Using Cloud Computing to Implement a Security Overlay Network

[1]K. Salah [2,3]J. M. Alcaraz-Calero [4]S. Zeadally [1]S. Almulla [1]M. Alzaabi

[1]Computer Engineering Department, Khalifa University of Science Technology and Research (KUSTAR), Sharjah, UAE
Email: {khaled.salah, sameera.almulla, mohammed.zaabi}@kustar.ac.ae

[2]Department of Communications and Information Engineering, University of Murcia, Murcia 30011, Spain
[3]Hewlett-Packard Labs, Cloud and Security Lab, Bristol, BS34 8QZ, UK
Email: jmalcaraz@um.es

[4]Department of Computer Science and Information Technology, University of the District of Columbia, Washington DC, 20008
Email: szeadally@udc.edu

Abstract

Cloud Computing and Overlay Networks have recently received a lot of attention in computing and networking areas. These technologies are being exploited and implemented in the design of large network infrastructures. They are being widely deployed by organizations, and research interests keep growing. We explore the use of Cloud Computing in implementing a security overlay network. In particular, we propose and analyze a general cloud-based security overlay network that can be used as a transparent overlay network to provide security services such as Intrusion Detection System (IDS), Anti-Virus software, Anti-Spam software and Distributed Denial of Service (DDoS). Each of these in-cloud security services is analyzed in terms of its resiliency, effectiveness, performance, flexibility, control, and cost.

Keywords: Cloud Computing, Overlay Networks, Security, Denial of Service, Intrusion Detection, Anti-virus, Anti-Spam.

1. Introduction

Cloud computing enables the usage of third-party IT infrastructures to be used on-demand according to the continuously changing customers' requirements in a *pay-per-use* model. This paradigm reduces the necessity of investing in hardware for customers while improving the elasticity of the

computational resources in order to adapt to the business requirements. Businesses are quickly adopting the cloud computing paradigm.

Overlay networks have also received a lot of attention in recent years due to its numerous benefits. The idea of an overlay network was first used in the deployment of the Internet over the existing telephone network. It can be defined as a virtual network that is built on top of an existing network. It consists of virtual nodes that are connected via virtual links. The main aim of overlay networks is to deploy a new network service that is not available in the underlying network. Cloud computing is mainly based on virtualization which enables multi-tenancy and scalable shared resources used on an on-demand basis by all tenants. Since overlay networks are also based on virtualized nodes for implementing network services, this fact allows combining both techniques to reap the benefits of each other together. This is particularly useful for the deployment of new transparent network security services over the current networks in order to enhance their protection.

The primary contribution of this paper proposes and analyzes a cloud-based security overlay network that can be used to offer an integrated set of several security services. We focus on the most popular types of security software that are widely deployed. These include Intrusion Detection System (IDS), Distributed Denial of Service (DDoS) prevention, Security Management in protected endpoints, mainly, Anti-Virus and Firewall and also E-mail protection, including Anti-virus and Anti-Spam software. Throughout this paper, we refer to a protected endpoint as a physical or virtual computing host to be protected. The endpoint can be a service endpoint such as a web server or a client endpoint. Several security solutions have been examined and we discuss how they are best suited to be deployed as cloud services.

The rest of the paper is organized as follows. Section 2 describes how cloud computing can be used as an overlay network for providing security services. Section 3 explains different overlay and cloud-based security systems. Section 4 describes and discusses a general architecture that can integrate different security solutions. Section 5 describes a proof-of-concept architecture deployed using today's available commercial solutions. Section 6 analyzes the proposed architecture in terms of performance, flexibility or cost. Finally, Section 7 concludes the paper and presents future work.

2. Cloud as a Security Overlay Network

Cloud Computing is composed of three well-known layers. Infrastructure-as-a-Service (IaaS) layer is in charge of providing on-demand virtual infrastructures to third-parties using physical resources such as memory, storage and processors. This virtual infrastructure typically allocates resources from data centers owned and managed by the cloud provider and are used by customers through the Internet. The Platform-as-a-Service (PaaS) layer provides automatic provisioning of ready-to-use middleware services. Finally, the Software-as-a-Service (SaaS) layer makes use of the previous layers to offer end-user software services to customers.

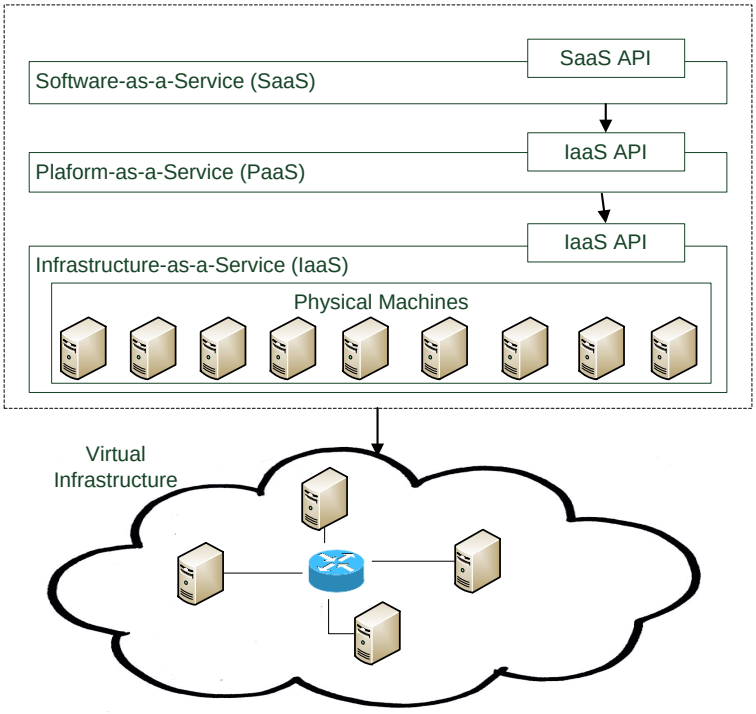

Figure 1. General overview of the Cloud Computing paradigm

Various security applications such as Antivirus (AV), email anti-spam and Intrusion Detection System (IDS) can be offered as Cloud services. These services can protect either the virtual infrastructure or the physical customer's infrastructure and are being designed as transparent services using an overlay network or as well-known endpoint services. This paper focuses on security systems designed to protect any virtual or physical machine using an overlay network. The collaboration among all of these security systems can provide a robust security elastic overlay network to protect customers' virtual infrastructures transparently.

