A Quantitative Analysis of Firewall Impact on Critical Data Communication

Minhaj Ahmad Khan*

Department of Computer Science, Bahauddin Zakariya Univ. Multan, Pakistan

Abstract: Multimedia communication is considered to engulf the entire transmission taking place through internet. Most of the applications running on clients communicating through internet incorporate video or audio data transmission. Such transmission may however hinder the performance of other critical applications running on the network. For instance, the clients connecting to a database may suffer large delays if the network bandwidth is being utilized for multimedia communication. In this regards, a firewall may be used to block the non-critical and unnecessary communication.

In this paper, we perform a quantitative analysis to record the impact of a firewall deployed in a network. We develop various network scenarios with voice and video data being transmitted in parallel with queries from a database client. As the database application is critical for its clients, the unnecessary communication causing the wastage of bandwidth is blocked through a firewall. We record the improvement in the performance of the database application due to the usage of firewall. We simulate all the scenarios using OPNET IT Guru v 9.1. Our results show that due to the blocking of video transmission, there is a significant improvement in performance of the database application. We also find that the use of a firewall has an overhead that depends mainly on the amount of communication taking place simultaneously and can also impact the performance of the critical application.

Keywords: Computer Networks, Firewall, Multimedia Communication, Voice over IP, Response Time.

1. INTRODUCTION

Computer networks depend upon various resources whose availability can change the performance of these networks. One of these resources is the available bandwidth. The computers connected through a network communicate with each other by making use of the bandwidth available to them. The response time of the applications running on the computers in the network depends heavily upon the concurrent usage of the bandwidth. Data traffic load changes for different applications, e.g. two computers involved in a voice chat require transmission of more data in comparison with the computers involved in a text chat. For an application critical for the system, it becomes inevitable to reserve the resources in order to improve its response time [1, 2]. For example, a database application running on a machine in a bank may be critical to perform transactions. A query from the client machine in the bank may connect to some remote server, get some data from the database and return it to the client. The query response time would therefore be very vital for smooth running of the system. In reality, as the query is being executed, some other non-critical applications may be executing in parallel. The non-critical applications may transfer data through the same route as being used for critical applications. The increase in the network traffic results impacts the performance of the critical applications.

There are several ways to ensure a better quality of network communication. The standards defined in the quality of service (QoS) [3-7] make it possible to ensure several metrics such as delay or throughput (rate of data transmission). Similarly, the resource reservation protocol (RSVP) [8] is defined to reserve resources for particular types of traffic flowing across the network. None of them however guarantees to eliminate the unnecessary network traffic passing through the route being used for a critical application.

A firewall installed on a network route aims at blocking unwanted network communication. Any particular traffic passing through the firewall may be blocked at that point and either no data transmission takes place or the data transmission is delayed for unnecessary traffic. This in turn results in improvement of the response time of the critical applications running on the network.

In this paper, we perform a quantitative analysis to find the impact of using a firewall in a network with a critical database application running in parallel with other non-critical multimedia applications. The unwanted traffic resulting from the voice and video communication is blocked to increase the response time of the database application. We perform experimentation using different number of clients to record its impact on the response time. Our scenarios representing networks with varying number of clients are developed using OPNET IT Guru v 9.1 [9].

*Address corresponding to this author at the Department of Computer Science, Bahauddin Zakariya Univ. Multan, Pakistan; E-mail: mik@bzu.edu.pk

ISSN: 1814-8085 / E-ISSN: 1927-5129/13

The rest of the paper is organized as follows. Section 2 describes the working mechanism of a firewall. In Section 3, we provide configuration of the parameters and architecture of the scenarios used for performing experimentation. The experimental results are presented and analyzed in Section 4 before the conclusion and future work given in Section 5.

2. FIREWALL WORKING MECHANISM

In a network, the firewalls are usually represented as a combination of software and hardware aiming at protecting data and network. A network may be affected by unintended use of its resources or by malicious attempts of intrusion. Users from outside a network may be attempting to enter into the system. Similarly, the users from within the network may be consuming network bandwidth for non-critical applications. All these effects can be mitigated by use of firewalls that are deployed to filter data packets flowing to/from the network.

