Experimental Analysis of improvement in Firewall Traffic by deployment of Bastion Host

N. Chiranjeeva Rao[1*], Shankha De[2], Chaitali Choudhary[3]
[1]*Assistant Professor, BIT, Durg*
[2]*Associate Professor, BIT, Durg*
[3]*Assistant Professor, BIT, Durg*
[1]*raonchiranjeev@gmail.com*, [2] *shankhada2009@gmail.com*,
[3]*chaitali.choudhary@bitdurg.ac.in*

Abstract

Firewalls play a vital role in the present day society. They not only protect the networks from various threats but also play a key role in improving traffic efficiency. One of the major deficiencies in using them is delay in network speed due to the various filtrations applied by them. Improvement in traffic speed is a major necessity. Modification in the existing firewall is very complicated and needs a lot of expertise and years of experimentation. This paper shows an experimental analysis of improving firewall traffic by doing some simple modifications to the existing system.

Keywords: *Firewalls, Bastion hosts, network analysis, network simulator*

1. Introduction

Network threats are on their all-time height and upgradation of firewalls is an ongoing process. There can never be a saturation point to this as novel threats always persist. New research and approaches need to be done for facing the threats constantly. Updated methods need to be applied from time to time. Moreover, hackers and attackers are also equipped with high technical capabilities and information and are capable of carrying typical attacks which are difficult to defend. Therefore, innovation in this field is a necessity to keep ahead.

Though there are many proven methods of security, but none can assure complete security. By going through the work done in this field, it has been observed that one of the best methods of securing a network firewall. In this paper a few modifications were carried out and results were analyzed in Network Simulator software so that by doing simple modifications better efficiency can be achieved.

2. Objective of the study

The main objective of the study is to find various options and approaches for bypassing some of the filtration safely and reducing the traffic by doing customization and to analyze the experimental results by implementing the improvements

By studying the various firewall, it has been found that security and speed of networks play a vital role. It has been found that though a lot of work has been done on the firewall. It needs implementation of various concepts on a working firewall with its own principals. There is a lot of difficulty in making modifications in the current firewall and any improvement needs a lot of painful effort as well as many resources.

This present work shows improvements in the performance and security by attaching a Bastion host before firewall to reduce threats reaching it. Since this is an external attachment, therefore no modification need to be done in the current firewall principles which result in a cost effective solution. Due to such an arrangement greater security can also be provided to the firewall which protects it from direct attacks such as Denial of Service and many more.

3. Methodology

3.1 Normal Arrangement of a Firewall

As per the problem identified it is quite clear that there is a constant requirement of upgradation in the present system and various techniques need to be applied. The normal and the modified arrangements of the firewall are explained here.

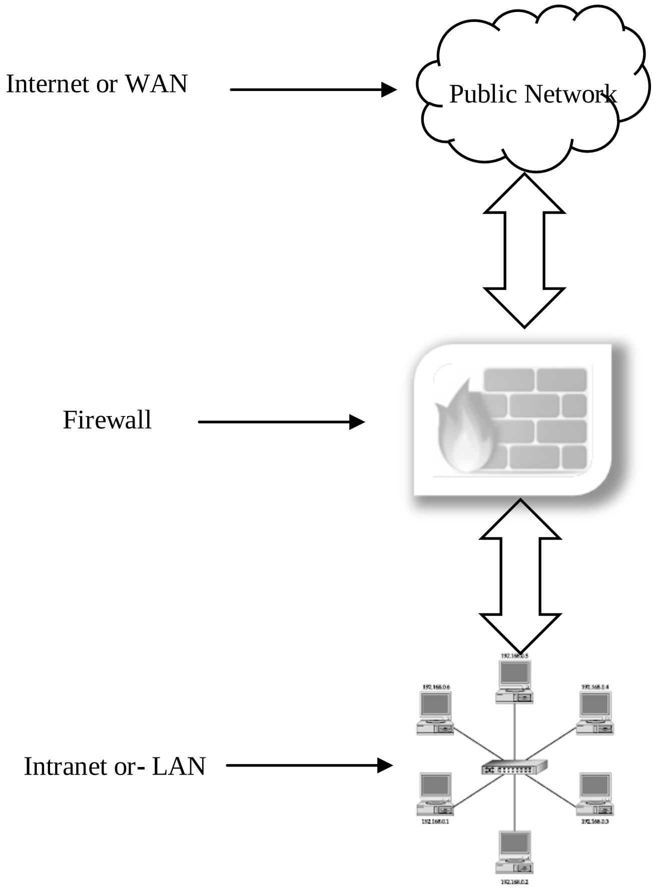


Figure 1 Normal Arrangement of a Firewall

A normal firewall is placed in between a Local Area Network or Intranet and public area network which is a Wide Area Network. All the packets flowing through the firewall either from intranet to internet or vice versa are checked for any threats and if such threats are suspected then the packet are dropped for security reasons. For allowing any packets in the firewall, the rules specified in it should accept the same and any exceptions should be specified in the rule list.

3.2 Modified Arrangement of a Firewall

The modification which is done at the firewall is the Deployment of Bastion host or deployment of Random Early Detection which will increase the security and efficiency of the firewall. This can be accomplished using a Bastion Host as an external DNS server or as a proxy server.

In the above arrangement the traffic instead of coming directly to the firewall can be made to pass through Bastion Host first which can directly suspend or redirect 20% of the traffic by using some of the standard methods. Redirecting include reverting the traffic directly to internal DNS server instead of passing through firewall thus improving its efficiency. The arrangement can be seen in figure 2 below.

