DOI: 10.5748/16CONTECSI/ITM-6115

PHYSICAL OR VIRTUAL FIREWALL FOR PERIMETER PROTECTION IN CLOUD COMPUTER INFRASTRUCTURE

Thiago Mello Valcesia - IPT - Instituto de Pesquisas Tecnológicas - thiago.valcesia@ensino.ipt.br
Antonio Luiz Rigo - IPT - Instituto de Pesquisas Tecnológicas - antonio.rigo@ensino.ipt.br

SUMMARY

This article presents an examination of the different types of firewalls geared toward protecting Datacenters. The idea is to perform a survey of the different ways of installation, the safety perceived by customers, the positive and negative points of each model and the market trends for perimeter protection.

In addition, it is intended to categorize rules, protection filters, application inspection criteria and services offered by firewalls, by analyzing the various protection schemes available in firewalls, regardless of the structure as a service in Cloud adopted.

Keywords: Physical firewall, Virtual firewall, Cloud firewall, Security, Cloud Computing.

INTRODUCTION

The term Digital Security is increasingly present in our daily lives. The need to protect computers or prevent corporate networks from receiving unnecessary traffic, improper access, and unknown packets, coupled with the concern of professional information security staff about content accessed by Internet users, make data control a vital task.

Firewall is much more than a "fire wall" isolating the company network from the external world represented by the Internet. The Firewall function is therefore essential to raise the level of security of the internal environment, protecting it from external attacks, increasing security and reducing the vulnerability of the local network.

There are currently three Firewall alternatives to install on enterprise networks that aggregate cloud network segments:

1. Software embedded in the operating system, such as IPTables or NFTables (Linux Platform) and Internet Connection Firewall or Windows Filtering Platform (Windows Platform) [1];

2. Physical devices (hardware) present at the junction of the Internet with the internal network, perimeter of the corporate networks. [2];

3. Cloud firewall solution developed to meet virtual environments and cloud demand in enterprises [3] [4].

The distinct ways of designing and deploying security devices such as the firewall came when companies began to comply with the international security regulations required for import, export, or business at the professional level [5]. Laws such as Sarbanes-Oxley, Gramm-Leach-Billey (GLB), Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS) are some of the major standards that prescribe requirements to audit information security as well as mentoring for the adoption of distributed firewalls as a standard for enterprise security in order to ensure protection from internal networks to the edge connections of the company's branch offices [6].

The deployment of firewalls segregating internal areas of companies began in mid-2006, that is, eight years before the great evolution provided by new solutions that serve not only the security department, but also a new modality of use called infrastructure as a service (IaaS) in cloud computing. IaaS aims to reduce capital costs (CAPEX) and provide solutions tailored to the actual consumption of a company as operational cost (OPEX), allowing the portability of data and applications in different delivery models. Such models can be Private, Hybrid or Public, according to Figure 1.

