UNIVERSITAS UTPADAKA SWASTIKA
Jl. KS Tubun No.11 Tangerang 15112 Banten, Telp. (021) 5589161-62 Fax. (021) 5589163
JISI Jurnal Ilmiah Sistem Informasi
Vol. 3 No. 02 (2025)
ISSN: 3046-711X

Implementation and Analysis of Multiple Interface Policies through System Feature Visibility on Fortigate FG-60F

*Moh. Alfaujianto[1], Fajar Muttaqi[2], Asep Surahmat[3], Lukas Umbu Zogara[4]

Utpadaka Swastika University, Tangerang, Indonesia 15112
[1]moh.alfaujianto@utpas.ac.id, [2]fajar.muttaqi@utpas.ac.id, [3]asep.surahmat@utpas.ac.id, [4]lukas.zogara@utpas.ac.id
*corresponding author: moh.alfaujianto@utpas.ac.id

Accepted: September 16, 2025 | Published: October 30, 2025

ABSTRACT

Fortigate FG-60F is one of the popular firewall appliances utilized by small and medium-scale networks in managing security. However, some of the needed features such as multiple interface policies are not displayed by default on the user interface. This study explores the functionality and effectiveness of enabling system-feature visibility for easier management of inter-interface policies. Employing an experimental approach, the Fortigate FG-60F device was configured to activate the hidden feature, and subsequently, a set of policy rule scenarios with multiple interfaces were established and tested. The results indicate that supporting system-feature visibility enhances significantly the administrator's ability to implement more specific traffic policies that are commensurate with network topology requirements. Moreover, performance analysis showed no negative impact on device performance after the implementation of multi-interface policy. The findings are expected to serve as a valuable reference for network administrators in optimizing Fortigate FG-60F security capabilities by leveraging advanced, previously hidden features.

KEYWORDS: Fortigate FG-60F, system-feature visibility, multiple interface policies, firewall, network management.

1. Introduction

With the rapid rate of development of information technology, the network systems must not only be trustworthy but also extremely secure. In this context, firewall devices are a vital component to protect data traffic from various forms of cybersecurity attacks, such as malware infection, unauthorized access, and system vulnerability exploitation [1]. One of the most highly sought-after firewall devices employed in small- and medium-scale networks is the Fortigate FG-60F. This device is well known for its outstanding performance, extreme configurability, and support for various network security functions such as Intrusion Prevention System (IPS), web filtering, and application control[2][3].

Although the Fortigate FG-60F offers a great deal of advanced security features, they are not all easily accessible in the standard user interface. One of the features that is normally hidden is support for multiple interface policies, under which handling traffic between multiple network interfaces with some security rules is allowed. To utilize this feature, network administrators must enable the hidden option through the system-feature visibility setting in System menu > Feature Visibility > Advanced Settings[4]. Unfortunately, the lack of official documentations and limited technical knowledge about how this feature operates is typically a limitation in its utilization, especially in medium-level complexity network environments.

Multi-interface policy management is critically essential in the modern dynamic network environment, where various segments of the network must support varying levels of security, i.e., internal networks, DMZs, and guest access [5]. In such settings, administrators need granular control over inter-interface traffic to allow for utmost security, efficiency, and segmentation. Such being the case, the use and enabling of the

system-feature visibility feature becomes a strategic step towards boosting the ability of the Fortigate FG-60F to allow adaptive and organized security policy management [6].

This study will examine how the system-feature visibility feature can be best used to support and manage different interface policies on the Fortigate FG-60F device. In an experimental method, this study will also examine the impacts of using such policies on system performance and flexibility as a whole. The outcomes are expected to contribute practically and theoretically to network management strategy planning as well as information system security strengthening.

2. Literature Review and Research Methodology

2.1 Firewall and Network Security

Firewall is an appliance or system that serves as a network traffic controller on the basis of preestablished security policies. At the network level, it scans, forwards, and rejects data traffic in accordance with some policies [7]. In real life, firewalls can either be hardware or software [8] depending on the size and requirement of the user.

Fortigate, which is a product of Fortinet, provides firewall solutions along with other security capabilities such as intrusion prevention, antivirus, content filtering, and policy management with adaptable levels [8]. The Fortigate FG-60F is just one of the widely used models that can support the needs of small and medium-sized networks with high-performance functions and levels of security that can be tailored [9].

