kriativ.tech

Edition No. 9 – 11-10-2021
ISSN Print: 1646-9976 | ISSN Online: 2184-223X |
http://www.kriativ-tech.com
DOI: 10.31112/kriativ-tech-2021-10-59

Next-Generation Firewalls: Concept, Features, and Their Benefits

Pedro Ramos Brandao
Coordinator Professor at ISTEC – pedro.brandao@istec.pt
José Almeida
Master's student in Computing at ISTEC – jose.almeida@my.istec.pt

Abstract: ***A firewall is a solution for securing computer networks; it can be a software program or a hardware device that allows or inhibits access to or from a system. Firewalls are used regularly to prevent untrusted Internet-originating traffic from accessing private systems and networks. All connection requests and packets that intend to pass through the firewall are analyzed according to the configured security criteria and denied or allowed. By rule, firewalls are designed to protect against unauthorized and abusive access. This paper is intended to provide a historical background on the technological evolution of firewalls and present the concept, functionalities, benefits of use, and aspects to be taken into account when choosing and setting firewalls.***

Keywords: *Firewall, next-generation firewall, information security, protection, technological evolution.*

I. Introduction

According to Sêmola [1], data security is defined as an area dedicated to the knowledge about the protection of information assets, namely, against improper and/ or unauthorized access. According to ISO 27001[2], physical actions and logical actions must be encompassed. Confidentiality, integrity, and availability are three pillars of data security and are part of the data protection process [3]. Although ISO 27001 does not define the technical details, ISO 27002 [4] provides recommendations on security controls to mitigate availability, integrity, and confidentiality risks. Conducting a risk assessment to identify the protection needed is of utmost importance for the composition and definition of your rules. The firewall is one of the security controls specified in ISO 27002. It is intended to provide security to the network you are protecting by monitoring and enforcing controls on who can and cannot access it. The firewall is composed of components that have characteristics such as traffic processing; whether it is from outside in or inside out must pass through the firewall; traffic will only be allowed to pass through if it is following the security policies [5] that are configured. The constant evolution of information technology infrastructures and the enhancement of increasingly sophisticated cyber threats have driven the generational development of firewalls. While these are not exactly a new concept, they have been known since the 1980s and the need to restrict access to existing networks. The first generation of firewalls, packet filters, was introduced in 1988 by the company Digital Equipment Corporation, limited to a packet filter that was responsible for performing packet evaluation of the TCP/IP protocol suite. The second-generation firewalls [6], called proxy firewall or application firewall, operated at the ISO / OSI model level [7], could interpret some protocols and applications (DNS, FTP, or HTTP) and detect suspicious usage on ports other than those used by the default protocols. The third generation of firewalls (stateful), known in the '90s, had as its main characteristic the ability to trace the connections that went through the firewall. It also stored data in memory, such as the beginning and end of each link, IP addresses, or

ports used. This generational evolution of firewalls has driven the arrival of the fourth and next generation of firewalls as a commercial solution for and to secure computer networks. Renowned companies with a significant presence in the market, such as Checkpoint and Forninet, have made considerable investments to improve this type of solution, namely, in packet inspection mechanisms, profiled traffic with application characteristics, implementation of a tool for examining packets and flows to assess the impact and help make decisions based on their relevance. Also, in this generation, the use of personal firewalls began both in corporate environments and for personal use, and the concept of endpoint security was born. The aim was to guarantee its security from the point where data is generated or shared. The benefits gained through this type of technology given organizations' need for data protection and the increasingly refined threats have led to the next-generation firewalls that we will discuss in more detail in the next chapter.

II. State-of-the-art

Recent attacks and penetrations into high-security corporate systems lead to reflections on the sufficiency of existing protection mechanisms [8] and place challenges on how unauthorized access [9] to critical systems [11] can be prevented. The coverage, product integration, and features in next-generation firewalls increase their effectiveness [12], yet it is still necessary to keep up with and monitor known threats [13]. Its coverage, i.e., the ability to deep traffic inspection [14], application control, the ability to detect and block suspicious activities [15], customizable content filtering, antivirus, and malware function, encryption [16], compression, bandwidth management, and quality of service (QoS) capability enable the protection of networks and systems against sophisticated attacks [17]. Furthermore, its scalability and flexibility allow for modeling and activation according to the moment's needs [18]. Next-generation firewalls are administered features, comprehensive user interfaces with well-defined access profiling [19] on access to the intended resource types. Typically, these accesses are provided in the form of a command line or a web format. The documentation [20] of this type of solution, feature activation, rule definition, configuration analysis, vulnerabilities, assessments, trends, traceability, reporting, and alerting is complete, precise, and objective [21]. According to the leading suppliers of next-generation firewalls, the global enterprise market is growing fast, aware of the organization's needs [22] and security requirements, regardless of its size or area of activity, and its development has enabled the simplification of tasks [23] for professionals in the are of business. In parallel with the incorporation of intelligence, threat learning capabilities, and with their ecosystem shown in figure 1, they'll become even more robust products, strengthening their security perimeter.

