnerable to Denial of Service (DoS) attacks. With either of these possibilities, even a network with a perfect firewall policy (short in length and optimally ordered [6], [7]) is susceptible to attacks resulting in prolonged delays, data loss, or both, and it is for this reason that a new firewall architecture is necessary. Parallel firewall designs provide a low latency solution, scalable to increasing network speeds [1], [8]. Unlike a traditional single firewall, the parallel design consists of an array of firewalls, each performing a portion of the work that a single firewall performed. As network speeds increase, the additional load is distributed across the array, providing a solution that can be implemented using standard hardware. The firewall that will be discussed is Microsoft firewall which called Internet Security and Acceleration firewall (ISA). In this paper a standalone (ISA) and parallel (ISA) will be discussed and tested in different scenarios and their effect on network performance will be calculated. In this paper integrations will be applied with firewalls like integrate an antivirus with firewall to work as a gateway antivirus to scan every traffic which pass through the firewall another monitor program will be added to monitor the sessions that are established through the firewall, an integrated program which split or distribute the bandwidth to users will be

added also and here the Microsoft firewall will have the responsibility to establish VPN connections. Therefore lots of test will be done to examine the performance of Microsoft firewall when it is in standalone and when using parallel Microsoft firewalls and a proposal will be presented to enhance the Microsoft firewall performance and this will happen by integration between Cisco and Microsoft products.

2. Microsoft parallel firewalls

Microsoft parallel firewall has another name called Microsoft Internet Security and Acceleration (ISA) integrated with Network Load Balance (NLB) here in this thesis ISA 2006 integrated with NLB will be used. Network Load Balancing (NLB) enables all cluster hosts on a single subnet to concurrently detect incoming network traffic for the cluster Internet Protocol (IP) addresses. On each cluster host, the NLB driver acts as a filter between the network adapter driver and the TCP/IP stack to distribute the traffic across the hosts. ISA Server takes over at this point, enabling NLB in complex deployment scenarios, including virtual private networking, Cache Array Routing Protocol (CARP), and Firewall Client. By enabling integrated NLB on an array of ISA Server firewalls, the framework will be established for NLB configuration at the network level. That is, ISA Server load balances traffic on a per-network basis. After enable NLB on the specific networks that wanted to be load balanced, ISA Server determines the network adapter that will be used for that network. If there is more than one network adapter available, ISA Server selects the network adapter based on name in alphabetical order. ISA Server performs stateful inspection on all traffic. For this reason, ISA Server works with Windows NLB to ensure that incoming and outgoing traffic for each session is handled by the same array member. This is important, because this enables ISA Server to perform stateful inspection on the traffic.

When NLB is configured for a network, at least one virtual IP address must be specified for the network. With NLB integration enabled, ISA Server modifies both the network properties and the TCP/IP properties of the network adapter. Using ISA Server Management, more than one virtual IP address can be configured for each load balanced network. In some scenarios, such as NLB publishing scenarios, multiple virtual IP addresses may be used and all the traffic will pass through firewalls using this virtual IP (VIP).

Here in this paper a proof will be done that the ISA integrated with NLB is not the best solution for all of cases and by using the proposal enhancements can be added to Microsoft firewalls.

3. Extra functions for Microsoft firewall

many integrated software will be added to Microsoft firewall (ISA) like Virtual Private Network (VPN) [9], antivirus software to examine the incoming traffic before being downloaded, bandwidth splitter software to distribute the bandwidth to all of authenticated users. After those integrations the test will be done by using different scenarios and topologies to examine the performance of Microsoft firewalls.

4. Proposed technique

The proposal is depending on distribute firewall tasks, this means that instead of using ISA integrated with NLB to work as a parallel firewalls use standalone ISA and put them behind two Cisco 6500 switch which will have NLB enabled through them by using (HSRP) protocol [10] so NLB algorithm here will depend on switches not in firewalls so as will be seen in the results this will enhance the network performance. Off course this will not exceed the budget because any network topology should use two products like 6500 Cisco switch to enable NLB through their internal network and enable high availability and fault tolerance so here this feature will be used with Microsoft firewall to distribute their functions. A proof of this proposal will be presented along with experimental results showing that the advantages of this techniques.

5. Experimental results

The test will be done by using Microsoft firewall standalone and parallel all of the firewall will have constant number of 3000 firewall policy and all of them have Antivirus integration, monitor integration and bandwidth splitter integration. Many scenarios will be tested as following:-

5.1 Without Firewall

There is no firewall on network, so there is only 2950 switch to connect servers, then generation of the traffic directly from source to destination will be done. Fig 1 shows transmissions of (8068560 Kbytes) In (699.6 sec) are done and the bandwidth usage is 94481 Kbits/sec.