The provisioning of services by Cloud providers or by third-parties opens up several challenges: the outsourcing of data and applications, the fulfillment of Service-Level Agreements (SLAs) between the cloud provider and customers, the extensibility and shared responsibility of the virtual infrastructures, the implementations of laws and the design of multi-tenancy services are some cloud computing related features which make security and privacy a real challenge. Takabi et al [1] present an overview of the security and privacy challenges in Cloud computing. It is worthwhile noting that this paper does not focus on providing novel approaches to these Cloud security challenges. Rather, we focus on providing security services to third-parties using a Cloud-based elastic and transparent overlay network assuming a secure cloud computing environment is already in place.

3. Related Work

The literature has reported several articles on cloud-based security solutions related to DDoS attacks, Intrusion Detection Systems (IDS), Anti-virus and e-mail security. For example, Du et al. [2] have proposed the CLoud-based Attack Defense (CLAD) architecture for preventing DDoS attacks launched against Web servers. It is basically a distributed system which runs over a Cloud infrastructure as a security overlay network to protect Web servers by means of a set of smart collaborative and transparent web proxies. CLAD is not yet provided as a commercial product. *Imperva Cloud DDos Protection Service* [3] is an analogous commercial cloud-based service that protects Web applications from DDoS attacks using an overlay network. *McAfee SaaS E-mail* [4] and *McAfee SaaS Web protection* are also commercial products focused on e-mail and web protection which provide resiliency against DDoS attacks using a cloud-based solution designed as an overlay network for protecting e-mail services and web browsing, respectively. *Arbor Peakflow SP* [5] is another similar commercial service which provides DDoS protection for HTTP, VoIP and DNS servers.

For Intrusion Detection Systems (IDS), Vieira et al. [6] proposed an intrusion detection architecture suitable for grid and cloud computing environments in which audit data is collected from the cloud and two intrusion detection techniques are applied. Roschke et al. [7] have proposed an extensible and distributed IDS architecture for Cloud Computing. This architecture involves several IDS sensors which are distributed across the Cloud and a central management unit. Each protected endpoint is monitored by a separate sensor. Each sensor reports alerts to the central management unit which

gathers all alerts from all sensors and processes them. Attacks can be detected by the correlated alerts from different IDS sensors. However, this prior work does not design such solution as an overlay network to offer such security service as a transparent service for customers' protected endpoints. Finally, Guan et al. [8] described the basic features of a framework for the construction of a Cloud Provider intrusion detection system that an E-Government environment should fulfill.

As for Anti-Virus (AV) solutions, Yan et al. [9] and Zheng et al. [10] proposed an automatic malware discovery system for providing anti-virus software support using the cloud. They proposed a hybrid approach in which the client has a lightweight version of the malware signatures and the central Cloud-hosted AV service hosts the large database of signatures. A hybrid processing model is established between the desktop and the cloud AV services. Oberheide et al. [11] proposed an in-Cloud architecture called CloudAV in which each host runs a process to detect executables entering a system which are then sent into the network for analysis, after which they are either executed or quarantined based on a threat report returned by the network service. *McAfee SaaS Endpoint protection* is a commercial product for providing a cloud-based AV service in which all the malware and viruses are intercepted in the cloud before they reach the customer mail servers.

As for Email protection, Feamster [12] has proposed to shift from home-based spam filtering to a Cloud-based outsourced management and operation of this service by third parties which may have both operations' expertise and a broader view of network activity. The *Zscaler* system provides anti-spam services, among others, in the Cloud. It uses a proxy for filtering the network traffic into the Cloud. Analogously, *McAfee SaaS Email protection* also provides a cloud-based e-mail anti-spam solution.

4. Proposed Security Overlay Network

Figure 2 depicts an overview of the proposed architecture for providing an elastic security overlay network, i.e. a network that is deployed on-demand and grows as needed utilizing the virtual infrastructures provided by Cloud providers. As illustrated in Figure 2, our proposed architecture is generic in nature and it can be used for the deployment of any cloud-based security solutions. The proposed design architecture is comprised of primarily cloud security and management units in addition to protected endpoints of the customer network. Different management units are used to

support specific security solutions. We describe these units below. The protected end points include web servers, email servers, and normal production workstations and desktops.

