Electronic Journal of University of Aden for Basic and Applied Sciences

EJUA-BA Vol. 6 No. 1 (2025)

https://doi.org/10.47372/ejua-ba.2025.1.420

ISSN: 2708-0684

RESEARCH ARTICLE

NETWORK PERFORMANCE ENHANCEMET. A CASE STUDY: NBY NETWORK

Lutfi Mohammed Omer Khanbary[1,*], Mohammed Anwar Qutb[1]

[1] *Dept. of Computer Science and Engineering, Faculty of Engineering, University of Aden, Yemen*

***Corresponding author: Lutfi Mohammed Omer Khanbary; E-mail: llkhanbari@gmail.com**

Received: 14 December 2024 / Accepted: 09 January 2025 / Published online: 31 March 2025

Abstract

In this paper, an extensive study is presented on the case of a network banking system. Through research, in order to improve the network performance, enhanced proposed models of the current system are designed. The performance of the proposed techniques has been evaluated by conducting the simulation experiments. The obtained performance metrics results of the comparative study between the current system and the proposed models, exhibits the reliability and accuracy of these models.

Keywords: Latency, Jitter, Packet loss, Quality of service, Performance metrics, Firewall.

Introduction

Among the new challenges nowadays, the enhancement of banking system's networks becomes most important for such entity to provide stable, reliable and best response time between headquarter and its branches, this improvement issue includes redundancy for the data and paths [1-2].
Considering the grow up of banking systems and the increase of challenges to provide the best optimum network system, it is needed to deliver best topology that can provide the requested results and functions from different networks topologies and to choose the best network topology among them.

National Bank of Yemen (NBY) is one of the prime banking entities with a main branch (the Headquarter) and 28 sub branches separated around the entire Republic of Yemen with un-centralized data [3].

The remainder of the paper is organized as follows. Section 2 shows the related works. The current NBY banking network system is discussed in section 3. Section 4 elaborates the proposed network models. Section 5 presents experimental results to evaluate the model's performance, followed by the observations from the conducted experimental study in section 6. Section 7 covers the concluding remarks.

1. Related Works

Improving the performance of such network systems has been considered by many researchers, below are summary of some of these researches.

A case study is implemented by Valerianus et al. to design secured and less expensive IPSec-based VPN service to connect remote users with University of Namibia (UNAM) data center. According to the results of the simulation of the broadband IPSec VPN connection that is not controlled by any third party is less expensive, more secure, and has a high level of latency and jitter [4].

Novandi Rizki et al., analyzed the implementation of high availability on FortiGate Firewall in specific scenarios, such as networks with sensitive data or networks with high-security requirements. A real-world case study is applied to evaluate the effectiveness of high availability implementation on FortiGate firewall in enhancing network reliability and security [5].

firewalls were analyzed by A. Shaji George and A. S. Hovan George in [6]. The evolution of (NGFWs and (WAFW) was studied by showing their characteristics and their strong role in safeguarding the enterprise's environment for the foreseeable future.

2. The NBY Banking Network System

Recently NBY headquarter has eight HP servers provide the banking system with the required services whereas two main servers for banking database and its applications, two servers are utilized as cluster system, the rest servers supporting applications for the banking system.

Those servers are connected together through fiber optics network that provides high speed dataflow rate and all are connected to a special switch called System Attached Network (SAN), additionally the headquarter has a firewall Fort iGATE model (200E, 1000D, WAF) and a Cisco router 1800 [3].

The sub-branches have a directing router Cisco 1800 which connected to the headquarter using leased-line provided by ISP, as shown in Figure 1.

2.1 The Current Network Scenario

In the currently used network topology, the main site (Aden) connected with two branches (Mualla and, Mukala), the dataflow between the main site and the branches is passing out from the firewall and the branches routers to the router and the firewall of the main site to reach the servers, as shown in figure 2.