2.2 System Feature Visibility on Fortigate

The concept of feature visibility in network security devices refers to the ability of the system to display or hide certain functions that can be enabled as needed by administrators. In Fortigate, this is implemented through the system-feature visibility option, which allows the activation of advanced functions such as multiple interface policies. From an academic perspective, this mechanism relates to adaptability and flexibility in firewall policy management.

Proposed the Firewall Regulatory Networks (FRN) model, which adopts a bio-inspired approach to automatically regulate firewall policies[10]. This work highlights the importance of visibility control in supporting policy adjustments against evolving cyber threats. Similarly Network intrusion detection using feature fusion with deep learning [11].

Therefore, the literature indicates that feature visibility is not merely a technical functionality in the user interface but has strategic implications for adaptive firewall policy management.

2.3 Multiple Interface Policies

Multiple interface policies refer to security mechanisms that allow administrators to define traffic rules specifically between pairs of network interfaces. This concept is crucial in complex network environments, such as VLANs, DMZs, and multi-cloud infrastructures.

Introduced a meta firewall approach to manage multiple firewalls in virtualized cloud environments[12], enabling administrators to efficiently define policies across interfaces. Found that the majority of firewall misconfigurations stem from limited inter-interface rule definitions, highlighting the necessity of granular policy control[13].

Demonstrated that policy-based network segmentation enhances data security in public information systems, confirming that granular interface-based policies are highly relevant not only in global industry practices but also for strengthening national cyber defense[14].

Overall, the literature underscores that multiple interface policies are a critical element of modern firewall architecture as they support traffic segmentation, enhance configuration flexibility, and reduce

misconfiguration risks that could expose security vulnerabilities.

2.4 Research Methodology

2.4.1 Research Approach

This research employs an experimental approach [15] to evaluate the efficacy of enabling and setting multiple interface policies via the *system-feature visibility* feature on Fortigate FG-60F. The aim is to quantify the impact of such settings on inter-interface traffic management flexibility and overall system performance.

2.4.2 Experimental Environment and Topology

The experiment was conducted in a laboratory network environment that replicates real-world global small to medium-scale scenarios. The Fortigate FG-60F was the main device utilized, with firmware 7.x installed. The three main sections in the network topology were LAN (internal), DMZ (demilitarized zone), and Guest Network. Each segment was attached to a different interface and configured with a distinctive IP subnet.

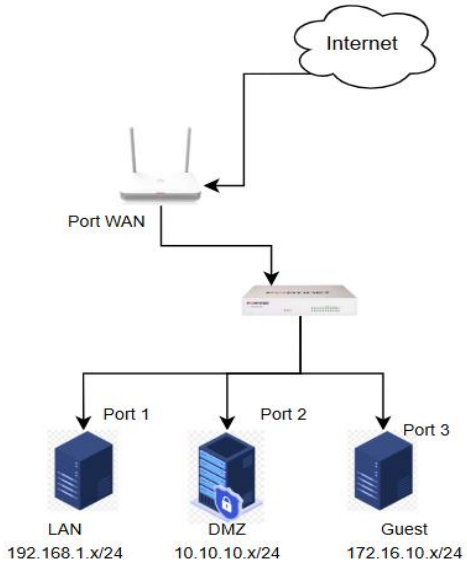

Figure 1. Experimental Network Topology

2.4.3 Experimental Procedures

a. System Preparation:
   a) Fortigate FG-60F installation and initial setup.
   b) All interface IP Address configuration (LAN, DMZ, Guest).
   c) Installation of monitoring tools such as FortiAnalyzer (if necessary), Wireshark, and internal log system.

b. System-Feature Visibility Activation:
   a) Login to Fortigate FG-60F.
   b) Go to the dashboard.
   c) Select the *System* menu.
   d) Choose the *System* submenu.
   e) Launch *Feature Visibility*.
   f) Enable *Multiple Interface Policy*Click sub menu Multiple Interface Policy.

c. Multiple Interface Policy Configuration:
   a) Define security rules between interfaces (e.g., LAN to DMZ, Guest to LAN).
   b) Set up services, actions, and logging for each policy.
   c) Test traffic using various protocols (HTTP, SSH, ICMP).Melakukan uji lalu lintas dengan berbagai protokol (HTTP, SSH, ICMP).

d. Data Collection and Analysis:
   a) Measure performance metrics: latency, throughput, and CPU and memory usage.
   b) Review access logs and traffic control to check the

effectiveness of traffic isolation.

c) Evaluate the flexibility of configuration and policy management.