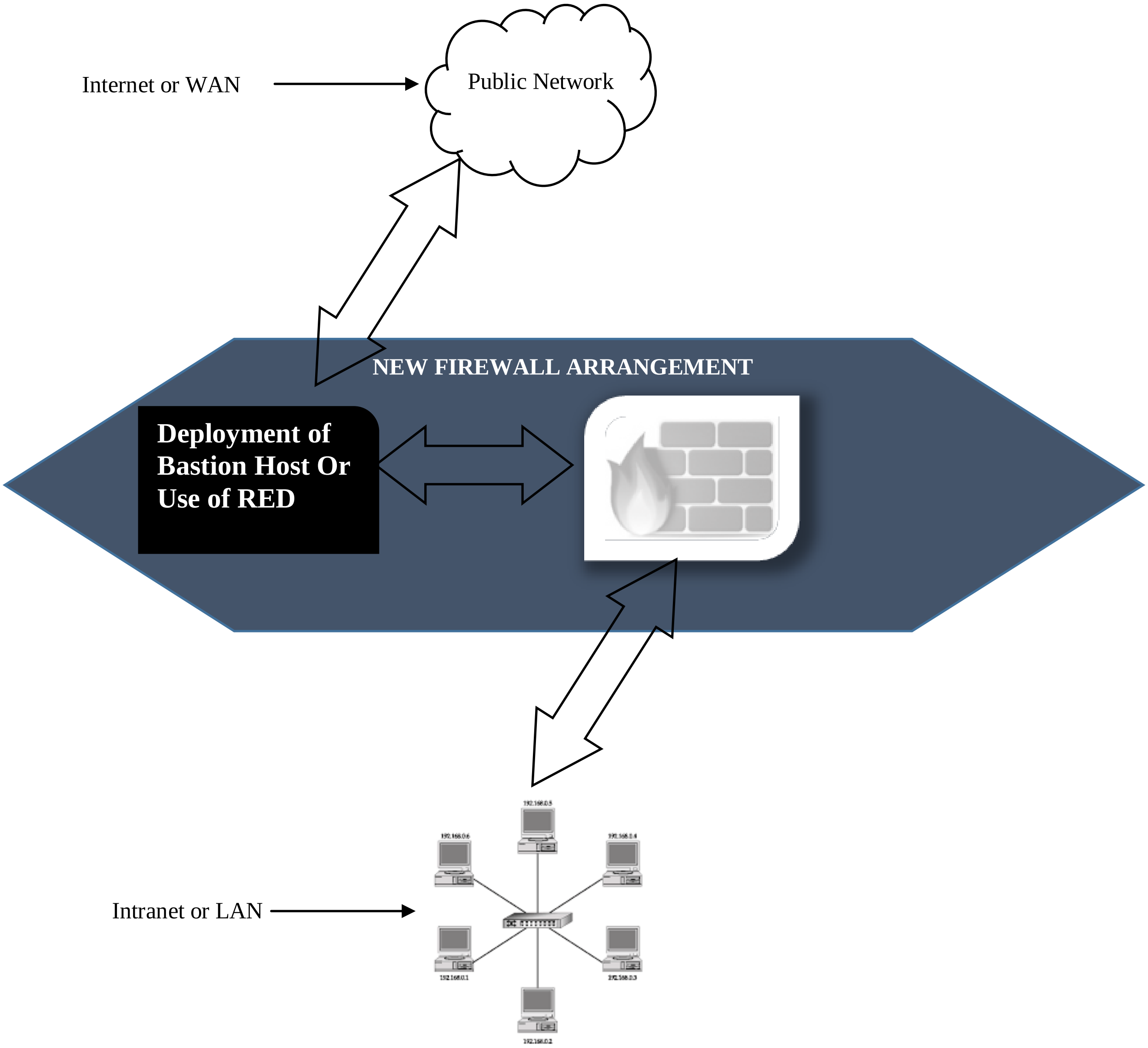


Figure 2 Modified Arrangement of a Firewall

3.3 Analysis of data for the above models using NS2

The above methods show that by the deployment of a bastion host or an RED 20-25% of the packets are bypassed (using a Bastion Host) or rejected at an earlier stage (using RED) or bypassed by the firewall thus improving the firewall efficiency. This has been simulated in NS2.

Arrangements in the below scenario are (Figure 3):

- Node 0 and Node 1 are the traffic generators for internet.
- Node 2 is acting as a firewall.
- Node 3 and node 4 are acting as internal networks.