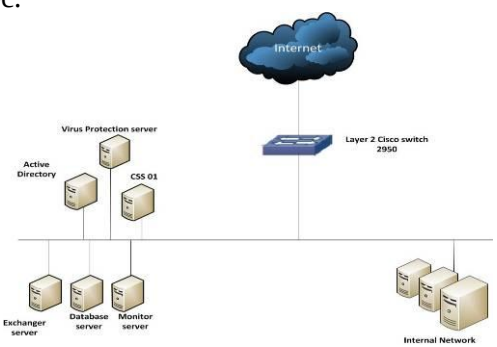

Fig 1 Topology for no firewall

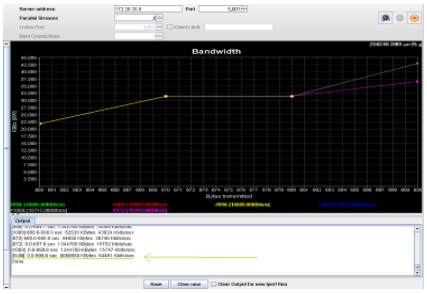

Fig 2 Result for no firewall

5.2 Standalone firewall Without VPN

Using only one single firewall without VPN and generate the same traffic but here it will pass first through the firewall going to the receiver servers and then the results will be as Fig 4 shows Results for generated traffic through standalone firewall from first client, transmissions of (8068560 Kbytes) In (1415.1 sec) are done, the bandwidth usage is 48121 Kbits/sec and Fig 5 shows Results for generated traffic through standalone firewall from second client, transmissions of (8068560 Kbytes) In (1401.3 sec) are done, the bandwidth usage is 48121 Kbits/sec. Fig 6 shows processor Usage for Standalone firewall which equal 45%.

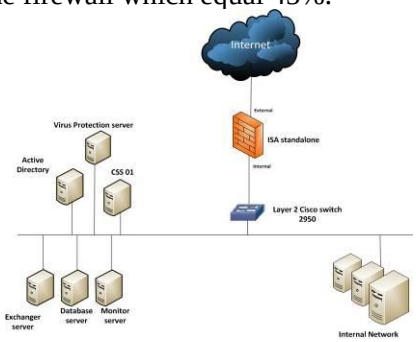

Fig 3 Topology Standalone firewall

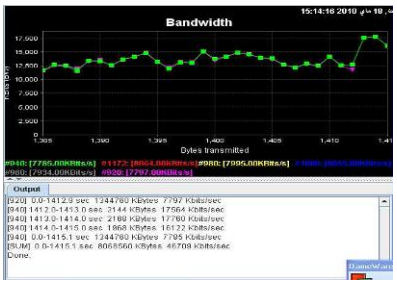

Fig 4 Results for generated traffic through standalone firewall from first client

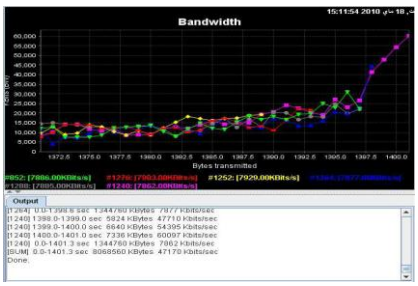

Fig 5 Results for generated traffic through standalone firewall from second client

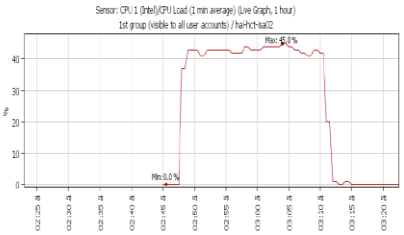

Fig 6 Standalone firewall processor Usage

5.3 Standalone firewall With VPN

Using only one single firewall with VPN and generate the same traffic. Fig 7 shows Results for generated traffic through standalone firewall from first client, transmissions of (8068560 Kbytes) In (1419.6 sec) are done, the bandwidth usage is 46560 Kbits/sec and Fig 8 shows Results for generated traffic through standalone firewall from second client, transmissions of (8068560 Kbytes) In (1365.8 sec) are done, the bandwidth usage is 48393 Kbits/sec. Fig 9 shows processor Usage for Standalone firewall with VPN which equal 91% and this is a huge number which will lead to hang the system up and thus becoming vulnerable to Denial of Service (DoS) attacks.