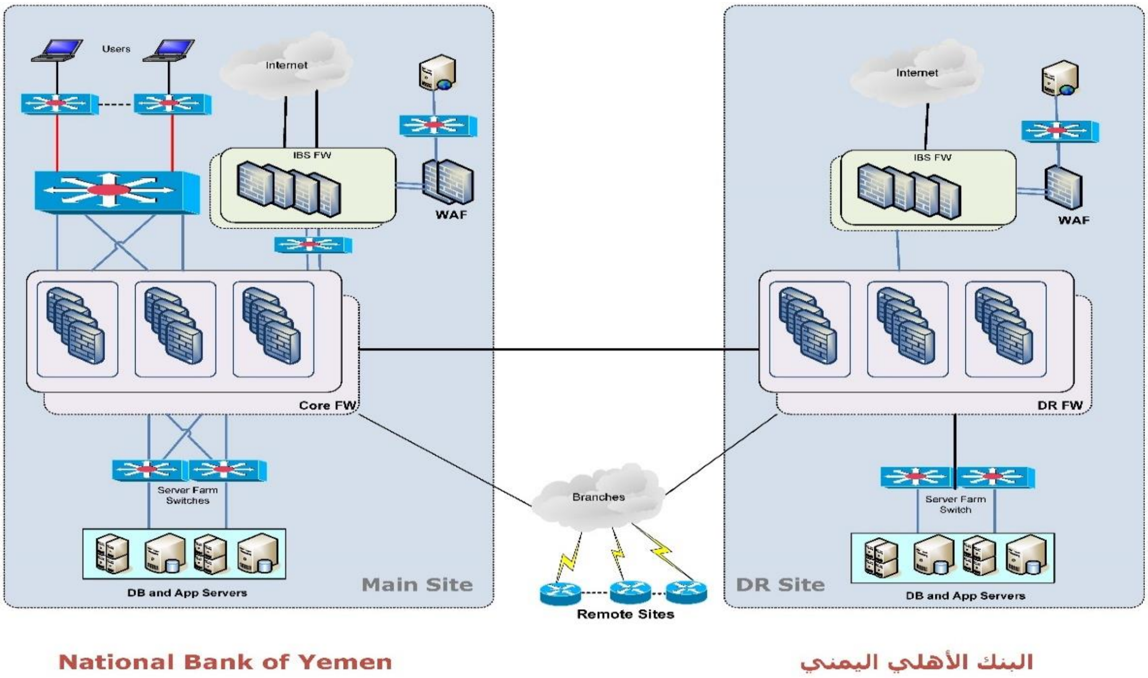


Fig. 1: the current network system

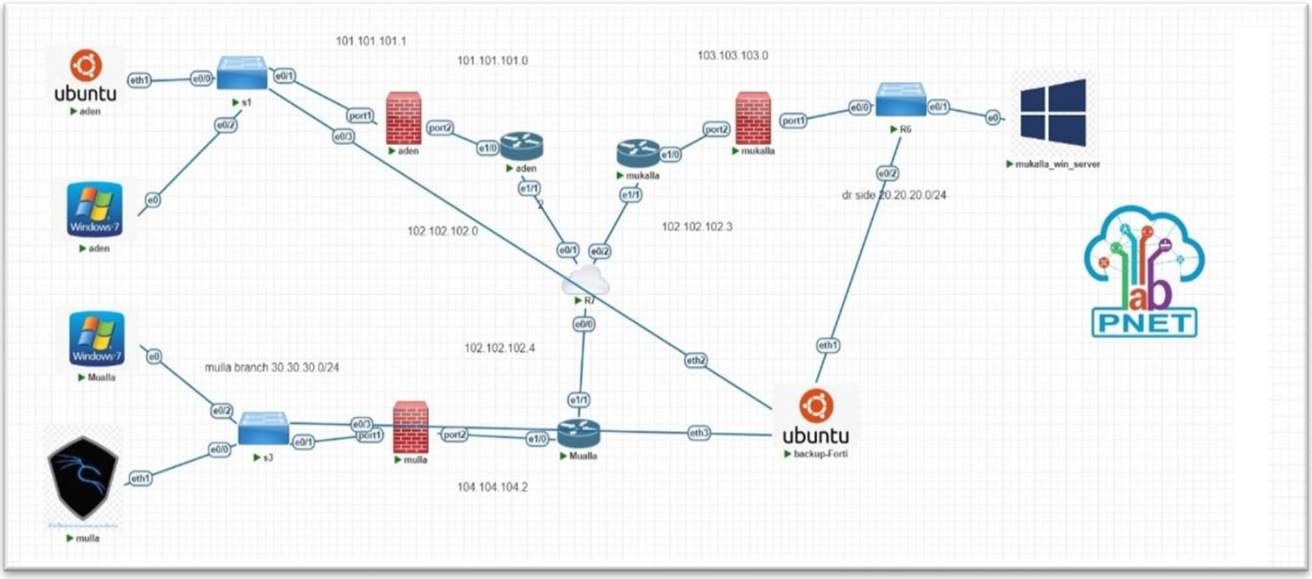


Fig. 2: current network scenario

In this network, shown in figure 2, jitter and Latency are high, so for better network performance they should be reduced. The dataflow time to reach from end to end is very high also, so improvement can be done by reducing the hop-count. An enhanced proposed modified models are discussed in the next section.

3. The Proposed Network Models

In this section, two proposed network scenario models are presented.

3.1 The First Proposed Scenario Model

In this scenario, the headquarter site and the branches are connected via FortiGate firewall instead of cisco routers and the static root in FortiGate's firewall is applied to reduce the latency time, and enhancing dataflow time, as shown in figure 3.

In this proposed network, shown in figure 3, the latency and jitter values are reduced, the dataflow time is minimized also.

3.2 The Second Proposed Scenario Model

The reliability of the network and the security of the data paths are improved in this scenario, the topology applied is explained below.

A path redundancy scheme is applied for both the main site and the branches connected to it, through FortiGate firewall, using static route with load balancing technique to enhance the reliability.

A main firewall redundancy scheme is applied by using the heart-bit technique that provides high availability, so if the main firewall failed, the next to knee firewall takes place to act as the main firewall with (Master-Slave topology).

The security is improved by applying a VPN (Site-to-site) technology between the main firewall and the branches firewalls, which provides high data security, with the VPN technique that checks the line stability, when the used path gets down it awake the reserved path [7], as illustrated in figure 4.

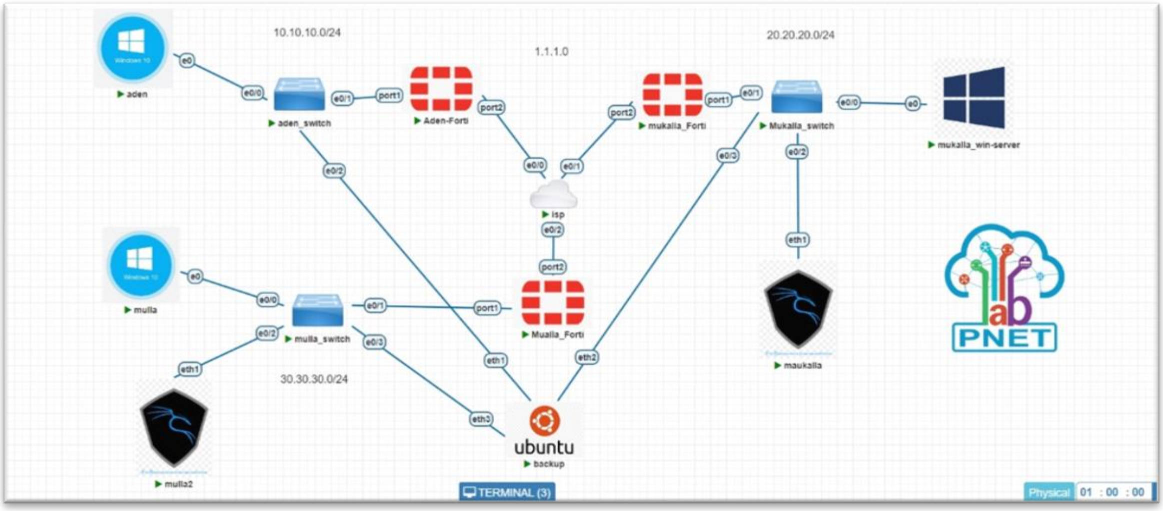


Fig. 3: First proposed scenario model

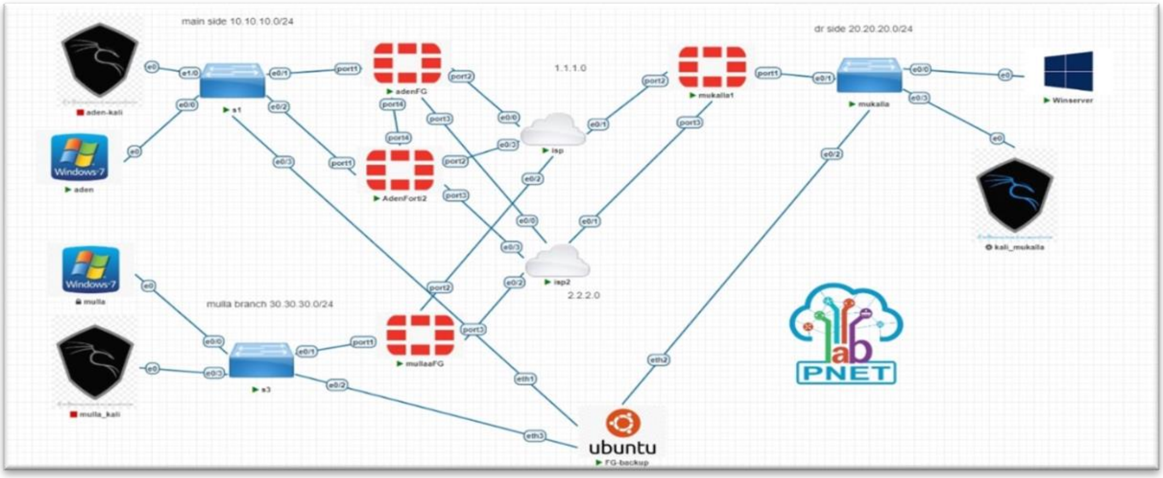


Fig. 4: Second proposed scenario model

In this second proposed network design, the latency and jitter reduced further more due to redundancy paths applied in this scenario. Applying the VPN technique between the main firewall and branches firewalls gives more security and reliability to the network. Hence, by the load balancing technique and the reduction of dataflow time, this scenario improves the quality of service. The simulation experiments for all mentioned models are presented in the next section.