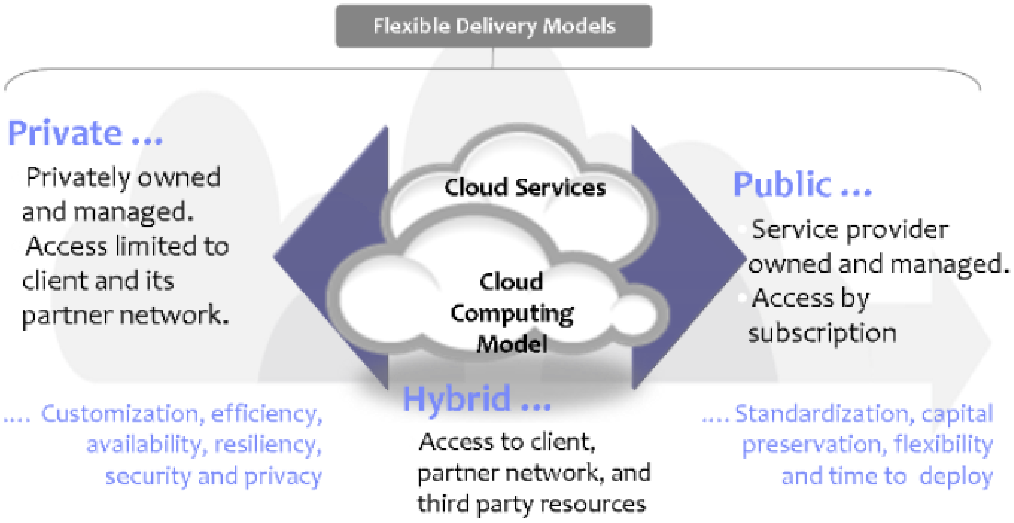

Flexible Delivery Models
Private ...
Privately owned and managed. Access limited to client and its partner network.
Cloud Services
Cloud Computing Model
Public ...
Service provider owned and managed. Access by subscription
.... Customization, efficiency, availability, resiliency, security and privacy
Hybrid ...
Access to client, partner network, and third party resources
.... Standardization, capital preservation, flexibility and time to deploy

Figure 1 – Flexible Delivery Models
Source: http://thoughtsoncloud.com, 2012

The new solution has great market acceptance and there are already several customers migrating their data and service platforms to the Cloud infrastructure: how the security area can ensure that all security practices and standards previously established by firewalls maintain compliance with this model? Will a new standard be established? Which option should be used: Physical, Virtual or Software Firewall?

The objective of this article is present alternatives and suggest best practices to achieve high security standards to the perimeter network in local area networks, using different infrastructure models.

THEORETICAL REFERENCE

Conceptualizing Firewall

Firewall is, by definition, a software or hardware implemented filter, whose function is to prohibit unauthorized traffic and release access previously approved by the IT staff. Data packets that travel freely over the Internet are subject to communication rules, which control what can and cannot flow between servers and workstations [2].

The idea of firewall technology was born in mid-1988, during research supported by the company Digital Equipment Corporation (DEC). But the first proofs of concept and the basis of the conceptual model emerged only a year later, by the dedication of researchers William Cheswick and Steven M. Bellovin [7]. In the first model created, called Packet Filters, the firewall restricted traffic only through addresses at the network layer (source and destination IP) and / or ports at the transport layer (TCP or UDP) [8].

Studies focused on the development of so-called revolutionary technologies of the 1990s have begun to introduce improvements in how firewalls worked in their first release. Firewalls were enabled to restrict accesses at the beginning of connections and at the same time recognize and rely on packet traffic initiated from protected networks. This second version has the possibility of storing connection states (New, Established and Related) and such firewalls are known as Session State Filters.

The third firewall evolution established the first commercial version, called DEC – SEAL [7]. Application Gateway, as named, aggregated old versions resources, functions such as {1} receive a connection; {2} application layer protocol decoding; and {3} communication interception between client-server to certify application layer rules.

The fourth version of the firewalls evolved and has functions capable of:

- Inspect packets and data traffic in all layers of the OSI model, called Stateful Inspection;
- Identify TCP / IP protocol abuse on all connections;
- Analyze and perform deep inspection on the transmitted packets by adding Deep Packet Inspection;

- Use firewalls for personal use, installed via software on home computers and workstations.

Conceptualizing Cloud Computing

The characteristics that define an architecture in Cloud Computing are related in the themes listed below [9]:

On-demand self-service: A user can provision computing resources, set the time-to-use and the available network resources automatically, without human intervention;

Broad Network Access: Features made available by the network or accessed through standard devices (Thin Clients, Notebooks, Computers, etc.) enable the use of different platforms (Windows, Linux, iOS, etc.);

Resource Pooling: Provider serves multiple consumers through a model called multi-tenant. Computational resources are dynamically assigned and reallocated according to consumer demand.

Rapid Elasticity: Rapid and elastic provision of infrastructure needed to meet market demand or to meet the different requirements that may exist.

Measured Service: Systems capable of controlling and accounting for the use of cloud resources automatically.