A firewall continuously monitors the data packets being transmitted in the network. The packet filtering may discard several packets while allowing others to be transmitted across the network. Similarly, while acting as a proxy, a firewall may get/transmit every packet from/to the network, check for its security rules, and then transmit or discard depending upon the security rule. Consequently, the intended data traffic flows while making full use of available resources. The firewall therefore improves the performance of the network for the intended particular type of traffic being used for a critical application.

The firewalls implemented in OPNET IT Guru make use of several proxies installed on them. For each type of traffic, the firewall may be configured to allow or disallow the data transmission. When a packet of the blocked traffic type is received, either it is not transmitted or it is delayed for a specific interval. Only the packets of allowed data traffic are transmitted instantly, thereby improving the performance of applications running on the network with the allowed data traffic. In order to impede the packet transmission for a specific interval, the firewall can be configured so that it can slow down a specific type of traffic. To accomplish that, the firewalls allows to specify a distribution and a value for the delay to be incurred during transmission. The combination of the distribution and the value is used to generate random values. Every packet of the specific type passing through the firewall is then forced to wait for the randomly generated value.

3. EXPERIMENTAL SETUP AND CONFIGURATION

We use two basic scenarios in order to represent various networks. The first scenario as shown in Figure **1** makes use of a firewall, whereas the second scenario as shown in Figure **2** works without a firewall. The communication takes place from the database server to LAN-2. The firewall lies in the route from database server to LAN-2 in first scenario. The firewall is set to block voice and video communication and allow only database query/response communication. The routers used in the scenarios are of built-in type *ethernet2_slip8_gtwy* connected using the *PPP_DS1* links. The LANs and the database server are connected to the routers using the *100BaseT* links.

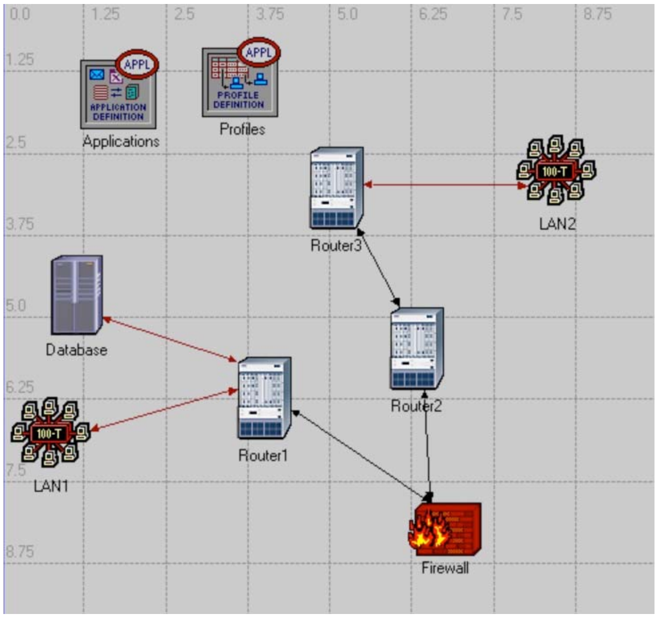

Figure 1: Communication with a firewall in the route from Database Server to LAN2; LAN1 and LAN2 also communicate for multimedia traffic in parallel.

To initiate communication, a query request is sent from clients in LAN-2 to the database server that in turn responds with some results to the client having sent the request. In parallel, there is multimedia traffic being transmitted. The clients from LAN-2 communicate using voice or video data with the servers in LAN-1. The traffic for database communication is set to have a low load, whereas for voice, we use IP telephony data load and for video, we use low resolution video data load. All the 10 clients in LAN-2 are allowed to send query requests to the database server. For voice/video communication, we have two cases:

