An Architecture to Manage Performance and Reliability on Hybrid Cloud-Based Firewalling

Fouad Guenane*, **Hajer Boujezza***, **Michele Nogueira**†, **Guy Pujolle***
*Sorbonne Universities, UPMC Univ Paris 06, UMR 7606, LIP6, F-75005, Paris, France
†NR2 - Federal University of Paranà, Brazil
Email: {fouad.guenane, hajer.boujezza, guy.pujolle}@upmc.fr; michele@inf.ufpr.br

***Abstract*—Firewalls are the first defense line for the networking services and applications. With the advent of virtualization and Cloud Computing, the explosive growth of network-based services, investigations have emphasized the limitations of conventional firewalls. However, despite of being impressively significant to improve security, cloud-based firewalling approaches still experience severe performance and reliability issues that can lead to non use of these services by companies. Hence, our work presents an efficient architecture to manage performance and reliability on a hybrid cloud-based firewalling service. Being composed of a physical and a virtual part, the architecture follows an approach that supports and complements basic physical firewall functionalities with virtual ones. The architecture was deployed and experimental results show that the proposed approach improve the computational power of traditional firewall with the support of cloud-based firewalling service.**

***Index Terms*—Security as a Service, Secaas, Firewall, Network security.**

I. Introduction

Firewalls are the primary defense line for networking services and applications. Hence, these impose significant cost for most business, especially smaller companies [1]. Firewall is the key element of the majority of network security architectures, being deployed not only at "the edge" of the network, but further and further as service [2]. The cost of physical firewall deployment and maintenance is estimated as $116,075 for the first year and an annual cost of $108,200 for a midsize US company with 5Mbps of Internet connectivity [1]. This high cost is resulted from the necessity of hiring administrators for firewall deployment, maintenance, monitoring, and tuning. Businesses also need to expend on training firewall administrators on new emerging firewall technologies. Also, as new firewall technologies are being developed and new types of attacks launch constantly, operational firewalls often need to be upgraded to new ones with higher capacity and capabilities.

In order to reduce firewall management and deployment costs, businesses outsource their firewalls to Cloud Providers, as part of their *Software as a Service* (SaaS) and *utility Computing* provided by the Cloud [3], [4]. The current demand for faster services forces organizations to often deploy and maintain innovative solutions. As Internet traffic and connection speed up very fast nowadays, the traditional firewalls would have to analyze a huge traffic and to enforce security policies thus firewall processing becomes the network bottleneck.

With the advent of virtualization and Cloud Computing, physical firewalls are no more designed to inspect and filter the vast amount of traffic from virtual machines [5]. In contrast, researchers develop Cloud-based firewalls, as a service, running in a virtualized environment and providing usual techniques, such as packet filtering and monitoring services [6].

In general, Cloud-based firewalls follow two approaches that we describe more in section II: (1) the virtual firewall is deployed in the hypervisor, and (2) it is positioned as a bridge between different network segments, becoming itself a virtual machine. However, such approaches introduce new issues and challenges mainly related to network performance and reliability [3]. They bring real improvements for network security, but in no case they solve performance issues [7]. There is a fundamental trade-off between the simplicity and flexibility brought by abstraction in Cloud Computing versus the ability to control services behavior by having visibility and control over the underlying resource infrastructure [8]. The deployment in the hypervisor, for instance, allows the firewall to manage only local traffic, since it is not considered a part of the network. Furthermore, many researchers point out the challenges related to performance, latency and reliability [3], [4]. In [3], authors present service continuity and availability as one of the main challenges for Cloud Computing. Organizations still worry about whether utility Computing services will have adequate availability, being this worry emphasized considering a firewall service.

Hence, this work presents an innovative and efficient architecture to manage performance and reliability in an hybrid cloud-based firewall service. The proposed architecture improves both the Throughput and the ability to detect abnormalities by increasing the computational power of physical firewalls by several orders of magnitude. The additional Computing power is achieved by the concept of virtual firewalls using the vast resources offered by the Cloud. The objective is to support and complete the basic physical firewall capacities with a virtual firewall in the Cloud with a very high computing power to deal with the huge traffic. Experimental results present significant improvements in latency, memory and CPU performance by the proposed architecture.

