ISSN: 0067-2904

Boosting the Network Performance using Two Security Measure Scenarios for Service Provider Network

Mustafa Abdulkadhim* ، **Sami Hasan**
Department of Networks Engineering, College of Information Engineering, Al-Nahrain University, Baghdad, Iraq

Abstract:
Network security is defined as a set of policies and actions taken by a network administrator in order to prevent unauthorized access, penetrated the defenses and infiltrated the network from unnecessary intervention. The network security also involves granting access to data using a pre-defined policy. A network firewall, on the other hand, is a network appliance that controls incoming and outgoing traffic by examining the traffic flowing through the network. This security measure establishes a secure wall [firewall] between a trusted internal network and the outside world were a security threat in shape of a hacker or a virus might have existed

Keywords: component, firewall, OPNET modeler, performance, response time.

Introduction:

The main security issue challenges that confront the service provider's community are resource depletion and excessive traffic by malware machines that may generate issues for service providers. Attacking [BGP] routing and injecting malicious BGP paths to redirect traffic is a technique attacker use to get the traffic [1]. Distributed Denial of service [DDoS] attack is targeted to disable authorized users to access different Internet services [2]. Domain Name System [DNS] sometimes information used in order to redirect Internet traffic to benefit those with criminal intentions [3].

These threats are linked with the following factors that are limited to service provider networks. Service providers must be able to fast deploy security measures against a huge number of users that may be attacked, and deploy these measures on a large number of nodes, usually the network entry nodes. In the enterprise universe, the number of devices the service providers have to take care of are typically smaller than those in the service provider space. Although some of the players in the enterprises have huge networks, this is still an exception in this case.

Size is one of the most important differences existed between the service provider and the enterprise security component. The number of the possible targets of and entry points for an attack is also much higher in the service provider space than that in the enterprise world; where usually a number of smaller clearly identified users frequently enjoy a maximum level of protection. Consequently, service providers must be able to secure multiple goals from multiple concurrent attacks [4].

Securing infrastructure of the carrying transit paths may not essentially secure the endpoints carries the set of encounters. Many of the standard edge-security actions that are valid in the enterprise world are not valid in the service provider security paradigm. The main variance is that firewall and [IDS/IPS] devices cannot be applied on those paths in service provider networks. Service providers cannot manage to provide granular access control. One of the main functionalities of the firewall is to transit traffic. However, firewalls cannot afford high level monitoring to transit traffic in order to detect indications of exploitation attempts in that way that IDSs/IPSs usually do. At the end, the whole set of security precautions available for securing endpoints, like host IPSs and antivirus software packages, is not of much interest in the service provider world of operation [5].

* Email: mstfkadum@gmail.com

The incentive to this research is to investigate the service provider network's performance showed by the average response time, average database response time and the average database Query response time. When we replace the firewall functionality with a router, what will happen to the network performance? how the performance will be affected and the magnitude of that effect.

The contribution of this research can be summed up in the following points.

1. Service provider network design topology.
2. Boosting the network performance while maintaining security.
3. The performance target was aimed at the service provider data center hence the DB performance effect was optimized.

Existing related work

Santoso improved the security performance and accuracy of the cloud-based network using a system called [NIDS] which stands for network intrusion detection system [6] Jun Ren et al attempted to increase the security of the data at the datacenter using a deferent privacy scheme for data duplication [7].

Theodoros et al, suggested an architecture of multilayer security in which the author suggested to divide the network infrastructure into zones to increase security control [8].

Hong Liang et al, Used an intrusion detection system collaboratively in the network to be secured. High performance cloud infrastructure are used to deploy the IDS collaboratively and efficiently [9].

Yongxin et al. evaluated major operational firewalls existed, because the operation of the organization depends on how well firewall in that organization will perform. Many performance criteria were compared in order for the service provider to know the best choice for the business needs [10].

Sheth et al. analyzed reported issues with the existing firewalls. Detailed comparison and analysis have been achieved in terms of security, cost, and implementation of an open source packet filter firewall. [11].

Tantipongsakul et al. proposed transferring the rules of the firewall using routing protocols. This will choose the optimum route to transit packets to. This will also reduce cost and evade issues encountered usually when using network routers [12].

M. Abdulkadhim measured the impact of a Routing Protocols Convergence Activity on the Network. [13] M. A. Neamah evaluated the Service Performance for WiMAX Networks Based on Node Trajectory.[14].

M. Abdulkadhim et al discussed a Future System: that uses Manet in Smartphones and created a new effiecient routing protocol that makes the job easy for routing in manets. [15].