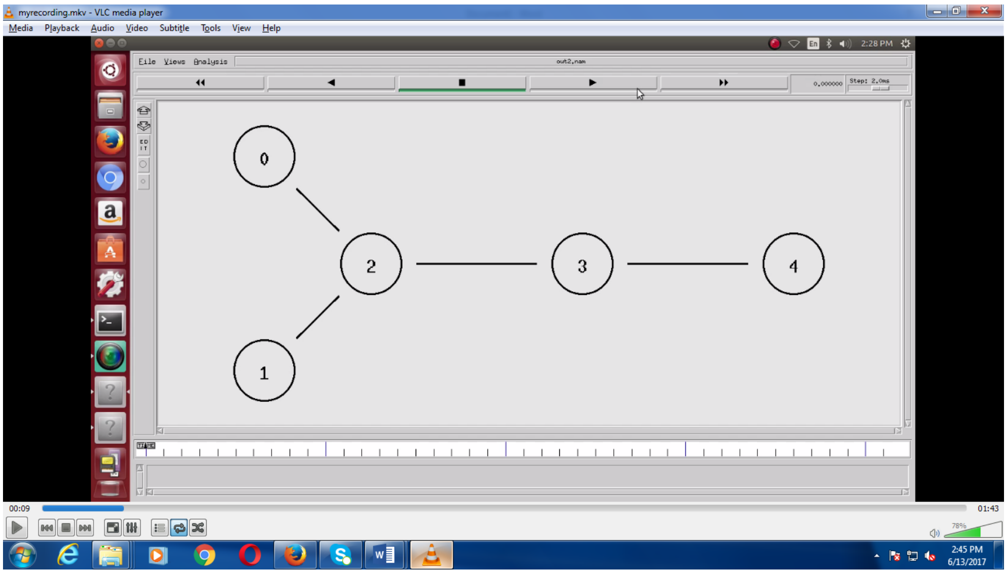

myrecording.mkv - VLC media player
Media Playback Audio Video Subtitle Tools View Help
File Views Analysis
out2.nam
0.000000
Step: 2.0ms
0
1
2
3
4
00:09
01:43
2:28 PM
2:45 PM
6/13/2017

Figure 3 Simulation in NS2 showing the node position in network

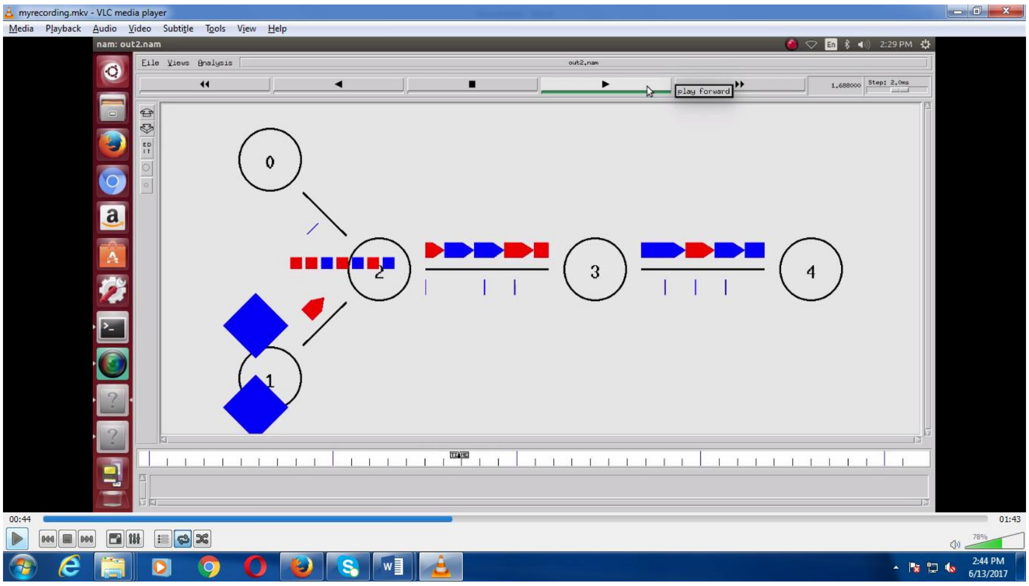


Figure 4 Output generating a severe drop at node 2 in TCP packets.

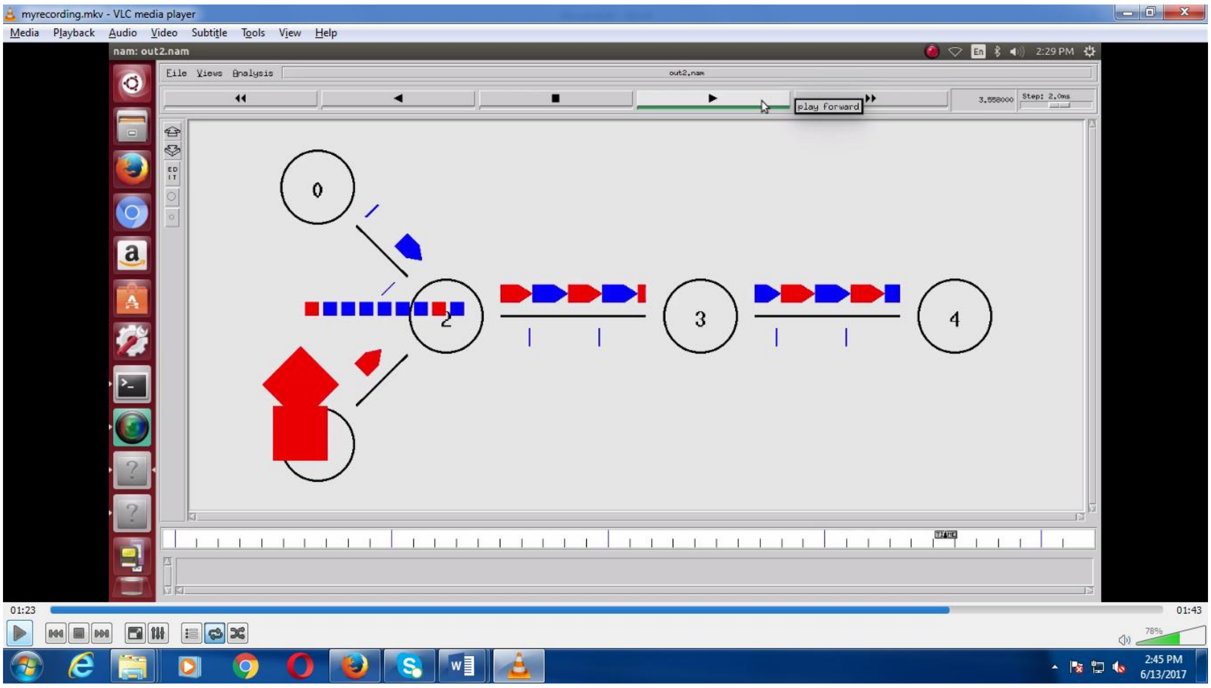


Figure 5 Output generated a severe drop at node 2 in UDP packets.

