Recep Tayyip Erdoğan Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 6(1) 69-81 2025
Recep Tayyip Erdogan University Journal of Science and Engineering, 6(1) 69-81 2025
ISSN: 2687-2315 / E-ISSN: 2757-7686

Optimizing Computer Networks from the Perspective of Security Policies and VLAN Configurations

Umut BABAYİĞİT [1], Ali GEZER [1]*

[1] Kayseri University, Cyber Security Application and Research Center, Kayseri, Türkiye

Sorumlu Yazar/Corresponding Author
e-mail: agezer@kayseri.edu.tr

Araştırma Makalesi/Research Article
Geliş Tarihi/Received: 27.07.2024
Kabul Tarihi/Accepted: 09.01.2025

Abstract

The rapid development of network technologies and the growing number of interconnected devices have introduced significant challenges in optimizing the efficiency of computer networks. Misconfigurations in network devices such as manageable switches, routers, modems, and firewalls may lead to performance degradation and security vulnerabilities. Moreover, complex and poorly designed network architectures may exacerbate these issues by creating inefficiencies and increasing the risk of information security breaches. To address these challenges, this study focuses on designing and evaluating network topologies that segment physical networks into logical structures. By assessing various network designs, VLAN structures, and firewall security policies, the study aims to identify configurations that achieve an optimal balance between speed, security, and cost. The research evaluates key performance metrics, including round-trip time delays, jitter, download, and upload speeds, under different firewall policies. The findings provide actionable insights into how network configurations impact local network performance, highlighting best practices for creating high-performing, secure, and cost-effective network topologies. The findings also underscore the inherent trade-off between security and performance. While firewall security policies and VLAN configurations enhance network security, they also introduce processing overhead, particularly when additional switches and routing are involved, leading to increased local network delays.

Keywords: Network technologies, information security, network topology, Vlan, delay, jitter

Güvenlik Politikaları ve VLAN Yapılandırmaları Perspektifinde Bilgisayar Ağ Optimizasyonu

Öz

Ağ teknolojilerinin hızla gelişmesi ve birbirine bağlı cihazların sayısının artması, bilgisayar ağlarının verimliliğini optimize etme konusunda önemli zorlukları da beraberinde getirmiştir. Yönetilebilir anahtarlar, yönlendiriciler, modemler ve güvenlik duvarları gibi ağ cihazlarındaki yanlış yapılandırmalar, performans düşüşlerine ve güvenlik açıklarına yol açabilir. Ayrıca, karmaşık ve kötü tasarlanmış ağ mimarileri bu sorunları daha da kötüleştirerek verimsizliklere ve bilgi güvenliği ihlallerine neden olabilir. Bu zorlukların üstesinden gelmek amacıyla, bu çalışma fiziksel ağları mantıksal yapılar halinde segmentlere ayırarak ağ topolojilerinin tasarımı ve değerlendirilmesine odaklanmaktadır. Çalışmada, çeşitli ağ tasarımları, VLAN yapıları ve güvenlik duvarı politikaları incelenerek hız, güvenlik ve maliyet arasında optimal bir denge sağlayan yapılandırmalar belirlenmeye çalışılmıştır. Araştırma, farklı güvenlik duvarı politikaları altında gidiş-dönüş gecikme süresi, gecikme değişkenliği (jitter), indirme ve yükleme hızları gibi temel performans metriklerini değerlendirmiştir. Bulgular, yerel ağ performansını etkileyen ağ yapılandırmalarının etkilerine dair uygulanabilir bilgiler sunmakta ve yüksek performanslı, güvenli ve maliyet açısından etkili ağ topolojileri oluşturmak için en iyi uygulamaları vurgulamaktadır. Ayrıca, bulgular güvenlik ve performans arasındaki doğal dengeyi de ortaya koymaktadır. Güvenlik duvarı politikaları ve VLAN yapılandırmaları ağ güvenliğini artırırken, ek anahtarlar ve yönlendirme eklendiğinde işleme yükü artarak yerel ağ gecikmelerinin yükselmesine neden olmaktadır.

Anahtar Kelimeler: Ağ teknolojileri, bilgi güvenliği, ağ topoloji, VLAN, gecikme, jitter

Cite as;
Babayiğit, U. and Gezer, A. (2025). Optimizing computer networks from the perspective of security policies and vlan configurations. *Recep Tayyip Erdogan University Journal of Science and Engineering,* 6(1), 69-81. Doi: 10.53501/rteufemud.1505777

1. Introduction

The rapid expansion of the Internet has transformed daily life, offering increased convenience, efficiency, and speed. However, these advancements have introduced significant challenges, including data breaches, phishing, cyberattacks, and the spread of misinformation. These threats pose risks not only to individuals but also to organizations, emphasizing the critical importance of information security—a concept centered on protecting data, ensuring secure transmission, and controlling access to authorized users. In the context of network design, cybersecurity presents a dual challenge: addressing security vulnerabilities while maintaining optimal performance. Higher levels of security, such as rigorous data inspection and encryption, often lead to increased latency and reduced throughput (Eldem, 2020). Conversely, prioritizing performance at the expense of security can leave networks vulnerable to attacks.

