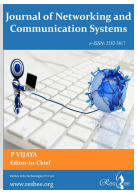
Vol.7 No.2 April 2024

Journal of Networking and Communication Systems

Received 14 March, Revised 17 March, Accepted 20 April



Enhancing Network Availability using Firewall Clustering

Jouma Ali AlMohamad

Faculty member at Al-Shahbaa Private University, Aleppo, Syria

Abstract: In the ever-evolving landscape of network security, the integration of advanced clustering methodologies within firewall infrastructures emerges as a pivotal strategy to enhance network service operability. This paper proposes the consolidation of multiple firewall entities into a unified structure through firewall clustering, capable of handling substantial data flows up to 100 gigabytes per second. By creating a collective logical unit, firewall clustering provides consolidated oversight and seamless integration into the network, thereby improving service accessibility and redundancy measures. Empirical research demonstrates a significant improvement of 45% in network service operability with firewall clusters, underscoring their importance in fortifying network resilience and throughput. This study explores the functional deployment and complexities of clustering, with a focus on Internet Service Provider networks, aiming to ensure continuous and reliable service delivery.

Keywords: Clustering, Firewall, Next Generation Firewall, Network Availability, Redundancy, Network Resilience

Nomenclature

Abbriviation	Expansion
FTP	File Transfer Protocol
ASA	**Adaptive Security Appliance**
DCI	Data Center Interconnects
SNN	Shallow Neural Network
PODT	Precision-Optimized Decision Tree
ML	Machine Learning
NGFW	Next-Generation Firewall

1. Introduction

In the contemporary digital landscape, characterized by escalating cyber threats and burgeoning network complexity, ensuring robust network security and availability has become paramount. Traditional firewall configurations, while foundational in safeguarding against threats, often fall short in addressing the evolving cyber security challenges. This necessitates the exploration of innovative defense mechanisms to bolster network resilience and mitigate potential vulnerabilities.

This study endeavors to fill this gap by demystifying the intricate realm of clustering, and elucidating its conceptual underpinnings, practical applications, and network integration nuances. Beyond exploration, the mission is to elevate service availability by strategically harnessing the clustering facet within firewall systems. By examining the challenges of network metamorphosis and illuminating the path to enhanced service availability, this research seeks to contribute to the advancement of network security practices in dynamic network environments.

In the realm of network systems, maintaining seamless connectivity amidst dynamic changes poses a persistent challenge. This instability can lead to data loss and communication disruptions, highlighting the critical importance of robust network resilience measures. The core proposition of this research revolves around comprehending and orchestrating firewalls through an administration server, with the Firewall Cluster element acting as a dynamic embodiment of provisioned firewalls entwined within the management server's framework.

Recognizing this imperative, this study proposes a strategic approach that embraces NGFW clustering—an advanced integration of firewalls node soperating as a unified mechanism. Unlike traditional single-node configurations, firewall clustering consolidates multiple firewall entities into a cohesive structure, thereby optimizing processing workloads, eliminating unnecessary processes, and enhancing firewall resilience against cyber threats.

https://doi.org/10.46253/jnacs.v7i2.a2

The remaining paper is aligned as follows: Section 2 covers the reference study. Section 3 explained the methodology. Section 4 included the practical implementation. Section 5 shows the simulation and result discussion. Section 6 mentions the conclusion and future direction.

2. Reference Study

The literature on network security and firewall technologies provides valuable insights into the challenges and opportunities associated with enhancing network availability. Previous studies have explored various aspects of firewall efficiency, including policy analysis, performance assessment, and dynamic algorithm advancements. However, there remains a gap in the literature concerning the comprehensive integration of clustering methodologies within firewall infrastructures to enhance network availability and resilience.

1. ***A Revolutionary Method to Strengthen Cyber Security*:** This study introduces a groundbreaking firewall decision framework that enhances cyber security through smart analytics. The framework integrates SNN and PODT techniques from machine learning, achieving remarkable accuracy levels.
2. ***Analyzing Firewall Policies*:** Focused on network security, this research utilizes advanced ML and data analysis techniques to identify irregularities in firewall configurations.
3. ***Assessing the Performance of Stateful Firewalls*:** This study incorporates stateful firewall functionality with a focus on flow scheduling, aiming to optimize control distribution.
4. ***Advancements in Dynamic Firewall Algorithms*:** This study aims to enhance the efficiency of firewalls in multi-cloud environments.