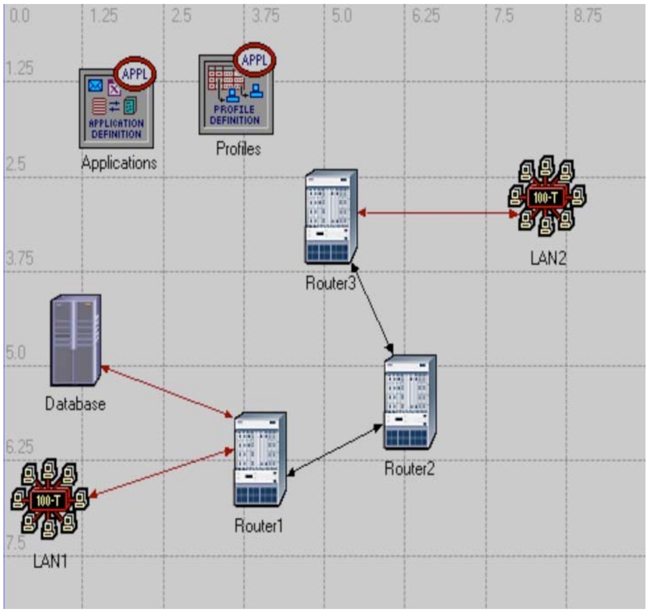

Figure 2: Communication without a firewall in the route from Database Server to LAN2; LAN1 and LAN2 also communicate for multimedia traffic in parallel.

a) Case 1: 2 clients in LAN-2 communicate with LAN-1

b) Case 2: 4 clients in LAN-2 communicate with LAN-1

The simulation for each network scenario is set to run for 300 seconds using OPNET IT Guru v 9.1.

4. PERFORMANCE RESULTS

We present results of database (DB) query response time for 2 clients and 4 clients deployed in LAN-2. Our scenarios use voice or video traffic one at a time flowing across the network and blocked by the firewall.

4.1. Results for Case 1 (2 Clients)

For case 1 in which 2 clients are used in LAN-2 to communicate with the servers in LAN-1, the performance results of DB query response time while using voice and video communication (one at a time), are given in Figures **3** and **4** respectively.

Figure **3** shows results for the voice communication taking place in parallel with the database communication. The network in the presence of a firewall has an average DB query response time of 0.010136 seconds, whereas the average DB query response time without firewall is 0.006822 seconds. Consequently, there is 1.49 times improvement in the DB query response time by blocking the voice communication. It is to be noted that the voice application for a small number of clients has low bandwidth requirements, and consequently, there is a small reduction of the DB query response time.

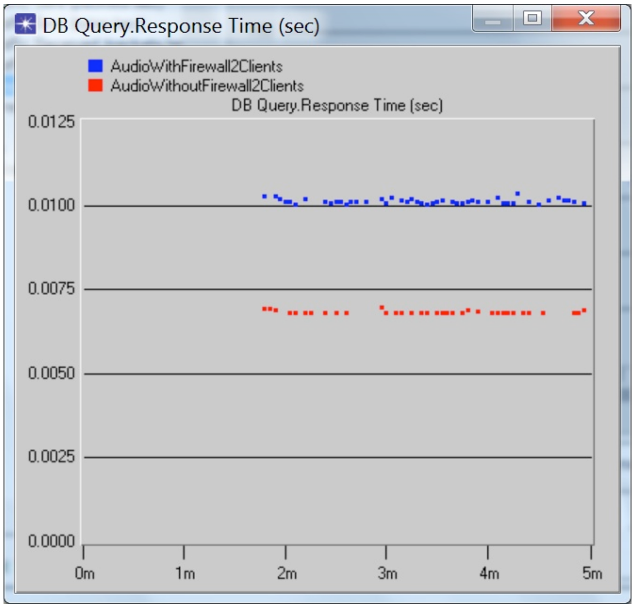

Figure 3: DB query response time results with parallel audio communication by 2 clients.

For video communication, the communication in the presence of firewall has an average DB query response time of 0.010137 seconds, whereas the average DB query response time without firewall is 48.62393 seconds, as shown in Figure **4**. Consequently, there is 4796.83 times improvement in the DB query response time. In general, the video

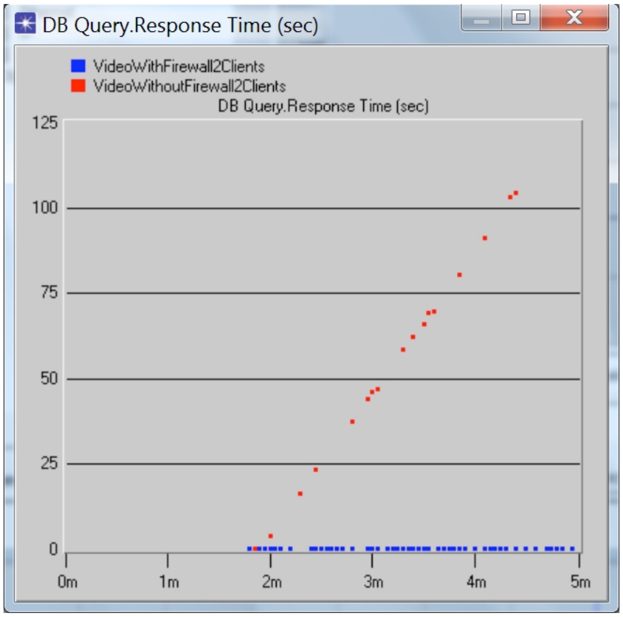

Figure 4: DB query response time results with parallel video communication by 2 clients.