Network devices, such as switches and firewalls, serve as frontline defenses against cyber threats. Their proper configuration is essential to ensuring rapid threat detection, blocking unauthorized access, and facilitating secure data exchange (Deepak and Varun, 2019). However, improperly configured devices can inadvertently introduce delays or disrupt network performance (Hautamaki and Hamalainen, 2021). For instance, firewalls operate based on rule sets that must be carefully designed to balance strict security enforcement with the need for smooth communication. Therefore, an optimal balance between security and performance must be achieved through strategic network topologies. Striking the right balance between these competing demands is essential for effective network management and forms the core question of this study.

A review of the literature reveals limited experimental studies focusing on the intersection of network performance and cybersecurity policies. While simulation-based studies dominate the field, they often lack the practical insights that real-time evaluations provide. Manukonda (2023) designed a system model with a simulation for assessing the performance of Ethernet services, including throughput, latency, packet loss, and scalability. Hossain et.al. (2023) emphasized secure inter-VLAN communication is essential for preserving the availability, confidentiality, and integrity of network resources with a simulation-based study. However, authors did not measure any performance metric in the study. Arpacı and Şentürk, (2024) performed a simulation-based study for performance analysis of firewall and virtual private network in video conferencing applications. Ikuomola et.al. (2023) designed a network security model within a local area network, but they did not test applicability of their model in real world. AI-Ofeishat and Alshorman (2024) used micro-segmentation and segmentation techniques to build a secure network. The technique is applied in a simulation environment without getting any performance metric such as delay, jitter, or speed.

Simulation methods are valuable for conceptualizing solutions but may fail to capture the nuances of live environments. Addressing this gap, our study benefits real-time experimentation with the usage of network performance metrics to provide a more comprehensive understanding of how cybersecurity policies influence network performance. In particular, the present study aims to evaluate the impact of security policies and network topologies on key performance metrics such as delay, jitter,

download speed, and upload speed. By analyzing these metrics under various configurations, the study seeks to identify strategies for optimizing both security and performance. Specifically, it addresses the following objectives:

- To analyze the impact of different firewall configurations on network performance.
- To investigate the trade-offs introduced by VLAN configurations in improving security and segmenting networks.
- To propose optimal network topologies that achieve a balance between robust security measures and minimal performance degradation.

2. Background

In today's digital era, ensuring information security is essential for protecting sensitive data and maintaining network integrity. The rapid growth in data generation, storage, and transmission has increased the need for effective security measures. In addition to adopting recognized standards like ISO 27001, organizations must provide user training and awareness programs to address the critical human factor in information security (Tekerek, 2008). Cybersecurity today extends beyond safeguarding information or resources; it includes protecting individuals using cyber resources and other assets, including those of the public, which could be at risk due to vulnerabilities (Von Solms and Van Niekerk, 2013).

From a technical perspective, the segmentation of physical networks into logical networks, such as through VLAN configurations, improves security. By logically dividing the network into different broadcast domains, VLANs ensure that traffic only flows through ports within the same VLAN (Rajaravivarma, 1997). VLANs reduce unnecessary traffic by isolating broadcast domains, ensuring efficient bandwidth utilization and enhanced security. This segmentation supports better control over network traffic while mitigating risks associated with unauthorized access (Taşkın, 2009).

With the ever-increasing data flows and connections in today's world, the optimal configuration of network devices is also crucial for protecting sensitive information and ensuring network safety. Firewalls play a pivotal role in enforcing network security policies and protecting sensitive information. By monitoring and filtering network traffic, firewalls act as barriers between internal systems and external networks, ensuring only authorized access to critical resources. Proper configuration and regular updates to firewall rules are essential to maintaining their effectiveness. System administrators must regularly review and update firewall rule sets to ensure ongoing network protection and effectiveness (Kim and Solomon, 2013; Voronkov et.al., 2020).