3. Methodology

Our proposed methodology employs advanced clustering techniques to create a hierarchical structure with Master and Subordinate units. This section elaborates on cluster member dynamics, cluster interface configuration, cluster management connectivity, and harmonious configuration redundancy. Additionally, it discusses the prerequisites for ASA clustering essentials and optimization of data center interconnects for cross-site clustering scalability.

3.1 Research Materials and Methods

- **Cluster Member Dynamics and Master/Slave Relationships:** Describes the hierarchical structure of a firewall cluster with a Master unit and subordinate members. Emphasizes the Master's exclusive role in configuration, and safeguarding certain features. Compares the Master to an ensemble, ensuring unity and replication of configuration changes.
- **Cluster Interface:** Cluster interfaces can be configured as Ether Channel bundles or individual interfaces. All interface data within a group should be of the same type.
- **Cluster Management Connectivity:** Each unit needs to allocate a minimum of one hardware interface to facilitate control communication within the cluster.
- **Configuration Redundancy:** Introduces the concept of a shared configuration tapestry within the cluster. Changes to configurations originate solely from the Master unit, initiating a synchronized cascade across all subordinate units, reinforcing harmony, unity, and impeccable synchronization.
- **5-ASA Cluster Management Symphony:** Unveils the advantages of simplified management within ASA clustering. Explores key themes such as the architecture of the management network, the significance of the management interface, roles of Master and Subordinate units, RSA key replication, and ASDM authentication complexities.

3.2 Management Network

Emphasizes the importance of a dedicated Management Network in ASA clustering. Advocates for a separate channel for management commands to flow unimpeded, enhancing the efficiency of cluster management.

3.3 Unveiling the Management Interface Elegance

Proposes the use of dedicated management inter faces for efficient clusters. The configuration options for these interfaces highlight the significance of IP addresses, individuality, and the Master unit's role in guiding the ensemble.

3.4 Mastery in Management: Master and Subordinate Units

Defines the roles of Master and Subordinate units in the cluster management. Describes the Master unit as the runtime statistics and monitoring tasks.

3.5 RSA Symmetric Key

In the RSA key generation, a primary unit (master) is the RSA key shared across the cluster. This synchronization is not merely a reflection but also for security. However, when there are transitions, the connection changes. An SSH session to the primary unit's IP address pauses if the master unit falters. Yet, with a new primary unit, SSH connections resume their process with the temporary storage of SSH host keys.

In the realm of ASDM connections, a self-signed certificate unfolds, tied to the local IP address. A dissonance arises when the primary IP address beckons—a warning of "IP Address Mismatch." Despite the warning, connections are possible, but a remedy can be arranged with certificates, embracing both the primary cluster's IP address and its local counterparts. The connection unfolds with a warning's echo.

In the inter-site deployment, ASA clustering plays a strategic role in arranging flow based on site identifiers. Clusters with distinct site layers with MAC and IP addresses resonating with each site's essence. Originating packets mirror the site's addresses, while received packets adopt a common address, preventing confusion among switches.

The ASA clustering licenses unfold a rule of harmony through diversity. Units in a cluster aren't bound by identical licenses. The master unit often carries a license, echoing to subordinate units, harmonizing their license status.

3.6 Prerequisites for ASA Clustering Essentials

ASA Fire POWER Inclusion Note

Highlights an inclusion note regarding ASA Fire POWER models.

- Direct clustering for ASA Fire POWER models is not supported.
- Despite this, these units can seamlessly integrate within the cluster arrangement.

3.7 Prerequisites for Hardware and Software

Uniformity in the Cluster: Emphasizes the need for consistency in hardware and software configurations within the cluster.

- All units must have the same model and identical DRAM memory.
- Flash memory variations are allowed.
- Software is maintained during image upgrades.
- Security context mode must be uniform across units, whether in singular or multiple contexts.
- In single context mode, a unified firewalling or routing mode is essential for consistency.
- New cluster members should replicate SSL encryption settings from the master unit for the initial control link connection.
- For ASA 5585-X with 10 GE I/O licenses, cluster and encryption modes must align.