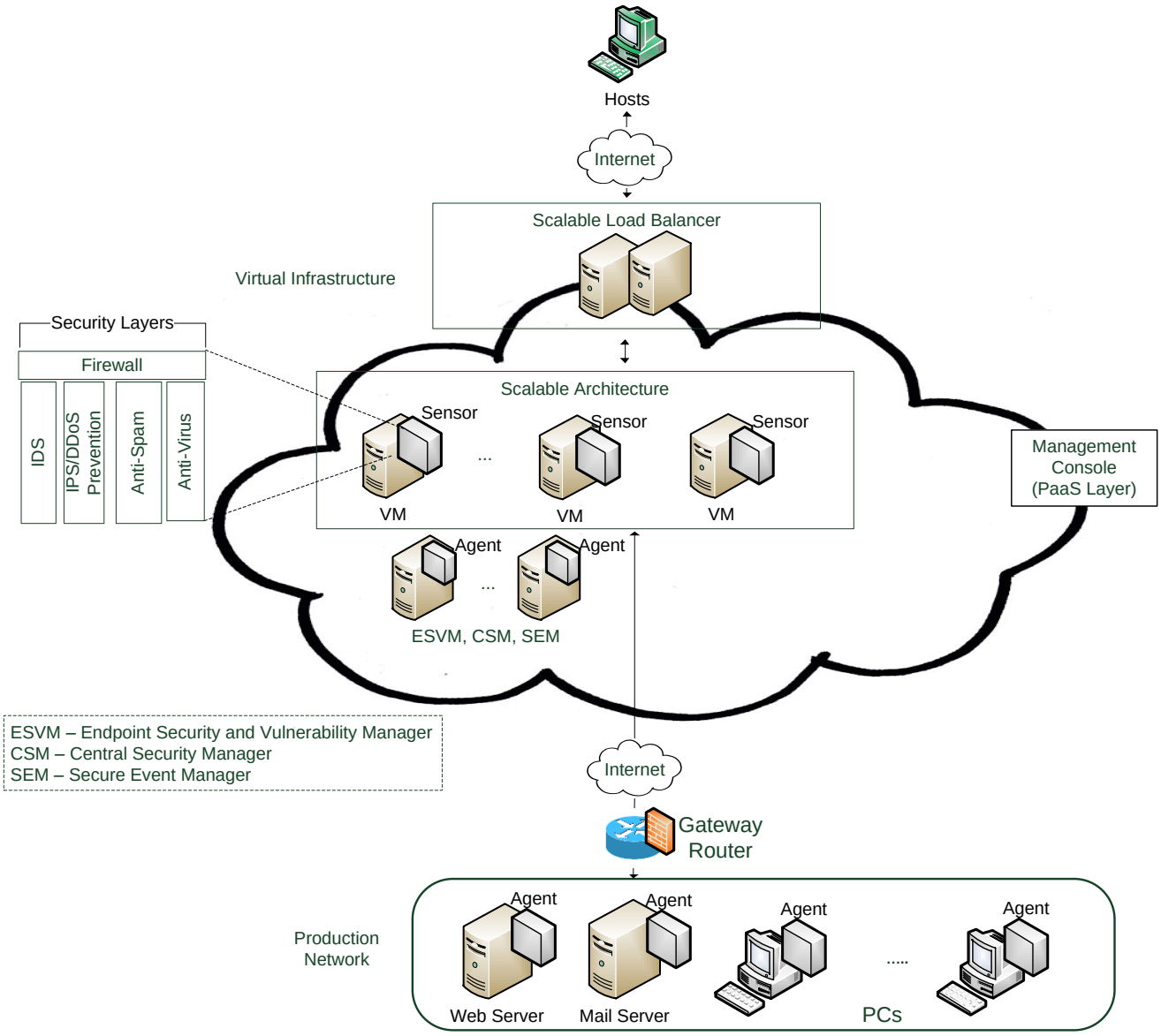

Figure 2. Conceptual Cloud-based Security Overlay Network

Agents are installed at protected endpoints of the customer's production network to handle or carry out any communication or computation requested by the cloud-based security central services employed in the cloud, or more precisely within the cloud-based security overlay network. The security overlay network implemented in the cloud is comprised of different security sensors and management units. Sensors are multi-purpose and can perform specific actions depending on the type

and the configuration of the cloud-based security solutions of interest. Each multi-purpose sensor is associated with a set of different security layers in which security checks are performed when information is crossing the sensor. A sensor acts as a proxy for monitoring the entire network traffic to a given customer's endpoint. We have chosen a proxy-based sensor because such an approach has already been validated by other research works [2] and by commercial solutions such as the provided by *McAfee*, *Arbor* and *Imperva* and this can benefit from the advantages of elasticity provided in the cloud.

It is to be noted that while the overall sensors of the cloud-based security services are deployed in a transparent overlay network, the management console for configuring such services is exposed to end-users. Such a configuration setting includes increasing or decreasing the virtual resources used by each of these security services.

4.1. Intrusion Detection System

A Network-based Intrusion Detection System (NIDS) passively monitors the traffic which traverses a given network which may carry malicious payload. Traffic is sniffed and captured by NIDS sensors. The collected data is analyzed to detect malicious activities and to respond or generate reports based on the detection. The NIDS examines the content of the network and the transport layer packet headers (such as TCP/IP), analyzes the sequence of packets and how these packets will affect applications that reside at the customer endpoints.

The location of the network-based device in a given network has a great impact on the malicious traffic detection. There is a need for a centralized strategic location to place network-based devices for analyzing intrusions. Also, an isolation of the network-based devices from their monitoring targets is clearly needed to overcome the shortcomings of traditional IDS systems. This can be accomplished by using in-cloud IDS systems in which the devices are moved to the cloud. Figure 2 shows the proposed cloud-based IDS architecture that contains NIDS devices which are sensors having the IDS security layer activated and deployed in the cloud as a Virtual Machine (VM). The NIDS devices communicate with each other to coordinate intrusion detection schemes. This communication is done using the standardized Intrusion Detection Message Exchange Format (IDMEF). IDMEF is also used to integrate different NIDS sensors' information and transfers such information to the *Central Security Manager* (CSM). This information is stored and retrieved in a *Security Even Manager* (SEM)

which is described later. This CSM is a cloud management unit which takes the role of gathering information from other sensors and processes the information from a global perspective. For this reason it does not constitute a central point of failure because if this unit fails, another VM will automatically take this role. The way to achieve this is by sending periodic alive messages to the well-known *CSM* and in case it does not respond, then the VM sending messages will take the role of the *CSM* and will notify the rest of the VMs about this change in the system structure.