In this study, we focused on evaluating the impact of firewall configurations and VLAN implementations on network performance metrics, specifically delay, jitter, download speed, and upload speed. The selected firewall policies are given and explained as follows:

- Antivirus: Detects and removes malware like viruses and ransomware.
- Web Filter: Blocks access to harmful or unwanted websites.
- Application Control: Manages and restricts application usage.
- Intrusion Prevention System (IPS): Stops network-based attacks.
- Email Filter: Filters spam and malicious emails.
- Data Leak Prevention (DLP) Sensor: Prevents unauthorized data sharing.
- VoIP Protection: Secures voice communication from threats.

By analyzing the effects of security measures such as VLAN configurations and firewall rule sets on these parameters, we identified configurations that balance security with performance. For instance, while advanced firewall settings like deep packet inspection enhance security, they introduce processing overhead that increases delay. On the other hand, basic settings such as web filtering provide moderate security with minimal impact on performance.

3. Methodology

Investigations into the protective properties of firewall rules and network performance parameters across different topologies were conducted in a controlled environment. The experimental setup included firewalls, switches, and desktop computers connected using CAT5 (category 5) cables of equal lengths to ensure consistency. Each topology comprised four desktop computers, two Cisco Catalyst 3750G Series switches, and a FortiGate 1240B firewall. We focus on fundamental performance indicators (Ping, Jitter, Download, and Upload) to evaluate the impact of varying security policies. The experiments were conducted under controlled conditions in a laboratory setting, with minimal external interference, to ensure consistency and reliability in the measurements.

The study employed Windows operating systems, CAT5 cables, and legacy network devices, including two Cisco Catalyst 3750G Series switches and a FortiGate 1240B firewall. This choice was influenced by the availability of hardware and compatibility with the software tools used. It is recognized that these hardware and software choices may not align with the performance and security requirements of modern networks, which increasingly rely on advanced devices such as fiber-optic cables and gigabit Ethernet standards. However, our testing environment reflects the performance results of many currently operating local area networks.

The test computers were equipped with the following Ethernet cards:

- PC-1: Intel(R) 82566DM-2 Gigabit Ethernet card
- PC-2: Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Controller
- PC-3: Broadcom NetXtreme Gigabit Ethernet card
- PC-4: Realtek PCIe GbE Ethernet card

The topologies were created by interconnecting the devices through the switches and firewall. The switches were configured with VLANs to logically separate network traffic, and the firewall rules were adjusted to enforce security policies. The FortiGate 1240B firewall was configured with antivirus, web filter, application control, IPS, DLP, email, VOIP protection firewall security profiles. While these configurations allowed for a systematic evaluation of specific security policies, the scope did not include complex, real-world setups such as VPNs, cloud-based systems, multi branch networks, hybrid Cloud environments, or SD-WANs. Our future research should expand to include these advanced architectures to provide a more comprehensive understanding of their security and performance implications.

For each topology, network performance was assessed by measuring ping, jitter, download, and upload speeds as they are fundamental indicators of network performance. Ping measures latency, representing the time it takes for a data packet to travel from the source to the destination and back, which is critical for evaluating network responsiveness. Jitter quantifies the variation

in latency, important for applications requiring consistent data flow, such as voice or video streaming. Download and upload speeds assess the network's data transfer efficiency, directly impacting user experience in tasks like file sharing, streaming, and browsing. Together, these metrics provide a comprehensive overview of the network's reliability and performance under various conditions (Rajaravivarma, 1997; Gezer, 2019, 2022). The workflow of how we obtained these performance parameters are explained as follows:

- Ping: Delays were measured within the local network using Wireshark to capture ICMP packet times and calculate latencies.
- Jitter: Variations in latency were derived from the captured Ping data.
- Download/Upload: Speeds were evaluated using standard file transfer and benchmarking tools.

These parameters provided insights into the impact of different security policies and mitigations on network performance. While these metrics are critical for understanding network performance, additional indicators such as CPU and memory usage, which reflect the resource overhead of security policies, were not included in this study. Incorporating these metrics in our future works will contribute to a more holistic view of the trade-offs between security and system performance.

3.1 Topology – 1

In this specific network setup, the goal is to measure delays solely caused by the firewall (Figure 1). To facilitate ping communication between computers, port forwarding has been configured within the firewall rules. The performance parameters obtained are summarized in Tables 1-4.