4. SIMULATION EXPERIMENTS

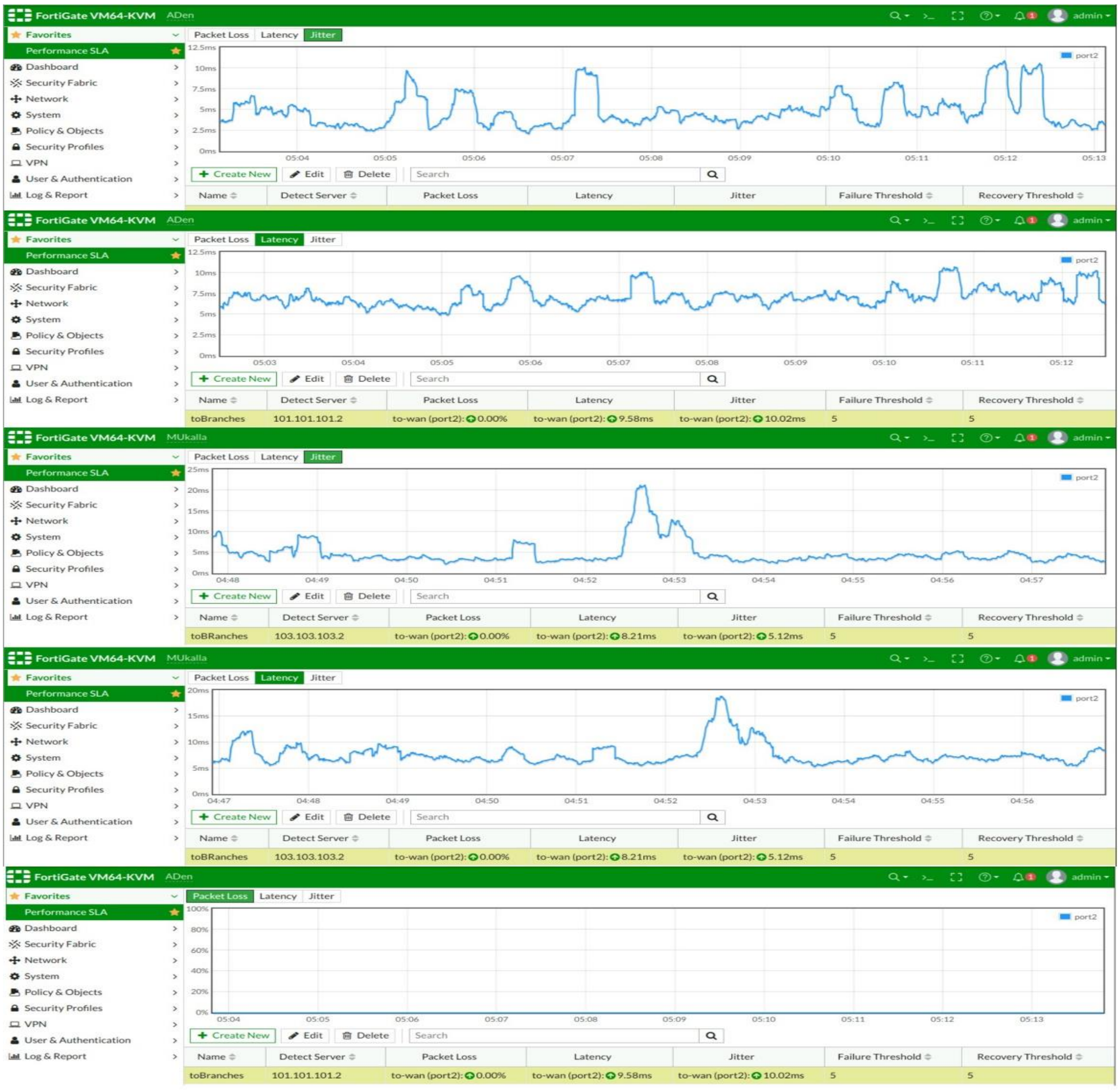
In this section, the previous designed systems are simulated. For this purpose, the PNET and virtual machine VBox, with FortiGate firewalls are utilized with the servers implemented in the network [8]. The PNET and spawn are used to evaluate the performance of the designed scenarios, analyzing the network packets and comparing the simulated models [9]. The simulation experiments are conducted for three regions network, the main headquarter (Aden), Mualla, and Mukalla.

PNETLab (Packet Network Emulator Tool Lab) is a platform that allows to download and share labs with the community. It includes PNETLab Box, with two modes, Offline and Online virtual machines, and PNETLap store, which installed on the local machine and the Lab is running on it. The NETLab store is a web platform with hundreds of free Labs in the fields of networking, and database systems. [10].

The performance of the network, is evaluated using the three-performance metrics, latency, jitter, and packet loss, the bandwidth is selected as 1Gbps for all experiments [11-16].

4.1 Current network scenario experiment

In this scenario as already shown in section 3.1, figure 2, an experiment is conducted by sending and receiving a 610 MB packet file to and from the main headquarter and the branches associated with it. The obtained results are shown on the next performance graphs in figures 5-10.



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold

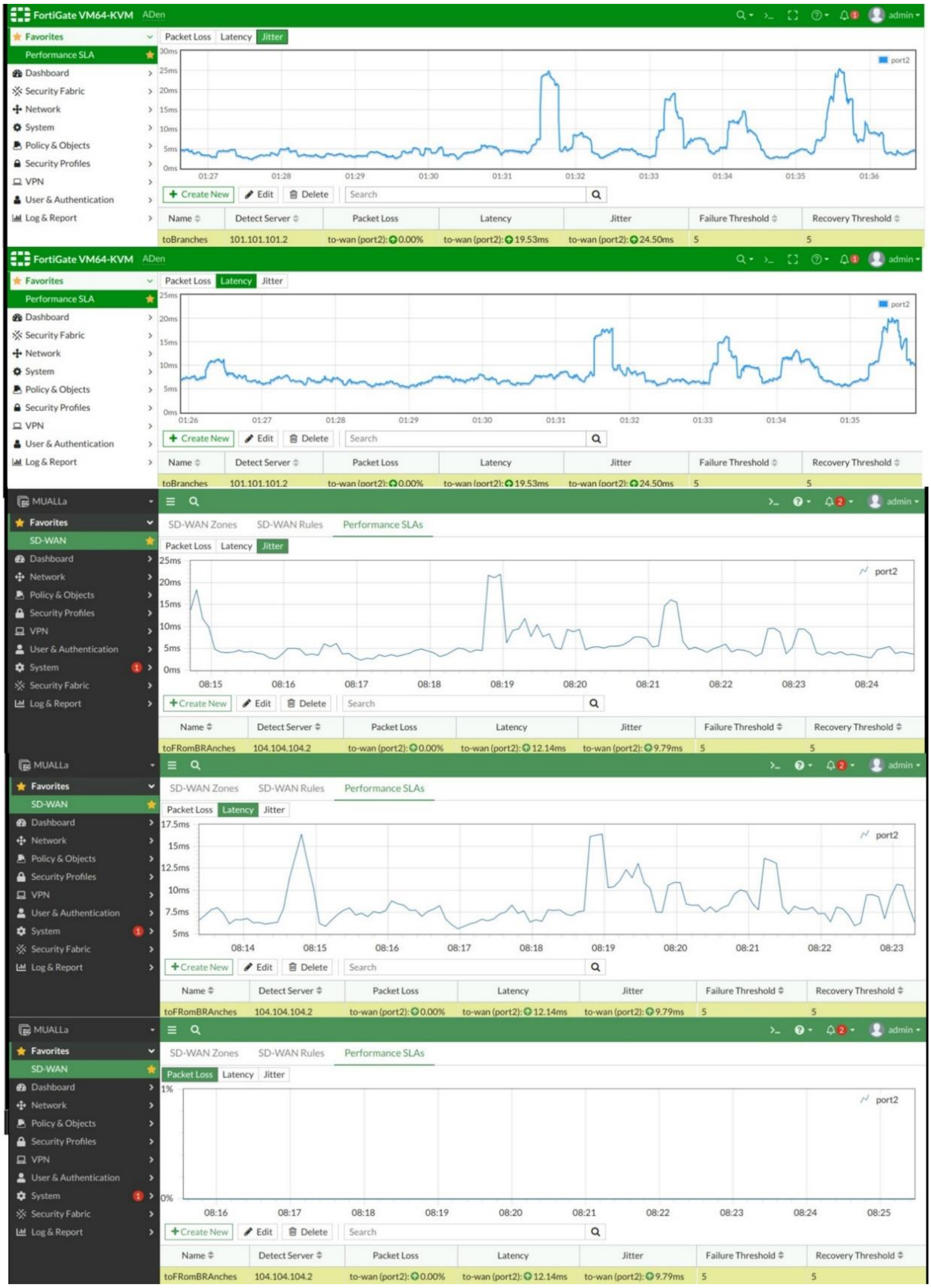
Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 9.58ms	to-wan (port2): 10.02ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 8.21ms	to-wan (port2): 5.12ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 8.21ms	to-wan (port2): 5.12ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 9.58ms	to-wan (port2): 10.02ms	5	5