3.8. ASA's Necessities: IP Addresses, Management, and More

Outlines individual prerequisites for ASA units regarding IP addresses, management, and specifi configurations.

- Each unit must have a unique IP address.
- Administrative IP addresses, except for the master units are transient.
- Upon a subordinate unit's entry into the cluster, its management interface configuration aligns with the master units.
- Jumbo frames require enabling before clustering for enhanced connectivity.

3.9. Optimizing Data Center Interconnects for Cross-Site Clustering Scalability

Balancing Bandwidth Dynamics Across DCI .In the cross-site clustering, the bandwidth reservation commences on the DCI link. Here, a calculation unfolds for cluster control traffic. The Calculation Ensemble: For each cluster member at a site, the calculation takes a measured step:

$$Reservation = \left(\frac{Number\ of\ cluster\ members\ per\ site}{2} \right) \times Cluster\ Control\ Link\ Size\ per\ member \quad (1)$$

Variation in Member Counts: When sites introduce their cast of cluster members, the count may vary. To guide this, the calculation calls for a unifying principle: the larger count shall lead. Thus, the calculation encompasses the grandest performance across the sites.

Minimum Bandwidth: The minimum DCI bandwidth mustn't fall below the cluster control link size of a single member.

Examples:

- For a quartet of members gracing two sites: Reservation = 5 Gbps (2/2 × 5 Gbps)
- For a hexad of members across three sites, the tempo escalates: Reservation = 15 Gbps (3/2 × 10 Gbps)
- For a duo of members sharing two stages: Reservation = 10 Gbps (1/2 × 10 Gbps, though the minimum DCI bandwidth must remain below the cluster control link size of 10 Gbps)

3.10 ASA Clustering Guidelines

- **Contextual Unison:** Emphasizes the importance of consistent context mode across all cluster members for configurations.
- **Security Resonance:** Stresses the need for firewall mode uniformity in single mode across all units.
- **Failover's Silent Retreat:** Acknowledges the absence of failover bypass in clustering, highlighting their separate yet essential roles in protection.
- **IPv6, the Absent Note:** Notes the focus on IPv4 in the cluster control link with IPv6 awaiting.
- **Switches as Supporting Cast**
    - Provides guidelines for switches supporting ASA clustering.
    - ASR 9006 seeks MTU, highlighting an elevation of 14 bytes for non-default MTUs.
    - Recommends Spanning Tree Port Fast for efficient entry of new units into the choreography.
    - Provides recommendations for load balancing techniques, proposing the utilization of source-destination IP or source-destination IP port to enhance efficiency.
    - Addresses compatibility issues with LACP and undisturbed throughput.
    - Highlights considerations for Supervisor 2T Ether Channels, Cisco Nexus switches, and L4 flow validation.
- **Local Device Aria**
    - Focuses on guidelines for local devices in the ASA clustering.
    - Ether Channels play the cluster and its control link used for separation, distinctiveness, and synchronization.

4. Practical Implementation

The practical implementation section illustrates the steps involved in implementing firewall clustering using the OPNET program. Through detailed instructions and diagrams, it demonstrates the configuration process and compares the performance of clustered and non-clustered firewall configurations in simulated network environments.

4.1 Unveiling the Ensemble

In this section of the practical realm, the steps of the network operation are cluster configuration, Interface Configuration, Routed Mode, Transparent Mode, and Convergence of Configuration.

Initially, the components a reconfigured then the potential outcomes and the resonance of implementation impacts come into view.

- **Cluster configuration**- Here, the approach groups the cluster control link cable, the management network's canvas, and the network's data threads.
- **Interface Configuration**- Unites interfaces and extends the core across the chassis, a channel where each unit contributes its ability.
- **Routed Mode**—a channel's identity. Here, the Ether Channel takes on a routed persona, bearing a single IP address, symbolizing its unity.
- **Transparent Mode**—a collective spirit. The Ether Channel, adorned with an IP address assigned to the BVI, stands as a beacon of unity, a guiding light through transparency.