Cloud Computing is a matter of common interest to consumers and corporate IT departments. The proposal to provide unlimited computing resources for a small monthly amount, with flexibility, agility and limited obligations, is a dream coming true. Many organizations, on the other hand, still worry about the safety factor of their adoption, taking the subject to the top of the research developed by IBM [10], reaching the 60-80% percentage.

Due to this scenario, a method was adopted to evaluate the different forms of Firewalls implementation based on the results of the project: Security for the Cloud and SOA, in The Open Group [11]. It is a joint venture that brings together the Cloud, SOA (Service Oriented Architecture) and Security Forums groups to study and promote information security model revisions. It aims to understand the potential risks associated with Cloud Computing through a policy-centric approach, leverage open standards and significantly increase the chances of using Cloud Computing more comprehensively.

The model in Figure 2 shows the protection of the access points for a totally private infrastructure. It is known that cloud adoption is a reality experienced by many people and companies, offering services such as Web Servers, Database, Application Servers, DHCP, DNS, LDAP, which can be part of an implemented cloud solution from infrastructure as a service.

The protection shown in the figure uses the distributed firewall concept. In the cloud, however, the devices would gain the virtual format. The cloud can provide extra features to increase the level of security by enforcing proper client-side protection (which is using the infrastructure) and / or provider-side (which offers the Cloud service). Your convenience should be evaluated on a case by case basis.

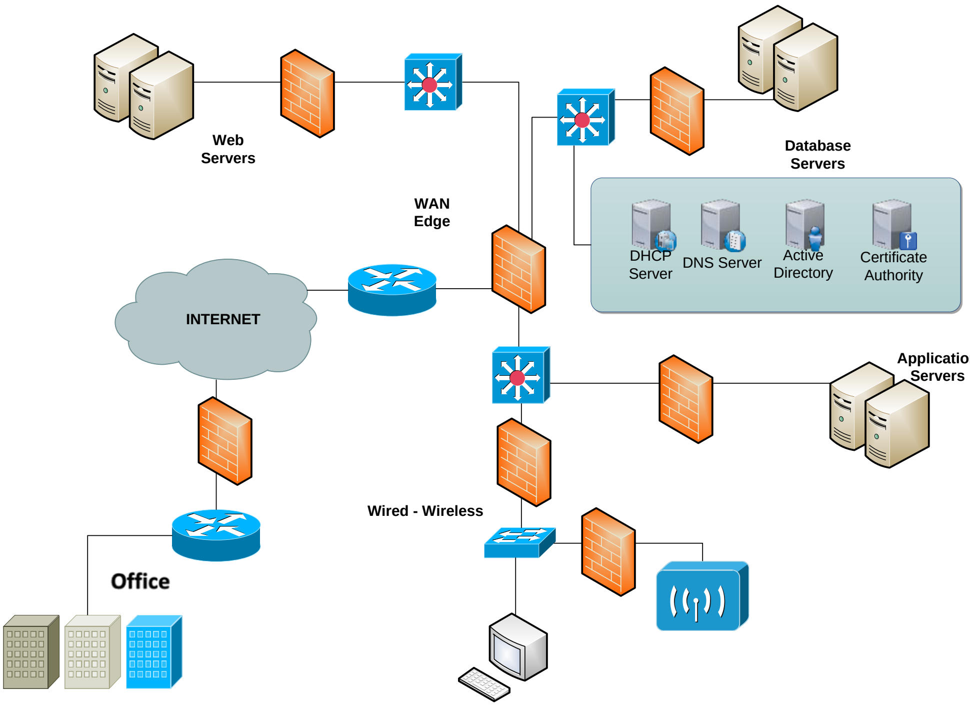


Figure 2 – Perimeter Firewall Protection
Source: Made by the Author

It follows analysis of a hybrid implementation model, that is, managed by the client and that gathers part of the network on premises and part hosted in the cloud. Using firewalls to access an infrastructure accessed only by company employees, with management of your IT staff and hired as a service does it even need protection? Yes! But how to implement such protection can and should be different.