When a host requests a service from any protected endpoint, the request has to pass through the in-cloud overlay network even if the endpoint is located in a virtual or a physical machine. Inside the cloud, a VM acts as a transparent proxy for the network traffic directed to a particular given endpoint. The way in which this transparency is accomplished is explained later in Section 5. The sniffed traffic information is processed by the associated sensor, and an alert or report is generated when necessary. It is worth noting that by inserting new on-demand NIDS sensors, the cloud elasticity mitigates the traffic bottlenecks of NIDS sensors when it is necessary do so.

4.2. Distributed Denial of Service Prevention

Most of the measures taken against DDoS attacks rely mostly on the use of prevention techniques. Generally, the collaboration between multiple prevention techniques such as firewall, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS) is the most widely adopted countermeasure. One of the well-known solutions is to use proxy servers between clients and the server. Note that these proxy servers are exactly the sensors described in the previous section but now, they are also acting as Intrusion Protecting System (IPS) because they are also able to enforce security protection techniques once the threat has been identified. In summary, the sensor performs the handshaking process with each client before forwarding the request to the endpoint or discarding it. This security solution introduces a potential bottleneck in the proxy server due to the latency associated with such processing. A trade-off between performance of the security solution and cost of the infrastructure has to be considered. Therefore, spending large amounts of money to prevent an attack that might happen with low probability is not a choice for small and medium size companies. As a result, cloud-based Anti-DDoS can be offered as an attractive and economical solution.

Figure 2 illustrates the underlying architecture of the in-cloud DDoS security solution. This architecture comprises VMs providing a fault-tolerance entry point for external nodes. The system is

set up as an overlay network in which protected endpoints should be isolated from the Internet and should only accept non-malicious requests. Each request from a client should be handled by at least one in-cloud VM to verify the client, and then relays the request to the protected endpoint. Otherwise the endpoint is never reached. Each VM acts in an independent manner filtering all the traffic. It acts as a firewalled transparent proxy with various control mechanisms, namely admission control, network-layer filtering and congestion control mechanisms. Elasticity in the number of VMs is actively used to mitigate DDoS attacks to the system. The network-layer attack defense sniffs all packets detecting any malicious packets such as SYN, HTTP and UDP flooding. All the malicious packets are then dropped by the active cloud firewall composed of VMs. Admission control limits the number of hosts served by the endpoints to only the legitimate ones. Note that this admission control acts as an access control to the production network for external hosts. Congestion control limits the amount of resources consumed by each client. This protects the server from exhausting its resources. All the endpoints only accept traffic coming from the cloud security solution, configured in the firewall available in the gateway router (see Figure 2). This firewall configuration hampers security threats which try to bypass the cloud-based overlay security solution to attack directly the protected endpoints. There is also a non-external visible coordinator point, analogous to the *CSM* (described in the previous section), which is in charge of detecting complex and selective DDoS attacks. This requires an analysis of the information of the sensors involved to identify the attack.

4.3. E-mail Protection

The premise with traditional anti-spam is that it can only detect threats or spam attacks which have already reached the enterprise network. Anti-spam does not proactively protect against network attacks. As the network of a typical organization grows, the centralized spam detection approach may not be able to support the different business locations. Scanning spam e-mails in the cloud enables their detection before reaching the target client. This early detection provides an efficient security system that can mitigate attacks by blocking them.

To date, some in-cloud anti-spam solutions are available on the market such as those of Symantec hosted Service and Zscaler. These solutions combine multiple commercial anti-virus and anti-spam engines, which result in a multi-layered defense to protect the client from email-based attacks. They detect embedded suspicious URLs in emails by the “following-link” capability and web links emails

are blocked in case malicious content is detected. This solution detects malwares that bypass the anti-malware and IDS/IPS systems. The solution examines email attachments,detects malicious ones and blocks them. With in-cloud anti-spam, the task of scanning for email with malicious URLs and attachments will be carried out by the cloud provider infrastructure which secures the enterprise network.

The proposed architecture for an in-cloud anti-spam solution is depicted in Figure 2. This architecture is composed of multiple mail servers as protected endpoints using different email protocols such as SMTP, POP3, and IMAP. The network traffic going to the mail servers passes through the in-cloud anti-spam security system. Then, mail traffic is proxied by the sensor and the associated anti-spam security layer processes it at the cloud provider. These anti-spam services analyze all inbound POP3 and IMAP traffic and the outbound SMTP traffic to detect spam mail. The in-cloud anti-spam engine is composed of several sensors used to implement distributed data processing. This feature enables load balancing to improve performance and spam detection if heterogeneous anti-spam solutions analyzed the same e-mail in parallel. The coordinator of all the sensors is involved in a mail inspection. This is a simple role which can be acquired by any sensor in a peer-to-peer fashion with no central point of failure.

4.4. Anti-Virus Service

The cloud-based AntiVirus (AV) security layer has been proposed in several places in the architecture. First, it is implemented as a security layer where all the files and malicious code filtered in the sensors are analyzed in real-time against a smart repository which acts as a collaborative repository where multiple users report threat activity collaboratively from around the world. It enables an efficient detection of the malware due to the up-to-date activity status of the threats which significantly reduces the time spent in performing the AV analysis. The idea is to provide, in real-time, the more probable signatures in the AV analysis in order to detect the current high active threats quickly. The cloud-based antivirus service is one of the security layers available in Figure 2. This cloud-based AV service is used in the previously described e-mail protection system to inspect e-mails and attached files for suspicious and malicious code.