- **Convergence of Configuration**- Unified modes—Spanned Ether Channels or individual interfaces. Unity prevails as clusters synchronize into a single interface type. No mixing of steps within this choreography.

4.2 Before Getting Started

- Ensure to set the mode independently on each ASA unit planned for cluster inclusion.
- The management interface can only be configured as a standalone interface. Even in Spanned Ether Channel mode, the management interface remains independent.
- If the management interface is configured as an individual interface in Spanned Ether Channel mode, dynamic routing for the management interface cannot be enabled, necessitating the use of a static path instead.
- In the multiple-context mode, a uniform interface type must be selected for all contexts.

4.3 Execution Mechanism

Step 1: Prioritize any incompatible configurations in advance to ensure the enforcement of the interface mode and facilitate subsequent configuration adjustments. This mode remains unchanged through the utilization of the following command:

$$cluster\ interface-mode\ \{individual\ |\ spanned\}\ check-details \tag{1}$$

Example:

$$ciscoasa(config)\#\ cluster\ interface-mode\ spanned\ check-details$$

Step 2: Set the interface mode for the cluster.

$$cluster\ interface-mode\ \{individual\ |\ spanned\}\ force \tag{2}$$

Example:

$$ciscoasa(config)\#\ cluster\ interface-mode\ spanned\ force$$

There are no default settings and the node must be chosen explicitly. If the mode is not set the clustering system won't be enabled. The "force" option changes the mode without checking the configuration for incompatible settings. After changing the mode, any configuration issues should be addressed manually. Since no interface configuration can be fixed until the mode is set, we recommend using the "force" option to at least start from your current configuration.
To remove the interface mode, the command is

$$no\ cluster\ interface\ mode \tag{3}$$

4.4Configuring Interfaces on the Master Unit

Before activating the clustering system, it's imperative to adjust any interfaces currently set with an IP address to align with cluster requirements. This section outlines the process of configuring interfaces to ensure compatibility with clustering. Data interfaces can be configured either as Ether Channels or individual interfaces, each employing distinct load-balancing mechanisms. It's important to note that configuring both types simultaneously is not feasible, except for the management interface, which can remain individual even in Spanned Ether Channel mode. They are

- Configure Individual Interfaces
- Configure Ether Channels

4.5Configuring Individual Interfaces

Standalone interfaces function are conventional routed interfaces each obtaining an IP address from the designated pool. The principal IP address of the cluster remains fixed and is allocated to the current master unit. When operating in Spanned Ether Channel mode, it is recommended to configure the management interface as an independent interface.

4.6 Prior to Initiation

- Except for the management interface, all interfaces should be set to individual mode.
- In multiple context mode, execute this process within each context. If you're not currently in the context configuration mode, employ the following command.

$$change\ to\ context\ name \tag{4}$$

- Load balancing needs to be configured on all adjacent devices for individual interfaces. External load balancing is unnecessary for the management interface.
- For Ether Channel interfaces, the channel is local to the unit.
- Management-only interfaces cannot be spanned interfaces.

Now, To implement the previously mentioned concepts using the OPNET program. The following steps will outline our approach:

Initially, examine a scenario involving users who request services such as email, web browsing, data transfer, and database access from remote servers over the Internet. This scenario is depicted in Fig 1.

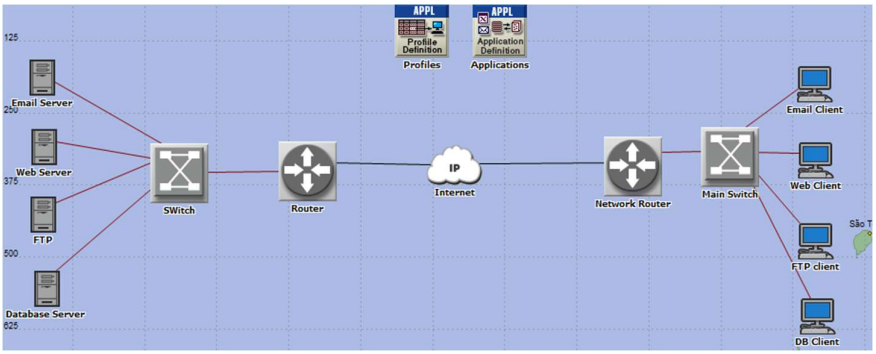


Fig.1. *The studied network without the use of firewalls.*

To ensure the protection of servers, a firewall is subsequently introduced into the network, as depicted in Fig 2. This firewall restricts any user from accessing the server containing the database, while allowing the rest of the services to operate, as illustrated in Fig 3.