M. A. Neamah discussed the Design and Implementation of an application framework in Wireless Sensor . [16].

M. Abdulkadhim proposed An End To End IoE-Based Solution for Healthcaresystem. [17].

M. Abdulkadhimet al discussed a improving the reliability of Routing in order to obtain QoS for Mobile Ad-Hoc Networks. [18].

The simulated network model

In order to examine the performance of the network with and without a network firewall, two scenarios were created, as shown below:

A. scenario#1 service provider network with a backbone router

In this scenario as shown in Figure-1, a network router is simulated to connect the service provider server to the internet and to technical departments as shown:

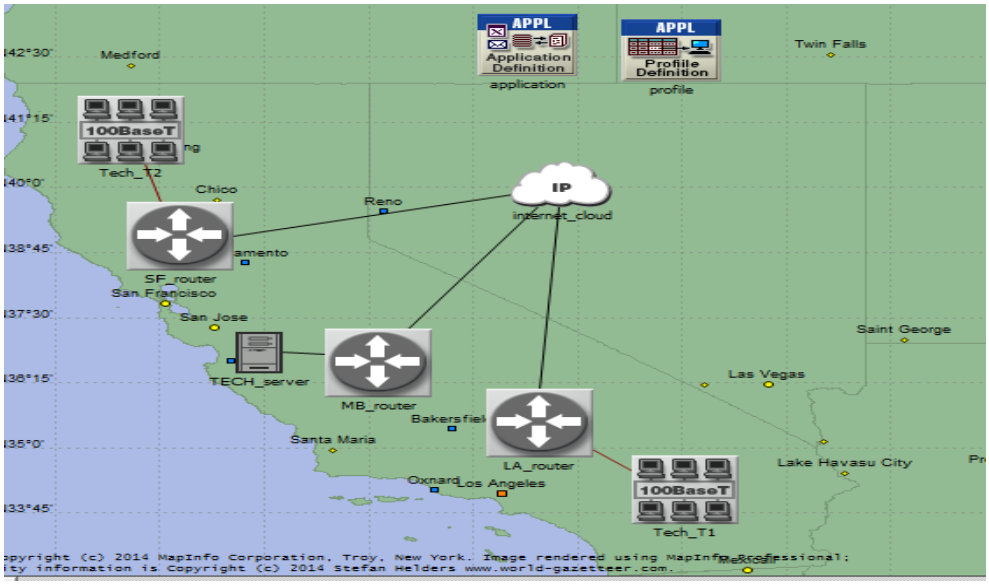

Figure 1-The router used as the backbone network device.

B. scenario#2 service provider network with a firewall router

As shown In Figure-2 above, the main backbone router was replaced by a firewall in order to examine the performance load that the firewall adds as compared to a network device like the router.

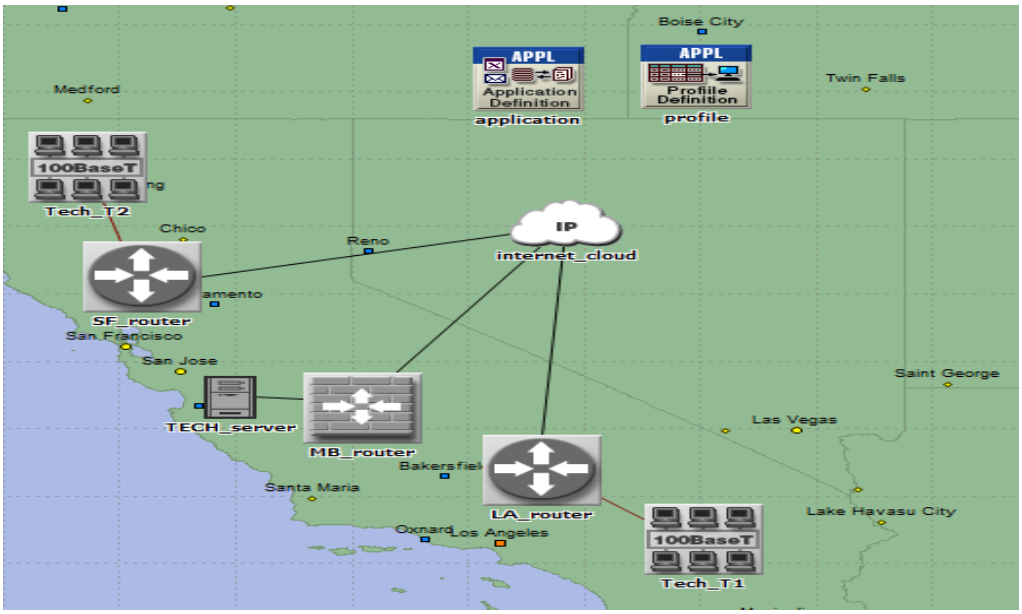

Figure 2-replacing the main service provider's router with a firewall

Performance Analysis

Http and database traffic were simulated through the network, passing as requests from clients to the company server; Passing through the router in scenario 1 and the firewall in scenario 2.

