Evaluation of Firewall Effects on Network Performance

H. Garantla*, and O. Gemikonakli**,
*MSc Computer and Network Security, **Tutor and Head of Department
Department of Computer Communications
School of Engineering and Information Sciences,
Middlesex University,
The Burroughs, Hendon,
London, NW4 4BT, UK e-mail: HG229@live.mdx.ac.uk

Abstract — This paper evaluates firewalls, their importance in protecting networks and their functions such as performance, efficiency and security. The relation between the security and performance efficiency is presented through different scenarios and the relationship between security and performance in firewalls is evaluated. Emphasis is on the relationship between network security and performance; the effects of firewalls on network performance. Various scenarios were evaluated through simulations using OPNET to show the effects of firewalls on network performance.

Keywords: Firewalls, network security, network performance

I. INTRODUCTION

In the cyber age, threats to computer networks are beyond any dispute. Any corporation would prioritise safety of their networked resources, availability of IT infrastructure, confidentiality, integrity and availability of information they store and or transmit. Threats come in various forms; malicious attacks, viruses, Trojan horses, spam, malware, masquerading, eavesdropping, theft, deletion, corruption, etc. Researchers and developers work round the clock to combat security risks. Firewalls are essential components in improving network security. Anti-virus developers always recommend the use of a separate firewall. Leading security companies such as Kaspersky, Symantec, Norton, McAfee as well as internetworking device manufacturers such as Cisco develop firewall solutions for this purpose. A firewall reduces risks that come from other networks which may have fatal consequences if succeeded. Firewalls restrict unwanted traffic or packets entering an enterprise network enhancing security. They allow configuration to fit purpose and work according to policies set by administrators/security specialists. A firewall can keep track of insecure protocols and services and protects systems from them. It keeps information about systems, networks, IP addresses, routes, protocols, ports, applications etc. [5] of its own network and provides protection from potential attacks. Firewalls also provide audit trails (log files) i.e. security and statistical data so that we can ensure that our network is operating in a safe and secured manner. Firewalls also allow configuring alerts so that we can notice any potential security breaches. A firewall provides centralized management of network security as it is linked to the external world. So as firewalls are having this much of importance in networking world and every organization or company depends on firewalls there is tremendous need for development of firewall security features and performance in our applications.

Incorporating a firewall into a network structure is likely to increase processing and even create bottlenecks. Hence, it is essential that the effects of firewalls on network performance are investigated. To do this, the following networks were considered: 1) without firewalls 2) with firewall and 3) with firewall filtering