3.4 Simulation Parameters

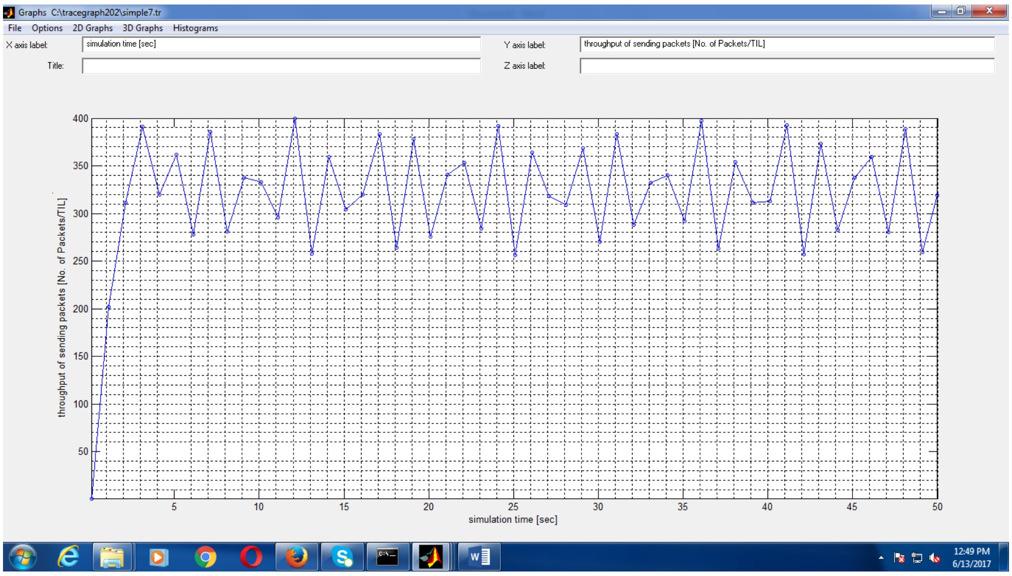
Simulation parameters used were, total number of nodes five, access-link bandwidth – $ns duplex-link $n0 $n2 2Mb 10ms DropTail, $ns duplex-link $n1 $n2 2Mb 10ms DropTail, $ns duplex-link $n2 $n3 1.7Mb 20ms DropTail, $ns duplex-link $n3 $n4 1.7Mb 20ms DropTail, Packet type : CBR, FTP, Schedule Events for CBR & FTP

The timing of the process was as below:

- $ns at 0.1 "$cbr start"
- $ns at 0.5 "$cbr start"
- $ns at 1.0 "$ftp start"
- $ns at 49.0 "$ftp stop"
- $ns at 49.0 "$cbr stop"
- $ns at 49.5 "$cbr stop"
- Minimum Packet Size : 40
- Maximum Packet Size : 1040

4. Result & Discussion

Comparison of charts obtained in NS2 as Figure 6 and 7 before and after deployment of RED shows that deployment of RED has smoothened the traffic flow significantly.



Graphs C:\tracegraph202\simple7.tr

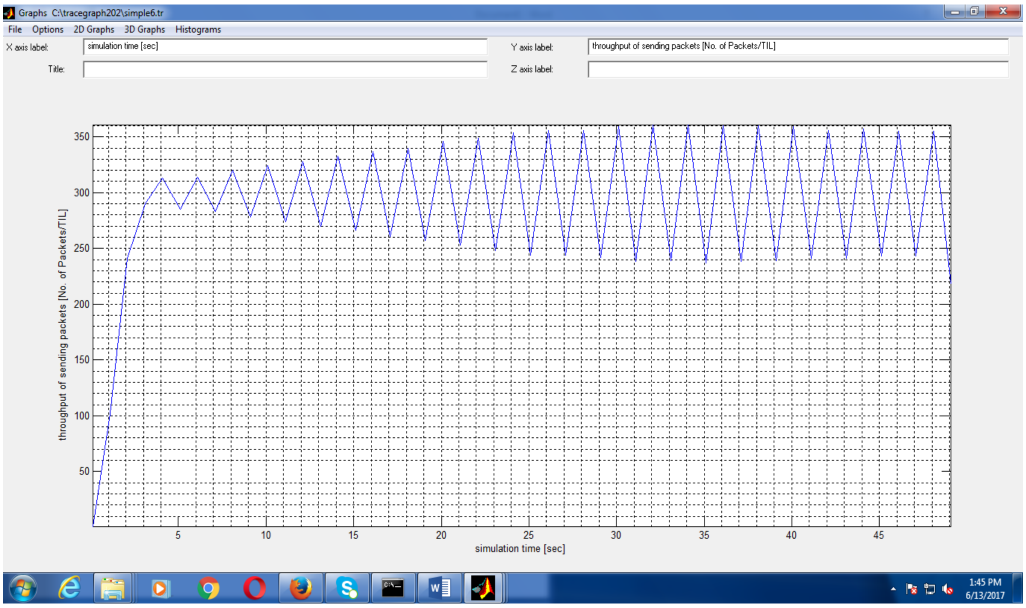
X axis label: simulation time [sec]

Y axis label: throughput of sending packets [No. of Packets/TIL]

Title:

Z axis label:

Figure 6 Throughput of sending packets before deployment of Bastion Host/RED



Graphs C:\tracegraph202\simple6.tr

X axis label: simulation time [sec]

