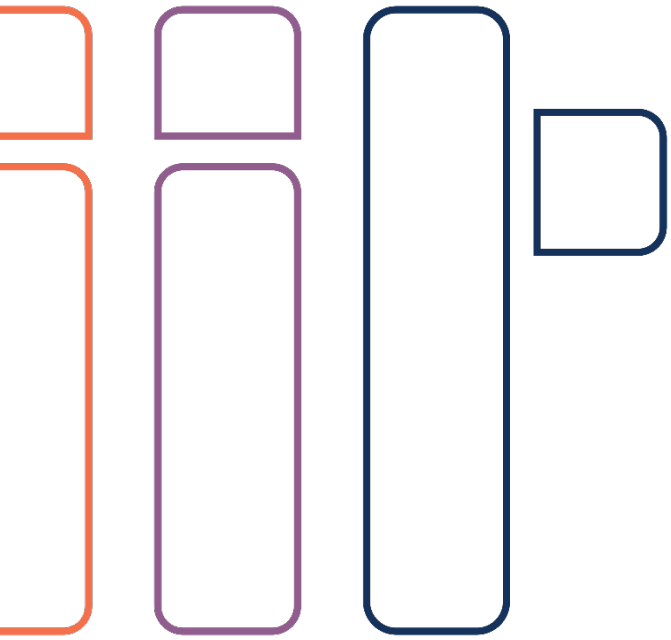

TECHNICAL REPORT

IIT TR-08/2021

Technical and administrative considerations on acquiring a NGFW-based network security solution

A. Gebrehiwot, F. Lauria, I. Sannicandro

ISTITUTO DI INFORMATICA E TELEMATICA

Consiglio Nazionale delle Ricerche

Technical and administrative considerations on acquiring a NGFW-based network security solution

Abraham Gebrehiwot, Filippo Maria Lauria, Irene Sannicandro
firstname.lastname@iit.cnr.it

Institute of Informatics and Telematics, Italian National Research Council
via G. Moruzzi, 1 - 56124 Pisa, Italy

Abstract

The network security solution in use at the Pisa Research Area since 2008, is based on two on premise Next Generation Firewalls (NGFWs) capable of protecting the network infrastructure using typical NGWF features such as application awareness, threat prevention, anti-virus, anti-spyware, URL filtering, file blocking, DDoS protection, etc. Unlike traditional packet filtering firewalls, NGFWs enforce security policies not only based on network traffic attributes (e.g. IP addresses, protocol numbers and port numbers, etc.) but also on other types of attributes, such as the username of an authenticated user, the name of the used application, the type of the transported data, etc. Furthermore, NGFWs support the concept of zone-based firewalling and allow the configuration of individual protection rules regardless of the used network layer protocol, thus implementing a dual stack (IPv4/IPv6) firewall.

There are various NGFW manufacturers in the market. Therefore, a public organization in need of acquiring a NGFW-based network security solution, should compare various products in order to select the best quality-price ratio. Unfortunately, at the time of writing of this document, there are no standard methods, i.e. benchmarks, for objectively evaluating and comparing performance indicators of NGFW devices from different manufacturers. For this reason, organizations are forced to make a choice by following a logical process that takes into account a series of different evaluation criteria (technical, practical, economical, administrative, etc.).

This document tries to address the various issues that an organization might face during the phases of selection and acquisition of a security solution based on NGFW technologies, mainly considering both technical and administrative aspects.

