Strong Hybrid Cloud-Based Firewalling Authentication using EAP-TLS Smart-Cards'

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

***Abstract*—The use of cloud computing is growing, and by 2016 this growth will increase to become the bulk of new IT spend. Companies are interesting in outsourcing security services to Cloud provider in order to reduce management and deployment costs. This outsourcing addresses many problems related to identification, authentication, secure data transfer, and privacy in Security As A Service (SECAAS) Model. Our article presents a secure, strong and efficient authentication architecture and identity management for hybrid cloud based firewalling services using EAP-TLS smart cards technology.**

***Index Terms*—Security as a Service, Secaas, Firewall, Network security, Authentication, Identity management, Smartcard, EAP-TLS, Grid server.**

I. Introduction

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 a cloud [1][2]. 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.

[3] presents an innovative and efficient architecture to manage performance and reliability in an hybrid cloud-based firewall service. The proposed architecture improves both the computation power 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 in order to support the basic physical firewall with a virtual firewall in the cloud characterized by very high computing resources to deal with the huge traffic. To ensure safe operation and secure data transfer between the physical and virtual part of the presented architecture in [3], we develop an authentication module using EAP-TLS smart cards technology. The authentication module is based in previous authentication architecture proposal presented in [4] that guarantees a trusted computing environment.

This paper is organized as follows. Section II presents the related works. Section III describes the proposed authentication model. Section IV presents our case studies. Finally, Section V concludes the paper and outlines future works.

II. Related Work

Several works have addressed the question of authentication and identity management and proposed different solutions to this problem. The user centric identity management approach provides a stronger mutual authentication between user and service providers, by enabling the storage of identifiers and credentials from different service providers in a single resistant hardware device called Personal Authentication Device(PAD) [5]. This solution offers protocol flexibility giving that the PAD supports different authentication protocols, user mobility and more important compatibility with legacy identity management systems.

A Hierarchical identity-based cryptography scheme was proposed in [6]. This scheme was considered as new solution for cloud computing security with federal identity management [7]. In fact, the federated identity management deals with problems between external user and internal network and *vice versa*. This approach creates a federated identity domain. So, the user's identity can be recognized across different networks. The Identity-Based authentication discussed in [8], presents a new method for identification within a cloud environment named Identity-Based Hierarchical Model for Cloud Computing (IBHMCC). In this method, node identity depends on identities of all parent nodes on hierarchical way: The hierarchical model is composed of three levels beginning by the root where each node has a unique name used to create its ID. This model comes with its corresponding encryption and signature schemes.

The authentication solution presented in [9] specifies a new design for a RADIUS server. Commonly used for authentication, and associated to the Grids of EAP-TLS smartcard. The Radius server will only process RADIUS datagrams and perform user authentication using EAP-TLS. We have to notice that the choice of EAP-TLS was not arbitrary. In fact, EAP protocol provides the transport and usage of keying material and parameters generated by EAP methods and guarantees network access authentication mechanisms and mutual authentication between the client and the server [10]. In addition, EAP-TLS is the most secure EAP type [11].

Authentication and identity management using EAP-TLS smartcard was deployed and tested in [12] with an Open-ID platform and has shown a strong authentication between the user and the Open-ID provider without using any password.

The strength of this solution is that server key verification is processed by the smartcard. Indeed, a smartcard is a highly secure computing environment. Moreover, user keys and certificates are handled by the smartcard.

All previous works provide a specific solution to deal with authentication and identification problems in cloud environment. But there are no work done in the context of cloud based security services. For this purpose, and since the EAP-TLS smartcard technology has shown remarkable results within cloud computing authentication, we expect to have the same results with cloud based security services environment.

III. Authentication Deployment Model

The primary mission of the authentication module is ensuring authentication and establishment of secure tunnel via VPN between the physical and virtual firewall. The authentication module offers the possibility to use different authentication protocols since it is based on a radius server, the latter use the open source tool FreeRADIUS providing users authentication via multiple protocols such as: PAP, CHAP, MS-CHAP, MS-CHAPv2, SIP Digest, and all common EAP methods. We use EAP-TLS based on SSL protocol because the SSL handshake is performed over EAP.