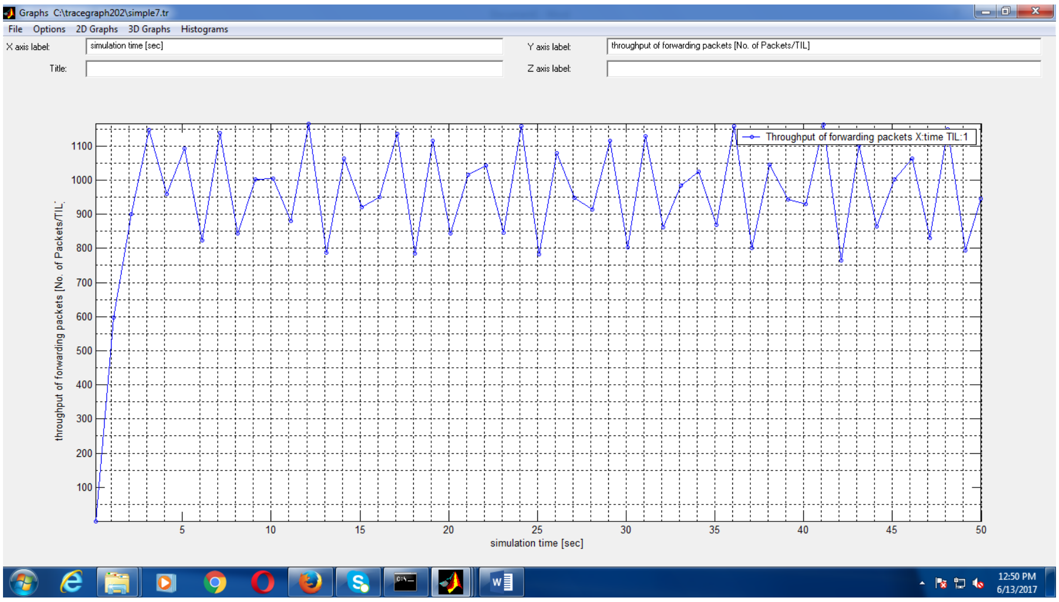
Y axis label: throughput of sending packets [No. of Packets/TIL]

Title:

Z axis label:

Figure 7 Throughput of sending packets after deployment of Bastion Host or RED.

Comparison of charts obtained in NS2 as Figure 8 and 9 before and after deployment of RED shows that deployment of RED shows a significant drop in the irregularity of forwarding packets.


Graphs C:\tracegraph202\simple7.tr

X axis label: simulation time [sec]

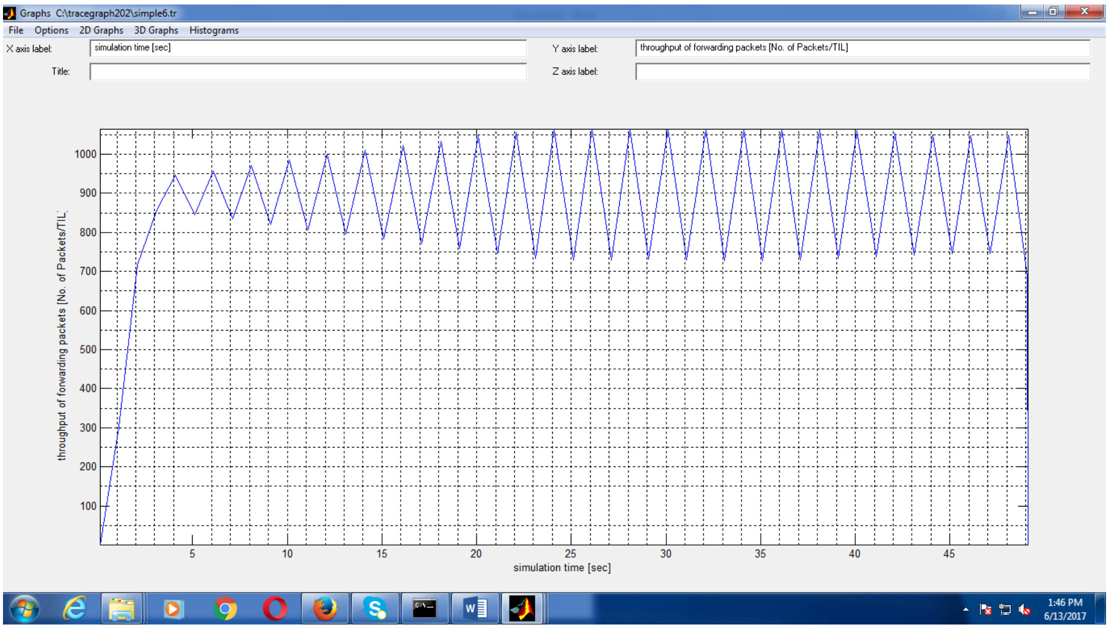
Y axis label: throughput of forwarding packets [No. of Packets/TIL]

Title:

Z axis label:

○

Figure 8 Throughput of forwarding packets when firewall is used directly


Graphs C:\tracegraph202\simple6.tr

X axis label: simulation time [sec]

Y axis label: throughput of forwarding packets [No. of Packets/TIL]