At the endpoint, AV agents need to be installed in order to protect against malicious files coming from external sources such as USB flash drives, disks, CD, DVD, etc. In addition to obtaining the latest AV

signatures from the cloud, the AV agents in protected endpoints exchange AV reports of the analysis done locally with the cloud-based AV service. Such an exchange helps in keeping a centralized AV database of signatures up-to-date and also enables generating global AV reports to the cloud customer about the security health of the production network.

4.5. Endpoint Security and Vulnerability Manager

All the previously described security solutions focus on providing an overlay security solution in order to protect endpoints from external hosts. However, internal security threats are also critically important. The control of the security status of the internal hosts available in the production network needs to be managed. Traditionally, a centralized domain controller has been in charge of enforcing all the security policies, network access control and managing the hosts available in the domain. However, now the boundaries of the administrative domain are fuzzy because security is distributed between the cloud provider and the user's domain, and moreover, this domain controller requires an important hardware and software investment for network management purposes. A cloud-based Endpoint Security and Vulnerability Manager (*ESVM*) service can act as a domain controller in which all the security policies can be enforced and network access control can be determined based on such security policies. To this end, the proposed system for managing the security in the internal production network is depicted in Figure 2. In essence, all the endpoints available in the production network have installed an agent that enables the automated management of the security in the hosts and the exchange of information between them and the ESVM. Such an agent becomes a critical element of the overall Network Access Control (NAC) mechanism in which the agent enforces the installation, configuration and automated execution of the host-based antivirus, firewall and web browsing security solutions as well as the security policies defined by the domain administrator using the *ESVM* service such as the AV updates and Windows updates requirements. This way the agent acts as an enforcing point to handle any violation of the security policies.

The log and report information obtained by the agents are exchanged with the *ESVM* which stores this security information in a central repository - the *Secure Event Manager (SEM)*. This information is globally available. To provide fault-tolerance, the roles of *ESVM* and *SEM* can be assigned to any VM in the cloud using a P2P approach. The *ESVM* service is not publicly available to prevent attacks and ensure that only the production network can reach such VMs. The *ESVM* can also use active

techniques such as port scanners and security checks at the endpoints and passive techniques such as processing of logs in order to determine the vulnerability available in the production network.

The *Management Console* (shown in Figure 2) shows all the information provided by the different security systems involved from the *SEM* providing a global integrated status of all the interoperable security systems and the associated vulnerabilities involved in a unified, coherent and integrated manner to the domain administrator. This console can interact with all the security solutions in order to configure and administer the different parameters involved.

5. Proof-of-Concept Implementation

This section describes a Proof-of-Concept (PoC) deployment of our proposed architecture in order to show how a cloud security overlay network can be implemented to provide a sound security service for a small-size production network. We have implemented this architecture using today's available technologies, primarily using *McAfee*'s and *Imperva* cloud security solutions.

Our small-size production network comprises a *DNS*, *SMTP* and *WEB* servers along with the rest of hosts available in the internal network, 40 VM hosts. To create 40 VM hosts, we used 8 physical HP xw8400 Workstations, each equipped with Intel Xeon CPU at 3.00 GHz and 6 GB of RAM in which the Open Stack Diablo release has been installed. Each workstation runs 5 Windows VMs, totaling 40 virtual hosts. We configured our production network such that physical machines are isolated from both the Internet and VMs, and only the virtual hosts are protected with the *McAfee SaaS Protection Endpoint*. This setup makes the production network similar to the shown in Figure 2. The deployed cloud-based security solution is shown in Figure 3.