2.4.4 Research Instruments

Table 1. Research Instruments

Instrumentt	Function
Fortigate FG-60F	Main firewall device to be tested
CLI FortiOS	Concealed feature configuration tool
FortiAnalyzer	Traffic recording and log analysis (optional)
Wireshark	Inter-interface traffic packet capture and analysis tool
PC Client/Server	Used to create test traffic between network segments

2.4.5 Parameters Analyzed

a. Flexibility of configuration: The degree to which rules can be defined in depth and conveniently upon enabling the feature.
b. Traffic isolation effectiveness: The ability to block or allow communication between different network segments.
c. System performance: Changes in CPU usage, memory usage, and firewall response time during policy execution.
d. Throughput: The rate of successful data transfer across interfaces, measured in Mbps, to evaluate how efficiently the firewall processes traffic under different policy scenarios.
e. Latency: The time delay experienced by packets when traversing the firewall, measured in milliseconds, to determine the impact of policy rules on communication speed.
f. Packet loss: The percentage of dropped or lost packets during transmission between interfaces, which serves as an indicator of reliability and stability under different policy configurations.

3. Result and Discussion

3.1 Network Topology for Testing

The testing was carried out on a simple network topology consisting of three Fortigate FG-60F interfaces, as shown in Figure 2:

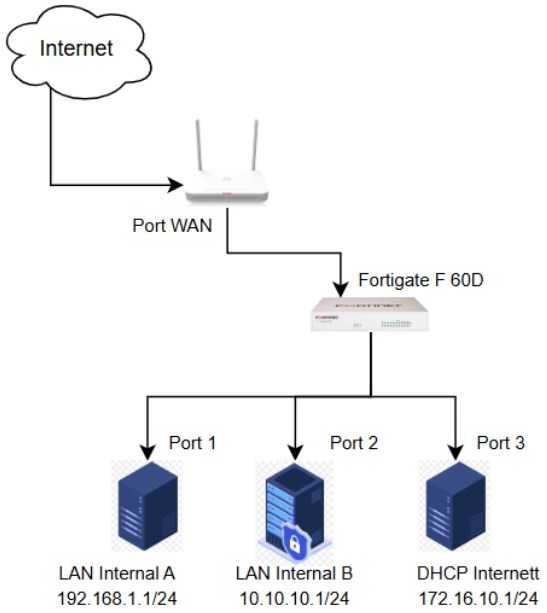

Figure 2. Network Testing Topology

Description:

- Port1 (LAN A):** 192.168.1.1/24 – used for internal client A
- Port2 (LAN B):** 10.10.10.1/24 – used for internal client B
- Port3 (WAN):** DHCP – internet connection

3.2 Configuration of Multiple Interface Policies

After enabling the *gui-multiple-interface-policy* feature, the Fortigate GUI displays additional options for explicitly configuring traffic policies between interfaces. Table 2 shows the applied configuration policies:

Table 2. Interface Policy Configuration

No	Source (Src Intf)	Destination (Dst Intf)	Services	Action	Description
1	LAN A (Port1)	LAN B (Port2)	HTTP, HTTPS	Accept	Allow web access from LAN A → B
2	LAN B (Port2)	LAN A (Port1)	DNS	Accept	Allow only DNS from LAN B → A
3	LAN A (Port1)	WAN (Port3)	Web, Apps Filter	Accept	Restricted internet access from LAN A
4	LAN B (Port2)	WAN (Port3)	Full Access	Accept	Full internet access from LAN B

3.3 User Interface Display

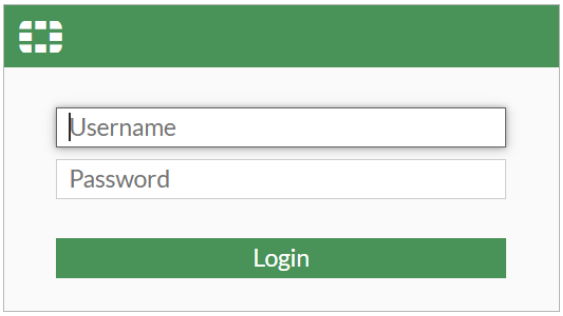

Figure 3. Fortigate Login Screen

The configuration process begins with authentication via the Fortigate login page, as shown in Figure 3. Administrators must enter a username and password to access the system. This step is critical in ensuring that only authorized users can enter the Fortigate Web-based Manager.