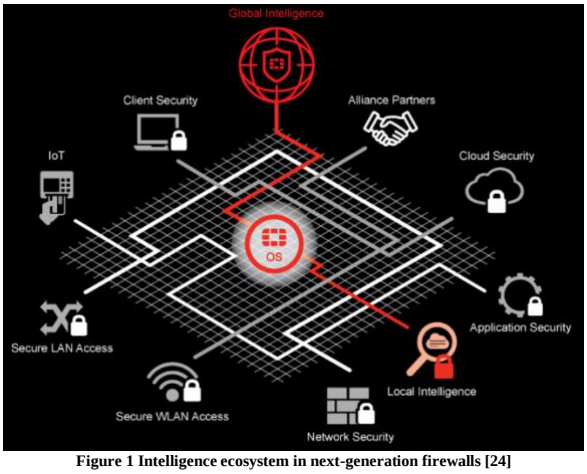

Figure 1 Intelligence ecosystem in next-generation firewalls [24]

III. Features, concepts, and benefits

Next-generation firewalls feature powerful, modern functionalities and can be cloud-hosted. In addition, they incorporate additional features such as intelligence from outside their solution, intrusion prevention, application control, and identification when compared to traditional models. According to Gartner [25], to be considered a next-generation firewall, it must include the common functionalities of a traditional firewall, it must have an integrated intrusion prevention system [26], and it must allow application control and validate user identification. However, due to the lack of regulation of this concept, each manufacturer identifies the minimum requirements and adds features they consider innovative to position and

differentiate themselves in the market to make their solution both more robust and efficient.

Its comprehensive protection allows you to detect and block sophisticated, large-scale attacks such as advanced persistent threats and malware, and it features an application and user policy-driven architecture. The learning capability of the environment allows you to monitor and manage events in real-time. Unlike the premise of traditional rule-based firewalls, next-generation firewalls have their administration access-oriented, essential in today's new paradigm and challenges of mobility, social networking, cloud computing, and collaboration. The ability to inspect the data packet header and its payload improves malware detection and mitigates malicious traffic. It is also possible to decrypt, analyze SSL / TLS traffic, and re-encrypt, thus acting as a proxy, essential for sites using secure HTTPS connections. Intelligent network traffic monitoring, sanitization of potential viruses, content filtering and segmentation, usage profiling, and the possibility of generating threat lists all increase its users' operational performance and productivity. The main benefit of next-generation firewalls is intrinsic to their very function, i.e., to maintain protection against threats, whether already identified or unidentified, within applications and improve application control through deep inspection and data analysis capabilities. They also allow you to visualize the entire surface of an attack and provide integration with cloud and multi-cloud formats. Its simplicity, versatility, feature aggregation, and unification will enable you to reduce the complexity of security components, simplify processes, and substantially reduce its operational cost. Furthermore, it allows greater control of the applications and services consumed by the users, thus improving the network.de.

IV. Performance

The implementation of next-generation firewalls that can be installed and configured on physical equipment [27] or virtual machines [28] and in a cloud format. The chosen structure and the functionalities that are enabled in the solution directly impact the solution's availability and performance. Some considerations that should be taken into account and that contribute to a better performing solution after the security requirements, circumstances, and needs have been identified are its sizing, high availability, component redundancy if applicable, the universe of users, number of connections per second, packets per second, the level of event logging, transfer rates, connection response time, processing load, its scalability or its price.

A firewall can also be optimized by removing unnecessary rules and objects that may actively contribute to performance degradation. Overlapping rules should also be minimized; placing the most used rules on top, depending on the manufacturer, may also influence performance and remove permissive or seasonal rules. Objects that require DNS lookups on all traffic should be avoided, matching the speed of the firewall interfaces to the related equipment, traffic separation, and VPN processing whenever possible, and performing software updates when available.