a. HTTP response time

Firstly, compare the response time for an HTTP page to load. The results are shown in Fig.3:

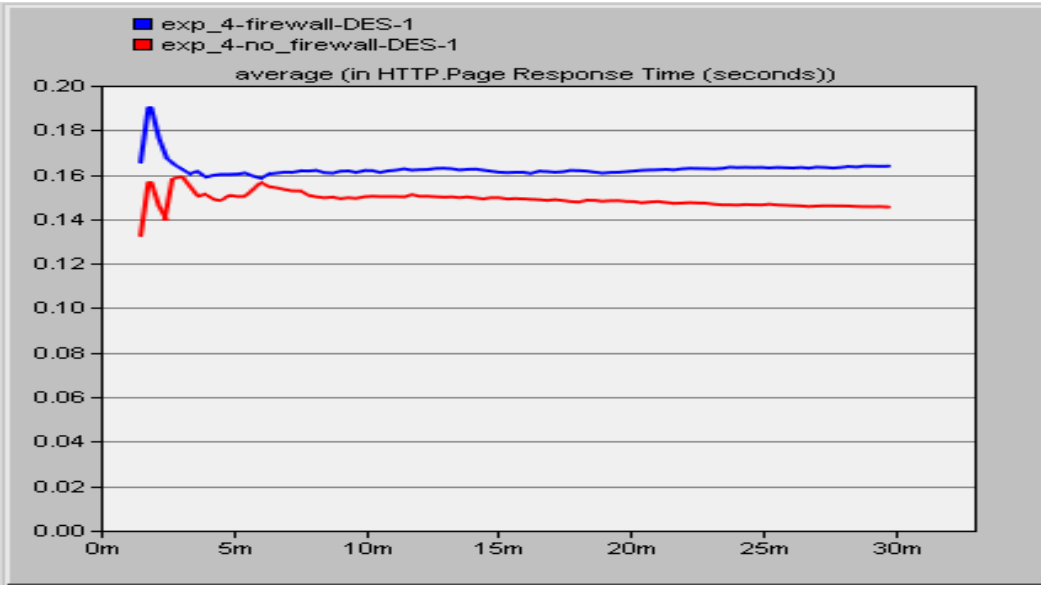

Figure 3-the average HTTP response time

From Figure-3 above, an observation may be noticed that the response time without a firewall in the network is relatively higher due to the fact that its existence will add security but also delay packet processing.

b. Database response time

The response time for database also is faster - as shown in Figure- 4, in the existence of a router than that of the firewall due to the same reason

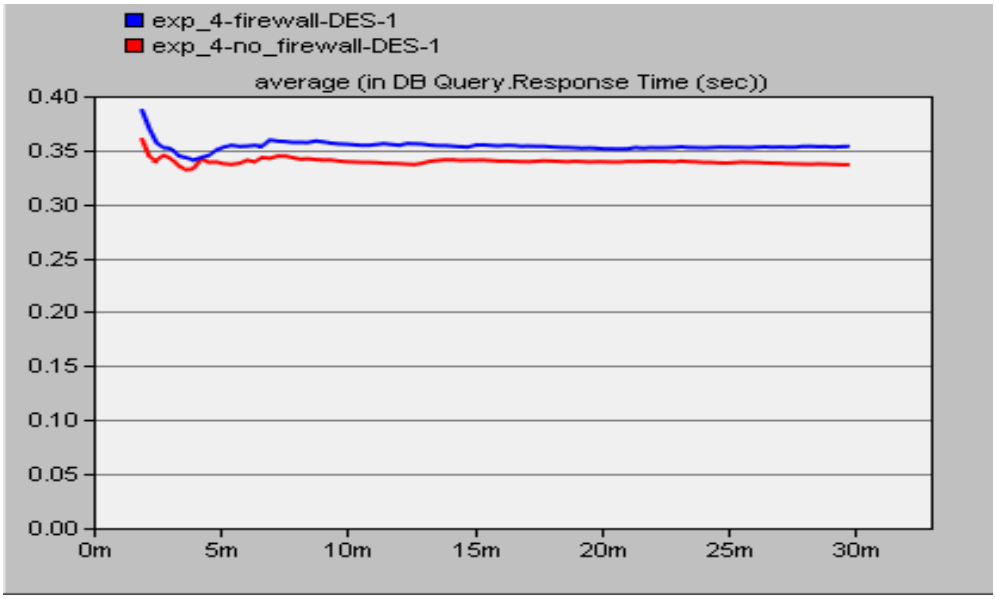

Figure 4-average DB**.** Query Response Time

In Figure-5, the traffic sent from the server to the clients was measured. We can see that the traffic sent without the existence of a security device [in this case the firewall] is higher than that with the existence of the firewall in the network.