communication involves a high overhead due to high bandwidth demands. Therefore, blocking the video communication results in a great improvement in efficiency in terms of the DB query response time.

4.2. Results for Case 2 (4 Clients)

For case 2 in which 4 clients are used in LAN-2 to communicate with the servers in LAN-1, the performance results of DB query response time while using voice and video communication (one at a time), are given in Figures **5** and **6** respectively.

As shown in Figure **5**, the communication in the presence of firewall has an average DB query response time of 0.010144 seconds, whereas the average DB query response time without firewall is 0.006828 seconds. Consequently, there is 1.49 times improvement in the DB query response time achieved by blocking voice communication.

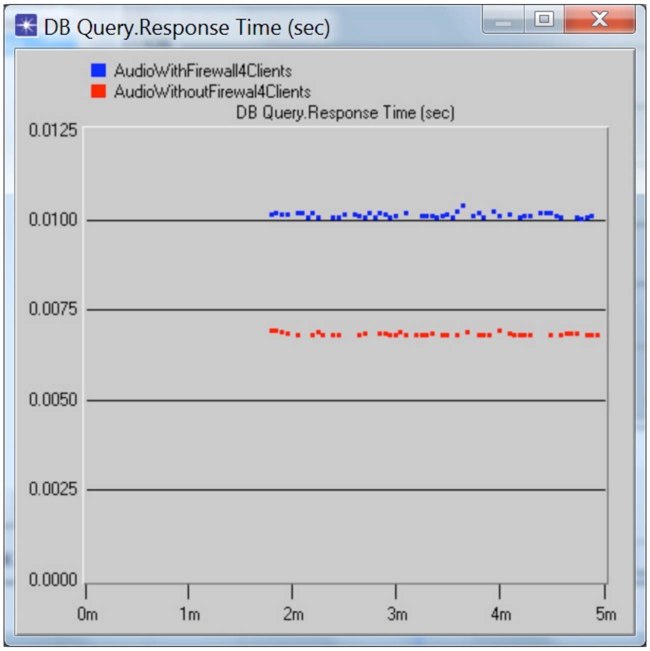

Figure 5: DB query response time results with parallel audio communication by 4 clients.

For video communication, the network in the presence of firewall has an average DB query response time of 0.010141 seconds, whereas the average DB query response time without firewall is 41.62215 seconds, as shown in Figure **6**. Consequently, there is 4104.27 times improvement in the DB query response time due to the deployment of firewall. We can see that as the number of clients increases, there is a decrement in the improvement of the DB query response time. This implies the fact that due to increase in the number of clients, a large overhead on the part of firewall is involved that also impacts the overall improvement.

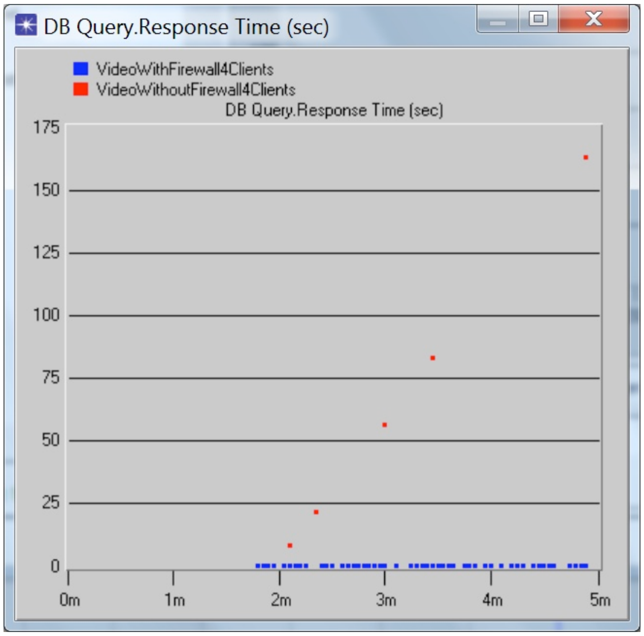

Figure 6: DB query response time results with parallel video communication by 4 clients.