IV. Examples

Nowadays, there are several manufacturers in the market that offer firewalls with state-of-the-art technology and high performance. However, according to the renowned consulting firm GARTNER [29] and its magic quadrant depicted in figure 2, in the quadrant of market leaders, Palo Alto is the leading manufacturer of firewall solutions.

Figure 2 Gartner Recognition Magic Quadrant for Firewalls

The platform for rating and analyzing software and information technology services by IT professionals and decision-makers - Gartner Peer Insights allows us to notice in figure 3 that the overall choices of enterprise customers and their positioning in the magic quadrant are different from the analysis performed in figure 1.

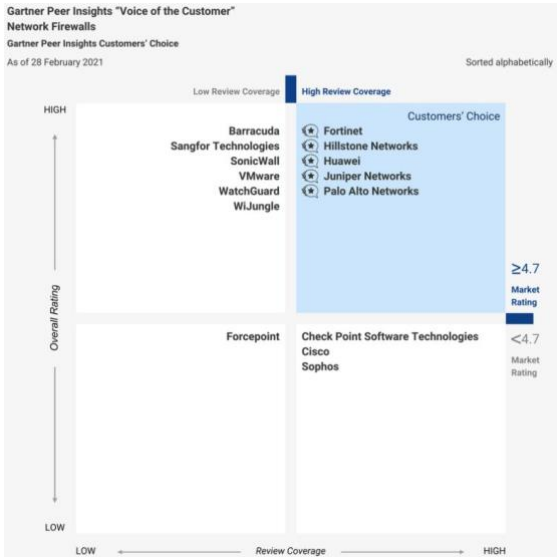

Figure 3 Gartner Peer Insights Magic Quadrant - Voice of the Customer Firewalls [30]

Figures 4 and 5 illustrate examples of the performance specifications of two major firewall manufacturers, Fortinet and Palo Alto, identified in Gartner's leader quadrant, wherein the differences in the performance and capacity component can be noted.

Table 1: PA-7000 Series Performance and Capacities

	PA-7080*	PA-7050*	PA-7000 DPC-A	PA-7000-100G-NPC-A
Firewall throughput (HTTP/appmix)†	610/687 Gbps	370/416 Gbps	73.8/83.1 Gbps	55.5/62.5 Gbps
Threat Prevention throughput (HTTP/appmix)§	342/405 Gbps	200/243 Gbps	38.5/46.3 Gbps	27.7/34.6 Gbps
IPsec VPN throughput‡	334 Gbps	200 Gbps	37.1 Gbps	28 Gbps
Max sessions	416M	245M	43M	32M
New sessions per second**	6M	4M	825,000	624,000
Virtual systems (base/max)††	25/225	25/225	–	–

Figure 4 Palo Alto PA7000 Serie Performance [31]

FORTIGATE	7060E-8 / 7060E-8-(DC)•	7040E-8 / 7040E-8-(DC)	7030E
Hardware Specifications			
Fortinet Processor Module (FPM) Slots	4	2	2
Fortinet Interface Module (FIM) Slots	2	2	1
Shelf Manager	2	1	1
System Performance and Capacity			
Firewall Throughput (1518 / 512 / 64 byte, UDP)	630 / 630 / 340 Gbps	315 / 310 / 200 Gbps	155 / 155 / 155 Gbps
Firewall Latency (64 byte, UDP)	7.00 µs	7.00 µs	7.00 µs
Firewall Throughput (Packet per Second)	510 Mpps	300 Mpps	220 Mpps
Concurrent Sessions (TCP)	320 Million	160 Million	160 Million
New Sessions/Sec (TCP)	1.8 Million	950,000	900,000
Firewall Policies	200,000	200,000	200,000
IPsec VPN Throughput (512 byte)	100 Gbps	100 Gbps	40 Gbps
Gateway-to-Gateway IPsec VPN Tunnels	16,000	16,000	16,000
Client-to-Gateway IPsec VPN Tunnels	64,000	64,000	64,000
SSL-VPN Throughput	15 Gbps	15 Gbps	15 Gbps
Concurrent SSL-VPN Users (Recommended Maximum)	48,000	48,000	48,000
IPS Throughput (Enterprise Mix) ¹	120 / 200 Gbps	60 / 100 Gbps	60 Gbps
SSL Inspection Throughput ²	79.9 / 120 Gbps	39.9 / 60 Gbps	39.9 Gbps
SSL Inspection CPS (IPS, avg. HTTPS) ³	47,000	32,500	32,500
SSL Inspection Concurrent Session (IPS, avg. HTTPS) ³	24 Million	12 Million	12 Million
Application Control Throughput ²	160 Gbps	80 Gbps	65 Gbps
NGFW Throughput ⁴	100 / 120 Gbps	50 / 60 Gbps	50 Gbps
Threat Protection Throughput ⁵	80 / 96 Gbps	40 / 48 Gbps	35 Gbps
CAPWAP Throughput	N/A	N/A	N/A
Virtual Domains (Default / Maximum)	10 / 500	10 / 500	10 / 500
Maximum Number of FortiSwitches Supported	256	256	256
Maximum Number of FortiAPs (Total / Tunnel Mode)	N/A	N/A	N/A
High Availability Configurations	A/A and A/P	A/A and A/P	A/A and A/P