Keywords:
firewall, NGFW, next generation firewall, network security, acquisition strategy

Features of an adequate NGFW-based network security solution

General features

Considering that a single NGWF equipment is both a networking and a security device, the technical staff[1] of a public organization in need of acquiring a NGFW-based network security solution, has to take into account that a proper solution should, at least, offer the following features:

- the ability to analyze bi-directional traffic of both unencrypted and encrypted sessions[2] which are nowadays heavily used within any enterprise network. The main goal is to perform proper security checks[3] on all network traffic types, including encrypted sessions;
- the ability to be managed both by a Command Line Interface (CLI) and a web interface (Web-GUI):
    - both ways should allow the total control of all the functions offered by the equipment. The use of additional management systems based on separate applications should be avoided[4];
    - both the CLI and the Web-GUI should be user friendly and provide easy-to-use features, with the aim of allowing the technical staff to perform a fast recovery from potential threats or faults;
- the ability to provide a software API that allows to automate the integration of some information coming from external sources, within the NGFW-based solution. For example, an organization which uses a custom application for user mapping[5] can decide to automatically integrate this information into the NGFW-based security solution, with the aim of using usernames, instead of IPv4/IPv6 addresses, within security policies;
- the ability to recognize threats by inspecting each session at the application layer (L7) and beyond[6]. For example, the ability to recognize a virus in an email attachment, or a malicious file downloaded from the web, etc. In other words, traffic filtering should overcome the limitations of both *packet filtering firewalls*[7] and *stateful packet firewalls*[8].
- the ability to apply security rules regardless of the used Layer 3 (IPv4/IPv6) protocol[9], which implies that each NGFW equipment of the solution should be a full dual stack (IPv4/IPv6) equipment;
- the ability to constantly receive only the updates released by the manufacturer for both the operating system and all the necessary services, such as application and threat signatures, URL database, as well as the maintenance support in case of hardware and/or software failures;

---

[1] i.e. network and firewall administrators
[2] HTTPS, FTPS, SSH, etc.
[3] identify the presence of viruses or the use of unauthorized applications or other threats
[4] because separate applications may require the technical staff to have additional vendor-specific skills and knowledge
[5] i.e. tracking the IPv4/IPv6 addresses assigned to all the devices used by a generic user and their username
[6] i.e. Deep Packet Inspection (DPI)
[7] *packet filtering firewalls* filter traffic based solely on attributes coming from network layer (L3) and transport layer (L4), e.g. source address, destination address, protocol name or port number
[8] leveraging the ability of tracking connections, *stateful packet firewalls* filter traffic based also on connection state
[9] e.g. recognize the youtube application regardless of the used Layer 3 network protocol

- the ability to make multiple configuration changes and save them all at once, both through Web-GUI and CLI. These changes should not be immediately operational or applied as the *"running configuration"* of each NGFW device. Instead, there should be a system command capable of checking in advance the actual functionality and consistency of the multiple changes and successively apply them to the *"running configuration"* with a single configuration transaction, only if the outcome of the previous checks is positive. In addition, there should be the ability to revert to one of the previous configuration versions in case of errors.

Hardware features and performances

The hardware architecture, including features and performances, varies widely from manufacturer to manufacturer. Despite this, a proper NGFW-based network security solution should at least provide the following hardware features:

it must guarantee the physical segregation *per device,* i.e. each NGFW device must provide distinct and dedicated hardware resources for both the *management part* (called *control plane)* and for the *forwarding part* (called *data plane).* The control plane and the data plane must use physically separated hardware, in order to allow the devices to efficiently use the available computational resources and guarantee the use of the management plane even in the presence of flooding or DoS attacks. In particular, a NGFW device must be able to forward the network traffic exclusively through the hardware resources dedicated to the data plane, without affecting the control plane. For these reasons, it is necessary to request the manufacturer for a simplified technical diagram containing a short description of the architecture, in order to be able to evaluate the hardware architecture of the proposed NGFW equipment.

In addition, each equipment should have several high throughput physical ethernet interfaces exclusively used for network traffic forwarding (data plane) and at least one management and one console interface.

The interfaces used for the network traffic should be capable of being configured for operating as transparent, Layer 2 (L2), Layer 3 (L3) and listening (TAP) operational modes. Furthermore, each interface should be capable of being configured in one of the possible operational modes regardless of how the other interfaces are configured. The interfaces that support the transparent operating modes, L2 and L3 should be capable of being expandable, using the 802.1Q protocol (VLAN Tagging), as virtual interfaces that should be able to be associated with distinct security zones. This feature is essential to allow the *micro segmentation* of the networking infrastructure allowing inspection of the network traffic between the various intra and inter security zones.