Fig. 5: Performance graph (Aden – Mukalla)



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 19.53ms	to-wan (port2): 24.50ms	5	5

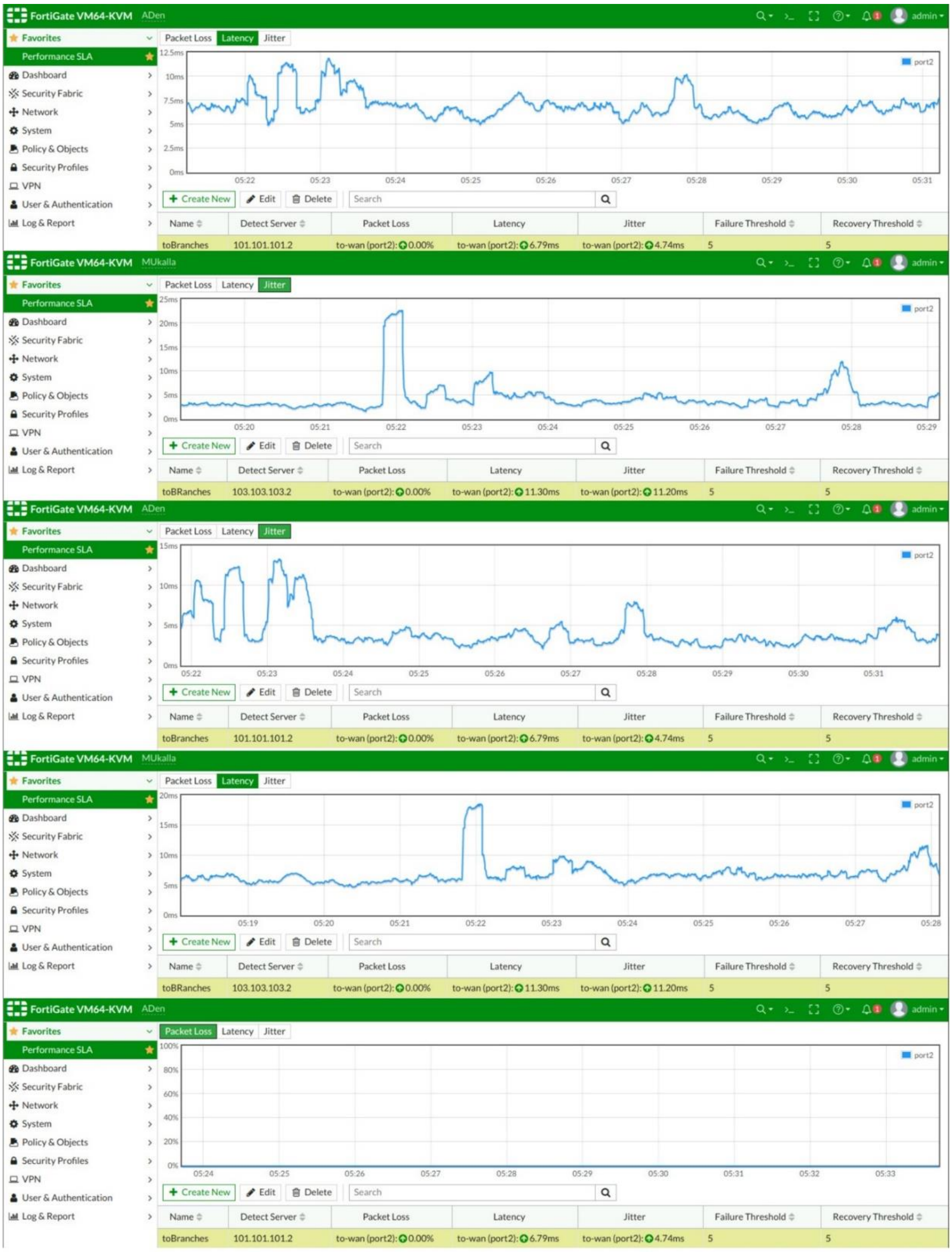
Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 19.53ms	to-wan (port2): 24.50ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 12.14ms	to-wan (port2): 9.79ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 12.14ms	to-wan (port2): 9.79ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 12.14ms	to-wan (port2): 9.79ms	5	5

Fig. 6: Performance graph (Aden – Mualla)



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 6.79ms	to-wan (port2): 4.74ms	5	5