This paper is organized as follows. Section II presents the background and related works. Section III describes the proposed architecture. Section IV presents tests and results. Finally, Section V concludes the paper and outlines future works.

978-1-4799-0913-1/14/$31.00

II. Background & Related Work

Firewall security policies are an ordered filtering rule that define actions performed over packets to satisfy special conditions. There are three main types of firewall: packet filter, stateful inspection and application firewall [9], [10], [11]. The oldest and the basic one is the **packet filter**, in which routers examine packets at the network or transport layers, allowing them to deliver good performance. It has some advantages such as adaptation to routing, low overhead, high throughput and inexpensive. However, its security level is very low.

Stateful inspection provides a capacity of application-level filtering while operating at the transport layer [12]. Stateful inspection improves the functions of packet filters by tracking the state of connections and blocking packets that deviate from certain states. However, this implies the use of more resources and more complexity for managing firewall operations [12]. **Application firewalls** contain a proxy agent acting as a transparent link between two hosts that wish to communicate with each other and never allows a direct connection between them. Thus, application firewalls do not protect against attacks at lower layers, they require a separate program per application and have a poor performance for a high resource consumption.

Next Generation Firewall (NGFW) represents an evolution of the traditional firewall [13] by integrating a variety of security features as the anti-spam filtering, anti-virus software, a detection system or intrusion prevention (IDS/IPS) in one box or platform integrated, NGFWs also provide more granular inspection and greater visibility of traffic than traditional firewall [14].

While Cloud Computing increases business agility, scalability and efficiency, it also introduces new security risks and concerns because the traditional physical security solutions become obsolete since traffic of virtual networks does not necessarily leave the physical server [5]. Until now virtualization solution vendors offers virtual firewalls as the best solution for isolation and network analysis traffic declined under different names, for Cisco it is the Virtual Security Gateway (VSG) distributed on physical nodes in the Cloud, it qualifies as a firewall for specific hypervisor, VMware has invested in terms of safety is therefore available with a battery of measurement called vShield Product.

A virtual firewall as previously defined is a firewall service running in a virtualized environment and providing the usual packet filtering and monitoring services that a physical firewall would provide [6]. It is available in two modes: **hypervisor mode** and **bridge mode**. The first is a virtual firewall running in the virtual machine monitor (VMM) [2]. Hence, it is not considered as a part of the network and it manages only local traffic. The second is positioned as a bridge between different network segments and it becomes itself a virtual machine. It has attracted attention from the point of view of performance by allocating resources on demand, but the migration of virtual machines becomes problematic for this type of virtual firewall because it must manage different security policies [2].

In this section, we over-viewed the various existing solutions for firewall deployment in physical or virtual environments. Physical firewalls are limited by the hardware capacity and its deployment model adds considerable financial cost. Virtual firewalls are promising because it is not limited by resources and allows a dynamic deployment. However, virtual firewalls are powerless against the massive attacks from the outside of the virtualized domain, compromising its reliability. Hence, we propose an architecture that consists of both physical and virtual approaches, thus uses the powerful of Cloud for service availability at the massive increase of the traffic under attack or not and we present our architecture in the next section.

III. Hybrid Architecture

We work on improving performance by increasing computational power of physical firewall to adapt existing technologies for the next generation broadband network. The innovation of our work is to propose an hybrid architecture based on Security As A Service model (SecaaS) provided by the Cloud. Our architecture is **hybrid** because it consists of two main parts, the virtual and physical part. The virtual part is composed of virtual machines, in which every virtual machine executes firewall programs with many functionalities such as analysis, monitoring, reporting and many others with a dynamic resources provisioning. The physical part represents the physical firewall of the company. A company agrees to purchase a security service offered by the Cloud Provider, this service comes as an additional resource that complements existing ones. The main idea is to redirect traffic destined to the physical firewall when this one is overloaded to virtual firewalls in the Cloud.