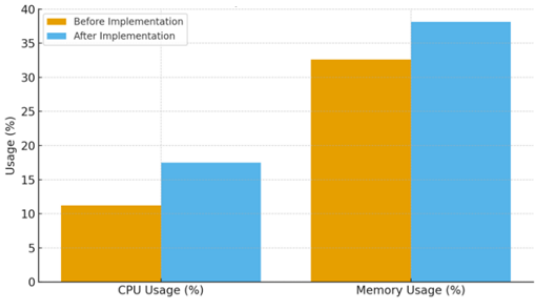

Figure 4. Comparison of Fortigate FG-60F Resource Utilization Before and Aftar Multiple Interface Policy Implementation

The following graph compares CPU and memory usage before and after implementing multiple interface policies on the Fortigate FG-60F. This graph shows that while there is an increase in resource usage, it is within reasonable limits and does not significantly impact device performance.

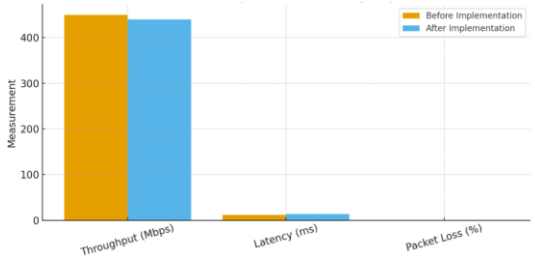

Figure 5. Comparison of Network Performance Metrics Before and Aftar Multiple Interface Policy Implementation

The following additional graphs show a comparison of throughput, latency, and packet loss before and after implementing multiple interface policies.

- Throughput decreased slightly (450 Mbps → 440 Mbps).
- Latency increased slightly (12 ms → 14 ms).
- Packet loss increased slightly (0.5% → 0.7%).

These changes are still within reasonable limits, so the feature implementation is still considered efficient without significantly sacrificing network performance.

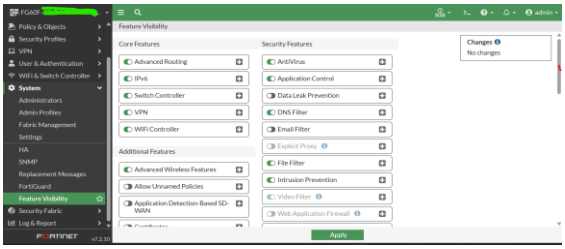

Figure 6. Feature Visibility Menu of Fortigate FG-60F

The next step is to access the *Feature Visibility* menu, which is used to display and manage the device's core functions (Figure 5). On this page, administrators can enable or disable features according to implementation requirements. Important available security features include Antivirus, Application

Control, DNS Filter, Email Filter, and Intrusion Prevention.

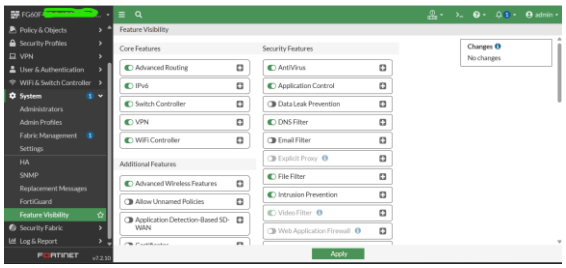

Figure 7. Core Features Menu of Fortigate FG-60F

Subsequently, administrators can perform more detailed activation in the *Core Features* section, as shown in Figure 6. The core features include IPv6, VPN, and Switch Controller, which play an important role in supporting network integration. Activating these features allows the device to function optimally within the applied network topology.

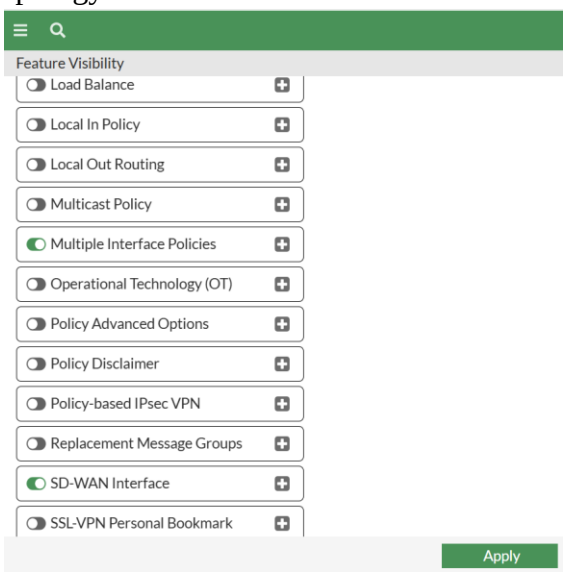

Figure 8. Multiple Interface Policy Activation of Fortigate FG-60F

The final stage of configuration is enabling *Multiple Interface Policies* via the *Feature Visibility* menu, as shown in Figure 7. This feature provides administrators with the flexibility to assign different policies to each network interface, thereby supporting traffic segmentation and enhancing network security. Once all settings have been applied, the administrator must press the **Apply** button to permanently save the configuration.