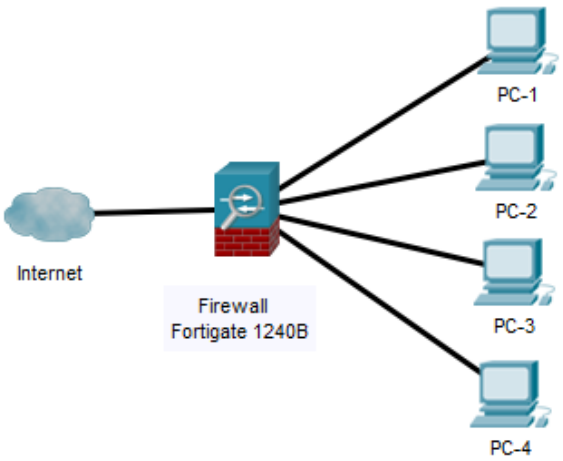

Figure 1. Topology-1 (firewall, and 4 computers)

Table 1. Topology-1 ping delay performance (µs)

	PC-1	PC-2	PC-3	PC-4	Avrg
PC-1	X	264.4375	369.3750	166.4375	266.7500
PC-2	226.625	X	412.1250	236.6250	291.7700
PC-3	394.6875	402.5625	X	343.7500	380.3330
PC-4	463.5000	517.9333	640.5000	X	540.6440

Table 2. Topology-1 jitter results (ms)

	PC-1	PC-2	PC-3	PC-4	Avrg
No security	1	3	1	1	1.50
Antivirus	2	2	1	1	1.50
Web Filter	2	2	0	1	1.25
Application Control	1	2	2	1	1.50
IPS	1	2	2	1	1.50
Email Filter	4	3	2	1	2.50
DLP Sensor	1	2	1	0	1.00
VoIP	3	2	1	1	1.75

Table 3. Topology-1 download performance (Mbps)

	PC-1	PC-2	PC-3	PC-4	Avrg
No security	106.7	107.2	107.1	106.9	106.97
Antivirus	106.9	107.1	106.6	107.1	106.92
Web Filter	106.8	107.0	105.7	106.7	106.55
Application Control	106.6	106.7	107.3	106.7	106.82
IPS	106.7	106.7	106.7	105.4	106.37
Email Filter	106.7	106.6	107.3	107.1	106.92
DLP Sensor	105.7	107.0	106.9	107.1	106.67
VoIP	106.4	106.6	106.7	105.3	106.25

Table 4. Topology-1 upload performance (Mbps)

	PC-1	PC-2	PC-3	PC-4	Avrg
No security	8.5	8.5	8.5	8.4	8.475
Antivirus	8.5	8.5	8.5	8.4	8.475
Web Filter	8.4	8.5	8.3	8.5	8.425
Application Control	8.4	8.3	8.2	8.4	8.325
IPS	8.4	8.5	8.4	8.3	8.400
Email Filter	8.4	8.5	8.5	8.4	8.450
DLP Sensor	8.5	8.5	8.4	8.5	8.475
VoIP	8.4	8.5	8.5	8.4	8.450

3.2 Topology – 2

In Topology-2, the goal is to measure the delays introduced by both the firewall and the switch (Figure 2). All computers were configured on the default VLAN on the switch to enable communication without requiring routing. In this topology, we aimed to observe performance parameters by positioning the switch after the firewall. The performance parameters obtained are summarized in Tables 5-8.

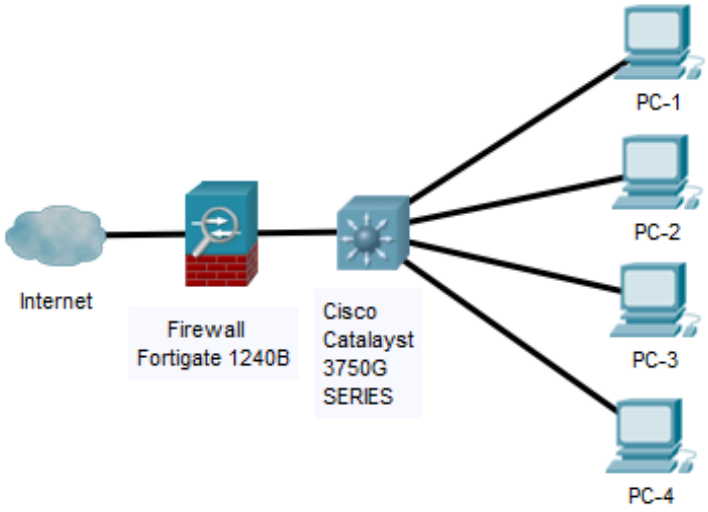

Figure 2. Topology-2 (firewall, switch, and 4 computers)

Table 5. Topology-2 ping performance (µs)

	PC-1	PC-2	PC-3	PC-4	Avrg.
PC-1	X	224.3125	341.8125	895.6600	487.2616
PC-2	209.3125	X	364.7500	1004.600	526.2208
PC-3	355.8750	384.5625	X	1139.600	626.6791
PC-4	280.4375	497.7500	614.3750	X	464.1875