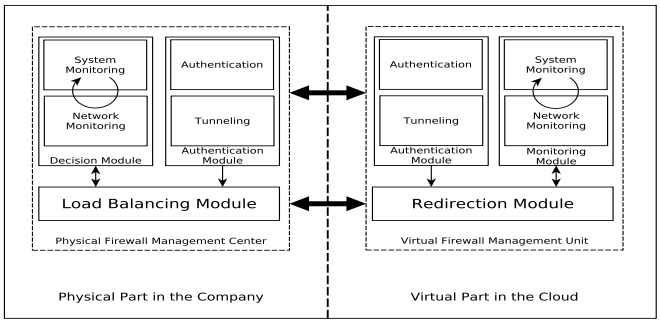

Fig. 1. Proposed Architecture framework

The **physical part** is a developed module in the physical firewall located in the company's headquarters, Physical Firewall Management Center (PFMC) which is illustrated in Fig. 1 is a management tool that helps us to provide greater performance and efficient architecture management. It comprises of three main modules: *authentication*, *decision* and *load balancing*. These modules are explained as follows.

A. Authentication module

It was first necessary to work in a Trusted Execution Environment (TEE) based on signed certificates (valid). For this goal, two steps are required: authentication and establishment

of secure tunnel between the physical and virtual firewall. The authentication module offers the possibility to use different authentication protocols, because it is based on a radius server, which can use the open source tool freeradius[1] allowing users authenticate via PAP, CHAP, MS-CHAP, MS-CHAPv2, SIP Digest, and all common EAP methods. We suggest to use EAP-TLS based on SSL protocol because the SSL handshake is performed over EAP, whereas, on the Internet, the SSL handshake is conducted through Transmission Control Protocol (TCP).

B. Decision Module

The decision module is the main component of the PFMC, its mission is to determine when traffic must be transferred or not to virtual firewalls in order to increase the overload of physical firewall. For this purpose, decision module needs to deal the system and network monitoring modules which is in charge of collecting a local ability information. This allow the decision module to detect if the firewall is overloaded or not. If it is overloaded then the decision is made to transfer a percentage of input traffic to the virtual firewall for analyzing. If the firewall is not overloaded, the module continues its monitoring function. For now, the percentage of redirected traffic is defined by the network administrator of the company, it would be interesting and more optimal to create a program that will calculate the percentage based on overloading the firewall. Supplementary information about the overload of the virtual firewall are sent from Monitoring Module of the Virtual Firewall Management Unit (VFMU) to slow down or change the transfer's parameters as destination (to another virtual firewall) or flow type (FTP, HTTP and SMTP).

C. Load Balancing Module

Load balancing module receives its orders from the decision module. The first function of this module is the ability to set up a shared traffic and therefore to apply the rule stated by the decision module. It works in a very dynamic way, specifying port, protocol and IP address. To operate, the module needs to receive the network information of the authenticate virtual firewall from the authentication module and the query from the decision module. However, to be more optimal we suggest to use Least Session Algorithm (LSA) for sharing the incoming traffic. As we noted, the percentage is allocated by the network administrator. The load balancing module needs to interact with the authentication module to get trusted information as IP-address and port number where redirect traffic. The second function is to switch the incoming traffic from the virtual firewall to the LAN of the company without any analysis procedure.

The **virtual part** consists in a set of virtual machines that is offers by a Cloud Providers based on IaaS model. Each virtual machine runs as a firewall and its job is to carefully analyze data sent from the physical firewall based on company configuration and redirect the legitimate traffic to Local Area Network (LAN). Hence, every virtual firewall is equipped with a Virtual Firewall Management Unit (VFMU) showed in Fig. 1. The VFMU is the device that allows virtual firewall to interact with the physical one (i.e. with PFMC). Comprised of three modules: Authentication Module, Monitoring Module and Redirection Module. The Authentication Module cooperates with its counterpart in the PFMC and has the same configuration.

[1] http://freeradius.org

D. Monitoring Module

As its name suggests, it monitors the network and systems parameters of the virtual firewall. If the virtual firewall is on overload, it sends an alert to the decision module of the physical firewall. Else, the module continues its monitoring function.

E. Redirection Module

Redirection module must to receive traffic only from the physical firewall and it rejects all other traffic. It must also forward the packets considered as legitimate by the virtual firewall to the corporate LAN via the PFMC.

IV. Tests and results

In order to observe the effectiveness of our architecture, we chose to develop a real test-bed and analyze two deployment scenario of our hybrid architecture. We discuss in detail the deployment and tests scenario that we have employed as proof-of-concept.