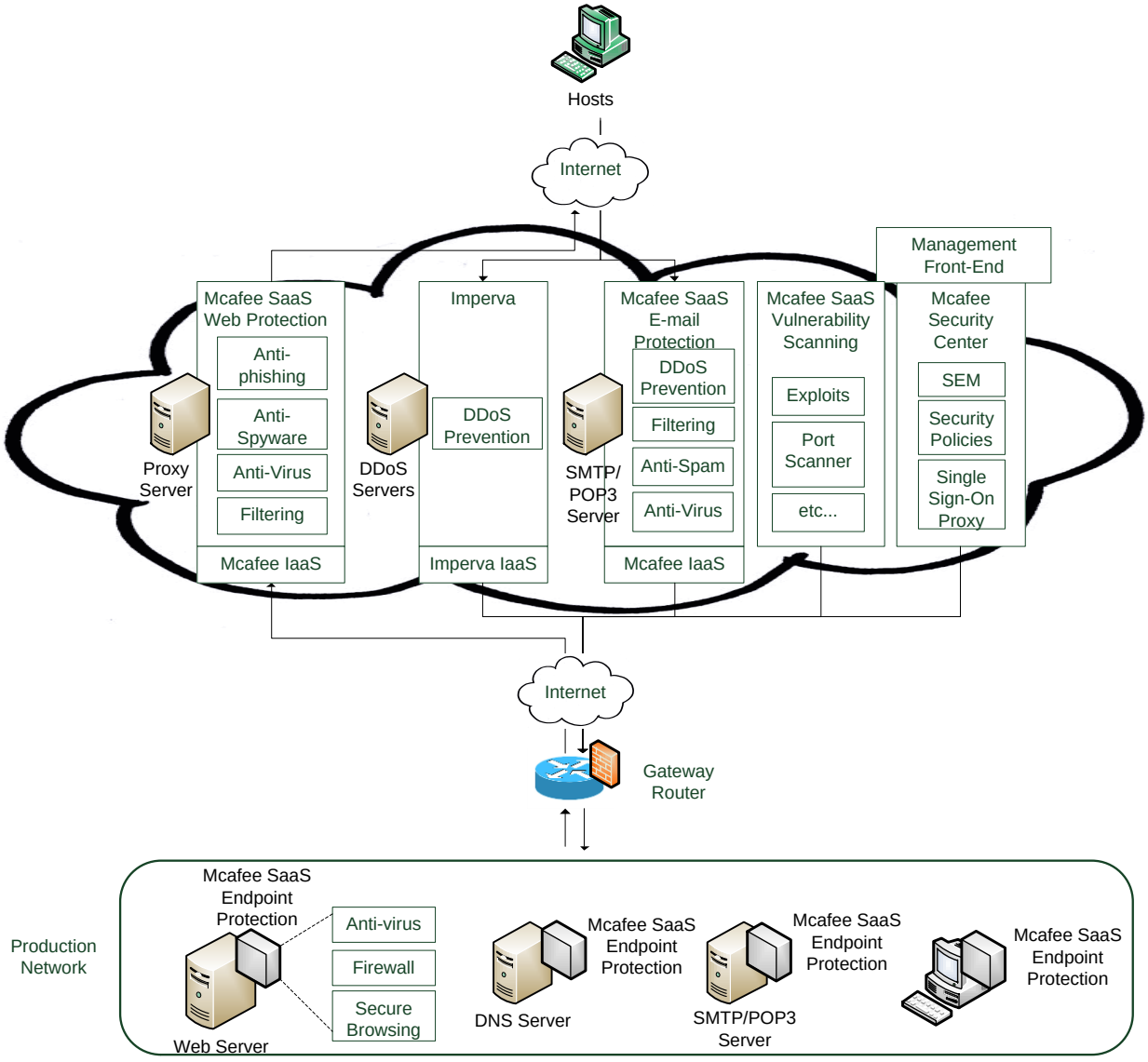

Figure 3. Deployed architecture using today's available commercial solutions

Our setup utilizes the security policies and network access control from the *McAfee Security Center* software which is similar to the *CSM* and *SEM* components shown in Figure 2. The configuration of the *McAfee Security Center* can be done online via a secure HTTPS web-based interface. This interface is also similar to the *Management Console* shown in Figure 2. We were able to manage and configure the firewall, web security, and all mail security aspects. The *Security Center* provides a central web interface where the rest of the other security services are integrated using *Single Sign-On (SSO)*. The traffic information generated by the endpoints available in the production network is filtered against anti-virus, anti-spam and anti-phishing using *McAfee SaaS Web Protection* service.

This service has been implemented as a transparent service from the hosts by a simple modification of the gateway router. Outbound traffic to this router is redirected to the *McAfee* service using a regular transparent proxy configuration. This modification is transparent to all hosts available in the internal network.

The gateway router exclusively allows incoming traffic from the *Mcafee* and *Imperva* servers to reach the production network avoiding any security thread attempting to skip the overlay network. Our mail server has been protected using the *McAfee SaaS Email Protection* service which analyzes anti-spam and anti-virus and protects against DDoS attacks to the mail server. This security system is enabled by a smart configuration of the mail servers' public MX DNS entries via inserting a *MX* entry which redirects all the inbound and outbound traffic to the *McAfee* services. This implementation acts as the anti-spam and anti-virus component shown in Figure 2. The *Cloud-based DDoS prevention* service provided by *Imperva* protects our corporate web server and all the incoming traffic to the production network against DDoS attacks by means of an IDS/IPS efficient solution. The only requirement for this deployment is to provide the *IP* associated with our web server to the *Imperva* security provider and a modification in our DNS (*A entry*) for which our domain name is resolved against the *Imperva* server. This service analyzed all the IP traffic received and acts as the DDoS prevention and IDS services shown in Figure 2. Note that the simple modification of these two DNS entries together with the basic setup of the gateway router allows a transparent overlay network which is not perceived by the hosts when accessing the production network.

It is to be noted that the *McAfee SaaS Vulnerability Assessment* solution provides a complete overview of all the vulnerabilities available in the protected endpoint network. This is an advanced solution for analyzing and managing vulnerabilities, risk and possible threats in all the hosts. This component is similar to the *ESVM* component shown in Figure 2.

6. Analysis of Cloud-based Security Overlay Network

This section discusses and analyzes the pros and cons of using cloud-based security overlay network in the context of our *PoC* implementation of the proposed architecture. We address key aspects related to resiliency to attacks, effectiveness, flexibility, control, costs and performance. To

accomplish this goal, we carried out a comprehensive penetrating testing using a *BackTrack* 5 R1 Linux distribution installed on an individual external host trying to attack the production network.

6.1 Network Security Assessment

The design of a transparent overlay network of security services has a key advantage over the traditional cloud-based solutions, particularly in concealing the internal network information of security appliances and production networks, thereby protecting against network enumeration and reconnaissance techniques. To evaluate this, we have tried to discover the security services running in the network by performing a complete port scan with *NMAP* over the DNS name of the domain associated to the production network. The list of open ports retrieved matches exactly 100% with the ports opened by the Web server which was configured in the *IDS* service as the default endpoint for all the legitimate IP traffic. The port scanner was detected by the overlay *IDS* and reported to the administrator via e-mail instantaneously. We also tried to discover management ports but the service was completely hidden. We also attempted to obtain information from the DNS name using a *whois* command but the information returned was that of the Web server belonging to *Mcafee*.