Table 6. Topology-2 jitter performance (ms)

	PC-1	PC-2	PC-3	PC-4	Avrg.
No security	2	1	1	1	1.25
Antivirus	2	0	1	0	0.75
Web Filter	2	1	0	1	1.00
Application Control	4	2	1	1	2.00
IPS	2	1	1	1	1.25
Email Filter	2	1	1	1	1.25
DLP Sensor	1	1	0	1	0.75
VoIP	5	1	1	0	1.75

Table 7. Topology-2 download performance (Mbps)

	PC-1	PC-2	PC-3	PC-4	Avrg.
No security	106.7	106.9	107.1	107.0	106.92
Antivirus	106.0	107.2	106.3	106.9	106.60
Web Filter	106.7	107.2	107.2	106.7	106.95
Application Control	106.7	106.8	106.9	106.0	106.60
IPS	106.6	107.2	106.3	106.8	106.72
Email Filter	106.5	107.1	107.0	106.6	106.80
DLP Sensor	106.6	107.0	107.3	106.9	106.95
VoIP	106.9	106.5	106.5	106.9	106.70

Table 8. Topology-2 upload performance (Mbps)

	PC-1	PC-2	PC-3	PC-4	Avrg.
No security	8.5	8.5	8.5	8.5	8.500
Antivirus	8.5	8.5	8.5	8.4	8.475
Web Filter	8.5	8.5	8.5	8.5	8.500
Application Control	8.4	8.5	8.5	8.5	8.475
IPS	8.4	8.5	8.4	8.5	8.450
Email Filter	8.4	8.5	8.5	8.5	8.475
DLP Sensor	8.5	8.4	8.3	8.4	8.400
VoIP	8.5	8.5	8.5	8.5	8.500

We observed an additional delay of approximately 200-300 µs compared to Topology-1. This extra delay is due to the positioning switch after the firewall.

3.3 Topology – 3

We investigated how adding an extra switch affects communication performance. The computers were grouped into two sets and connected to two different switches as seen in Figure 3. All computers were in the default VLAN, so no routing rules were needed. The performance results for this scenario are shown in Tables 9-12.

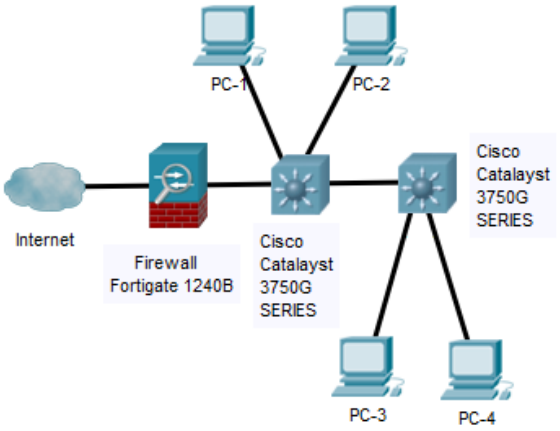

Figure 3. Topology-3 (firewall, 2 switches, and 4 computers)

Table 9. Topology-3 ping delay performance (µs)

	PC-1	PC-2	PC-3	PC-4	Avrg.
PC-1	X	256.4375	387.0625	936.1875	526.5625
PC-2	212.1250	X	413.9375	1041.937	555.9998
PC-3	354.7500	410.5000	X	1118.000	627.7500
PC-4	386.9375	513.9333	526.1875	X	475.6861

Table 10. Topology-3 jitter results (ms)

	PC-1	PC-2	PC-3	PC-4	Avrg.
No security	2	2	0	0	1.00
Antivirus	0	1	1	1	0.75
Web Filter	2	1	2	0	1.25
Application Control	0	1	1	1	0.75
IPS	2	1	1	1	1.25
Email Filter	2	1	1	1	1.25
DLP Sensor	2	1	1	1	1.25
VoIP	1	2	1	2	1.50

Table 11. Topology-3 download performance (Mbps)

	PC-1	PC-2	PC-3	PC-4	Avrg.
No security	106.6	106.0	107.0	106.9	106.62
Antivirus	105.2	105.6	106.7	106.7	106.05
Web Filter	106.9	106.2	107.1	107.0	106.80
Application Control	106.8	106.5	107.1	105.6	106.50
IPS	106.9	106.2	106.7	106.5	106.57
Email Filter	106.1	106.3	107.1	107.1	106.65
DLP Sensor	106.7	106.2	107.1	107.0	106.75
VoIP	106.2	106.5	107.3	106.9	106.72

Table 12. Topology-3 upload performance (Mbps)