Observe the example in Figure 3:

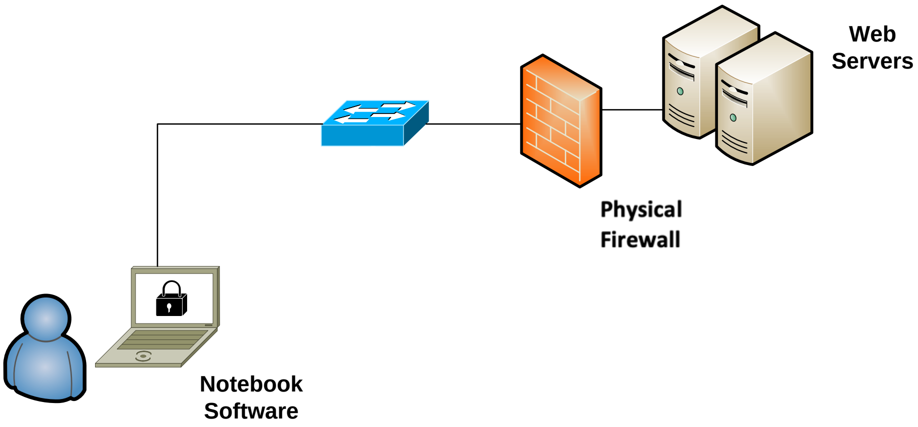
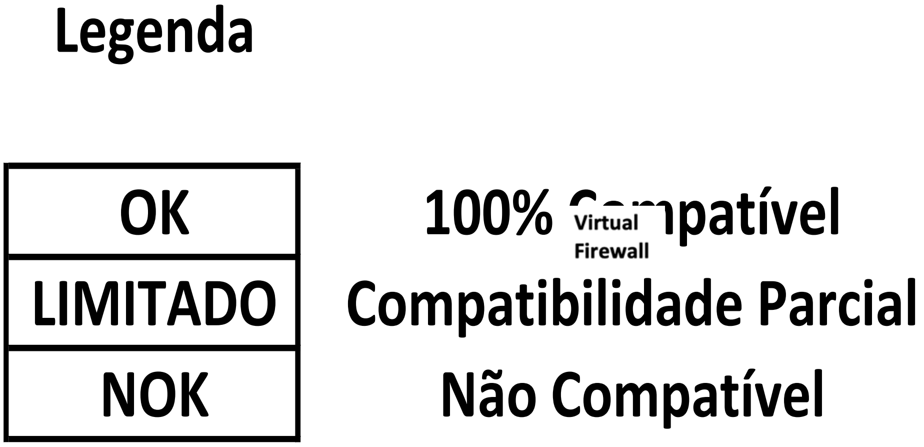


Figure 3 – Physical Firewall Model
Source: Made by the Author

The drawing shows an architecture where the Physical Firewall gets connected in the path between the Server and the Accessing User. In Cloud architecture, one of the facilities of this service is precisely to meet the seasonal demands of its client. With that in mind, we can remove or increase the number of Web Servers on this path. Or change the way the servers are accessed, or the way users access them. When using a Physical Firewall for this activity, the type of change would follow a change process, which would consist of opening a change request, scheduling a technical stop, changing the settings necessary for the fix to be applied, and then informing access is available again.

A similar solution, however, with the Firewall hosted on the Cloud infrastructure, the required change would be made more easily and with benefits that would meet demand in a simple way.