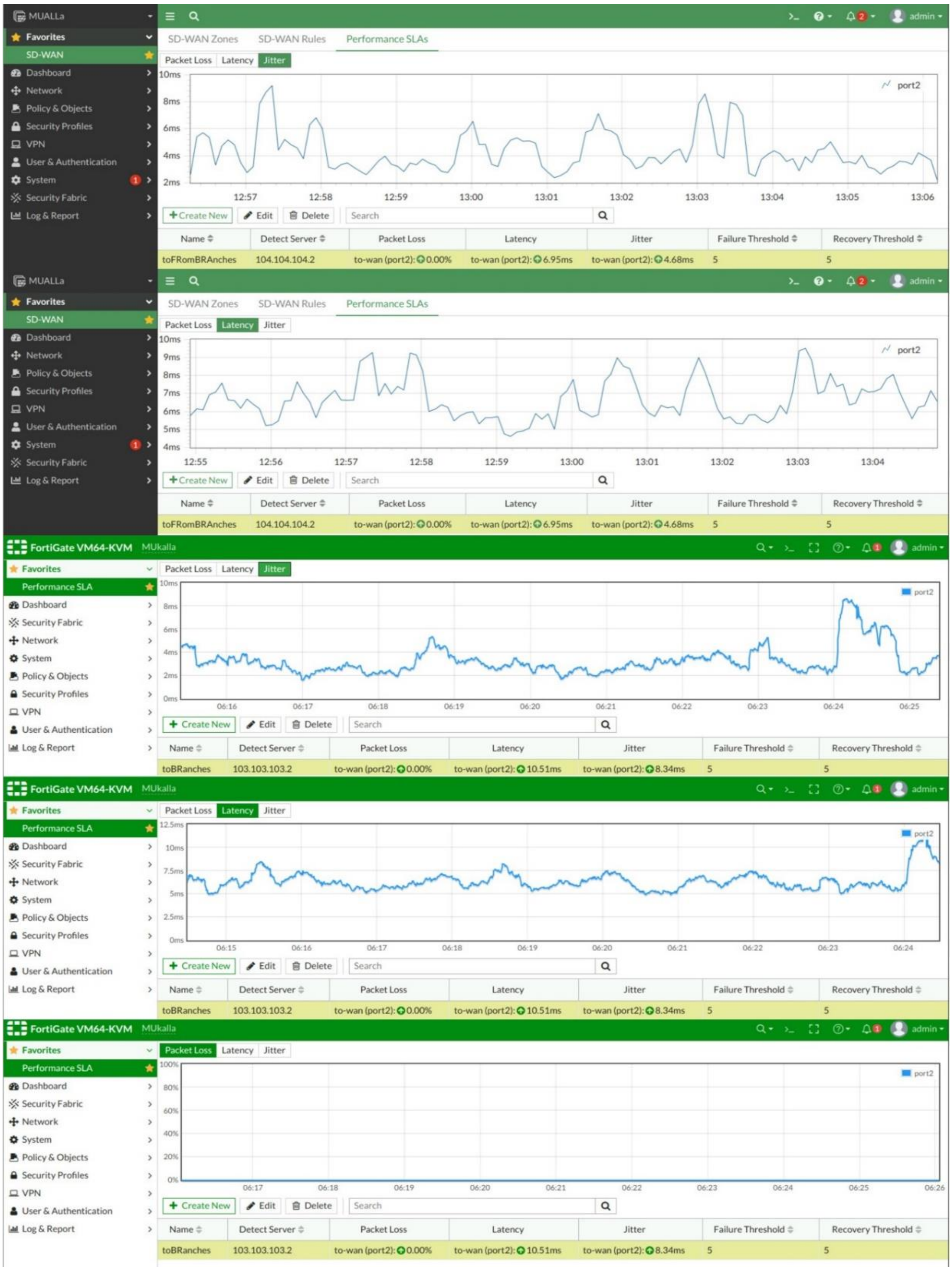
Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 11.30ms	to-wan (port2): 11.20ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 6.79ms	to-wan (port2): 4.74ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 11.30ms	to-wan (port2): 11.20ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 6.79ms	to-wan (port2): 4.74ms	5	5

Fig. 7: Performance graph (Mukalla –Aden)



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 6.95ms	to-wan (port2): 4.68ms	5	5

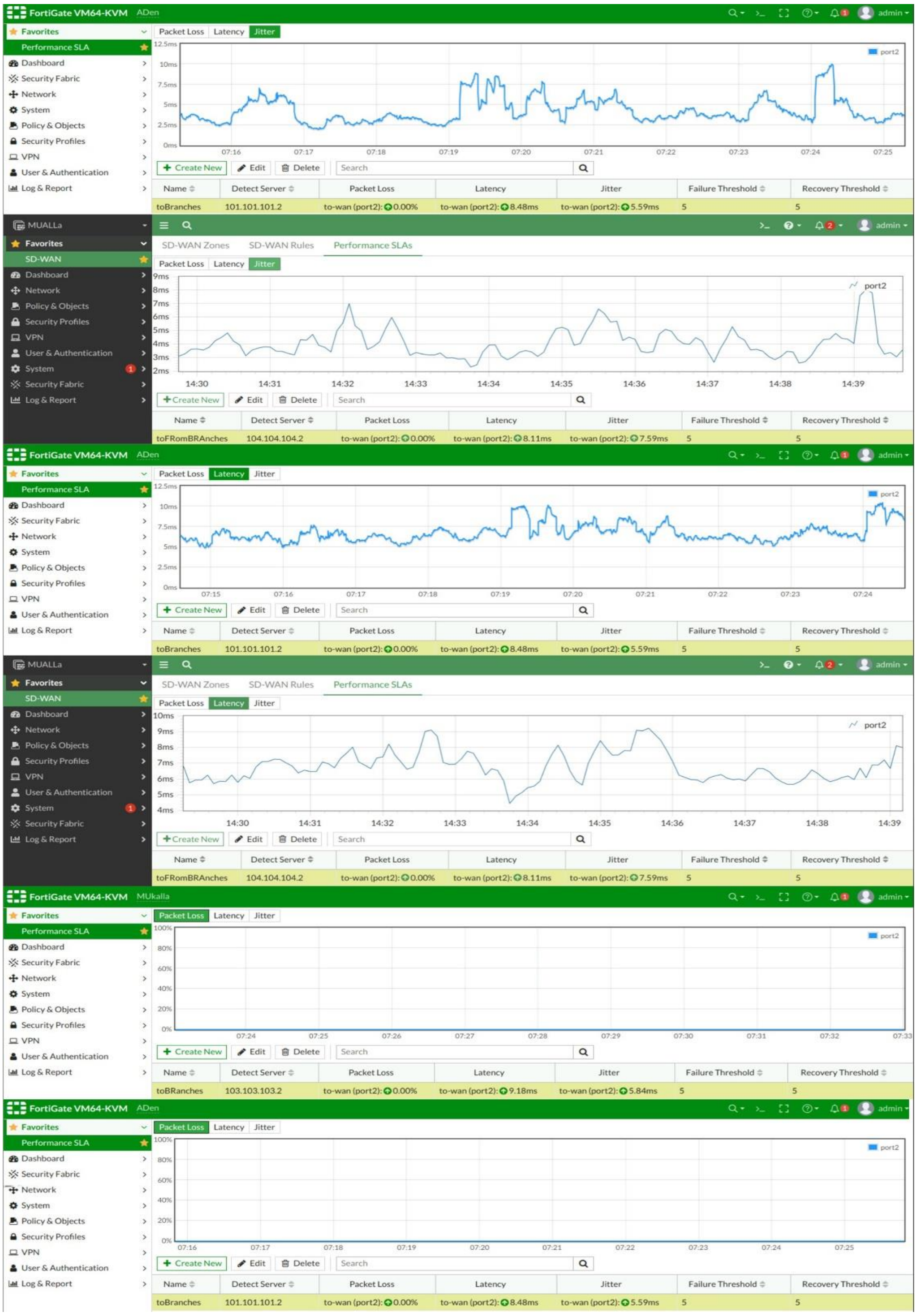
Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 6.95ms	to-wan (port2): 4.68ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 10.51ms	to-wan (port2): 8.34ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 10.51ms	to-wan (port2): 8.34ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 10.51ms	to-wan (port2): 8.34ms	5	5

Fig. 8: Performance graph (Mukalla –Mualla)



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 8.48ms	to-wan (port2): 5.59ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 8.11ms	to-wan (port2): 7.59ms	5	5