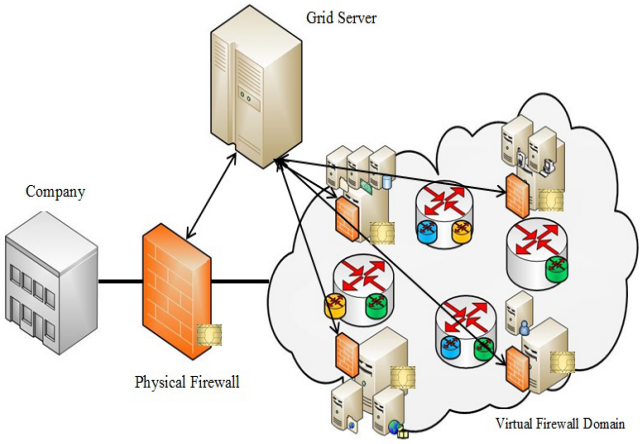

Fig. 1. Strong Hybrid Cloud-Based Firewalling Authentication Architecture

We design and develop a coherent authentication architecture for hybrid cloud based firewalling service as shown in Fig-1. The proposed architecture ensures an efficient management of secure communications between the virtual firewall located in the Cloud and the traditional company's firewall. Our work provides a robust identification scheme and a strong authentication system using secure micro-controllers. The solution must take into consideration the virtual environment specificities essentially dynamism.

The proposed authentication module should identify both the virtual and the physical firewall. It is based on five key elements which are: Virtual Firewall *VF*, Grid Server *GS*, Physical Firewall *PF*, Cloud Server *CS* and Certificate as illustrated in Fig-2.

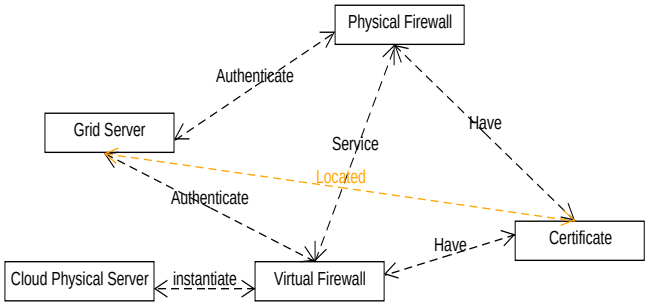

Fig. 2. Steps of Establishment of Secure communication Tunnel

- *A* is a set of *PF*, each company possesses a K number of physical firewall. $|A| = K$
- Virtual Firewall is a virtual machine which executes firewall programs with operations as analysis, monitoring, reporting and many others with dynamic resources provisioning. VF is located in CS, Each *CS* supports up to N *VF*, consequently each CS is equipped with N smartcards.
- Cloud physical Server is a physical server supports virtualization which allows users to maximize physical resources in the most efficient way possible. Server virtualization functions by running multiple, independent, virtual operating systems on a single computer.
- Grid Server is an array of smartcards supporting up to M Physical Firewall, up to $(K \times N)$ Virtual firewalls and total number of physical and virtual firewalls equal to $M + (K \times N)$
- Physical Firewall represents the physical security infrastructure of the company
- Each physical and virtual firewall has a unique certificate stored in its smartcard.

The Physical Firewall establishes a secure tunnel to a given Virtual Firewall in order to manage and forward traffic. This access can not be allowed until the authentication step succeed. The proposed steps may be divided into three major steps as presented in Fig-3:

1) Physical Firewall authentication
2) Virtual Firewall authentication
3) Establishment of a secure tunnel via EAP-TLS between Physical and Virtual Firewalls.

The first step is to authenticate the PF and we consider the exchange protocol between the Physical Firewall and the Grid server based on the Client/Server protocol. Thus, we proceed as follows to authenticate the PF:

- ClientHello: This message contains: version of the SSL protocol, random number, session ID, cipher suite: the list of cipher suites selected and decompression algorithms.
- ServerHello: This message contains the same elements as the ClientHello message but related to the Grid Server.
- Certificate: This message contains either the server certificate.