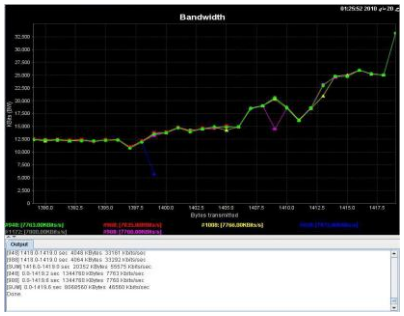

Fig 7 Results for generated traffic through standalone firewall from first client while using VPN

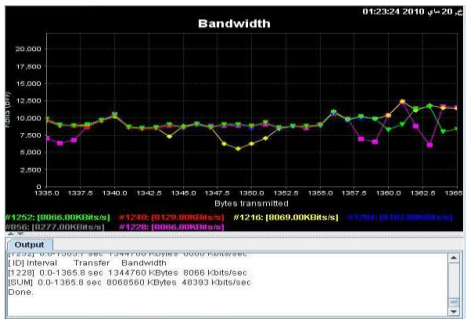

Fig 8 Results for generated traffic through standalone firewall from second client while using VPN

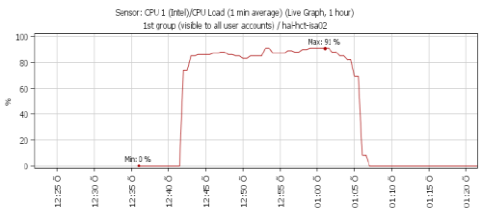

Fig 9 Standalone firewall processor Usage while using VPN

5.4 Enterprise edition ISA integrated with NLB for only internal Without VPN

Using Enterprise edition ISA integrated with NLB for only internal Without VPN and generate the same traffic. Fig 11 shows Results for generated traffic through ISA integrated with NLB for only internal from first client, transmissions of (8068560 Kbytes) In (1063.3 sec) are done, the bandwidth usage is 62165 Kbits/sec and Fig 12 shows Results for generated traffic through ISA integrated with NLB for only internal from second client, transmissions of (8068560 Kbytes) In (14532.2 sec) are done, the bandwidth usage is 45484 Kbits/sec. Fig 13 shows processor Usage for first firewall host which equal 41% Fig 14 shows processor Usage for second firewall host which equal 45%.

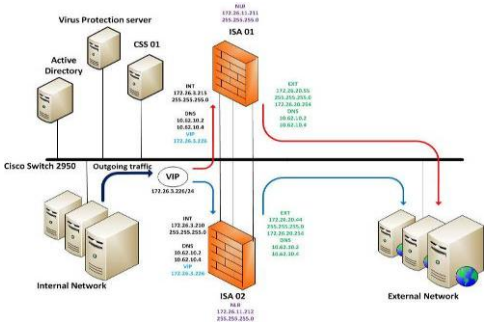

Fig 10 Topology parallel firewall integrated with NLB for only internal

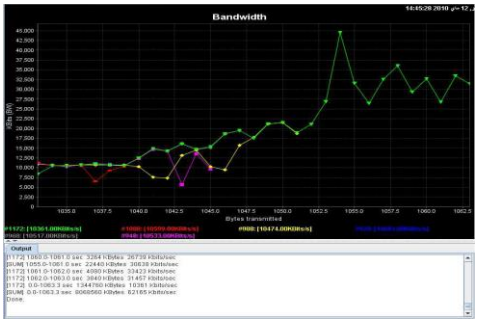

Fig 11 Results for generated traffic from first client through parall firewall integrated with NLB for internal network.

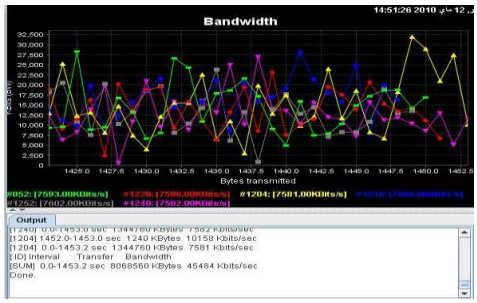

Fig 12 Results for generated traffic from second client through parallel Firewall integrated with NLB for internal network.

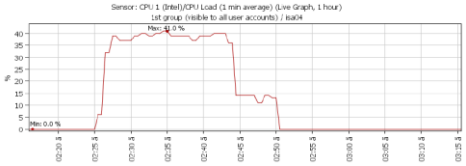

Fig 13 processor Usage for first parallel firewall integrated with NLB for internal network

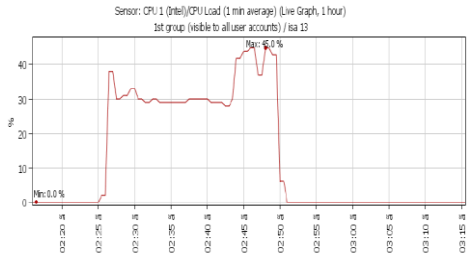

Fig 14 processor Usage for Second parallel firewall integrated with NLB for internal network

processor Usage for second firewall host which equal 75%.