In order to avoid a single point of failure, a valid NGFW-based network security solution:

- must be implemented using devices with redundant essential physical elements such as power supply, cooling, etc.
- must support the possibility of configuring multiple devices in High Availability with active/active or active/passive modes: in case of the isolation of one device (e.g. caused by a software/hardware fault, ecc.) the remaining devices must be able to automatically guarantee the operational continuity, without causing any disruption of service to end users.

It is also necessary to select the NGFW devices that have an overall height (in Rack Unit) lower than the available height in the rack used for their deployment.

Other important hardware features and performance indicators to consider during the evaluation process of a generic NGFW equipment are:

- the maximum throughput declared by the manufacturer with threat prevention enabled[10] in Gbps;
- the maximum number of sessions;
- the number of new sessions/sec;
- the maximum number of virtual firewalls;
- the maximum throughput of IPsec VPN in Gbps.

Advanced cyber security features

In addition to traditional IT security features, a valid NGFW-based network security solution must *natively provide*[11] advanced security features such as:

- the identification of thousands of applications and *sub-applications*[12] based on signatures through DPI and not on static associations such as:
  - *transport protocol/port number ↔ application*[13],
  - *URL or IP Address ↔ application*[14];
- the identification of groups of applications based on predefined or custom *application categories*[15];
- the identification of a single user or a group of users based on the user mapping feature, regardless of the used devices or IP addresses;
- the identification of hosts by IP address, FQDN or by IP range including the use of wildcard and CIDR notation;
- the ability of geolocating IP addresses;
- the ability of inspecting the traffic in transit for real-time identification of any threats (e.g. viruses, spyware) or attacks (e.g. through a Intrusion Prevention System (IPS));

---

[10] during the performance evaluation process the following functionalities should be turned on: application identification, intrusion prevention system (IPS), antivirus, anti-spyware, zero-day detection, file blocking. Unfortunately, there is no standard benchmarking methodology that all NGFW manufacturers use to measure performances.

[11] without relying on third-party solutions, i.e. using a proprietary operating system based on a proprietary software architecture

[12] for example, in the case of facebook application, it is necessary to distinguish the generic facebook application from facebook chat, facebook posting, facebook video, facebook audio, etc.

[13] e.g. statically mapping UDP/53 as DNS

[14] for example mapping www.facebook.com statically to a generic facebook application

[15] e.g. all peer-to-peer applications, all instant messaging applications, etc.

- the identification of botnets using an anti-botnet engine;
- the identification and mitigation of DoS attacks for protecting entire security zones or specific services;
- the use of an extremely fast and efficient zero-day vulnerability analysis;
- the identification of traffic to and from specific URLs or URL categories, through the use of URL filtering and URL categorization engines.

Through the aforementioned Web-GUI, the technical staff must be able to easily create security rules to filter the traffic (allow, deny, etc.), using the entities listed above (applications, application categories, application groups, users, user groups, hosts, host groups, geolocation, threats, URLs, etc.). Furthermore, the implementation of the listed security features and functions must be provided through natively integrated modules implemented within the software stack of the operating system of the NGFW devices. In other words, it should not be implemented through the use of additional and/or external and/or third-party software or hardware modules.

In addition, each NGFW equipment is recommended to:

- have the ability to apply machine learning (ML) algorithms and techniques to prevent unknown attacks/cyber threats and identify unusual device behaviors. At the time of writing of this document, Machine Learning algorithms capable of suggesting and protecting potential flaws related to security aspects, are available and can be used in the cybersecurity contest[16];
- be equipped with an easy-to-use analytical tool that allows the technical staff to analyze the logs collected by the device itself[17] and present them graphically, directly from the Web-GUI. This feature must ensure a thorough visibility of both the traffic and the network threats, highlighting the trends of activities in progress on the network and allowing the technical staff to interact with the displayed data[18], with the aim of increasing the enforcement of a security policy;
- support the ability to control unknown or non-standard applications, also allowing the technical staff to create custom application signatures directly from the Web-GUI, without the need for new software development by the manufacturer;