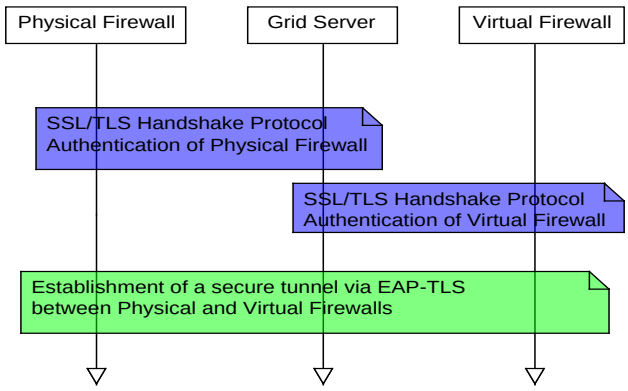

Fig. 3. Steps of Establishment of Secure communication Tunnel

- ServerKeyExchange: contains the signing certificate
- CertificateRequest: the server requires a client certificate
- ServerHelloDone: the end of the message sending
- ClientKeyExchange: This message contains PreMaster-Secret encrypted using using the public key of the server.
- CertificateVerify: explicit verification of the client certificate
- Finished: end the handshake protocol and the beginning of the data transmission

Now the GS must identify all virtual firewalls related to the authenticated PF. So, The next step consists of VF authentication. as developed before in the authentication steps of the physical firewall, the VF realizes the same authentication schema. These steps are performed by a pair of smartcards located in GS and CS and processes EAP-TLS protocol as specified in [13].

Once authenticated, the server sends to the PF all information about its Virtual Firewall, allowing the full access to all virtual firewall resources.

IV. Case Studies

In this section we present our two secure topologies to provide a high level physical firewall's computing power. The first is "secure forwarding architecture", and the second's "secure sharing architecture". In both cases, we have operated great benefits of virtualization, due to cloud, like improving overall system security and relying by isolating multiple software stacks in their own VMs. All communication between virtual and physical firewall will be based on the secure communication protocol TLS.

A. Secure Forwarding architecture

In this model, The Physical firewall (PF) is compared in this topology to a simple router. It just redirects all incoming packets. The Virtual Firewall is employed to ensure filtering function. The idea is to watch all income traffic and redirect accepted packets to the physical firewall after inspection. As illustrated in Fig-4 For each received packet we apply this Sequence diagram which resumes the messages list communication between firewalls:

1) redirect-traffic (): physical firewall forwards traffic to the virtual by affecting NAT (Network Address Translation) function.
2) intercept-traffic (): virtual firewall intercepts the flow.
3) traffic= analyze-traffic (): virtual node will process an arriving packet using its local policy to determine the first match. If the correspondent action is ACCEPT the physical firewall will then apply the action.
4) packets= analyze-traffic: virtual node redirects again accepted packets to the company's firewall.

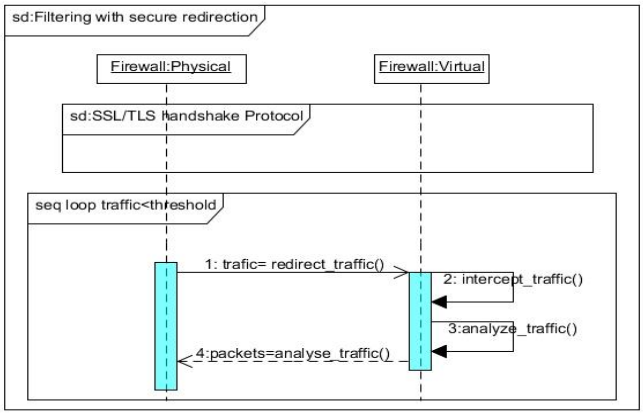

Fig. 4. Sequence diagram of the messages list communication between firewalls of Secure Forwarding architecture

B. Secure Share architecture

In this second case, the Physical 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 multiple virtual firewalls. The load balancer module is added to forward requests to one or more virtual firewall.