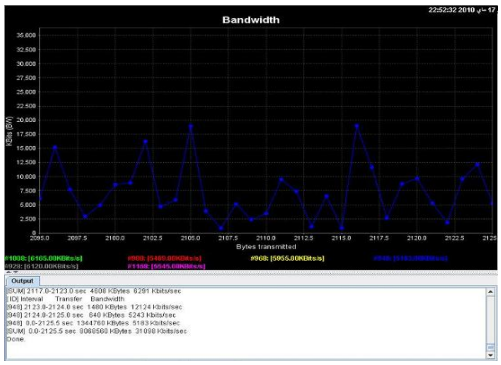

Fig 15 Results for generated traffic from first client through parallel firewall integrated with NLB for internal network with VPN Enabled

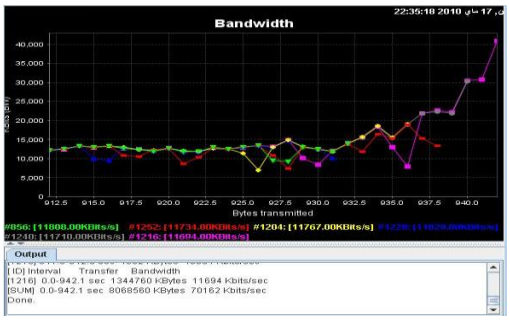

Fig 16 Results for generated traffic from Second client through parallel
firewall integrated with NLB for internal network with VPN Enabled

5.5 Enterprise edition ISA integrated with NLB for only internal With VPN

Using Enterprise edition ISA integrated with NLB for only internal With VPN and generate the same traffic. Fig 15 shows Results for generated traffic through ISA integrated with NLB for only internal with VPN from first client, transmissions of (8068560 Kbytes) In (2125.5 sec) are done, the bandwidth usage is 31098 Kbits/sec and Fig 16 shows Results for generated traffic through ISA integrated with NLB for only internal with VPN from second client, transmissions of (8068560 Kbytes) In (942.1 sec) are done, the bandwidth usage is 70162 Kbits/sec. Fig 17 shows processor Usage for first firewall host which equal 47% Fig 18 shows

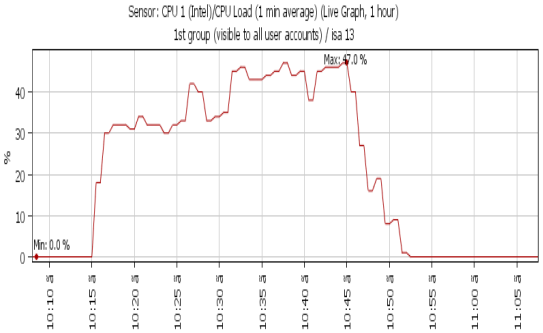

Fig 17 processor Usage for first parallel firewall integrated with NLB for internal network with VPN enabled

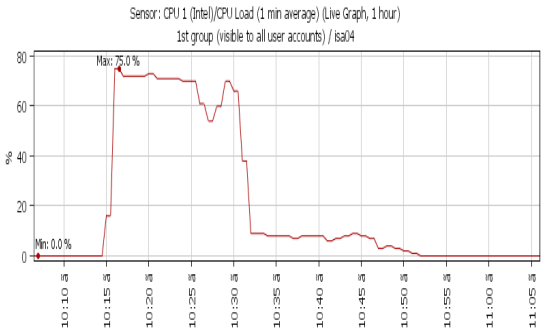

Fig 18 processor Usage for second parallel firewall integrated with NLB for internal network with VPN enabled

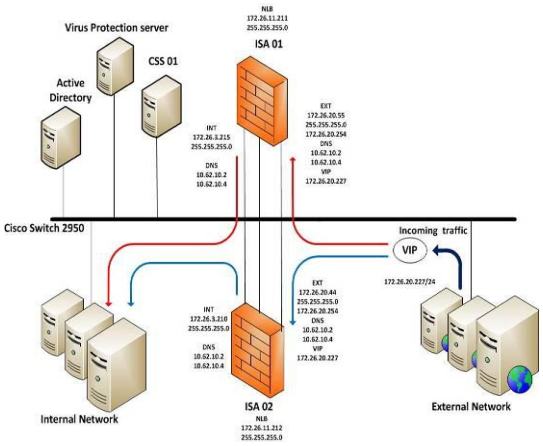

Fig 20 Topology parallel firewall integrated with NLB for outgoing traffic

5.6 Enterprise edition ISA integrated with NLB for only internal & External Without VPN

Using Enterprise edition ISA integrated with NLB for only internal & external Without VPN and generate the same traffic. Fig 21 shows Results for generated traffic through ISA integrated with NLB for internal & external without VPN from first client, transmissions of (8068560 Kbytes) In (1900.2 sec) are done, the bandwidth usage is 34785 Kbits/sec and Fig 22 shows Results for generated traffic through ISA integrated with NLB for internal & external without VPN from second client, transmissions of (8068560 Kbytes) In (932.9 sec) are done, the bandwidth usage is 70852 Kbits/sec. Fig 23 shows processor Usage for first firewall host which equal 33% Fig 24 shows processor Usage for second firewall host which equal 44%.