Figure 5 Fortigate 7000 Serie Performance [32]

V. Practical examples

In recent years several next-generation firewall solutions with cutting-edge technology have emerged on the market from global security manufacturers such as Fortinet, Checkpoint, Palo Alto, Sophos, or Cisco. Managing this type of solution requires efforts from security professionals in routine activities and according to the good practices that must be undertaken. Furthermore, centralizing features can make it challenging to handle them and respond to urgent actions. Therefore, the solution's technical knowledge becomes imperative, and the pleasantness of the available interfaces can be critical factors for the commitment and timely response by professionals in the area. The following figures are screenshots of the administration panels of five of the world's most prominent next-generation firewall vendors, in which you can notice the formats of the administration interfaces and how simple they are to set up.

a) Fortinet's solution provides a user-friendly interface allowing a fast, granular, and intuitive configuration, as seen in figure 6.

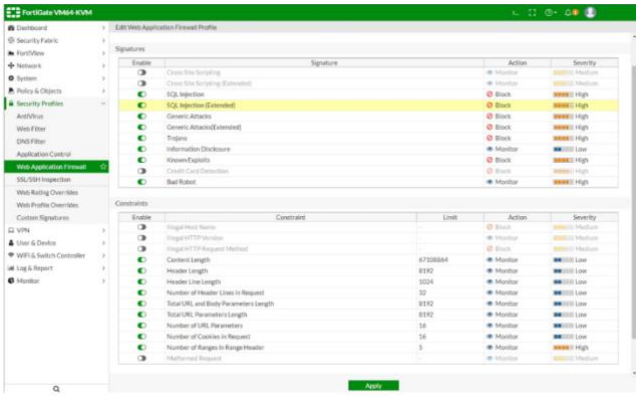

Figure 6 Admin Dashboard: Fortigate

b) Checkpoint's solution provides a unified management dashboard with a simplistic and flexible interface, as shown in figure 7.

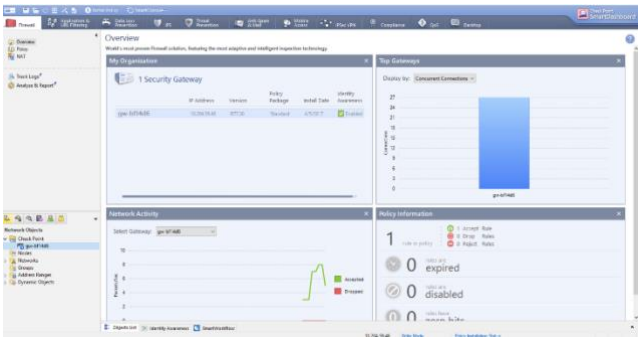

Figure 7 Admin Dashboard: Security Management

c) Palo Alto's solution features an objective look and feels, allowing the quick creation and implementation of policies to control applications, users, and content, as shown in figure 8.

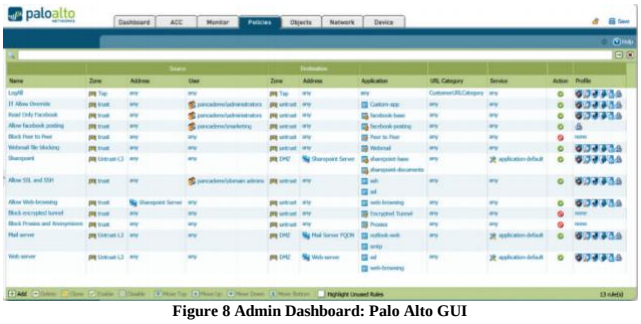

Figure 8 Admin Dashboard: Palo Alto GUI

d) Sophos' solution provides an out-of-the-box peripheral view of the network, applications, and users from its control dashboard, as shown in figure 9.