[16] for example, they can be used for verifying the consistency of a security policy in use, with the goal of reducing the potential human error and avoiding potential security faults
[17] network traffic, suspicious activities, anomalies, etc.
[18] e.g. providing the ability to query and analyze specific types of data

- have a correlation engine for objects and events related to all the different security related *activities and functions*[19]. This correlation engine is required to:
    - be not limited to a simple aggregated view of information but should also guarantee an effective correlation functions in terms of event analysis;
    - be natively embedded on each NGFW device and use the computational resources of the control plane, without impacting on the performance level of the data plane;
    - guarantee an aggregated and correlated real-time view of suspicious activities or events related to malicious activities, based on tables or graphs available from the Web-GUI.

  As mentioned above, the correlation function needs to be available on each NGFW device natively. Solutions based on additional and/or external and/or third-party hardware or software modules to the NGFW equipment itself should not be preferred or accepted;
- be equipped with advanced reporting functions, without using additional and/or external and/or third-party hardware or software modules. These reporting functions must be provided by each NGFW device and must allow to:
    - generate reports
        - preferably by using templates based on different types of information[20];
        - defined by the technical staff using custom reports;
        - that highlight the activity of a single specific user or a group of users, by specifying a selected time interval;
    - export the generated reports in various formats, such as PDF, CSV and XML formats.

  These reports should be generated through the Web-GUI, using dedicated display and/or export features. Each NGFW should also be able to generate reports automatically in a scheduled manner (e.g. daily at a certain time) and send them to pre configured email addresses;
- be integrated with an external cloud-based data mining system, capable of detecting new threats from the initial propagation phase, conveying the experience of multiple external sources (feeders) being able to share third-party indicators of compromise (IoC), e.g. lists of IP addresses or URLs, etc. These indicators of compromise should be able to be integrated into the security rules defined within each NGFW in the form of dynamic objects.

[19] e.g. firewall, IPS, anti-malware, URL Filtering, etc.
[20] e.g. traffic, applications, threat, URL, etc.

Networking features

Since NGFWs are also networking devices, they also have to provide common networking protocols and features and allow the technical staff to manage and configure them through the previously mentioned Web-UI. Common networking features that each single NGFW device has to provide are:

OSPF v2/v3 with graceful restart, multi-protocol BGP with graceful restart, RIP, static routing, Policy-based forwarding, Point-to-point protocol over Ethernet (PPPoE), DHCP support for dynamic address assignment, PIM-SM, PIM-SSM, IGMP (v1, v2, and v3), Bidirectional Forwarding Detection (BFD), 802.1Q VLAN tags (a total of 4094), Aggregate interfaces (802.3ad), LACP, the following NAT modes: static IP, dynamic IP, dynamic IP and port (PAT), NAT64, NPTv6.

Secondly, each NGFW equipment should provide traffic control features that go beyond the ability to merely permit or deny particular applications, allowing to manage bandwidth or prioritize application level traffic. In other words, it should provide traffic classification and traffic shaping features.

Finally, each NGFW device should provide "Policy-based forwarding" (PBF) features. It must not be based exclusively on network layer (L3) and transport layer (L4) attributes[21] and it should be capable of forwarding the traffic according to the selected application flows (L7).

Maintenance and warranty services

Based on our experience, the minimum life cycle of an on premise NGFW-based network security solution may range from three to six years. For this reason, it is advisable to verify that all the selected hardware components are covered by the manufacturer's direct warranty and maintenance for at least three years and renewable for another three years.

The maintenance service should include:

- the replacements of damaged units including the NGFW devices themselves and all the hardware spare parts;
- the download of software updates released by the manufacturer, for both the operating system and all the required security services indicated in the previous paragraphs[22].