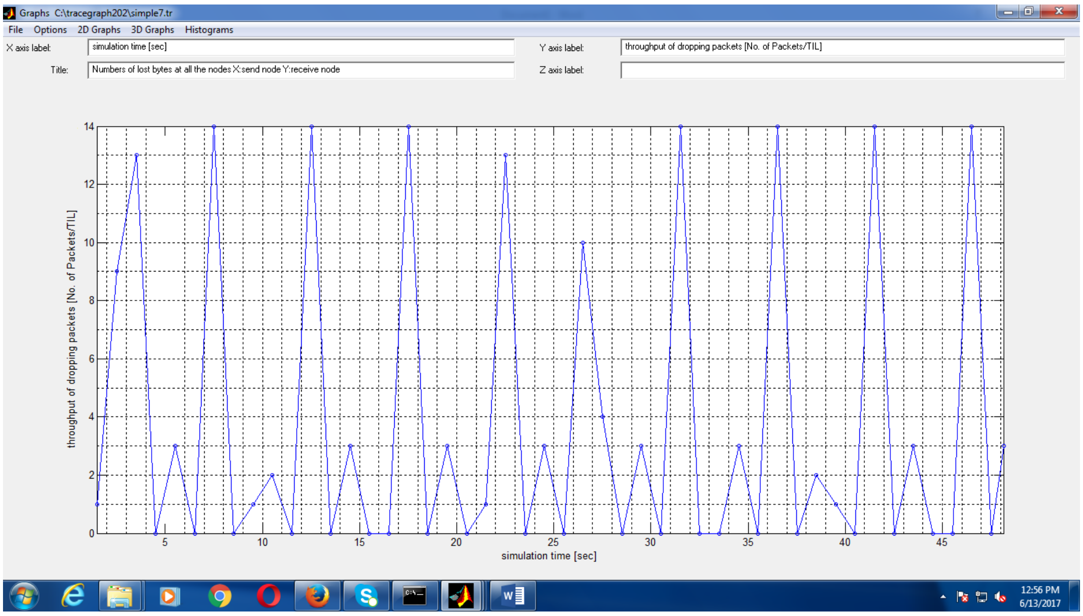
Title:

Z axis label:

○

○ *Figure 9 Throughput of forwarding packets after deployment of Bastion Host or RED*

Comparison of charts obtained in NS2 as Figure 10 and 11 before and after deployment of RED shows that deployment of RED shows a significant drop in the irregularity of forwarding packets.



Graphs C:\tracegraph202\simple7.tr

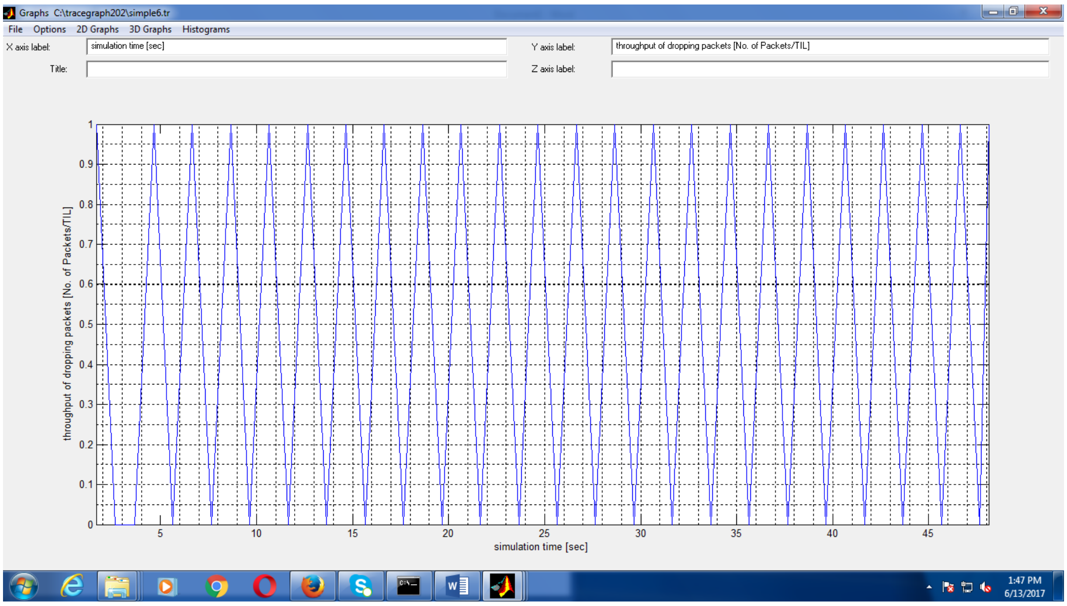
X axis label: simulation time [sec]

Y axis label: throughput of dropping packets [No. of Packets/TIL]

Title: Numbers of lost bytes at all the nodes X:send node Y:receive node

Z axis label:

Figure 10 Throughput of dropping packets when firewall is used directly



Graphs C:\tracegraph202\simple6.tr

X axis label: simulation time [sec]