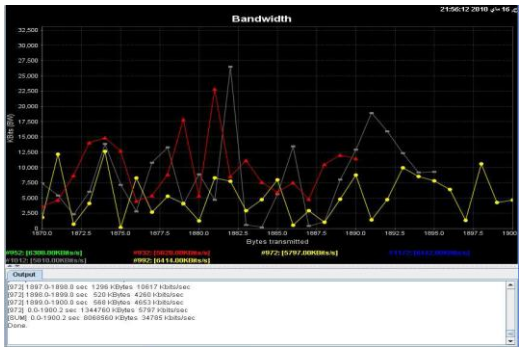

Fig 21 Results for generated traffic from first client through parallel firewall integrated with NLB for internal & External network.

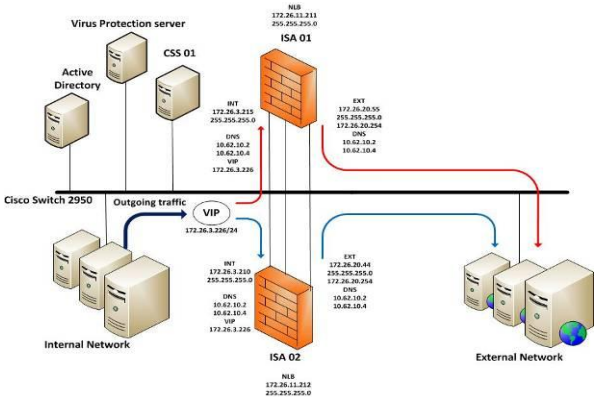

Fig 19 Topology parallel firewall integrated with NLB for incoming traffic

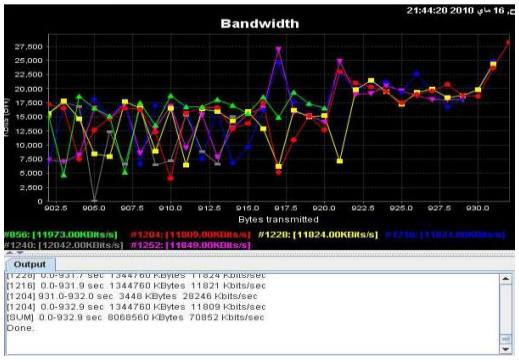

Fig 22 Results for generated traffic from second client through parallel firewall integrated with NLB for internal & External network.

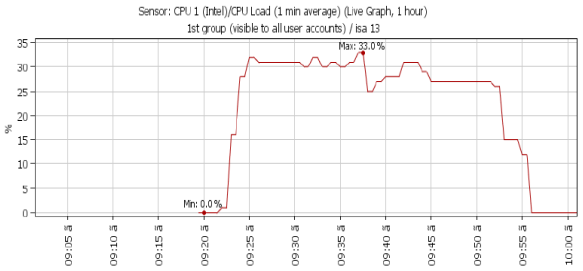

Fig 23 processor Usage for first parallel firewall integrated with NLB for internal & External network.

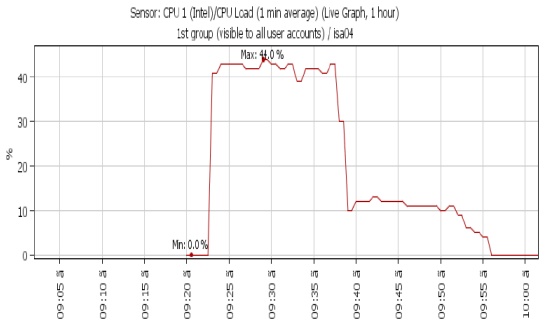

Fig 24 processor Usage for second parallel firewall integrated with NLB for internal & External network.

5.7 Enterprise edition ISA integrated with NLB for only internal & External With VPN

Using Enterprise edition ISA integrated with NLB for only internal & external With VPN and generate the same traffic. Fig 25 shows Results for generated traffic through ISA integrated with NLB for internal & external with VPN from first client, transmissions of (8068560 Kbytes) In (1461.9 sec) are done, the bandwidth usage is 45213 Kbits/sec and Fig 26 shows Results for generated traffic through ISA integrated with NLB for internal & external with VPN from second client, transmissions of (8068560 Kbytes) In (1092.4sec) are done, the bandwidth usage is 60509 Kbits/sec. Fig 27 shows processor Usage for first firewall host which equal 80% Fig 28 shows processor Usage for second firewall host which equal 69%.