Therefore, The Virtual firewall is always allocated to participate to filtering function when we reach or exceed a threshold value. Virtual nodes are dispersed and deployed in different and perhaps unknown sites. Thus, a mutual high strong authentication should be conducted before any sharing like we have described in the previous architecture.

The Fig-5 summarizes the parallel execution. In fact, for each entering flow, the "load balancer" (physical firewall) shares all incoming packets using the algorithm "Least session". 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. Thus, the distribution of connections is based on various aspects such as analysis of server performance in real time, the current number of connections per node or the response time of the fastest node.

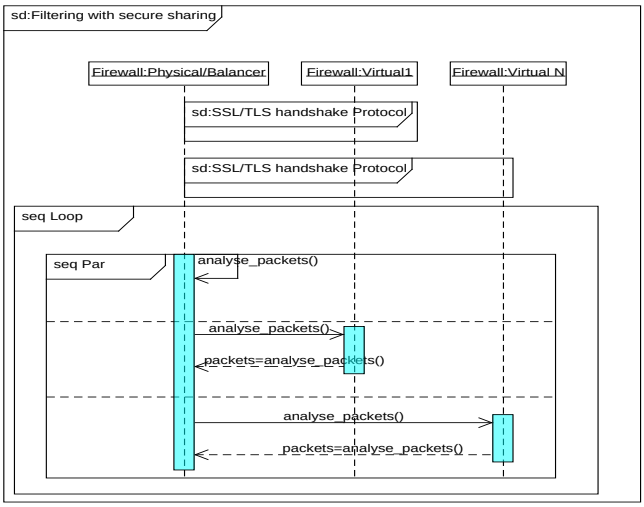

Fig. 5. Sequence diagram of the messages list communication between firewalls of Secure Sharing architecture

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. As discussed in the previous case: only accepted packets will be redirected to company's firewall. Additionally, we have to minimize signaling messages and responses time, liberate resources as well increase QoS.

V. Conclusion & Perspectives

In this paper, we present a strong hybrid Cloud-Based Firewalling Authentication architecture using EAP-TLS Smartcards, This architecture provides identification and authentication of all elements of the hybrid Cloud-based firewalling Services.

We work on the migration of the Virtual Firewall. Thus, the authentication module needs take into consideration this aspect. We think that this problem is manageable since we have a central authentication server that keeps all necessary information about a Virtual Firewall.

References

[1] 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.

[2] 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.

[3] F. Guenane, H. Boujezza, M. Nogeuira, and G. Pujolle, "An architecture to manage performance and reliability on hybrid cloud-based firewalling."

[4] F. Guenane, N. Samet, G. Pujolle, and P. Urien, "A strong authentication for virtual networks using eap-tls smart cards," in *Global Information Infrastructure and Networking Symposium (GIIS), 2012*, 2012, pp. 1–6.

[5] A. Jøsang and S. Pope, "User centric identity management," in *AusCERT Asia Pacific Information Technology Security Conference*. Citeseer, 2005, p. 77.

[6] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography," in *Advances in cryptology—ASIACRYPT 2002*. Springer, 2002, pp. 548–566.

[7] L. Yan, C. Rong, and G. Zhao, "Strengthen cloud computing security with federal identity management using hierarchical identity-based cryptography," in *Cloud Computing*. Springer, 2009, pp. 167–177.

[8] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in *Cloud Computing*. Springer, 2009, pp. 157–166.

[9] P. Urien, E. Marie, and C. Kiennert, "An innovative solution for cloud computing authentication: Grids of eap-tls smart cards," in *Digital Telecommunications (ICDT), 2010 Fifth International Conference on*. IEEE, 2010, pp. 22–27.

[10] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowetz *et al.*, "Extensible authentication protocol (eap)," RFC 3748, June, Tech. Rep., 2004.

[11] D. Simon, B. Aboba, and R. Hurst, "The eap-tls authentication protocol," *RFC5216, IETF, March*, 2008.

[12] P. Urien, "An openid provider based on ssl smart cards," in *Consumer Communications and Networking Conference (CCNC), 2010 7th IEEE*. IEEE, 2010, pp. 1–2.

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