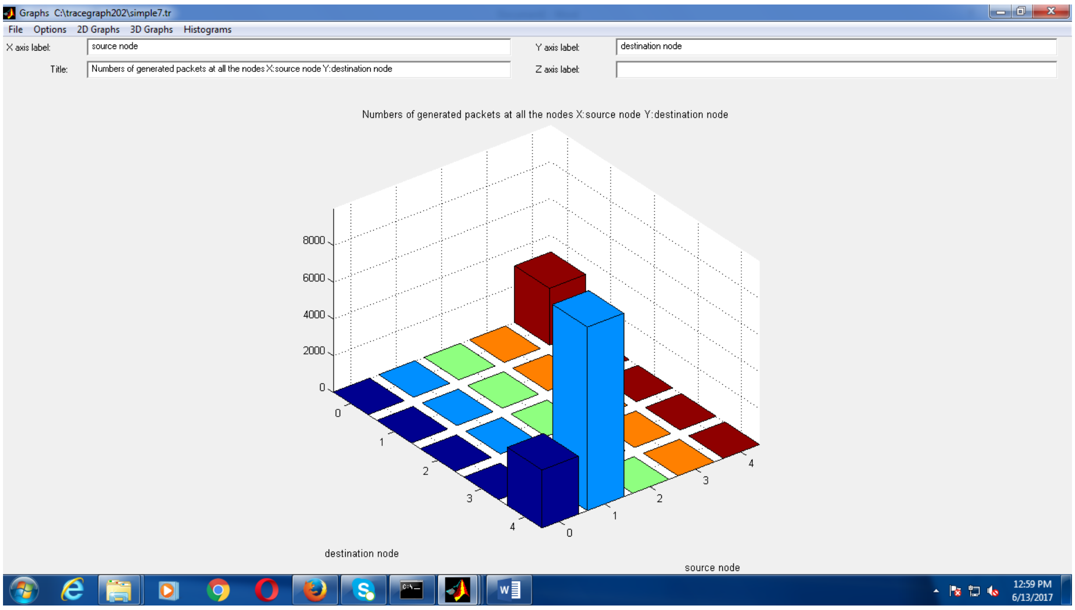
Y axis label: throughput of dropping packets [No. of Packets/TIL]

Title:

Z axis label:

Figure 11 Throughput of dropping packets after deployment of Bastion Host or RED

Comparison of charts obtained in NS2 as Figure 12 and 13 before and after deployment of RED shows that deployment of RED has reduced the packet drop significantly and also the packet drop is smoother as compared to the previous arrangement.



Graphs C:\tracegraph202\simple7.tr

X axis label: source node

Y axis label: destination node

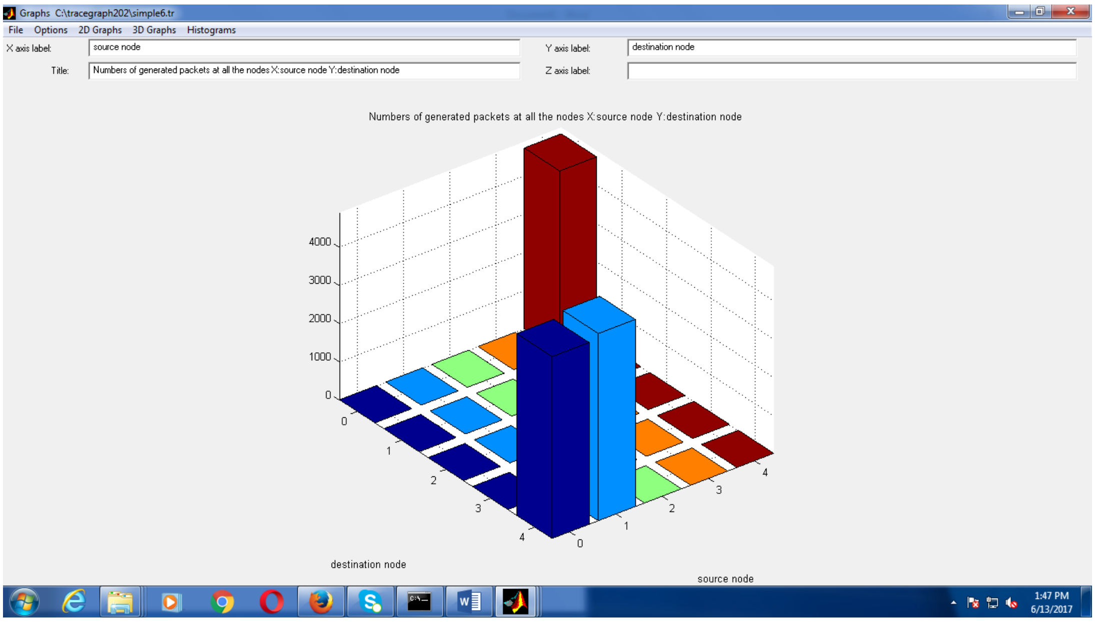
Title: Numbers of generated packets at all the nodes X:source node Y:destination node

Z axis label:

○

○ *Figure 12 No. of generated packets at all nodes when firewall is used directly*

○



Graphs C:\tracegraph202\simple6.tr

X axis label: source node

Y axis label: destination node

Title: Numbers of generated packets at all the nodes X:source node Y:destination node

Z axis label:

Figure 13 No. of generated packets at all nodes when firewall is used with Bastion Host or RED