Figure 9 Admin Dashboard: Network Security Control Center

e) Cisco's solution provides a robust, agile, and versatile administration dashboard that allows for very detailed configuration, as shown in figure 10.

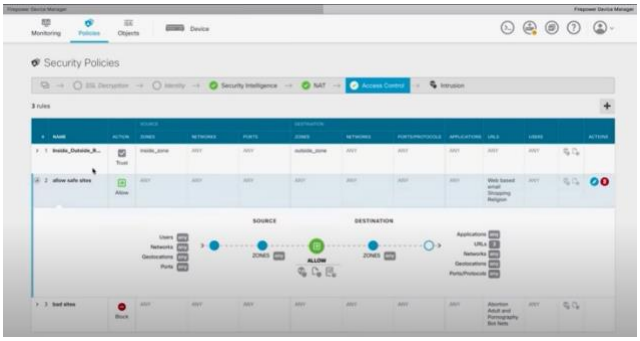

Figure 10 Admin Dashboard: Firewall Manager

VI. Discussion

Next-generation firewalls portfolio is vast, and their architectures are becoming increasingly complex, making it more challenging to secure your perimeter. Professionals are looking for simplicity in implementing and managing this type of solution, which is presented as an investment priority by IT departments in organizations. The attack sophistication and distribution require in-depth technical knowledge of mitigation actions and, consequently, handling the new generation firewall administration tools present within an organization. Its cost-benefit can be measured through the architecture, the security controls that can be implemented, the cost of support, evolutionary or intelligence-based engine, and signature updates. The number of

devices, connections, users, and other needs is essential to understand and identify. Otherwise, they will significantly penalize the data transfer rate or influence the choice of solution manufacturer or the physical or virtual equipment. Periodic audits and reevaluations are also essential to assess the solution's efficiency in engine updates or the intelligence mechanisms adopted to set configurations. The visibility and monitoring of next-generation firewalls must have the broadest possible coverage of their perimeter; an end-to-end view of the entire infrastructure is essential to monitor activity in real time permanently and block any potential threats that may be detected. The possibility of creating automatisms for security tasks such as impact assessments, policy adjustments, user identification, and their ability to integrate with other corporate systems with security architectures or their agility in detecting threats should be considered when evaluating this type of solution.

VII. Conclusion

The author's purpose was to present the advantages of using next-generation firewalls and understand their differences compared to conventional firewalls. It was possible to notice firewalls evolution that at first, they were limited to display status. They evolved and added layers of protection such as web filtering, anti-spam, and intrusion detection until the arrival of next-generation firewalls that incorporated application controls and application perception to learn and apply rules according to customer and application behaviors. The author's approach is to conclude that no environment can be completely secure by installing a firewall in isolation and expecting the network to be protected against attackers. The firewall should be regarded as one component in a suite of technological security solutions for enhanced protection. It is essential to be aware of the environmental requirements to be protected to find the best solutions on the market. As the firewall component has become a crucial tool, and new generation firewalls should be adopted. Conventional firewalls have neither an application view nor intelligence, that is, the ability to learn about the environment to be protected. Therefore, the selection should be for the one that best fits the identified requirements. Once installed, a good and efficient configuration should be applied to assure a robust, performant, and effective protection of your network and your security perimeter.

VIII. References

[1] SÊMOLA, Marcos. Gestão da Segurança da Informação, uma visão Executiva. (Information Security Management, an Executive View). Rio de Janeiro: Elsevier,2003

[2] ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação — Requisitos. (Information Technology - Security Techniques - Information Security Management Systems - Requirements).

[3] BEAL, Adriana. Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações (Information Security: principles and best practices for the protection of information assets within organizations) – São Paulo: Atlas, 2005.

[4] ABNT NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação. (Information Technology - Security Techniques - Code of practice for information security controls).

[5] KUROSE James F., ROSS, Keith W. (2010), Redes de Computadores e a Internet 5a. Edição. (Computer Networks and the Internet 5th Edition). 2010. Pearson Publishing.