	PC-1	PC-2	PC-3	PC-4	Avrg.
No security	8.3	8.4	8.5	8.5	8.425
Antivirus	8.4	8.5	8.5	8.5	8.475
Web Filter	8.5	8.5	8.5	8.4	8.475
Application Control	8.5	8.4	8.5	8.5	8.475
IPS	8.4	8.5	8.4	8.4	8.425
Email Filter	8.5	8.4	8.5	8.5	8.475
DLP Sensor	8.5	8.5	8.5	8.5	8.500
VoIP	8.4	8.4	8.4	8.4	8.400

3.4 Topology – 4

In Topology 4, we created two different VLANs to observe how VLAN creation and routing affect performance (Figure 4). Communication between the VLANs was managed through VLAN routing implemented via firewall rules. The performance results obtained for Topology-3 are shown in Tables 13-16.

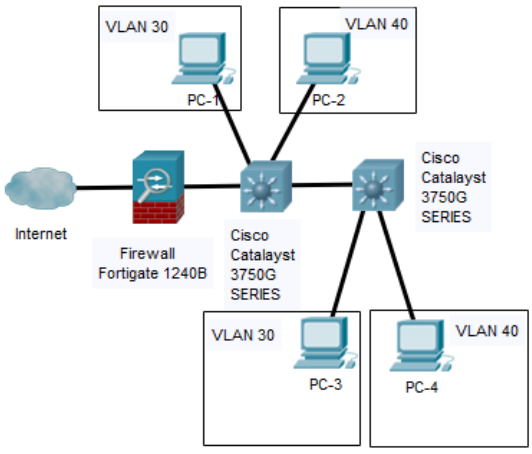

Figure 4. Topology-4 (firewall, 2 switches, and 4 computers)

Table 13. Topology-4 network ping performance (μs)

	PC-1	PC-2	PC-3	PC-4	Avrg.
PC-1	X	300.1875	347.0000	949.0714	532.0863
PC-2	283.1875	X	439.9375	1033.562	585.5623
PC-3	356.0000	418.2500	X	1205.500	659.9166
PC-4	419.2500	516.0625	641.7857	X	525.6994

Table 14. Topology-4 network jitter results (ms)

	PC-1	PC-2	PC-3	PC-4	Avrg.
No security	1	3	0	1	1.25
Antivirus	1	2	0	1	1.00
Web Filter	4	2	2	0	2.00
Application Control	2	1	1	0	1.00
IPS	1	1	2	1	1.25
Email Filter	2	1	0	1	1.00
DLP Sensor	1	4	1	1	1.75
VoIP	1	1	2	1	1.25

Table 15. Topology-4 network download performance (Mbps)

	PC-1	PC-2	PC-3	PC-4	Avrg.
No security	107.0	106.0	107.1	107.0	106.77
Antivirus	106.5	105.7	107.1	107.0	106.57
Web Filter	106.7	105.2	107.2	106.8	106.47
Application Control	106.9	107.0	107.0	106.5	106.85
IPS	107.1	106.6	106.8	106.7	106.80
Email Filter	107.0	105.8	107.2	106.9	106.72
DLP Sensor	105.3	105.7	107.2	107.0	106.30
VoIP	106.1	106.6	106.9	106.9	106.62

Table 16. Topology-4 network upload performance (Mbps)

	PC-1	PC-2	PC-3	PC-4	Avrg.
No security	8.5	8.4	8.5	8.5	8.475
Antivirus	8.5	8.5	8.4	8.5	8.475
Web Filter	8.5	8.4	8.4	8.5	8.450
Application Control	8.4	8.4	8.5	8.5	8.450
IPS	8.5	8.5	8.5	8.5	8.500
Email Filter	8.5	8.3	8.5	8.4	8.425
DLP Sensor	8.5	8.4	8.5	8.4	8.450
VoIP	8.5	8.4	8.5	8.5	8.475

A comparative analysis was performed using column charts to observe performance differences across the topologies. As shown in Figure 5 adding an extra switch significantly increases delay (Topology-2). However, adding one more switch and positioning computers on different switches without VLAN configuration results in only a slight increase in delay (Topology-3). VLAN configuration and routing lead to increased delays (Topology-4).

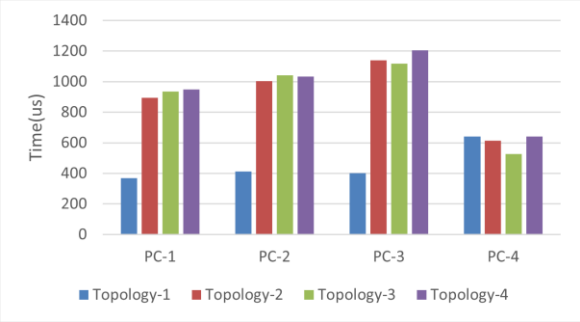

Figure 5 Maximum ping latency on computers within the local network.