II. BACKGROUND

As the proverb says necessity is the mother of invention. If there is no problem there is no necessity to find a solution. So if there are no threats and security risks there is no need to develop or improve security features or services. To improvise the tools we have for enhancing security, we need to look into the types and kinds of security threats and risks which disturb our basic objective of providing confidentiality, integrity, and availability. Protocol and application development started before vulnerabilities were anticipated and security was not inherent to such developments. Even when developers considered vulnerabilities, sometimes protocol/application design and development can lead to flaws and bugs. Attackers are good at exploiting such flaws and vulnerabilities to gain
of death is an exploitation of this weakness where oversized packets are only some examples used by attackers. Stacheldraht is a distributed denial of service attack where compromised hosts are used to overwhelm a target. When this happens the attacker system or computer can become a powerful tool in the hands of attackers. Misleading ICMP messages can create serious performance issues for computer networks. Ping of death is an exploitation of this weakness where oversized ICMP messages may cause a system to crash. One of the most dangerous threats is probably the distributed denial of service attack. The coordinated and distributed form of this attack makes it very difficult for network administrators to detect and prevent. The encryption techniques which were later developed make it more difficult to track down the attacker. When this happens the legitimate traffic or a legitimate connection could run at a slow pace or could be terminated. The encryption techniques which were later developed make it difficult for network administrators to detect and prevent. Firewalls can give limited protection against viruses and Trojan horses that can enter a system using email exchanges, downloads, or portable memory devices. These type of attacks are very dangerous and should be detected in time and prevented. Firewalls can give limited protection from these as they look for any indications, fingerprints, known viruses or Trojan horses. The simple mail transfer protocol can easily be manipulated. Forged usernames can fool a system easily. Break-ins are possible exploiting any trust a network administrator extends to any host or system on the Internet. Using user accounts and passwords is the most common practice in any organization. Intruders and hackers can easily guess weak passwords. There are tools for hackers or intruders to steal and decode passwords (e.g. CRACK) [2]. Many other exploits are possible: backdoors, traffic snooping, IP spoofing and impersonation etc. Firewall technologies have improved significantly since the early 1990s. In the initial days the firewalls comprised of only packet filtering devices. New firewalls work with features such as filtering packets statefully, virtual private networks (VPN), authenticating connections, intrusion detection systems, multicast routing, dynamic host configuration protocol (DHCP) services like these and many others are still emerging [1]. In time, firewall functioning became more relevant to OSI Reference Model. Firewall functions can cover up to 5 layers, e.g. they work on application, session, transport, network and data link layers. For example access control lists (ACLs) function at the 3rd layer while the extended ACLs function at 3rd and 4th layers of OSI. For a firewall to be more effective in its functionality, it should cover more layers of OSI. For example the firewall that functions only on OSI layers 4 and 3 can filter only internet protocol information, addresses, UDP or TCP port numbers. It cannot keep an eye on the application information like authentication of the users or data or commands entered by the users. So the more layers covered by firewall functioning the more security and effectiveness of firewalls can be used. Of course the more is expected from firewalls, the more likely they are likely to degrade performance – at least in theory. This is an issue to be addressed.

Firewalls comprise of many devices or parts. One of those is filtering traffic devices and it is called as filtering firewall. Stateful firewalls, Packet-filtering firewalls, application gateway firewalls, address-translation firewalls, host based firewalls, and hybrid firewalls all have different effects on network performances. Packet filtering firewalls are the basic and simple form of firewalls. This can be compared with a router and it has the capability to filter on the contents of packets. It examines OSI layer 3 information and sometimes layer 4. Packet filtering usually support different protocols. Packet filtering is implemented once the rules are defined. The rules which are established in firewalls are used to match the packet contents to decide whether to allow or deny traffic. There are two situations for denying traffic: acknowledging the sender that the packets or traffic is dropped or discarding them without any notification. Selecting a choice is important because when the user is notified of his packet drop he can know that the firewall is protecting the network and if the user is a legitimate user he can consult the administrator and he can change the filtering rules and allows the user if he has the privilege. So if the firewall doesn’t send any notification the user is not able to understand why the connection could not be set up and tries on setting it up [1]. It is likely that acknowledgments may provide potential attackers with useful information of firewall configuration which may empower them in further refining their attempts to gain access to a protected target. Following information can be checked by packet filtering firewalls: Layer 3 - IP addresses, protocols such as OSPF, TCP, IP, UDP, ICMP and others, the description; layer 4 – the port numbers of UDP and TCP, the flags of TCP such as ACK, RST, SYN, FIN, and PSH, etc [1]. All at a cost.

So, what should be prioritized? Security or performance? Clearly, in an attack free cyber world where no preventive and/or corrective measures are necessary, demand for resources such as CPU time would be less. However, we live in a vulnerable world of networking and in the middle of an undeclared war. Hence, security measures are unavoidable; absence of these is an open invitation to disaster. Therefore, what are positive aspects of combined security and performance? What are the negative aspects?
The main advantage is that firewalls can filter or examine packets at tremendous speeds. These firewalls provide lot of flexibility in defining security policies as they can match or observe the most fields in layer 3 and headers of layer 4 [1]. However, connection authentication is not supported in most firewalls, logging features or capabilities are limited, they usually support protection against layer 3 and layer 4 only, and application layer attacks cannot be examined, configuration or changes in the rule sets or defining them can be complex, and firewalls are susceptible to some kind of TCP/IP protocol attacks.