This is due to the fact that it adds processing time to the traffic before being sent and creates a bottleneck like an effect on the network traffic for packets screening.

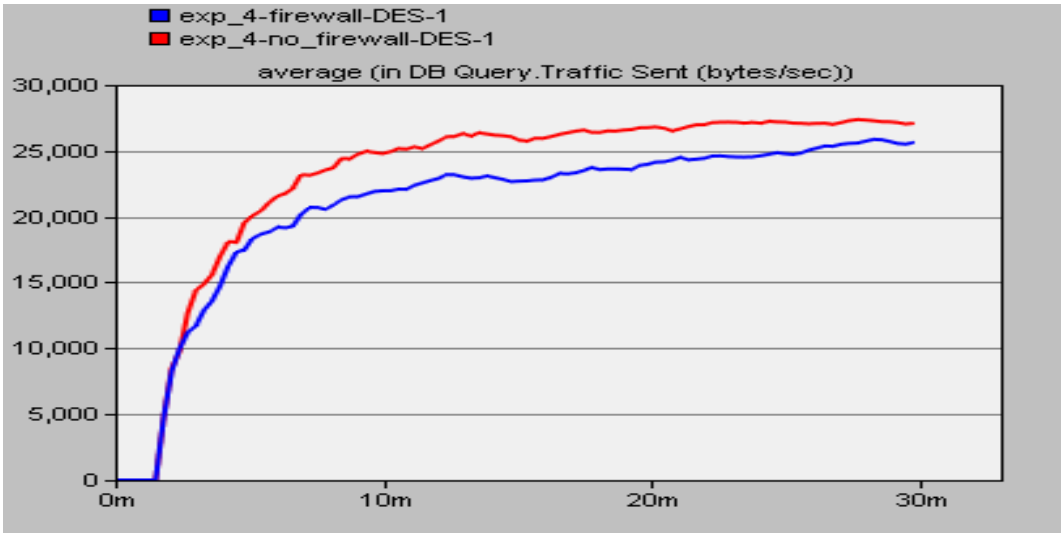

Figure 5-Average DB. Query traffic sent in bytes/second

Conclusions

The achievement security in service provider networks is vital and advantageous to the service provider as a feature to compete in the industry and satisfy the poyential clients. However, the downside for securing the network is sacrificing some performance. This paper has investigated by simulating both scenarios to show how the performance might be affected.

The future work of this project is to implement both scenarios in ASIC or FPGA [19-24].

References

1. Hiran R, Carlsson N. and Shahmehri N. **2016**. Does scale, size, and locality matter? evaluation of collaborative bgp security mechanisms. In2016 IFIP Networking Conference [IFIP Networking] and Workshops 2016 May 17 [pp. 261-269]. IEEE.
2. Akbar S. and Wibawa AD. **2016**. The impact analysis and mitigation of DDoS attack on local government electronic procurement service [LPSE]. In2016 International Seminar on Intelligent Technology and Its Applications [ISITIA] 2016 Jul 28 [pp. 405-410]. IEEE.
3. Hesselman C. and Moura GC. **2017**. de Oliveira Schmidt R, Toet C. Increasing DNS security and stability through a control plane for top-level domain operators. *IEEE Communications Magazine*. 2017 Jan; **55**(1):197-203.
4. Kurt B, Zeydan E, Yabas U, Karatepe IA, Kurt GK. And Cemgil AT. **2016**. A network monitoring system for high speed network traffic. In2016 13th Annual IEEE International Conference on Sensing, Communication, and Networking [SECON] 2016 Jun 27 [pp. 1-3]. IEEE.
5. Salek Z. and Madani FM. **2016**. Multi-level Intrusion detection system in cloud environment based on trust level. In 2016 6th International Conference on Computer and Knowledge Engineering [ICCKE] 2016 Oct 20 [pp. 94-99]. IEEE.
6. Santoso BI., Idrus MR. and Gunawan IP. **2016**. Designing Network Intrusion and Detection System using signature-based method for protecting OpenStack private cloud. In2016 6th International Annual Engineering Seminar [InAES] 2016 Aug 1 [pp. 61-66]. IEEE.
7. Ren J, Yao Z, Xiong J, Zhang Y, Ye A. **2016**. A secure data deduplication scheme based on differential privacy. In2016 IEEE 22nd International Conference on Parallel and Distributed Systems [ICPADS] 2016 Dec 13 [pp. 1241-1246]. IEEE.
8. Mavroeidakos T, Michalas A, Vergados DD. **2016**. Security architecture based on defense in depth for Cloud Computing environment. In2016 IEEE Conference on Computer Communications Workshops [INFOCOM WKSHPS] 2016 Apr 10 [pp. 334-339]. IEEE.
9. Liang H, Ge Y, Wang W, Chen L. **2015**. Collaborative intrusion detection as a service in cloud computing environment. In2015 IEEE International Conference on Progress in Informatics and Computing [PIC] 2015 Dec 18 [pp. 476-480]. IEEE.