Observe the example in Figure 4:



Legenda

OK	100% Compatível
LIMITADO	Compatibilidade Parcial
NOK	Não Compatível

Virtual
Firewall

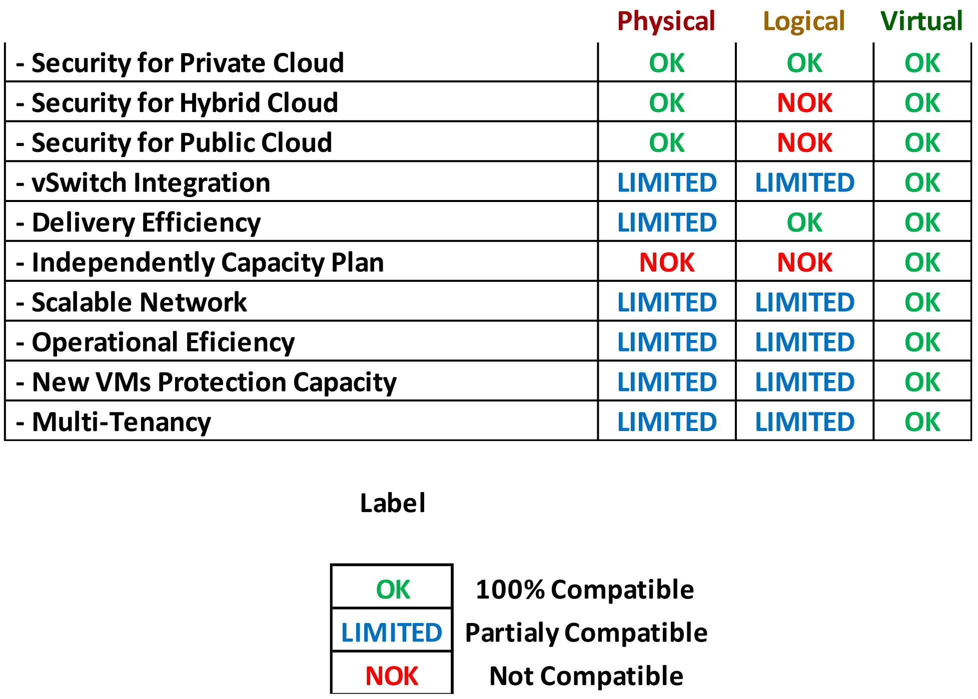
Figure 4 – Virtual Firewall Model
Source: Made by the Author

By using a virtual firewall installed next to the servers, you create what the Cloud solution calls a Template, that is, a master image with all the settings, locks, and permissions required for Web servers, such as example shown, carry out its activities in a normal way and with safety applied to the environment.

This way of proceeding allows to reduce the time of implantation and to speed up the answer for the requested demands. The actions are executed faster, minimizing delays and mainly, avoiding expenses with the technical team due to overtime and night overtime. This efficiency gain reflects an increase in productivity and a greater dedication to the company's business activity, broadening the spectrum of activities carried out by its employees.

In Table 1, a comparison between the versions of firewall and its functionalities:

Table 1 - Firewall Features for Cloud Computing



	Physical	Logical	Virtual
- Security for Private Cloud	OK	OK	OK
- Security for Hybrid Cloud	OK	NOK	OK
- Security for Public Cloud	OK	NOK	OK
- vSwitch Integration	LIMITED	LIMITED	OK
- Delivery Efficiency	LIMITED	OK	OK
- Independently Capacity Plan	NOK	NOK	OK
- Scalable Network	LIMITED	LIMITED	OK
- Operational Eficiency	LIMITED	LIMITED	OK
- New VMs Protection Capacity	LIMITED	LIMITED	OK
- Multi-Tenancy	LIMITED	LIMITED	OK

Label

OK	100% Compatible
LIMITED	Partialy Compatible
NOK	Not Compatible

Source: Made by the Author

Adopting Virtual Firewall allows you to adapt the Cloud Computing infrastructure according your needs [4]. The installation takes advantage of the benefits and features that the virtual machines offer and the Firewall features that consists of Packet Filters, State Filters, Session Filters and Application Filters [12]. You can implement such functionality to work separately and independently, ensuring continuity of services with security and elasticity.

CONCLUSION

The most appropriate way to protect virtual machines in a Cloud Computing infrastructure and to maintain resource provisioning, elasticity, and data protection at the established security levels is to align security with virtualization paths. When comparing physical, logical and virtual firewalls, it is possible to identify that all of them are useful and functional in the world of computing. The study, focused on Cloud Computing, makes it clear that Virtual Firewall is the most appropriate to guarantee the virtual security and business demand of the company that has decided to migrate its services to an Infrastructure as a Service (IaaS).