[6] CHAURE, Rupali. An Implementation of Anomaly Detection Mechanism for Centralized and Distributed Firewalls. NRI Institute of Information Science and Technology. 2010. Bhopal, India.

[7] Tanenbaum, Andrew S. Redes de Computadores - Tradução da 4ª Edição. (Computer Networks - Translation of the 4th Edition). 2003. Editora Campus / Elsevier (Campus / Elsevier Publisher)

[8] Kagermann H., Wahlster, W., & Helbig, J. Recommendations for implementing the strategic initiative Industrie 4.0, Final report of the Industrie 4.0 Working Group. 2013

[9] Ashibani, Y. & Mahmoud, H. M. Cyber-physical systems security: Analysis, challenges, and solutions. Computers & Security. 2017

[10] Ahram, T., Arman, S., Saman, S., Daniels, J., & Amaba, B. Blockchain Technology Innovations. Conference: IEEE-Technology-and-Engineering-Management-Society Conference. 2017

[11] Babiceanu, R. F., & Seker, R. Cybersecurity and resilience modeling for software-defined networks-based manufacturing application. In: Service Orientation in Holonic and Multi-Agent Manufacturing. Studies in Computational Intelligence. Springer, Cham. 2017

[12] Corallo, A., Lazo, i M., & Lezzi, M. Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Science Direct, Elsevier, Computers in Industry. 2020
[13] Dimase, D., Collier, Z.A., Heffner, K., et al. Systems engineering framework for cyber-physical security and resilience. 2015
[14] European Union Agency for Network and Information Security (ENISA). Good Practice for Security of Internet of Things in the Context of Smart Manufacturing, ENISA. 2018
[15] Greitzer, F. L., J., Purl, Y. M., & Leong P. J. S. Positioning your organization to respond to insider threats. IEEE Engineering Management Review. 2019
[16] Industrial Control Systems Cyber Emergency Response Team ICS-CERT. Annual Assessment Report. National Cybersecurity and Communications Integration Center (NCCIC). 2016
[17] Kaplan J., Weinberg, A., & Sharma, S. Meeting the cybersecurity challenge. Digit. McKinsey. 2011
[18] Liu, Y., &Xu, X. Industry 4.0 and cloud manufacturing: A comparative analysis. Journal of Manufacturing Science and Engineering. 2017
[19] Lu, T., Lin J., Zhao, L., Li, Y., & Peng, Y. A security architecture in cyber-physical systems: security theories, analysis simulation, and application fields. 2015
[20] National Security & Defense. Memorandum on Space Policy Directive 5 –Cybersecurity. https://www.whitehouse.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems. 2020
[21] Zhu, Q., Craig, R., & Basar, T. A hierarchical security architecture for cyber-physical systems. In: 2011 4th International Symposium on Resilient Control Systems. 2011
[22] Theron, P., & Lazari, A. The IACS Cybersecurity Certification Framework (ICCF). Lessons from the 2017 study of state of the art., EUR 29237 EN, Publications Office of the European Union, Luxembourg, ISBN 978-92-79-85968-7, 10.2760/856808, JRC111611. 2018
[23] Stouffer, K., Pillitteri, V., Lightman, S., Abrams, M., & Hahn, A. NIST Special Publication 800-82. Guide to Industrial Control Systems (ICS) Security. National Institute of Standard and Technology (NIST). 2015
[24] Fortinet the Next Step in Enterprise Firewall Evolution. https://www.fortinet.com/blog/industry-trends/the-next-step-in-enterprise-firewall-evolution
[25] Gartner. Available at: http://www.gartner.com/it-glossary/next-generationfirewalls-ngfws. 2015
[26] MANECA, Miguel António Moreira Boavida. Firewalls: A Próxima Geração, 2018. (The Next Generation, 2018).
[27]. Shinder T.W., Shimonski R.J., Shinder D.L., 2003, The Best Damn Firewall Book Period" Syngress Publishing, Rockland.
[28] Y. Yongxin, 2011, The comparative study on network firewalls performance, 2011 IEEE 3rd International Conference on Communication Software and Networks.
[29] GARTNER Global Research and Advisory Company. www.gartner.com
[30] GARTNER Peer Insights. https://www.gartner.com/reviews/market/network-firewalls
[31] Palo Alto Networks. https://www.paloaltonetworks.com/resources/datasheets/pa-7000-series
[32] Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_7000_Series_Bundle.pdf