10. Yongxin Y. **2011**. The comparative study on network firewalls performance. In2011 IEEE 3rd International Conference on Communication Software and Networks 2011 May 27 [pp. 427-430]. IEEE.

11. Sheth C, Thakker R. **2011**. Performance evaluation and comparative analysis of network firewalls. In2011 International Conference on Devices and Communications [ICDeCom] 2011 Feb 24 [pp. 1-5]. IEEE.

12. Tantipongsakul K, Khunkitti A. **2009**. Dynamic Policy-Based Routing Using Firewall Rules. In2009 Third UKSim European Symposium on Computer Modeling and Simulation 2009 Nov 25 [pp. 540-545]. IEEE.

13. Abdulkadhim M. **2015**. Routing Protocols Convergence Activity and Protocols Related Traffic Simulation With It's Impact on the Network. *International Journal of Science, Engineering and Computer Technology*. 2015 Mar 1; **5**(3): 40.

14. Abdulkadhim M. **2015**. Service Performance Evaluation for WiMAX Networks Based on Node Trajectory.

15. Abdulkadhim M, Korabu KS. **2011**. Future System: Using Manet in Smartphones the Idea the Motivation and the Simulation. In International Conference on Computational Intelligence and Information Technology 2011 Nov 7 [pp. 716-721]. Springer, Berlin, Heidelberg.

16. Abdulkadhim M. **2018**. Design and Implementation of a Wireless Sensor Networks Application Framework. *International Journal of Computer Applications*.; **975**: 8887.

17. Abdulkadhim M. **2018**. An End To End IoE- Based Technology Solution for Diabetic Healthcare. *International Journal of Engineering & Technology* 2018; **7**: 196-200.

18. Abdulkadhim M, Hasan S, Mohammed Ali S. **2018.** Reliability Improved Routing as a Qos Measure for Mobile Ad-Hoc Networks. *International Journal of Engineering & Technology* 2018; **7**: 201-204,

19. Hasan S, Boussakta S, Yakovlev A. **2010**. Improved parameterized efficient FPGA implementations of parallel 1-D filtering algorithms using Xilinx System Generator. In The 10th IEEE International Symposium on Signal Processing and Information Technology 2010 Dec 15 [pp. 382-387]. IEEE.

20. Hasan S, Boussakta S, Yakovlev A. **2011**. Parameterized FPGA-based architecture for parallel 1-D filtering algorithms. InInternational Workshop on Systems, Signal Processing and their Applications, WOSSPA 2011 May 9 [pp. 171-174]. IEEE.

21. Hasan S. **2016**. Performance-vetted 3-D MAC processors for parallel volumetric convolution algorithm: A 256× 256× 20 MRI filtering case study. In 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications [AIC-MITCSA] 2016 May 9 [pp. 1-6]. IEEE.

22. Humaidi AJ., Hassan S. and Fadhel MA. **2018**. Rapidly-fabricated nightly-detected lane system: An FPGA implemented architecture. *The Asian International Journal of Life Sciences*. 2018; 16[1]: 343-355.

23. Humaidi AJ., Hassan S. and Fadhel MA. **2018**. FPGA-based lane-detection architecture for autonomous vehicles: A real-time design and development. *The Asian International Journal of Life Sciences*.2018; **16**(1): 223-237.

24. Humaidi AJ., Hasan S. and Al-Jodah AA. **2018**. Design of Second Order Sliding Mode for Glucose Regulation Systems with Disturbance. *International Journal of Engineering & Technology*. 2018; **7**(2.28): 243-7.