We present our two secure deployment scenario to provide a high computational power for physical firewall. The first deployment is "Secure Forwarding Architecture" (SFA), and the second one is "Secure Sharing Architecture". In both cases, we have used benefits of virtualization as dynamic provisioning of resources. All communications between virtual and physical firewall are via secure tunneling based on secure protocol EAP-TLS. We consider as baseline deployment a "Single firewall architecture" (Basic) to which the two others are compared. Note that we use this baseline since it is a basic topology commonly used by most of small and medium-sized businesses.

Secure Forwarding Architecture (SFA): In this architecture we have two principal actors: the physical (PF) and virtual firewall (VF) nodes. We compare the PF node in this topology to a simple router. It just redirects all incoming packets. We employ the virtual node to ensure filtering function. The idea is to watch all income traffic and redirect accepted packets to the company's firewall after inspection. This inspection's based on the same security policy which was specified in the basic architecture.

Secure sharing architecture (SSA): The SSA we have the same components but deployed in a different manner. The traditional firewall provides the filtering function, but it may delegate inspection to one or many virtual firewalls. In fact, we have implemented a monitor network and system properties in order to trigger load balancing. Consequently, it (PF) distributes workloads across one or multiple virtual

firewalls. The load balancer forwards a part of traffic to one or more of the "back-end" virtual firewall, which usually replies to the load balancer.

For each entering flow, the "load balancer" (physical firewall) shares all incoming packets using the "least session" algorithm. This dynamic load balancing method selects the server that currently has the smallest number in the persistence table entries, and works best in environments where the virtual equipment used in load balancing has similar capabilities. The distribution of connections is based on various aspects of analysis of server performance in real time, such as the current number of connections per node or the response time of the fastest node. Once the load balancing is set up, we have to intercept traffic on the virtual machine in order to be analyzed and forwarded to the physical firewall again and as it is illustrated in the previous architecture that only accepted packets will be redirected to company's firewall. In this step, our goal is to minimize signaling messages and responses time, liberate resources as well increase QoS.

Our testbed consists of several elements as shown in Fig. 2. Firewall gateway: to ensure filtering function we use Netfilter tool. Server/Client: We use this configuration to know the level of QoS and evaluate network performance improvements of our deployment using Iperf, it has a client and server functionality, and can measure the throughput between the two ends. Virtual Firewall: a virtual machine to ensure filtering function we use NetFilter with the same rules as the firewall gateway.

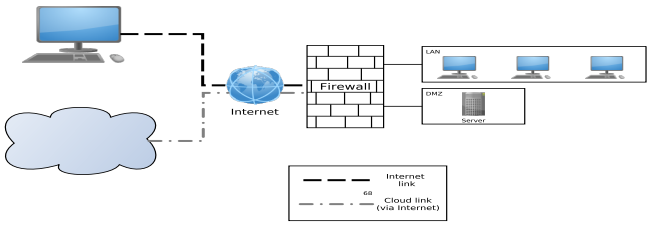

Fig. 2. Virtual firewall testbed

We run our three deployment architectures: Basic, SFP and SSA. For each one we tested the variation performance rate based on various percentages of bandwidth saturation in which we are interested by system and network performances. Fig. 3, 4 and 5 showed the different results.

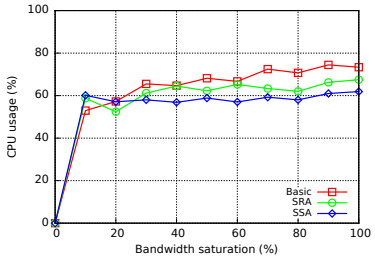

Fig. 3. CPU load of physical firewall according to bandwidth saturation

In Fig. 3 we see that increasing the saturation of bandwidth induced increasing of CPU load which is quite normal because the number of processed packet is increasing too. we note that SSA offers a gain of more than 10%. We remark that SSA is more stable comparing basic and SRA despite the increased load. Thus, the memory consumption confirms this trend. Indeed, we note that the consumption of SSA is not greater than the Basic architecture, the difference being the memory consumed by the load balancing software. On the other side, SRA has a large memory consumption, it is the result of the routing mechanism in place that is complex and induces the storage of packets before they are processed.