As future work, after showing performance gains using Virtual Firewalls instead of Physical Firewalls, it is interesting to verify if there is a saturation threshold for competing users, as well as, to estimate a confidence interval to emit alerts of the imminence of contracted bandwidth exhaustion and the degradation of the quality of connections.

BIBLIOGRAPHIC REFERENCE

[1] WIKIPEDIA (Org.). **Iptables.** 2019. Available: <https://en.wikipedia.org/wiki/Iptables>. Access Date: March 17th - 2019.

[2] CHECK POINT SOFTWARE TECHNOLOGIES LTD (Org.). **Check Point Firewall Security Solution.** 2015. Available: <https://sc1.checkpoint.com/documents/R77/CP_R77_Firewall_WebAdmin/92746.htm>. Access Date: March 15th - 2019.

[3] CISCO (Org.). **Cisco ASA 1000V Cloud Firewall Data Sheet.** 2014. Available: <https://www.cisco.com/c/en/us/products/collateral/security/asa-1000v-cloud-firewall/data_sheet_c78-687960.html>. Access Date: March 15th - 2019.

[4] VMWARE (Org.). **Distributed Firewall.** 2018. Available: <https://docs.vmware.com/en/VMware-NSX-Data-Center-for-vSphere/6.4/com.vmware.nsx.admin.doc/GUID-95600C1C-FE9A-4652-821B-5BCFE2FD8AFB.html>. Access Date: March 17th - 2019.

[5] GO ANYWHERE (Org.). **Meeting Compliance Regulations and Privacy Laws for Sensitive Data Transfers.** 2011. Available: <https://www.goanywhere.com/blog/2011/01/10/compliance-and-regulations-for-sensitive-data-transfers>. Access Date: March 17th - 2019.

[6] CISCO (Org.). **Cisco IOS Firewall Common Deployment Common Deployment Scenarios.** 2006. Available: <https://www.cisco.com/c/dam/en/us/products/collateral/security/ios-firewall/prod_presentation0900aecd804e1307.pdf>. Access Date – March 15th - 2019.

[7] BELLOVIN, Steven M. Security Problems in the TCP/IP Protocol Suite. **Computer Communication Review**, Murray Hill, v. 19, n. 2, p.32-48, April.15th - 1989. Available: <https://www.cs.columbia.edu/~smb/papers/ipext.pdf>. Access Date – March 15th - 2019.

[8] AVOLIO, Frederic (Org.). Firewalls and Internet Security, the Second Hundred (Internet) Years. **Firewalls And Internet Security - The Internet Protocol Journal.** San Jose, June 10th - 1999. Available: <https://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-1/ipj-archive/article09186a00800c85ae.html>. Access Date: March 17th - 2019.

[9] NIST (Org.). **The NIST Definition of Cloud Computing.** 2011. Available: <https://csrc.nist.gov/publications/detail/sp/800-145/final>. Access Date: March 17th - 2019.

[10] IBM. IBM Study Reveals Businesses Using Cloud Computing for Competitive Advantage Can Generate Double Revenue and Profit Compared to their Peers. 2013. Available: <https://www-

03.ibm.com/press/us/en/pressrelease/42304.wss>. Access Date: March 17th - 2019.

[11] THE OPEN GROUP CLOUD COMPUTING WORK GROUP (Org.). **AN ARCHITECTURAL VIEW OF SECURITY FOR CLOUD.** 116. ed. Usa: The Open Group, 2011. 22 p. Available: <https://publications.opengroup.org/w116>. Access Date: March 15th - 2019.

[12] VMWARE (Org.). **How Virtualization Works.** 2019. Available: <https://www.vmware.com/solutions/virtualization.html#how-it-works>. Access Date: March 17th - 2019.