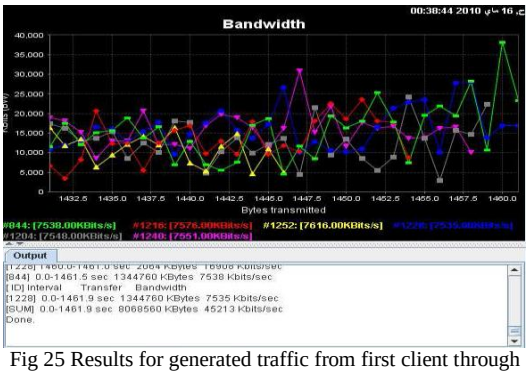

Fig 25 Results for generated traffic from first client through parallel firewall integrated with NLB for internal & External network with VPN enabled

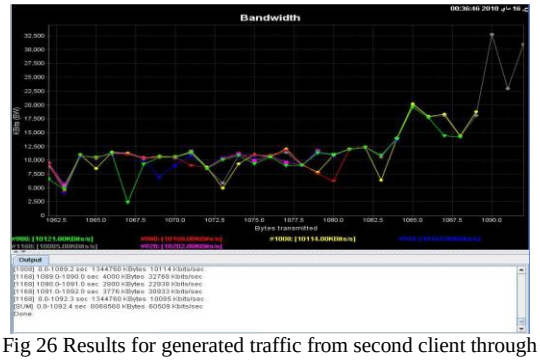

Fig 26 Results for generated traffic from second client through parallel firewall integrated with NLB for internal & External network with VPN enabled

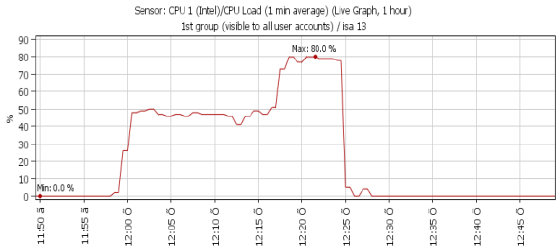

Fig 27 processor Usage for first parallel firewall integrated with NLB for internal & External network with VPN enabled

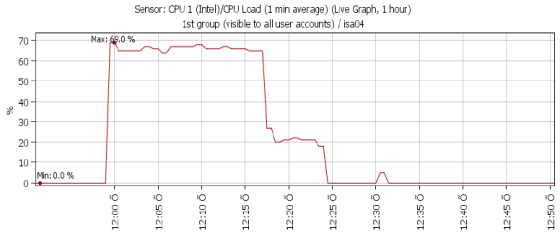

Fig 28 processor Usage for second parallel firewall integrated with NLB for internal & External network with VPN enabled

5.8 Two standalone firewall with two Cisco 6500 switch with HSRP enabled without VPN

Using two stand alone firewalls with two Cisco switches 6500 with HSRP enabled Without VPN and generate the same traffic. Fig 30 shows Results for generated traffic from first client through two standalone firewall with two Cisco 6500 switch with HSRP enabled, transmissions of (8068560 Kbytes) In (821.3 sec) are done, the bandwidth usage is 80476 Kbits/sec and Fig 31 shows Results for generated traffic from second client through two standalone firewall with two Cisco 6500 switch with HSRP enabled, transmissions of (8068560 Kbytes) In (1388.5 sec) are done, the bandwidth usage is 47603 Kbits/sec. Fig 32 shows processor Usage for first firewall host which equal 43% Fig 33 shows processor Usage for second firewall host which equal 41%.

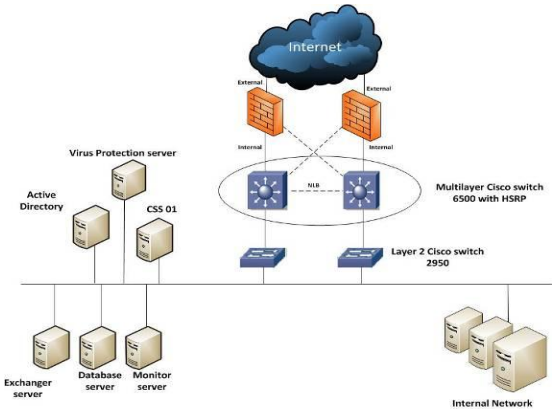

Fig 29 Topology for two standalone firewall with two Cisco 6500 switch with HSRP enabled