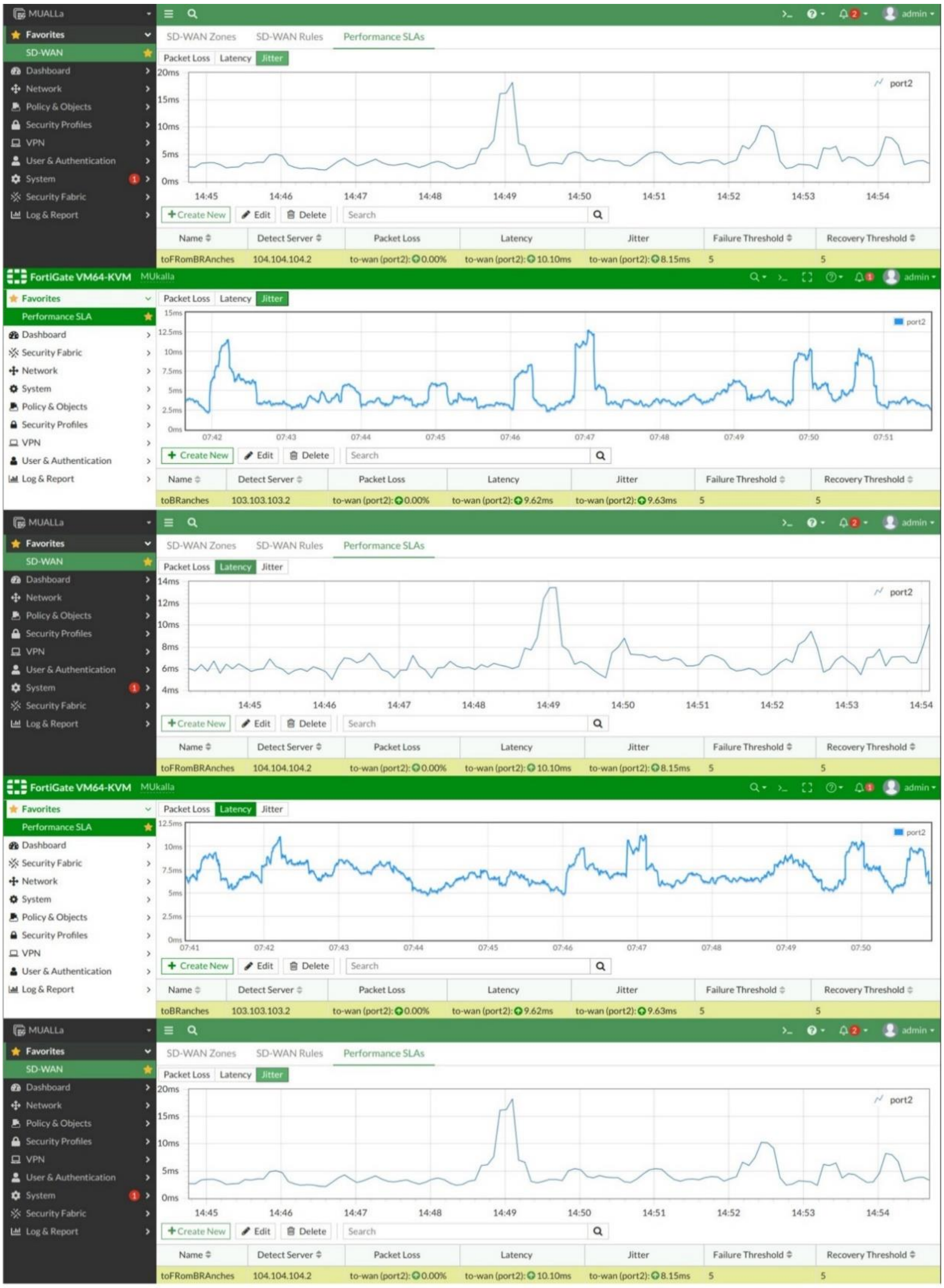
Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 8.48ms	to-wan (port2): 5.59ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 8.11ms	to-wan (port2): 7.59ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 9.18ms	to-wan (port2): 5.84ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBranches	101.101.101.2	to-wan (port2): 0.00%	to-wan (port2): 8.48ms	to-wan (port2): 5.59ms	5	5

Fig. 9: Performance graph (Mualla –Aden)



Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 10.10ms	to-wan (port2): 8.15ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 9.62ms	to-wan (port2): 9.63ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 10.10ms	to-wan (port2): 8.15ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toBRanches	103.103.103.2	to-wan (port2): 0.00%	to-wan (port2): 9.62ms	to-wan (port2): 9.63ms	5	5

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Threshold	Recovery Threshold
toFRomBRAnches	104.104.104.2	to-wan (port2): 0.00%	to-wan (port2): 10.10ms	to-wan (port2): 8.15ms	5	5

Fig. 10: Performance graph (Mualla –Mukalla)

The transactions in each branch's firewall are measured and all the obtained results are summarized below in table 1.

Table 1: Results obtained from the Current network scenario

Main Site - aden															
ISP	file name	File Size	Transmitted Time	Remark	Link port	Bandwidth	Main-FG			Mukalla-FG			Mualla-FG		
							Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms
ISP1	nvedia_driver	610MB	44m4sec	Link1:Main to Mukalla	1.1.1.1 to 1.1.1.2	1Gbps	9.58ms	0%	10.02ms	8.21ms	0%	5.12ms	-	-	-
	nvedia_driver	610MB	37m28sec	Link1:Main to Mualla	1.1.1.1 to 1.1.1.3	1Gbps	19.53ms	0%	24.50ms	-	-	-	12.14ms	0%	9.79ms

Mukalla Site															
ISP	file name	File Size	Transmitted Time	Remark	Link port	Bandwidth	Mukalla-FG			aden-FG			Mualla-FG		
							Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms
ISP1	nvedia_driver	610MB	42m:20sec	Link1:Mukalla to main	1.1.1.2 to 1.1.1.1	1Gbps	11.30ms	0%	11.20ms	6.79ms	0%	4.74ms	-	-	-
	nvedia_driver	610MB	50m22sec	Link1:Mukalla to Mualla	1.1.1.2 to 1.1.1.3	1Gbps	10.51ms	0%	8.34ms	-	-	-	6.95ms	0%	4.68ms

Mualla Site															
ISP	file name	File Size	Transmitted Time	Remark	Link port	Bandwidth	Mualla-FG			aden-FG			Mukalla-FG		
							Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms
ISP1	nvedia_driver	610MB	51m37sec	Link1:Mualla to Main	1.1.1.3. to 1.1.1.1	1Gbps	8.11ms	0%	7.59ms	8.48ms	0%	5.59ms	-	-	-
	nvedia_driver	610MB	45m50sec	Link1:Mualla to Mukalla	1.1.1.3 to 1.1.1.2	1Gbps	10.10ms	0%	8.15ms	-	-	-	9.62ms	0%	9.63ms

Table 2: Results obtained from the first proposed scenario

Main Site - aden															
ISP	file name	File Size	Transmitted Time	Remark	Link port	Bandwidth	Main-FG			Mukalla-FG			Mualla-FG		
							Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms
ISP1	nvedia_driver	610MB	12m41sec	Link1:Main to Mukalla	1.1.1.1 to 1.1.1.2	1Gbps	4.15ms	0%	5.74m	6.02ms	0%	8.71ms	-	-	-
	nvedia_driver	610MB	9m44sec	Link1:Main to Mualla	1.1.1.1 to 1.1.1.3	1Gbps	4.23ms	0%	5.73ms	-	-	-	3.00ms	0%	3.76ms

Mukalla Site															
ISP	file name	File Size	Transmitted Time	Remark	Link port	Bandwidth	Mukalla-FG			aden-FG			Mualla-FG		
							Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms
ISP1	nvedia_driver	610MB	8m:41sec	Link1:Mukalla to main	1.1.1.2 to 1.1.1.1	1Gbps	3.85ms	0%	4.53ms	2.52ms	0%	2.97ms	-	-	-
	nvedia_driver	610MB	12m2sec	Link1:Mukalla to Mualla	1.1.1.2 to 1.1.1.3	1Gbps	3.35ms	0%	4.66ms	-	-	-	4.11ms	0%	6.21ms

Mualla Site															
ISP	file name	File Size	Transmitted Time	Remark	Link port	Bandwidth	Mualla-FG			aden-FG			Mukalla-FG		
							Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms
ISP1	nvedia_driver	610MB	8m:51sec	Link1:Mualla to Main	1.1.1.3. to 1.1.1.1	1Gbps	2.49ms	0%	1.98ms	2.27ms	0%	2.38ms	-	-	-
	nvedia_driver	610MB	7m:20sec	Link1:Mualla to Mukalla	1.1.1.3 to 1.1.1.2	1Gbps	3.24ms	0%	4.68ms	-	-	-	1.36ms	0%	0.72ms

From table 1, It is obvious that, the transmission time is too long as well as the latency and jitter.