In cases of security incidents, the manufacturer maintenance service should also include an advanced support, in order to help the technical staff in the incident response process. In particular, the manufacturer's *threat intelligence experts* should be able to support the technical staff in making initial investigations, by facilitating the collection of indexes and indicators of compromise (IoC) from compromised systems, in order to speed up the incident response operation.

[21] e.g. source address, destination address, protocol name or port number
[22] threat signatures, application signatures, URL categories, etc.

Supplied products, terms and conditions verification

All the supplied products should be brand new and provided in their original packaging. Hardware and software licenses should be original and specifically issued by the manufacturer for the organization that is acquiring the NGFW-based network security solution. Such organization should be the first purchaser of the products and the first licensee of any copy of the software and the included products. In other words, the product should not be counterfeit, reconditioned or coming from illegal or unauthorized channels. The supplier must also provide all the certificates of the originality, origin and warranty of the supplied products and should not provide software licenses that are illegal (in violation of intellectual property rights) or from unauthorized sources. To this end, the organization is advised to carry out checks and controls with the goal of documenting the origin of the products.

The supplied products should also not require subsequent acquisition of additional hardware and/or software components or, in any case, they should not need modifications that require further economic effort for their operation.

The contract must include termination clauses in the case of non-compliance to the previous requirements or in the case of other contractual discrepancies (e.g. discrepancies emerged from the tests carried out by the technical staff on the received products, etc.).

Further considerations on acquiring a NGFW-based network security solution

Technical consideration

An organization in need of acquiring a NGFW-based network security solution should go through a selection process of the proper product. The technical staff of that organization may resort to a comparison of different technical specifications declared by each manufacturer. Unfortunately, this approach does not allow to make an accurate evaluation for the following reasons:

- the operating system and the management interfaces of the various solutions differ from manufacturer to manufacturer. This implies that the technical staff cannot *a priori* have an in-depth knowledge of how all NGFW-based network security solutions available on the market work. It is common to have a steep learning curve, sometimes months and even years to become expert on using a specific new product. For this reason, it is difficult to acquire a generic solution and use it directly in a production environment. Furthermore, introducing a new generic solution, without an in-depth knowledge of how it works and how it should be used, may also increase the risk of cybersecurity incidents, with serious inconveniences on the proper functionality of the IT infrastructure;

- in most cases, the reported technical details and performance indicators refer to measurements taken in *different contexts*[23];
- common cyber security terminologies assume different meanings, depending on the manufacturer that uses them.

In addition, replacing an existing NGFW-based solution with a different one from another manufacturer, may lead to the reconfiguration of the existing IT infrastructure. In particular, the use of a product belonging to a specific manufacturer plays a central role in the configuration, securing and monitoring the IT infrastructure. Consequently, there is the risk that moving to a solution of a different manufacturer may cause compatibility issues with other network devices and/or configurations in use.

For these reasons, the technical staff of the organization that need to acquire a NGFW-based security solution cannot easily make an objective comparison between solutions provided by different manufacturers.

Moreover, there are others technical-practical aspects that the technical staff of the organization has to take into account:

- when possible, it is highly recommended to test the essential performances and functionalities declared by the manufacturer before acquiring the NGFW-based solution;
- in order to have the highest compatibility, the staff should avoid *hybrid solutions*[24]. In other words, within a single organization, it is recommended to use NGFW-based solutions of the same model and manufacturer;
- the staff has to select easy-to-use solutions, in order to meet the needs of the organization based on the criteria discussed in the previous paragraphs;
- the staff must be trained continuously, with the aim of having an in-depth knowledge of different NGFW-based solutions from different vendors; however, it is recommended to avoid frequent change of models and manufacturers.