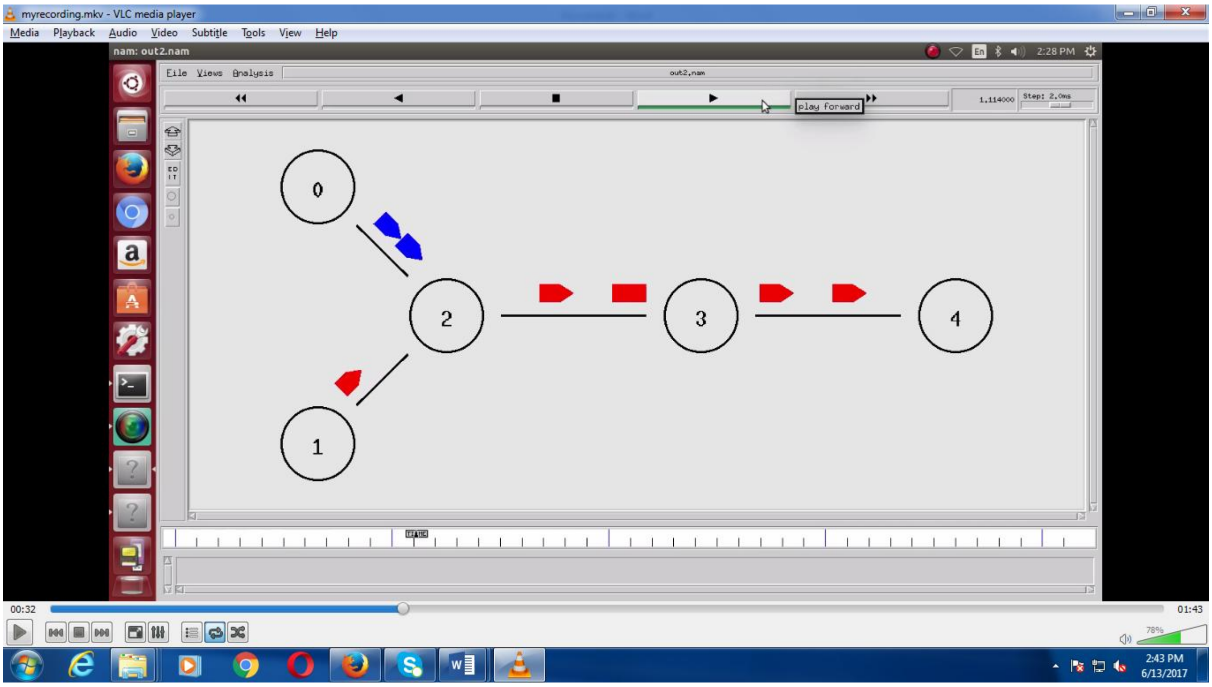


Figure 14 Smooth flow of data after implementation of Bastion Host or RED

6. Conclusion

Thus it can be concluded that the above work proposes a firewall with an enhancement so as to improve its efficiency and security. The first method was using a Bastion server for security management. In the next part, use of RED for improving firewall efficiency was discussed. This model rejects the traffic which is unwanted at an initial (early) stage and thus improves the performance of the firewall. This model is also very useful for traffics of high rejection rates.

References

[1] N Chiranjeeva Rao, Shankha De, “Deployment of Bastion Host, RED before Firewalls to improve Security & Firewall Efficiency”, Research Journal of Computer and Information Technology Sciences, Vol. 5, Issue 5, **(July 2017)**, pp 9-11, ISSN: 2320-6527.

[2] N Chiranjeeva Rao, Shankha De and Chaitali Choudhary, “Study of User Behaviour for Firewall Configuration”, International Journal of Scientific Research in Computer Science, Engineering and Information Technology, Vol. 2, Issue 3, **(May 2017)** pp 387-389, ISSN : 2456-3307

[3] Dr. Ajit Singh, Madhu Pahal and Neeraj Goyat, “A Review Paper on firewall”, International Journal for Research in Applied Science & Engineering Technology, Vol. 1, Issue 2, **(September 2013)**

[4] Mr. Sachin Taluja, Mr. Pradeep Kumar Verma and Prof. Rajeshwar Dua, “Network Security Using IP firewalls”, International Journal of Advanced Research in Computer Science & Software Engineering, Vol. II, Issue 8, **(August 2012)**, pp 348-354

[5] Ashwin Ganesh, Anirudhan Sudarsan, Ajay Krishna Vasu and Dinesh Ramalingam, “Improving Firewall Efficiency by using a Cache Table”, International Journal of Advances in Engineering & Technology, **(Nov., 2014)**, pp 1594-1607

[6] Ehab S. Al-Shaer and Hazem H. Hamed, “Discovery of Policy Anomalies in Distributed Firewalls”, IEEE Journal, **(2004),** pp 2605-2616

[7] Umniya Mustafa, Mohammad M. Masud, Zouheir Trabelsi, Timothy Wood and Zainab Al Harthi, “Firewall Performance Optimization Using Data Mining Techniques, IEEE, 2013, pp 934-940

[8] Zouheir Trabelsi and Safaa Zeidan, “Multilevel Early Packet Filtering Technique based on Traffic Statistics and Splay Trees for Firewall Performance Improvement”, IEEE Communication and Information Systems Security Symposium, **(2012)**, pp 1074-1078

[9] Safaa Zeidan, Zouheir Trabelsi, “ A Survey on Firewall’s Early Packet Rejection Techniques”, International Conference on Innovations in Information Technology, **(2011)**, pp 203-208

[10] Neha M. Qureshi, “A Trace Study and Performance Analysis of Wireless Network using NS2”, International Journal Advanced Research in Computer Science and Software Engineering, Vol. V, Issue 3, **(March 2015)**, pp 11-16

[11] S.Jeneeth Subashini, D. Guna Shekar, C.Harinath Reddy and M. Manikanta, “Implementation of Wired and Wireless Networks, Analysis Simulation and Result Comparison Using Ns2”, International Journal of Electrical and Electronics Research, Vol. 2, Issue 3, pp 209-225

[12] Sachi Pandey, Vibhore Tyagi, “Performance Analysis of Wired & Wireless Network using NS2 simulator”, International Journal of Computer Applications, Vol. 72, Issue. 21, **(June 2013)**, pp 38-44

[13] Rahul Malhotra, Vikas Gupta, Dr. R. K. Bansal, “Simulation & Performance Analysis of Wired and Wireless Computer Networks”, International Journal of Computer Applications, Vol. 14, No. 7, **(February 2011)**, pp 11-17

Books

[14] Andrew Lockhart, “Network Security Hacks”, O'Reilly Media, **(2004)**

[15] William Stallings, “Network Security Essentials”, Pearson Education, **(2011)**