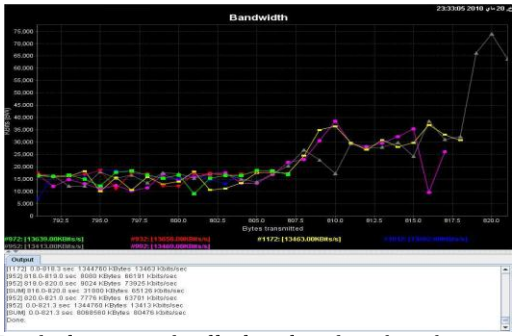

Fig 30 Results for generated traffic from first client through two standalone Firewall with two Cisco 6500 switch with HSRP enabled

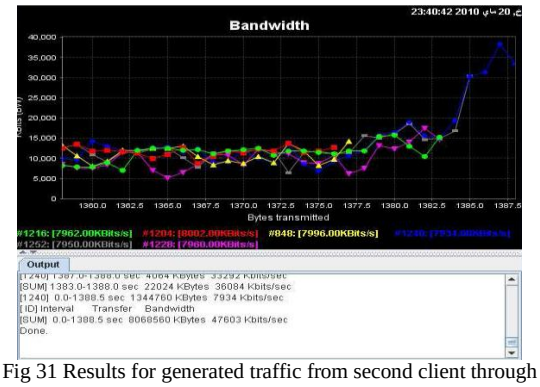

Fig 31 Results for generated traffic from second client through two standalone firewall with two Cisco 6500 switch with HSRP enabled

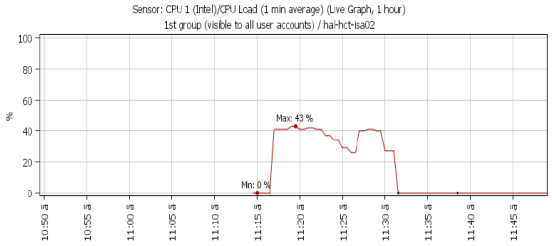

Fig 32 processor Usage for first firewall of two standalone firewall with two Cisco 6500 switch with HSRP enabled

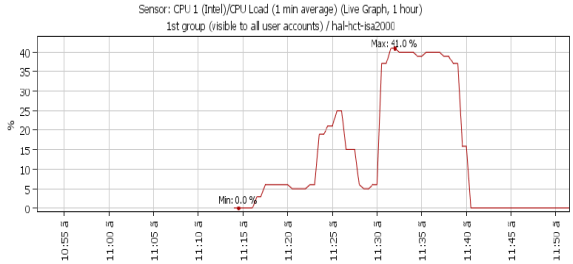

Fig 33 processor Usage for first firewall of two standalone firewall with two Cisco 6500 switch with HSRP enabled

5.9 Two standalone firewall with two Cisco 6500 switch with HSRP enabled witt VPN

Using two stand alone firewalls with two Cisco switches 6500 with HSRP enabled With VPN and generate the same traffic. Fig 34 shows Results for generated traffic from first client through two standalone firewall with two Cisco 6500 switch with HSRP enabled, transmissions of (8068560 Kbytes) In (942.4 sec) are done, the bandwidth usage is 70135 Kbits/sec and Fig 35 shows Results for generated traffic from second client through two standalone firewall with two Cisco 6500 switch with HSRP enabled, transmissions of (8068560 Kbytes) In (1410.1 sec) are done, the bandwidth usage is

46873 Kbits/sec. Fig 36 shows processor Usage for first firewall host which equal 75% Fig 37 shows processor Usage for second firewall host which equal 81%.

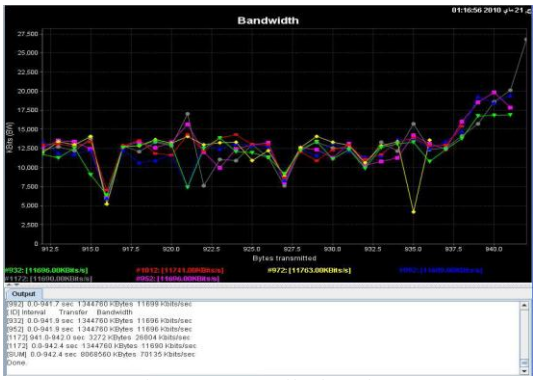

Fig 34 Results for generated traffic from first client through two standalone firewall with two Cisco 6500 switch with HSRP enabled using VPN

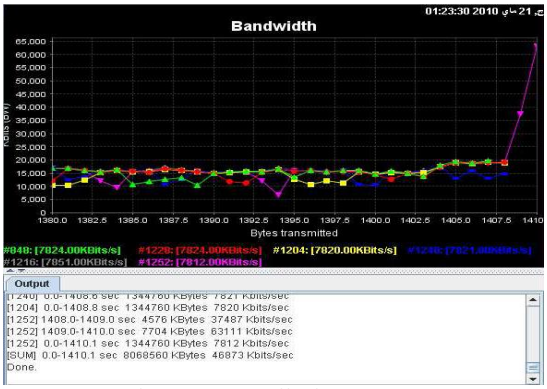

Fig 35 Results for generated traffic from second client through two standalone firewall with two Cisco 6500 switch with HSRP enabled using VPN