III. WORK DONE & RESULTS

In this work, the aim is to evaluate firewalls from a different perspective: Do they degrade the performance of networks they are deemed to protect from performance degradation or complete failure? Even standard IP ACLs require processing at an entry point which may have a long list of control statements. Extended, reflexive, and context-based ACLs may demand more processing power than the standard ones due to their improved functionality. Therefore, what are the pros and cons of firewalls? Since the interest here is the performance of a network incorporating firewalls, we modelled networks with and without firewalls and different firewall functionality and simulated such networks with an eye on their performances. We used OpNET for our simulations. Figure 1 shows one of the scenarios implemented on OpNET. This first scenario depicts a network in the absence of a firewall. The second scenario incorporates a firewall. In the third scenario, the functionality of the firewall is further increased incorporating filtering http traffic entering the system.

The scenarios assumed 100 users on different subnets (shown as a cloud) database and web servers. Heavy loads are assumed in terms of database and web traffic. After configuring traffic patterns for applications considered user types were configured. The simulation is used to measure the following: database query response time, http page response time/sec, point-to-point link utilizations. Simulation results are given in the figures 2-5. Figure 2 shows the database’s response to user requests under three different scenarios. Response times change between just under a second and just over 1.25 seconds. Introduction of a firewall increases response times by less than 10%, however, when web traffic is filtered; the performance improves over no firewall scenario by more than 10%.

Figure 3 shows the http response time with and without a firewall for the network. Here again, the performance of the two scenarios are very close where there is a little deflection showing some performance degradation when a firewall is in use.

Inevitably, the least link utilisation is achieved when firewall is used with http traffic filtering. Figure 4 depicts link utilisation (IP cloud and router incoming). When http traffic is not filtered, link utilisation is almost independent of the use of a firewall.

Fig. 1: A configuration incorporating firewall filtering

Fig. 2: Database server mean response time
Figure 5 also depicts utilisation (IP cloud and router outgoing). In this case, a sharp drop is evident in link utilisation when there is a firewall filtering web traffic. Obviously, input parameters used would have a decisive effect in the performance of servers and links considered. Hence, results are only valuable for the situations given and similar experiments must be carried out for individual cases in order to derive meaningful conclusions. However, it will not be an overestimation to suggest that, under the current threats, firewalls do not only secure a network but also contribute to network performance by stopping attacks, improving network availability, and reducing unnecessary processing of illegitimate requests.

IV. Conclusion and Future Work

Importance of firewalls in securing network communications and resources is essential. However, more processing of networked information may lead to performance degradation of networks. Hence, it is important that as firewalls are scrutinized in terms of their contribution to network security, they should also be investigated in terms of their effects to network security. In this work, various scenarios incorporating firewalls are
analysed with regard to their effects on network performance. For this, simulation models were developed and implemented on OpNET for calculating network performance with and without firewalls. Clearly, addition to a device that would introduce extra processing is likely to increase response time, i.e. degrade system performance. However, the study shows that, when firewall filtering is involved, due to the filtering of unwanted traffic, network performance can increase considerably. Hence, the employment of firewalls is not only essential for improved network security but also they contribute to meeting service level agreements and improving quality of service not only in terms of availability, but also in terms of performance. Finding show that, the intuitive belief about firewalls that security and performance efficiency are inversely proportional does not necessarily hold in every situation, and certainly not in today’s cyber world where threats are not myths but the reality of the daily life. The impact on the performance due to the increases level of security may be seen only in some particular and specific environments or situations that requires or demands more enhanced security which could incur some overhead on firewall. However, this is offset by filtering unwanted access to the network considered. This work supports and emphasises the importance of firewalls in the world of networking. There is still a tremendous need to look further into firewalls and their enhancements which are going on and will go on together with their influences on network performance.

REFERENCES