Figure 6 shows that VLAN configuration and routing do not meaningfully affect jitter. However, Topology 1, which uses only firewall devices for switching, exhibits a lower jitter compared to the other scenarios.

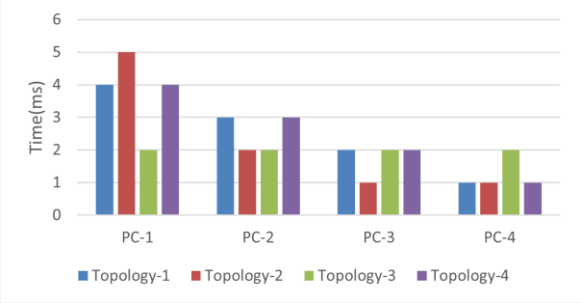

Figure 6. Maximum Jitter latency on computers.

Topology-3 gives the best result for download performance, which computers were grouped into two sets and connected to two different switches as seen in Figure 7. Topological and firewall policy changes do not have any effect on upload speeds as seen in Figure 8.

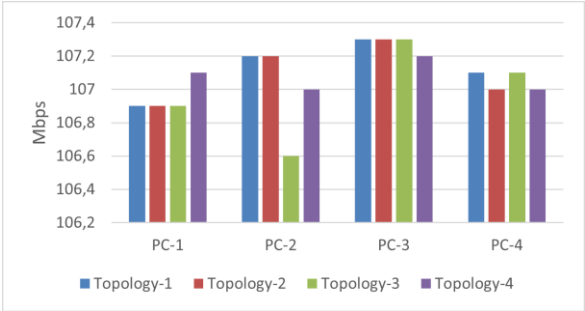

Figure 7. Maximum download speed on computers.

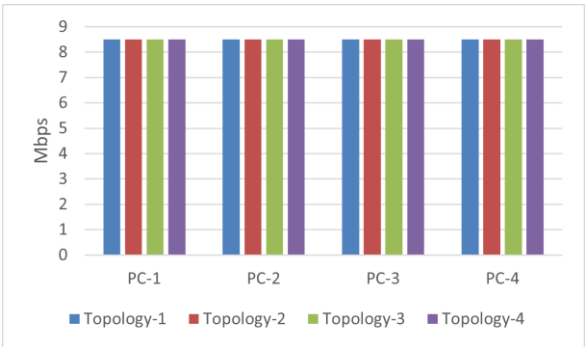

Figure 8. Maximum upload speed on computers.

To ensure reliability, each experimental result was calculated as getting the average of eight measurements, minimizing the impact of random errors or anomalies on performance results. This approach enhances repeatability and provides a more consistent representation of the network's performance under the tested conditions.

To ensure accuracy and security, potential risks associated with VLAN, and firewall configurations were identified and mitigated as follows:

VLAN Hopping: To prevent this attack, switch port security was configured to limit access to trusted devices only. Additionally, trunking was restricted to specific ports, and unused ports were disabled to reduce attack vectors.

Firewall Misconfigurations: Regular audits of firewall rules were conducted to detect overly permissive or redundant rules.

Network Loops and Broadcast Storms: Spanning Tree Protocol (STP) was enabled on the switches to prevent network loops and maintain stability.

Testing Environment: Tests were conducted in a laboratory setting with minimal external interference. The network traffic levels were controlled to mimic a typical small-to-medium enterprise environment. The physical layout of the lab ensured equal cable lengths and minimized electromagnetic interference.

4. Conclusion

In this study, we investigated the effects of firewall security policies, the number of network appliances, and VLAN configuration to determine the optimal network topology. The goal was to enhance network security while maintaining optimal communication speed, considering configuration settings made through firewalls and switches. The results showed that ping delay is minimized when using only one firewall in the topology. However, when a firewall is used with two interconnected switches in a cascade design and VLANs are configured with termination at the firewall, ping delay increases by approximately 55%. Jitter, download, and upload performance remain relatively unchanged under different firewall security policies across various topologies. These findings highlight the trade-off between security and performance for local area networks. However, the results may change for wider area networks. While firewall security policies and VLAN configurations improve network security, the addition of extra switches and routing introduces processing overhead that can increase local network delay. Among the tested policies, resource-intensive configurations, such as deep packet inspection and application control, were found to contribute more significantly to performance degradation. Conversely, policies such as basic antivirus and web filtering maintained better performance while still providing a reasonable level of security. To establish a balance between security and performance, it is recommended to tailor security configurations to specific network needs such as critical systems may require advanced security measures like intrusion prevention systems or data leak prevention, despite the potential performance trade-offs; non-critical systems can operate effectively with lighter policies, such as antivirus and basic content filtering, to prioritize performance.