4.2 First Proposed Scenario Experiment

In this scenario, as shown previously in section 4.1, figure 3, an experiment is conducted by sending and receiving a 610 MB packet file to and from the main branch and the branches associated with it with no routers, using FortiGate firewalls. Similarly, the transactions in each branch's firewall are measured and all the obtained results are summarized below in table 2. From table 2, It is obvious that the transmission time is reduced comparing to the currently used network system, similarly latency and jitter are improved and no packet loss.

Although both sending and receiving times are improved, still some issues should be addressed, first, there is no data encryption, second, if the main link is failed, it may cause the network to stop permanently. Lastly, if a fault arisen in the main firewall, the branches will stop working.

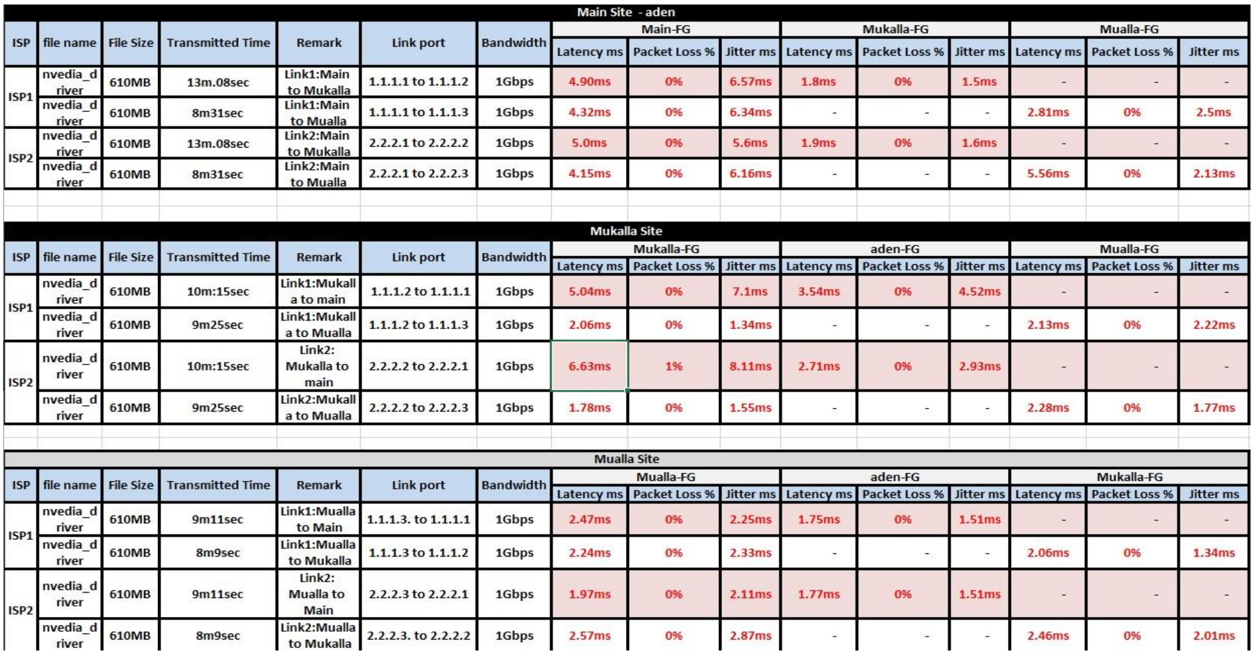
Solutions to the stated above issues are presented next in the second proposed scenario.

4.3 Second Proposed Scenario Experiment

In this scenario, as shown in section 4.2, figure 4, the limitations in the first scenario are fixed. A VPN technique is developed to encrypt the transmitted data. Also, additional link is added next to the main link to avoid the problem of network link failure, the two links work with load balancer technique, so if one link is failed, the second link will work automatically. Also, another firewall next to the main firewall is added, if the main firewall crashes, all settings will be transferred to the backup firewall using clustered technology.

With these modifications, an experiment is conducted by sending and receiving a 610 MB packet file to and from the main branch and the branches associated with it. The three transactions in each branch's firewall are measured. All the obtained results are summarized below in table 3

Table 3: Results obtained from the second proposed scenario



Main Site - aden															
ISP	file name	File Size	Transmitted Time	Remark	Link port	Bandwidth	Main-FG			Mukalla-FG			Mualla-FG		
							Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms
ISP1	nvedia_driver	610MB	13m.08sec	Link1:Main to Mukalla	1.1.1.1 to 1.1.1.2	1Gbps	4.90ms	0%	6.57ms	1.8ms	0%	1.5ms	-	-	-
	nvedia_driver	610MB	8m31sec	Link1:Main to Mualla	1.1.1.1 to 1.1.1.3	1Gbps	4.32ms	0%	6.34ms	-	-	-	2.81ms	0%	2.5ms
ISP2	nvedia_driver	610MB	13m.08sec	Link2:Main to Mukalla	2.2.2.1 to 2.2.2.2	1Gbps	5.0ms	0%	5.6ms	1.9ms	0%	1.6ms	-	-	-
	nvedia_driver	610MB	8m31sec	Link2:Main to Mualla	2.2.2.1 to 2.2.2.3	1Gbps	4.15ms	0%	6.16ms	-	-	-	5.56ms	0%	2.13ms

Mukalla Site															
ISP	file name	File Size	Transmitted Time	Remark	Link port	Bandwidth	Mukalla-FG			aden-FG			Mualla-FG		
							Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms
ISP1	nvedia_driver	610MB	10m:15sec	Link1:Mukalla to main	1.1.1.2 to 1.1.1.1	1Gbps	5.04ms	0%	7.1ms	3.54ms	0%	4.52ms	-	-	-
	nvedia_driver	610MB	9m25sec	Link1:Mukalla to Mualla	1.1.1.2 to 1.1.1.3	1Gbps	2.06ms	0%	1.34ms	-	-	-	2.13ms	0%	2.22ms
ISP2	nvedia_driver	610MB	10m:15sec	Link2: Mukalla to main	2.2.2.2 to 2.2.2.1	1Gbps	6.63ms	1%	8.11ms	2.71ms	0%	2.93ms	-	-	-
	nvedia_driver	610MB	9m25sec	Link2:Mukalla to Mualla	2.2.2.2 to 2.2.2.3	1Gbps	1.78ms	0%	1.55ms	-	-	-	2.28ms	0%	1.77ms