4.3. Accumulated Results

Overall, the voice communication in the presence of firewall has an accumulated average DB query response time of 0.020279 seconds, whereas without firewall it has an accumulated average DB query response time of 0.04651 seconds. Consequently, there is 2.29 times improvement for voice communication by using firewall. In contrast, for the video communication with firewall, there is an accumulated average DB query response time of 0.020278 seconds, whereas without firewall it is 496.5108 seconds. Consequently, there is an improvement of 24485.37 times in the DB query response time due to the usage of firewall. We find that the great improvement in the response time for video communication is due to the fact that despite the low resolution video transmission, there is a large volume of video traffic flowing across the network. As the firewall blocks the entire flow, the DB query response time reduces significantly, thereby producing a great improvement in the performance of the critical application.

5. CONCLUSION AND FUTURE WORK

In this paper, we present a quantitative analysis of the impact of using a firewall in a network. We make use of database communication as a critical one being run in parallel with the unnecessary voice/video communication. and compare the performance of the simulated networks in terms of the database (DB) query response time. A database query request is sent from clients in a LAN to a database server also connected to the network. As long as the network bandwidth is being shared by the multimedia communication, the database query response time is high. To minimize the delay in the DB query response, we deploy a firewall and record its impact on the database query response time. We have incorporated scenarios with different number of clients (2 & 4) involved in multimedia communication to find the impact on reduction in the query response time by blocking the traffic through a firewall.

We find that with the voice communication taking place in parallel with the database communication, there is a small improvement in the performance of the database query response time if the voice communication is blocked. For both the cases, i.e. with 2 clients and 4 clients, the DB query response time reduces by 1.49 times due to the usage of firewall. The situation is different in case of video communication taking place in parallel with the database communication. For 2 clients and 4 clients, the DB query response time reduces by 4796.83 times and 4104.27 times respectively. This is due to the fact that the video communication has a higher bandwidth requirements than the voice communication. The blocking of video communication by the firewall significantly improves the performance of the database application by reducing the DB query response time.

Our current networking scenarios process voice and video transmission using a wired network. As future work, we intend to apply the same scenarios for wireless networks in order to analyze the impact of multiple firewalls being used in conjunction with several topologies.

REFERENCES

[1] Schneider S, Altenbernd P. Combining Multimedia Response-Time Analysis and the Resource Reservation Protocol for Efficient Network Scheduling of Media Streams. In Proceedings of the 7th Australian Conference on Parallel and Real-Time Systems, Australia 2000.

[2] Abeni L. Resource Reservations for General Purpose Applications. IEEE Trans Indust Inform USA 2009.

[3] ITU-T. Terms and definitions related to quality of service and network performance including dependability. ITU-T Recommendation E.800 1994.

[4] Ferguson P, Huston G. Quality of Service: Delivering QoS on the Internet and in Corporate Networks. John Wiley & Sons, USA 1998.

[5] IETF. Specification of Guaranteed Quality of Service -- RFC 2212 (Standards Track). Internet Engineering Task Force (IETF) RFC-2212 1997; Available: http://www/ietf.org/rfc/rfc2212.txt.

[6] IETF. Framework for IP Performance Metrics---RFC 2330. Internet Engineering Task Force (IETF) RFC-2330 1998; Available: htp://www.ietf.org/rfc/rfc2330.txt.

[7] ITU-T. Internet protocol aspects - Quality of service and network performance. ITU-T Recommendation Y.1540 2007.

[8] IETF. Resource Reservation Protocol (RSVP) Version 1 Functional Specification-- RFC 2205. Internet Engineering Task Force (IETF) RFC-2205 1997; Available: http://tools.ietf.org/html/rfc2205.

[9] OPNET Tech. OPNET IT Guru Academic Edition. OPNET Technologies, USA 2011; Available: http://www.opnet.com/university_program/itguru_academic_edition/

Received on 20-07-2012 Accepted on 29-12-2012 Published on 05-01-2013

http://dx.doi.org/10.6000/1927-5129.2013.09.02