Author Contribution

Babayiğit, U: Data gathering, Literature Search, Data Processing, Writing

Gezer, A.: Idea, Conceptualization, Editing, Writing

Acknowledgment

We would like to extend our thanks to Kayseri University Cyber Security Application and Research Center and Türk Telekom A.Ş. for providing the network devices and infrastructure.

Conflict of interest

All the authors declare no conflict of interest.

Ethical standards

No Ethics Committee Decision is required for this study.

References

Al-ofeishat, H., Alshorman, R. (2024), Build a secure network using segmentation and micro-segmentation techniques. *International Journal of Computing and Digital Systems*, 16(1), 1499-508, http://dx.doi.org/10.12785/ijcds/1601111.

Arpacı, S., Şentürk, A. (2024). Performance analysis of firewall and virtual private network (VPN) usage in video conferencing applications. *Düzce University Journal of Science & Technology*, 12, 1879-1894 https://doi.org/10.29130/dubited.1462133.

Deepak, I., Varun, D. (2019). A survey on: Network security and management, threats and firewalls. *Journal of Emerging Technologies and Innovative Research*, 6(3), 199-203.

Eldem, T. (2020). The governance of Turkey's cyberspace: Between cyber security and information security. *International Journal of Public Administration*, 43(5), 452-465. https://doi.org/10.1080/01900692.2019.1680689

Gezer, A. (2019). Large-scale round-trip delay time analysis of IPv4 hosts around the globe. *Turkish Journal of Electrical Engineering and Computer Sciences*, 27(3), 1998-2009. https://doi.org/10.3906/elk-1803-137 -12

Gezer, A. (2022). The delay measurement and analysis of unreachable hosts of internet. *The International Arab Journal of Information Technology*, 19(1), 63-71. 1 https://doi.org/10.34028/iajit/19/1/8 -13

Hautamaki, J., Hamalainen, T. (2021). A model of Cyber Threat Information Sharing with the Novel Network Topology, 12th International Conference on Advances in Information Technology, 07/2021, 1-10. https://doi.org/10.1145/3468784.34688 -2

Hossain, M.A., Harun M., Rana. A., Anower, S. (2023), Secure Inter-VLAN routing in multi branches Office network. *International Journal of Communication and Information Technology*, 4(2), 01-11 https://doi.org/10.33545/2707661X.2023.v4.i2a.65.

Ikuomola, A.J., Owoputi, K.S. and Johnson-Rokosu, S.O. (2023), Design and Implementation of a Network Security Model within a Local Area Network (1st Edition). **In***: Intelligent Data Analytics, IoT, and Blockchain*, eBook ISBN: 9781003371380 Auerbach Publications, 14p.

Khelf, R., Ghoualmi-Zine, N. (2018). Ipsec/firewall security policy analysis: A survey. In 2018 International Conference on Signal, Image, Vision and their Applications (SIVA). 26-27/11/2018, Guelma, Algeria ,1-7. https://doi.org/10.1109/SIVA.2018.8660973 -5

Kim, D., Solomon, M. G. (2013). Fundamentals of information systems security. *Jones and Bartlett Publishers*. ISBN:978-0-7637-9025-7, USA.

Manukonda, K.M.R (2023). Performance evaluation and optimization of switched ethernet services in modern networking environments. *Journal of Technological Innovations*, 4(2).

Rajaravivarma, V. (1997). Virtual local area network technology and applications. *Proceedings The Twenty-Ninth Southeastern Symposium on System Theory*. 9-11/3/1997, Cookeville, TN, USA, 49-52. https://doi.org/10.1109/SSST.1997.581577

Taşkın, C. (2009). Ağ Teknolojileri ve Telekomünikasyon. *Pusula*, ISBN:978-9944-711-25-8, Beşiktaş İstanbul. -8

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Doğa Bilimleri Dergisi,* 11(1), 132-137.

Von Solms, R., Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, 38, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Voronkov, A., Martucci, L. A., Lindskog, S. (2020). Measuring the usability of firewall rule sets. *IEEE Access*, 8, 27106-27121. https://doi.org/10.1109/ACCESS.2020.2971093

Wang, S. S. (2019). Integrated framework for information security investment and cyber insurance. *Pacific-Basin Finance Journal*, 57, 1-12 https://doi.org/10.1016/j.pacfin.2019.101173 -3.