Through this sequence, the Fortigate configuration process proceeds systematically, beginning with user authentication, device monitoring via the dashboard, and continuing to the activation of both core and advanced features that support network security policies.

3.4 Test Results

Connectivity testing and traffic analysis confirmed that all policies implemented on the Fortigate FG-60F operated as designed. Access patterns between networks were successfully restricted according to requirements. Clients on LAN A were only permitted to access web services in LAN B and restricted internet access, while clients on LAN B were limited to accessing DNS services in LAN A but were granted full access to the internet. This demonstrates that policy-based routing effectively provides segmentation and control of network traffic.

Furthermore, device performance analysis showed that feature activation and the addition of policies did not impose a significant load on system resources. Based on monitoring results using the `diagnose sys top` command, average CPU usage increased from 11.2% to 17.5%, while memory usage rose from 32.6% to 38.1% after implementation (Table 3). These increases remain within acceptable thresholds, well below the device's critical performance limits of 20% for CPU and 40% for memory.\

Table 3. Average Resource Usage of Fortigate FG-60F

Parameter	Before Implementationsi	After Implementation
CPU Usage (%)	11.2	17.5
Memory Usage (%)	32.6	38.1

These results indicate that the Fortigate FG-60F can accommodate the

implementation of multiple interface policies and activation of the *system-feature visibility* option without compromising stability or system performance. Wireshark capture results (Figure 8) further reinforce these findings, showing that traffic between networks was filtered according to the defined policies.

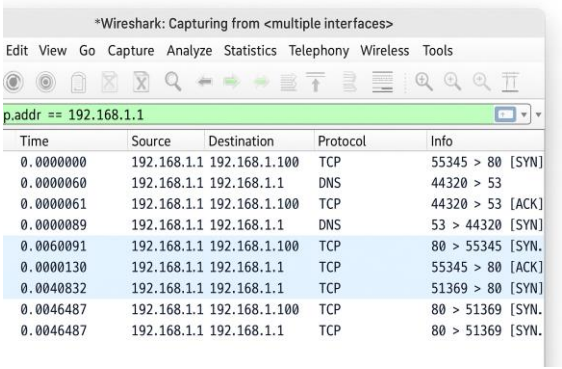

Figure 9. Wireshark Capture Results from Multiple Interfaces of Fortigate FG-60F

Thus, it can be concluded that the implemented policy not only successfully limits access as needed but also maintains efficient resource utilization. This confirms that the implemented configuration method is an effective solution for medium-scale network segmentation needs.

3.5 Discussion

The implementation of multiple interface policies through the system-feature visibility feature provides high flexibility in managing inter-interface traffic, particularly in networks requiring complex segmentation. Without this feature, inter-interface configuration is limited to generic rules, which may leave potential security gaps.

The results also show that enabling this advanced feature remains efficient and does not significantly compromise device performance, making it suitable for medium-scale networks with limited hardware resources.

This study demonstrates that the system-feature visibility feature, often overlooked or poorly documented, can unlock more granular security configurations in the Fortigate FG-60F. Experimental results confirm that the use of multiple interface policies not only enhances the flexibility of traffic management but also maintains system performance stability.

The practical implications of this study are important for network administrators managing infrastructures that require complex segmentation and access control. From an academic perspective, this study provides empirical contributions that may serve as a basis for further developments, such as integrating interface-based policies with automated monitoring systems or AI-driven orchestration platforms. Moreover, this research can serve as a reference for evaluating other hidden features in network security devices that have not yet been fully optimized in practice.

4. Conclusion

Based on the testing and analysis conducted, it can be said that the enforcement of the *system-feature visibility* feature on the Fortigate FG-60F indeed brought advanced configuration features, including multiple interface policies, within reach that are inaccessible under the standard user interface. Enforcing specific inter-interface policies was successfully accomplished and as per the planned scenarios without overloading system performance.