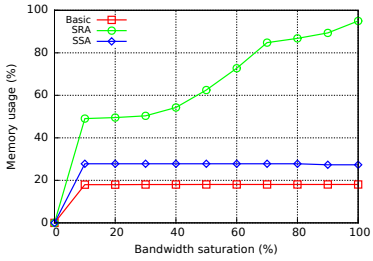

Fig. 4. Memory load of physical firewall according to bandwidth saturation

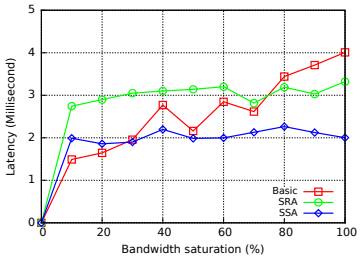

Fig. 5. Latency Network according to bandwidth saturation

Network performance are shown in Fig. 5, the latency is an important metric for judging the quality of service for a network, the interpretation of the curves in Fig. 5 allows several observations. The first one is that the two proposed architectures have significantly improving the network latency. The second one is that improvements of the SSA are more significant than the SRA. The third is that SSA has a tendency to stability and improves performance by 30% on average. This supports the choice of SSA for an optimal deployment of our hybrid architecture.

V. Conclusion and Perspective

Our paper presents a hybrid security architecture which its main purpose is to increase the computational power of physical firewall, with low financial cost, using the vast resources offered by the Cloud. It has shown good performance in adapting existing technologies for the next generation broadband network. In order to demonstrate the effectiveness of the proposed hybrid architecture we use a real testbed and results presented a significant improvement in Computing

power, system and network performances. As future work, it is scheduled to study the impact of the proposed architecture on the application layer.

REFERENCES

[1] A. Khakpour and A. Liu, "First step toward cloud-based firewalling," in *Reliable Distributed Systems (SRDS), 2012 IEEE 31st Symposium on*, 2012, pp. 41–50.

[2] E. L. Haletkyl, "Are virtual firewalls a real solution for vm security?" Aug. 2013. [Online]. Available: http://www.cio.com/

[3] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," *Commun. ACM*, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[4] S. Subashini and V. Kavitha, "Review: A survey on security issues in service delivery models of cloud computing," *J. Netw. Comput. Appl.*, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[5] "Five best practices to protect your virtual environment," Juniper Network, Tech. Rep., 2012.

[6] D. Basak, R. Toshniwal, S. Maskalik, and A. Sequeira, "Virtualizing networking and security in the cloud," *SIGOPS Oper. Syst. Rev.*, vol. 44, no. 4, pp. 86–94, Dec. 2010.

[7] Q. Duan and E. Al-shaer, "Traffic-aware dynamic firewall policy management: techniques and applications," *IEEE Communications Magazine*, vol. 51, no. 7, 2013.

[8] C. A. Lee, "A perspective on scientific cloud computing," in *Proceedings of the 19th ACM International Symposium on High Performance Distributed Computing*, ser. HPDC '10. New York, NY, USA: ACM, 2010, pp. 451–459.

[9] A. Bouhoula, Z. Trabelsi, E. Barka, and M.-A. Benelbahri, "Firewall filtering rules analysis for anomalies detection," *International Journal of Security and Networks*, vol. 3, no. 3, pp. 161–172, 2008.

[10] J. E. Canavan, *The Fundamentals of Network Security*. Artech House, 2001.

[11] S. Suehring and R. Ziegler, *Linux Firewalls (Novell Press)*. Novell Press, 2005.

[12] J. Garcia-Alfaro, F. Cuppens, N. Cuppens-Boulahia, S. Martinez, and J. Cabot, "Management of stateful firewall misconfiguration," *Computers & Security*, no. 0, 2013.

[13] J. Pescatore and G. Young, "Defining the next-generation firewall," *Gartner RAS Core Research Note, from http://www. ga1tner. com*, 2009.

[14] A. Abdel-Aziz and J. Esler, "Intrusion detection & response - leveraging next generation firewall technology," SANS - Institue, Tech. Rep., 2009.