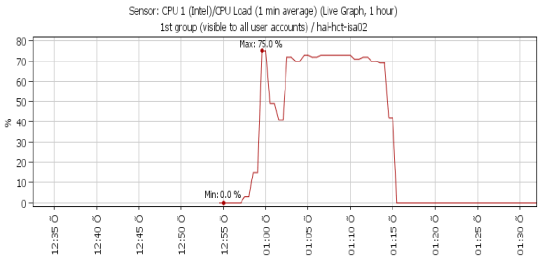

Fig 36 processor Usage for first firewall of two standalone firewall with two Cisco 6500switch with HSRP enabled using VPN

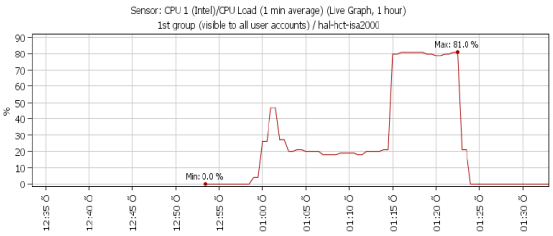

Fig 37 processor Usage for second firewall of two standalone firewall with two Cisco 6500 switch with HSRP enabled using VPN

6. Conclusion

Functional parallelism is a scalable solution for inspecting packets in a high-speed environment. However, the system performance is dependent on the number of integrated functions that the firewall can do and also the number of firewall policy or firewall rules that the firewall apply to traffic. This paper described guidelines for Microsoft parallel firewall (ISA) in different scenarios but in all scenarios a fixed number of firewall policy (rules) is used it consists of 3000 rules and generations of 8068560 Kbytes are used from computers. As shown in the previous results the best solution when using firewall without VPN is the proposed technique (two standalone firewalls with HSRP enabled in two Cisco switch) because this technique allow us to send 8068560 Kbytes in 821.3 Second and using bandwidth 80476 Kbits/s and the firewall processor usage is 43% all of those from the first client computer, in second client computer the proposed technique allow us to send 8068560 Kbytes in 1388.5 second and using bandwidth 47603 Kbits/s and the firewall processor usage is 41% and this is the best result comparison with other techniques because the proposed technique allow us to use more bandwidth and use smaller time than others. And also the best solution when using firewall with VPN is the proposed technique (two standalone firewalls with HSRP enabled in two Cisco switch) because this technique allow us to send 8068560 Kbytes in 942.4 second and using bandwidth 70135 Kbits/s and the firewall processor usage is 75% all of those from the generated traffic come from first client computer, in second client computer the proposed technique allow us to send 8068560 Kbytes in 1410.1 second and using bandwidth 47873 Kbits/s and the firewall processor usage is 81% and this is the best result comparison with other techniques because the proposed technique

allow us to use more bandwidth and use smaller time than others.

References:

[1] C. Benecke, "*A parallel packet screen for high speed networks*," in Proceedings of the 15th Annual Computer Security Applications Conference, 1999.

[2] O. Paul and M. Laurent, "*A full bandwidth ATM firewall*," in Proceedings of the 6th European Symposium on Research in Computer Security ESORICS'2000, 2000.

[3] E. D. Zwicky, S. Cooper, and D. B. Chapman, Building Internet Firewalls. O'Reilly, 2000.

[4] A. Wool, "*A quantitative study of firewall configuration errors*," IEEE Computer, vol. 37, no. 6, pp. 62 –67, June 2004.

[5] R. L. Ziegler, Linux Firewalls, 2nd ed. New Riders, 2002.

[6] E. W. Fulp, "*Optimization of network firewall policies using directed acyclical graphs*," in Proceedings of the IEEE Internet Management Conference (IM'05), 2005.

[7] S. Acharya, J. Wang, Z. Ge, and T. F. Znati, "*Traffic-aware firewall optimization strategies*," in Proceedings of the IEEE International Conference on Communications, 2006.

[8] E. W. Fulp and R. J. Farley, "*A function-parallel architecture for highspeed firewalls*," in Proceedings of the IEEE International Conference on Communications, 2006.

[9] Virtual Private Networks http://technet.microsoft.com/en-us/network/bb545442.aspx

[10] Hot Standby Router Protocol (HSRP) http://tools.ietf.org/html/rfc2281

[11] R. L. Ziegler. Linux Firewalls. New Riders, second edition, 2002.