This level of success demonstrates that the research objective—namely, examining the effectiveness of activating hidden features to support flexible network security management—was fully achieved. Furthermore, the findings confirm that optimizing such hidden features can serve as a strategic approach in the development of adaptive and efficient network security systems, especially in small to medium-scale network environments with complex segmentation requirements.

5. Recommendations

As a follow-up step, it is also proposed that future work explore combining multiple interface policies with real-time security monitoring solutions and script-based or API-based configuration automation. Further, testing can be extended to more complex topologies, such as the deployment of VLANs, VPNs, or multi-layer firewall integration. Comparison testing with firewall products from other vendors may also serve to draw broader lessons regarding the utility of similar features in terms of interoperability and resource optimization.

References

[1] S. N. Adzimi, H. A. Alfasih, F. N. G. Ramadhan, S. N. Neyman, and A. Setiawan, "Implementasi Konfigurasi Firewall dan Sistem Deteksi Intrusi menggunakan Debian," J. Internet Softw. Eng., vol. 1, no. 4, p. 12, 2024, doi: 10.47134/pjise.v1i4.2681.

[2] E. Dwi Setiawan, Ridwansyah, and M. Raharjo, "Perancangan Keamanan Jaringan Next-Generation Firewall Menggunakan Router Fortinet Pada Pt. Alodokter Teknologi Solusi," J. Inform. Terpadu, vol. 9, no. 1, pp. 34–39, 2023, [Online]. Available: https://journal.nurulfikri.ac.id/index.php/JIT

[3] R. Kurniawan and F. Prakoso, "Implementasi Metode IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System) untuk Meningkatkan Keamanan Jaringan," SENTINEL, vol. 3, pp. 231–242, Jan. 2020, doi: 10.56622/sentineljournal.v3i1.20.

[4] M. Alfaujianto, "Utilizing LED Usage on FortiManager Device as a Software Monitoring Indicator for Fortinet Access Points," Sci. J. Inf. Syst., vol. 2, no. 2, pp. 22–26, 2024.

[5] D. Conorich, "Internet Security: Securing the Perimeter," Local Area Netw., 2020, doi: 10.1201/9781003069393-c35.

[6] F. Nielson, R. R. Hansen, and H. Nielson, "Adaptive Security Policies," pp. 280–294, 2020, doi: 10.1007/978-3-030-61470-6_17.

[7] P. Grace, J. Saini, S. Sharma, and R. Gandhi, "Introduction to 'Network Security' Firewall," Ind. Eng. J., 2022, doi: 10.36893/iej.2022.v51i8.032-038.

[8] T. V. Krishna and P. Karthik, "Dominance of Hardware Firewalls and Denial of Firewall Attacks (Case Study BlackNurse Attack)," Int. J. Sci. Res., 2022, doi: 10.21275/sr22330164222.

[9] N. G. Firewall, "FortiGate ® FortiWiFi 60F Series," pp. 1–6.

[10] Q. Duan and E. Al-Shaer, "Firewall Regulatory Networks for Autonomous Cyber Defense," 2025. [Online]. Available: https://arxiv.org/abs/2505.01436

[11] A. Ayantayo et al., "Network intrusion detection using feature fusion with deep learning," J. Big Data, vol. 10, pp. 1–24, 2023, doi: 10.1186/s40537-023-00834-0.

[12] G. Carvalho, I. Woungang, and A. Anpalagan, "Cloud Firewall Under Bursty and Correlated Data Traffic: A Theoretical Analysis," IEEE Trans. Cloud Comput., vol. 10, pp. 1620–1633, 2022, doi: 10.1109/TCC.2020.3000674.

[13] M. Alicea, M. Alicea, and I. Alsmadi, "Digital Commons @ Texas A & M University-San Antonio Misconfiguration in Firewalls and Network Access Controls : Literature Review Misconfiguration in Firewalls and Network Access Controls : Literature Review," 2021.

[14] S. K. Mani, K. Hsieh, S. Segarra, R. Chandra, Y. Zhou, and S. Kandula, "Securing Public Cloud Networks with Efficient Role-based Micro-Segmentation," pp. 1033–1048, 2025, [Online]. Available: https://consensus.app/papers/securing-public-cloud-networks-with-efficient-rolebased-mani-

kandula/376c2b5d053559999438aaf8706c0814/

[15] L. Ceragioli, P. Degano, and L. Galletta, "Can my firewall system enforce this policy?," Comput. Secur., vol. 117, p. 102683, 2022, doi: 10.1016/j.cose.2022.102683.