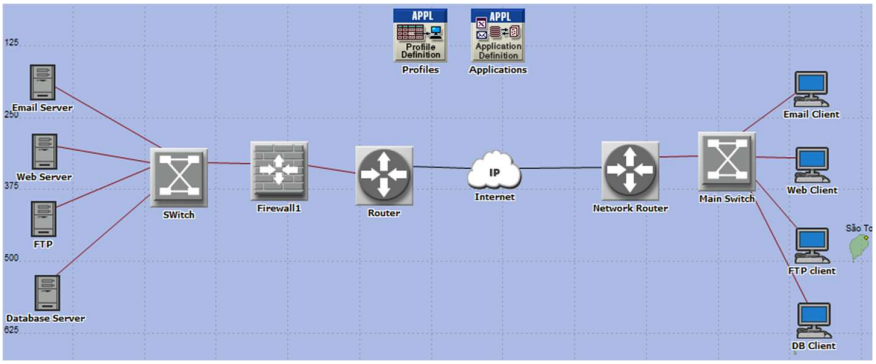


Fig.2. *The studied network with a single firewall.*

	Application	Proxy Server Deployed	Latency (secs)
0	Custom Application	Yes	constant (0.00002)
1	Database	No	exponential (0.00005)
2	Email	Yes	No Latency
3	Ftp	Yes	uniform (0.00005 0.0001)
4	Http	Yes	No Latency
5	Print	Yes	constant (0.0002)
6	Remote Login	No	N/A
7	Video Conferencing	Yes	exponential (0.00001)
8	Voice	Yes	No Latency
9	Other Applications	Yes	constant (0.00002)

Fig. 3. *The firewall prevents external access to the database server.*

In the network illustrated in Fig. 4, the concept of clustering is implemented by employing multiple firewalls within the cluster. This ensures redundancy and surplus in the communication process, eliminating the Single Point of Failure scenario. Additionally, the load is distributed among the three firewalls, enhancing the performance and productivity of the communication process. The concept of clustering is applied to the studied network as depicted in Fig. 5.