Mualla Site															
ISP	file name	File Size	Transmitted Time	Remark	Link port	Bandwidth	Mualla-FG			aden-FG			Mukalla-FG		
							Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms	Latency ms	Packet Loss %	Jitter ms
ISP1	nvedia_driver	610MB	9m11sec	Link1:Mualla to Main	1.1.1.3. to 1.1.1.1	1Gbps	2.47ms	0%	2.25ms	1.75ms	0%	1.51ms	-	-	-
	nvedia_driver	610MB	8m9sec	Link1:Mualla to Mukalla	1.1.1.3 to 1.1.1.2	1Gbps	2.24ms	0%	2.33ms	-	-	-	2.06ms	0%	1.34ms
ISP2	nvedia_driver	610MB	9m11sec	Link2: Mualla to Main	2.2.2.3 to 2.2.2.1	1Gbps	1.97ms	0%	2.11ms	1.77ms	0%	1.51ms	-	-	-
	nvedia_driver	610MB	8m9sec	Link2:Mualla to Mukalla	2.2.2.3. to 2.2.2.2	1Gbps	2.57ms	0%	2.87ms	-	-	-	2.46ms	0%	2.01ms

In this scenario, having two links functioning with the load-balancer, the transmission time, latency, and jitter still much better compared to the current system. Adding the VPN technique does not make a significant change to the network speed, and there is no packet loss.

5. Observations From Experimental Results

Based on the performance graphs and tables presented in section 5, the following observations have been made.

- In the currently used network, the transmission time, from Aden site to Mukalla is 44m and 4sec, the average latency time is 8.89 ms and average jitter 7.57 ms.
- In the first proposed model, the transmission time, as an example, from Aden site to Mukalla is improved to12m and 41sec, the average latency time is 5.08 ms and average jitter 7.22 ms, which are much better than the current network system results.
- In the second proposed model, the transmission time, for example, from Aden site to Mukalla is improved to 13m and 08sec, the average latency time is 3.35 ms and average jitter 4.03ms, which are again much better than the current network system obtained results.

Hence, significant improvements in transmission time, latency, and jitter, were achieved by optimizing the network infrastructure, with enhancement in reliability and security. Similarly, there are improvements for all the other simulated transactions.

Conclusion

In this research work, the current model of the National Bank of Yemen network was evaluated through number of performance metrics. Different proposed scenarios are designed for the current system and simulated using the PNET software. The obtained results showed the efficiency of the proposed models in terms of improving in the transmission time, latency and jitter. More enhancement to the security of the network system is gained by applying a VPN technique to the network. The branches connectivity to the main center is improved by adding one extra link, and a load balancing is implemented to mitigate the server load, thus providing higher reliability, another firewall also added next to the main firewall to provide high availability to the system. The simulated experiments justify the effectiveness of the proposed approaches and they are more flexible and robust as well.

References

[1] Z. Guo et al., "Exploring server redundancy in nonblocking multicast data center networks," *IEEE Trans. Comput.*, vol. 64, no. 7, pp. 1912-1926, Jul. 2015.

[2] S. Jain et al., "Using redundancy to cope with failures in a delay tolerant network," in *Proc. ACM SIGCOMM*, pp. 109–120, 2005.

[3] NBYemen. *Homepage*.
Available: https://www.nbyemen.com, Accessed: 20-April-2024.

[4] V. Hashiana, "Design and implementation of an IPSec virtual private network: A case study at the University of Namibia," in *Proc. IST-Africa Conf.*, pp. 1–6, May, 2020.

[5] N. R. Fattahillah, "High availability's implementation on the Fortigate firewall using SD-WAN zone and HA cluster active-passive," *BINUS J.*, vol. 2, no. 11, pp. 3937–3952, Aug. 2023.

[6] S. George, "A brief study on the evolution of next generation firewall and web application firewall," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 10, no. 5, May 2021, doi:10.17148/IJARCCE.2021.10504.

[7] J. M. Stewart, *Network Security, Firewalls, and VPNs*, 2nd ed. Burlington, MA: Jones & Bartlett, 2015.

[8] P. Dash, *Getting Started with Oracle VM VirtualBox*. Birmingham, UK: Packt, 2013.

[9] F. Basile, "PNetLab: A tool for the simulation, analysis and control of discrete event systems based on petri nets," *IFAC Proc.*, vol. 37, no. 18, pp. 213–218, Sep. 2004, doi:10.1016/S1474-6670(17)30748-6.

[10] PNetLab. *Documentation*. Available: https://www.pnetlab.com/pages/documentation, Accessed: 20-May-2024.

[11] J. T. Kendall, "VoIP: Call quality vs jitter and packet loss" Dec. 2023. Available: https://www.amazon.com/VoIP-Call-Quality-Jitter-Packet/dp/1738212408.

[12] E. Paulson et al., "On the latency and jitter evaluation of software defined networks," *Bull. Electr. Eng. Inform.*, vol. 8, no. 4, pp. 1507–1516, Dec. 2019, doi: 10.11591/eei.v8i4.1578.

[13] N. Mesbahi et al., "Delay and jitter analysis in LTE networks," in *Proc. IEEE WINCOM*, 2016, doi:10.1109/ WINCOM.2016.7777202.

[14] W. Sugeng et al., "The impact of QoS changes towards network performance," *Int. J. Comput. Netw. Commun. Secur.*, vol. 3, no. 2, pp. 48–53, Feb. 2015.

[15] Abubakar et al., "Performance evaluation of LTE networks," in *Proc. ICECCO*, 2019, doi:10.1109/ICECCO48375.2019.9043271.

[16] W. Adjardjah et al., "Performance evaluation of VoIP analysis and simulation," *J. Eng. Res. Rep.*, vol. 25, no. 7, pp. 176–191, 2023, doi: 10.9734/JERR/2023/v25i7951.

Author information

ORCID

Lutfi Mohammed Omer Khanbary: 0009-0008-8384-4394

مقالة بحثية

تحسين أداء الشبكة.
دراسة حالة: شبكة NBY

لطفي محمد عمر خنبري[1،*]، محمد انور قطب[1]

[1] قسم علوم وهندسة الحاسوب، كلية الهندسة، جامعة عدن، عدن، اليمن

* الباحث الممثّل: لطفي محمد عمر خنبري؛ البريد الالكتروني: llkhanbari@gmail.com

استلم في: 14 ديسمبر 2024 / قبل في: 09 يناير 2025 / نشر في 31 مارس 2025

المُلخّص

في هذه الورقة البحثية، تُقدم دراسة موسعة حول حالة نظام مصرفي شبكي. ومن خلال البحث، ولتحسين أداء الشبكة، صُممت نماذج مقترحة مُحسّنة للنظام الحالي. وقد تم تقييم أداء التقنيات المقترحة من خلال إجراء تجارب محاكاة. وتُظهر نتائج مقاييس الأداء المُحصل عليها من الدراسة المقارنة بين النظام الحالي والنماذج المقترحة موثوقية هذه النماذج ودقتها.

الكلمات المفتاحية: زمن الوصول، التذبذب، فقدان الحزمة، جودة الخدمة، مقاييس الأداء؛ جدار الحماية.

How to cite this article:

L. M. O. Khanbary, M. A. Qutb, “NETWORK PERFORMANCE ENHANCEMET A CASE STUDY: NBY NETWORK”, *Electron. J. Univ. Aden Basic Appl. Sci.*, vol. 6, no. 1, pp. 19-31, March. 2025. DOI: https://doi.org/10.47372/ejua-ba.2025.1.420