[23] for example, each manufacturer may use different testbed environments, incompatible networking and/or firewalling configurations, etc.
[24] i.e. solutions that involve different models and manufacturers

Administrative consideration

In the light of the aforementioned considerations, taking into consideration Italian laws and regulations, it is appropriate to proceed with a good acquisition strategy aiming to:

- choose the best legal and contractual arrangement to be used, in order to meet the identified need;
- choose an appropriate contract value that will be decisive in the choice of the procedure to be carried out. *ANAC*[25] has stated that the contracting authority may resort to a comparison of market price lists, previous offers for identical or similar contracts or an analysis of the prices charged to other authorities. In any other case, the comparison of cost estimates from two or more suppliers represents a best practice also in the light of the competition principle;
- pay attention to the rotation principle and the risk of artificial splitting.

For example, in case there is the need to acquire an evolutionary maintenance service, for the technical reasons indicated in the preceding paragraphs, the conditions exist for the acquisition through a negotiated procedure without a call for tenders pursuant to Article 63 paragraph 3 letter b of Legislative Decree 50/2016 as amended and supplemented[26].

Although this is a standardised service, so the adequacy of the price could be assessed through market price lists or by comparing prices charged by other administrations, it is advisable to ask for quotations in order to carry out the market survey especially when the amount of the auction base is quite important.

[25] Italian National Anti-Corruption Authority

[26] Article 63 paragraph 3 letter b: in the case of additional deliveries by the original supplier which are intended either as a partial replacement of supplies or installations or as the extension of existing supplies or installations where a change of supplier would oblige the contracting authority to acquire supplies having different technical characteristics which would result in incompatibility or disproportionate technical difficulties in operation and maintenance; the length of such contracts and recurrent contracts may not, as a general rule, exceed three years.

By requesting several quotes, even if only for the market survey and therefore not binding on the contracting authority, it must be ensured that the different economic operators involved are treated in accordance with the constitutionally guaranteed principle of impartiality. Accordingly, the comparison of quotations may not take place on the basis of the criteria used for negotiated procedures but rather on the basis of a criterion for choosing the best contractor which is discretionary yet complies with the principle of impartiality and transparency; comparative assessment may take place on the basis of non-discriminatory criteria taking into account, but not limited to:

- the experience and technical expertise;
- the previous fruitful cooperation;
- the cost of the service.

Once the contractor has been identified, it is possible to proceed with a direct negotiation on the *Mepa*[27] with the single operator to assign the tender.

Conclusions

As previously described in this document, an organization in need of acquiring a NGFW-based network security solution should consider different aspects both technical and administrative. Firstly, this document has covered generic features, hardware features and performance indicators, advanced cyber security features and networking features that a proper NGFW-based network security solution should provide. Secondly, the document has provided considerations on the maintenance and warranty services and the verification of the supplied products and the terms and conditions. Finally, the document has presented further technical and administrative considerations on acquiring a NGFW-based network security solution.

[27] Electronic market of Italian public administrations

References

- Firewall / Types - Wikipedia
  https://en.wikipedia.org/wiki/Firewall_(computing)

- Deep packet inspection - Wikipedia
  https://en.wikipedia.org/wiki/Deep_packet_inspection

- Comparison of firewalls / Firewall appliances - Wikipedia
  https://en.wikipedia.org/wiki/Comparison_of_firewalls

- Network Firewalls Reviews and Ratings - Gartner
  https://www.gartner.com/reviews/market/network-firewalls

- Gartner Magic Quadrant for Network Firewalls - Gartner
  https://www.gartner.com/en/documents/4007809

- Benchmarking Methodology for Network Security Device Performance - IETF
  https://datatracker.ietf.org/doc/html/draft-ietf-bmwg-ngfw-performance-11

- FortiGate Network Security Platform - Top Selling Models Matrix - Fortinet
  https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/Fortinet_Product_Matrix.pdf

- Palo Alto Networks ML-Powered Next-Generation Firewall Specifications and Features Summary - Palo Alto Networks
  https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/product-summary-specsheet

- Cisco Secure Firewall - Cisco Systems
  https://www.cisco.com/c/en/us/products/security/firewalls/index.html

- Decreto legislativo 18 aprile 2016, n. 50 - Codice dei contratti pubblici - Bosetti, Gatti & partners
  https://www.bosettiegatti.eu/public/2016_0050_codice_contratti.pdf