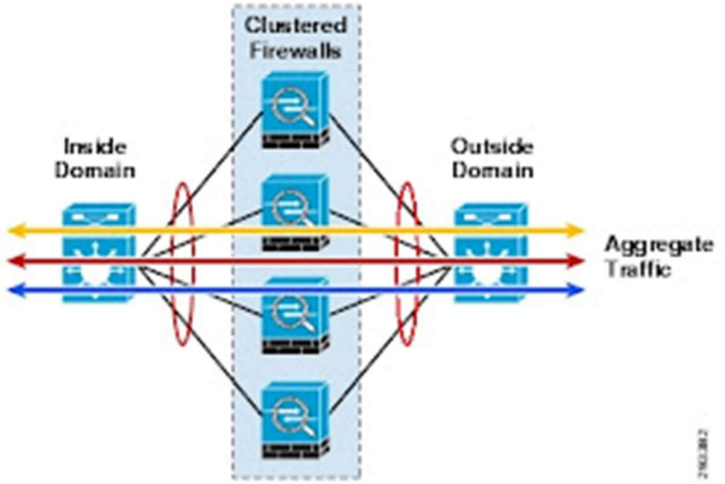


Fig. 4. *Clustering concept with multiple firewalls.*

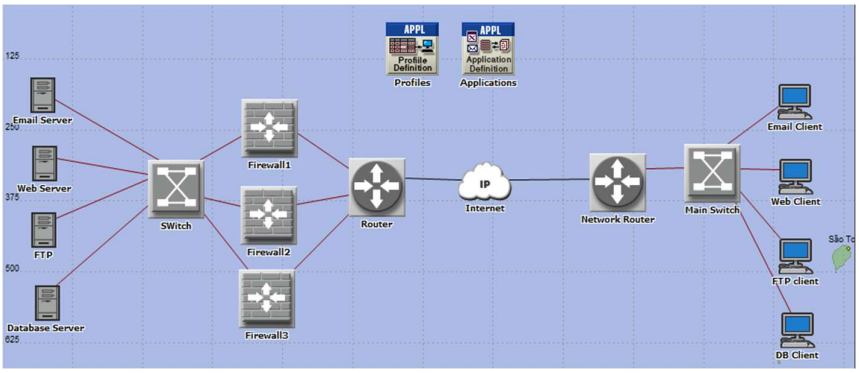


Fig. 5. *The studied network using three firewalls within the clustering concept.*

5. Simulation and Results Discussion

Empirical testing conducted using the OPNET program demonstrates the efficacy of firewall clustering in enhancing network availability and resilience. By analyzing data volume handling and network productivity in clustered and non-clustered firewall configurations, the study provides valuable insights into the tangible benefits of firewall clustering in real-world network scenarios.

We will simulate the three previously described networks using the OPNET program, which stands out among simulation tools for its ability to measure sent and received data volumes, delay, and loss. It provides realistic results for the performance of the studied networks. We configure the network terminals to request services over the Internet from servers (Email-FTP-Web-Database). Then, we compare the performance of this network under three operational scenarios:

1. **No_Firewall:** No firewall is used in the network.
2. **NO_Clustering:** A single firewall is employed to prevent access to the database server.
3. **Clustered_Firewall:** The clustering concept is applied using three firewalls to restrict access to the database server.

Fig. 6 illustrates the received data volume for the database application across the three aforementioned operational scenarios. In the "No Firewall" scenario, received data is evident as users request the database service from the remote server. However, for scenarios with firewalls (both clustering and single firewall), the received data value is zero. This is due to the firewall preventing users from accessing the database application.

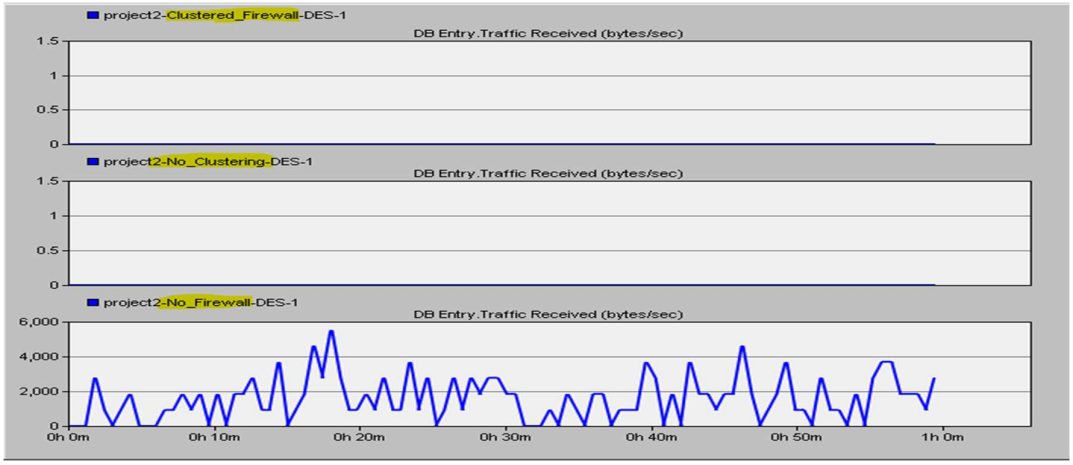


Fig. 6. *Received Data Volume for the Database Application.*

Fig. 7 and **Fig. 8** show the measurement of received data volume for the Data Transfer (FTP) and Web Browsing applications respectively. The received data volume for both applications is larger in the "Clustered_Firewall" scenario compared to the other scenarios. This can be attributed to the clustering operation of the firewalls, which effectively distributes the received data load across the firewall cluster. As a result, a greater quantity of data can be processed, ultimately enhancing the network's productivity.