In addition, we have also evaluated accessing the cloud using the actual IP address of nodes resolved previously by the DNS server in order to bypass the overlay network. To account for this case, we configured the firewall *iptables* to redirect such direct traffic to the overlay security network to be analyzed. As for remote management and administration, a different IP address managed by the *Mcafee* and *Imperva* is provided. This IP address is the entry point for all the *Mcafee* customers using this service and requires a sophisticated monitoring. We have issued commands such as *whois* and *traceroute* for this IP address. Neither the *traceroute* information nor the HTTP header revealed any valuable network address.

Next, we have evaluated the resiliency and effectiveness of our proposed architecture against popular attacks and threats. First, we tested the effectiveness of the anti-spam detection. To accomplish this, we executed the *GFI* [13] email security test against an email client host with the *Mcafee Total Protection 2012* and also against an e-mail client host located in our PoC. The test sends 24 emails (out of which 22 were spams) to an e-mail client. With our PoC architecture, the email client received 2 emails, and the other 22 were correctly identified as spams. Whereas without the PoC architecture,

all the emails were received by the targeted email client. Second, we tested the effectiveness of the IDS. We executed a complete set of modern and sophisticated attacks using the *Metasploit Framework* 4.3 from the *BackTrack* 5 R1 Linux distribution. Specifically, we have launched: i) *SQL Injection attack (using SQLMAP external module)*; ii) *Cross-site Scripting attack* (using *XSSF module*); iii) *Remote File Inclusion attack* (Using the *php_include* module); and iv) *Directory Transversal attack* (using *VMWare Directory Transversal external module*). In all the cases, the attacks were detected, reported, and mitigated successfully.

Third, we have assessed the effectiveness of AV detection. Rather than performing a horizontal assessment to check for different viruses and malware, we have preformed a vertical assessment in order to test the architecture. We sent 5 e-mails with malware attached using both encrypted and non-encrypted SSL communications in the e-mail setup. In both cases, the malware was successfully detected and quarantined. We have tried to upload the same files to the Web server using both HTTP and HTTPS. In this case, the malicious HTTP upload was detected but the encrypted HTTP malicious upload was not detected. This is a limitation of the architecture.

Advantages. A cloud-based *NIDS* service may seem to offer equal effectiveness in detecting threats when compared with the traditional non-cloud solution. However, this is not clearly the case for the anti-spam and the AV services. With the AV service, the cloud-based solution is far more effective than the conventional approaches due to the large data collected from various sources (collective intelligence), thereby offering the opportunity to quickly respond to new threats. The cloud-based anti-spam service is also more effective because email spam and threats can be quickly detected before reaching the end user as stated in the penetration testing performed.

Disadvantages. The security effectiveness of the overall system primarily depends on the instant and the constant update, upgrade and improvement of the security tools offered by the cloud provider. To support this requirement, the cloud provider needs to state clearly in the SLA agreement the rate and constant update of signatures and tools.

6.2 Performance

Advantages. The elasticity of the cloud-based architecture enables an efficient distribution of the processing among multiple sensors with a load balancing mechanism that can reduce the latency. The

elastic nature of the cloud provider can be configured to provide enough flexibility. The endpoints are relieved of the processing required by traditional security solutions in which endpoints must do complete AV protection in addition to Web and spam filtering thereby enhancing the performance of endpoints. The bandwidth consumption of the production network is reduced because a good percentage of noisy and unwanted network packets are filtered by the overlay security network nodes. For example, SMTP consumes one third of an organization's bandwidth and about 90% of this bandwidth is used by spam mails.

Disadvantages. Some cloud-based security solutions, such as Web security or mail security introduce significant network latency because network packets get intercepted and examined in the cloud before being sent to the production network elements. The interception is done by placing sensors between clients and the production network. To quantify such a latency, we have sent 100 consecutive pings to the protected web server and we compare it with the unprotected web server scenario. The results show that the average times are about 78 ms vs. 53 ms. For the case of downloading a 5 kilobytes file, the average times are 1123 ms and 1179 ms, respectively. This additional delay can be further reduced with the introduction of faster and load-balanced sensors.

6.3 Flexibility

Advantages. The overlay design enables the extension, modification, upgrade and improvement of the security solution in a transparent way from the cloud adopters and users. The way in which the security solution is provided enables flexibility in growth and size. The unified set of security policies can ensure the same expected behavior for all the cloud users. The proposed architecture is flexible enough to provide security services to mobile and remote clients as well. The elastic nature of the cloud is a major benefit for the Anti-DDoS system to reconfigure on demand by adding and removing VMs when required in order to mitigate DDoS attacks. Additional benefits such as fault-tolerance and load-balancing are achieved by services that are directly provided by the IaaS provider.

Disadvantages. The scalability of the proposed architecture directly relies on the cloud providers. For example, *McAfee,* used in our implementation, uses data centers allocated in Sydney, Tokio, Denver, Atlanta, Santa Clara, London and Amsterdam to provide scalability for the proposed solution. However, this scalability management is out of the control of the customer. Another disadvantage is

the clear dependence which is established between the cloud provider and the customer being susceptible to receive an on-cascade attack.

6.4 Control

Advantages. The cloud-based network overlay solution offers a centralized point of security management in which the complete security aspects of the infrastructure can be configured, managed, and administered.

Disadvantages. The burden of maintenance and support is placed on the cloud providers which take control of the management of the security systems ensuring that everything will be running, up-to-date and correctly configured. The dependency on the cloud provider can cause potential security risks in terms of privacy, migration, reliability, and sniffed traffic. Such risks can be overcome if clear and detailed SLAs can be established to protect against abuse of leakage or disclosure of sensitive information.