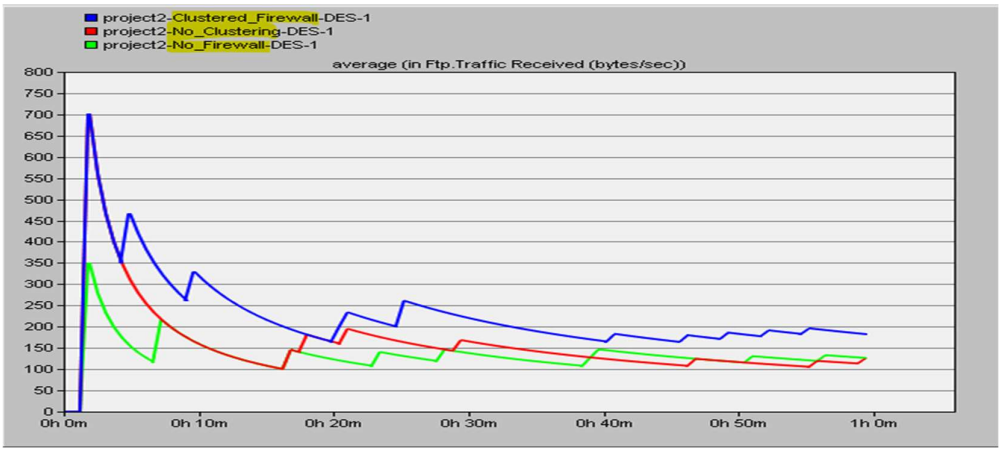


Fig. 7. *Received Data Volume for the File Transfer (FTP) Application.*

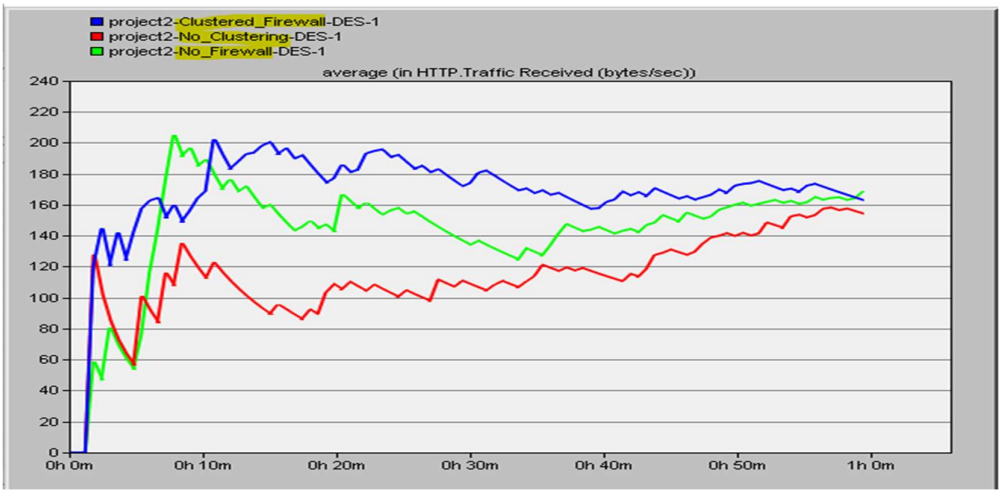


Fig. 8. *Received Data Volume for the Web Browsing (HTTP) Application.*

6. Advantages and Disadvantages

Advantages of the Proposed Method

1. Enhanced Network Security.
2. Improved Performance and Reliability.
3. Efficient Load Balancing.
4. Redundancy and Failover Protection.

Disadvantages of the Proposed Method:

1. Increased Complexity in Configuration.
2. Higher Implementation and Maintenance Costs.
3. Potential Performance Bottlenecks.
4. Complex Troubleshooting and Diagnostics.

7. Conclusion and Future Directions

In conclusion, firewall clustering emerges as a promising strategy to enhance network availability and resilience in the face of evolving cyber security threats and network complexities. Future research could explore the optimization of clustering algorithms, integration with emerging technologies like SDN and AI, and practical implementation challenges in diverse network environments.

Compliance with Ethical Standards

Conflicts of interest: Authors declared that they have no conflict of interest.

Human participants: The conducted research follows the ethical standards and the authors ensured that they have not conducted any studies with human participants or animals.

References:

[1] Noonan, W. and Dubrawsky, I., "Firewall fundamentals", Pearson Education, 2006.
[2] Abu Al-Haija, Q. and Zein-Sabatto, S., "An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks", Electronics, Vol. 9(12), pp.2152, 2020.
[3] E. Ucar, E. Ozhan, "The Analysis of Firewall Policy Through Machine Learning and Data Mining", Wireless Personal Communication, Springer, vol. 96, pp. 2891–2909, 2017.
[4] Al-Shaer, E.,"Managing firewall and network-edge security policies", In 2004 IEEE/IFIP Network Operations and Management Symposium (Vol. 1, p. 926). Seoul: IEEE, 2004. doi:10.1109/NOMS.2004.1317810.
[5] Al-Shaer, E., Hamed, H., Boutaba, R., & Hasan, M. "Conflict classification and analysis of distributed firewall policies", IEEE Journal on Selected Areas in Communications, Vol. 23(10), 2069–2084, 2005. doi:10.1109/JSAC.2005.854119.
[6] Al-Shaer, E.S. and Hamed, H.H., "Firewall policy advisor for anomaly discovery and rule editing", Integrated network management VIII: Managing it all, pp.17-30, 2003.
[7] Ben-Itzhak, Y., Barabash, K., Cohen, R., Levin, A. and Raichstein, E., "EnforSDN: Network policies enforcement with SDN", In 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM) (pp. 80-88), IEEE, 2015, May.
[8] Diekmann, C., Michaelis, J., Haslbeck, M. and Carle, G., 2016, May. Verified iptables firewall analysis. In 2016 IFIP Networking Conference (IFIP Networking) and Workshops (pp. 252-260). IEEE.
[9] Michelle Suh, SaeHyong Park, Byungjoon Lee, SunheeYang, "Building Firewall over the Software-Defined Network Controller", Proceedings of 16th International Conference on Advanced Communication Technology – 2014 – P. 744-748.
[10] Barbir, A. (2002). Network address translation (NAT) terminologies. IETF Network Working Group. Retrieved from https://tools.ietf.org/html/rfc2663
[11] Sobin, C.C., Raychoudhury, V., Marfia, G. and Singla, A., "A survey of routing and data dissemination in delay tolerant networks", Journal of Network and Computer Applications, 67, pp.128-146, 2016.
[12] Li, L., & Li, Y.,"Dynamic firewall policy adaptation in response to network attacks", IEEE Transactions on Parallel and Distributed Systems, Vol. 19(8), 1061-1074, 2008. doi:10.1109/TPDS.2007.70720
[13] Shibata, M., Mega, T., Ooshita, F., Kakugawa, H. and Masuzawa, T., "Uniform deployment of mobile agents in asynchronous rings", In Proceedings of the 2016 ACM Symposium on Principles of Distributed Computing (pp. 415-424), 2016, July.
[14] Chand, S. and Om; H., "Efficient staircase scheme with seamless channel transition mechanism", Computer Networks, Vol. 54(3), pp.462-474, 2010.

[15] Ristic, I., “Bulletproof SSL and TLS: Understanding and deploying SSL/TLS and PKI to secure servers and web applications”, Feisty Duck, 2014.
[16] Velte, A.T., Velte, T.J. and Elsenpeter, R.C., “Cloud computing: a practical approach”, McGraw-Hill, 2010.
[17] Diogenes, Y. and Ozkaya, E., “Cybersecurity-attack and defense strategies: Infrastructure security with red team and blue team tactics”,Packt Publishing Ltd, 2018.
[18] Abu Al-Haija, Q. and Zein-Sabatto, S., “An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks”, Electronics, Vol. 9(12), p.2152, 2020.
[19] K. C. Fuerstenberg, "A new European approach for intersection safety - the EC-Project INTERSAFE," Proceedings. 2005 IEEE Intelligent Transportation Systems, 2005., Vienna, Austria, 2005, pp. 432-436, doi: 10.1109/ITSC.2005.1520072.
[20] J. Y. Lee and S. G. Choi, "Linear programming based hourly peak load shaving method at home area," *16th International Conference on Advanced Communication Technology*, Pyeongchang, Korea (South), 2014, pp. 310-313, doi: 10.1109/ICACT.2014.6778971.