6.5 Cost

The basic cloud-based security solution described in the previous section costs around $22 + 19N$ € per year, where N is the number of protected endpoints, or a cost of 782€ in our scenario. Using traditional IT approach, this solution would approximately cost 3100€ for hardware and $53N$ € per year for software maintenance, or in our scenario, totaling a cost of 5220€. Table 1 compares the cost of cloud-based security solutions with traditional IT security solutions used for our deployed scenario. The listed cost is based on advertised prices as of November 2011 gathered directly from official sources. According to VeriSign [14], a typical DDoS prevention solution requires at least 11 workers when compared to the cloud-based solution which may require 1 or 2 workers. Assuming an average IT engineering salary around 30000€/year (obviously, it depends on geographical locations), the difference in the investment is 5.5 times less expensive for the cloud-based solution. The costs involved demonstrate the maintenance and management of cloud-based security solutions can be very attractive.

Table 1. Cost comparison between traditional and cloud-based basic security solutions

		Traditional IT Solution	Cloud-based Solution
Complete Security Solution	**Basic Security Solution:** web, mail, and endpoint protection	McAfee Email and Web Security Appliance cost 3100€	McAfee SaaS web and mail protection cost 22€/year
		McAfee total endpoint protection standard costs 53€/year/VM	McAfee SaaS endpoint protection costs 19€/year/VM
	Vulnerability Management	McAfee vulnerability manager Starter Kit of 1000 IP addresses costs 8300€	McAfee SaaS vulnerability assessment costs 155€/year
	Advanced IDS/IPS DDoS Prevention	Hardware and software cost 75000€	Software costs 12000 €/year No cost for hardware
	Maintenance	11 Workers	2 Workers

Figure 4 and Table 1 compare the total annual cost of traditional and cloud-based security solutions with respect to the number of protected virtual host endpoints. We assume that a security hardware can handle a maximum of 1000 IPs. Figure 4(Left) shows the prices of the complete solution which may be adopted by big organizations, whereas Figure 4(Right) shows the prices of the basic solution which may be adopted by small and medium size organizations. The cost calculation in the figure take into account both security services and maintenance costs shown in Table 1. The calculation is based on linear formulas assuming a reasonable average lifetime of 7 years for hardware failure, with hardware acquisition costs divided over a period of 7 years with 0% interest.

Advantages. The results show how the complete and basic cloud-based security solutions are on average 3.6 and 3.5 times, respectively, less expensive for organizations with a size 0-100 PCs. For organization with a size of 101-500 PCs, the complete and basic solutions are on average 3.6 and 2.9 times cheaper. For larger sizes, both types of solutions are on average 2.8 times cheaper.

Disadvantages. In the case of a traditional non-cloud based solution, the acquisition of software licenses and hardware allows an organization to resell part of the equipment, thus recovering part of the investment made. This is not possible in case of the cloud-based solutions which are renting the services and hardware rather than owning them.

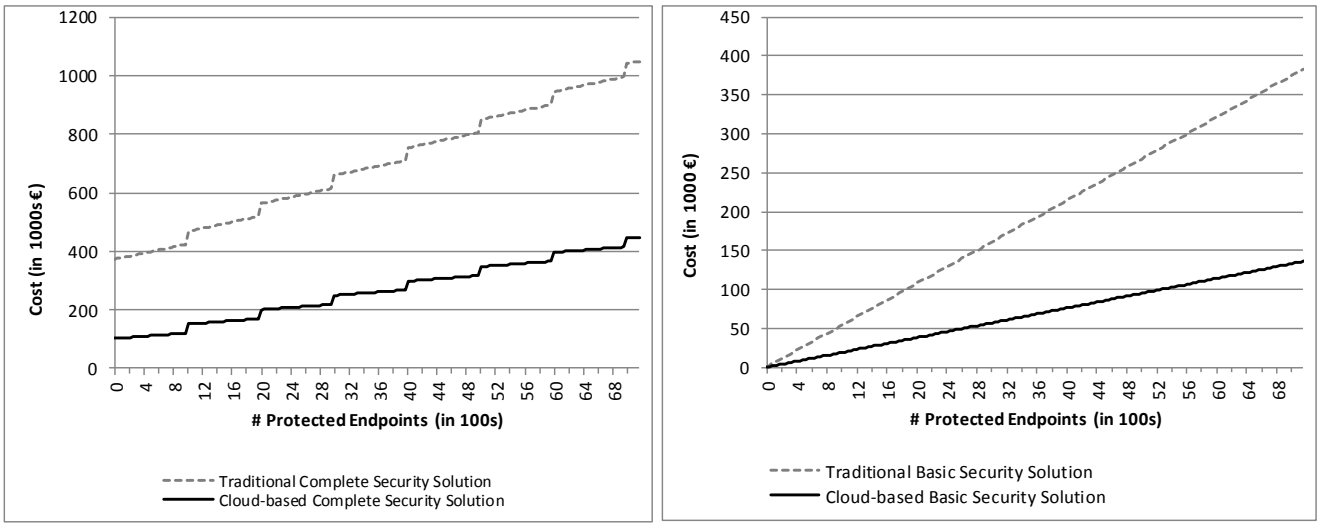

Figure 4. Comparing the cost of protection for cloud-based and traditional security solutions with the complete solution (Left) and with the basic solution (Right)

7 Conclusions

In this paper, we have discussed a wide range of security solutions and how they can successfully be deployed and supported in the cloud. These in-cloud solutions may include Intrusion Detection System (IDS), Anti-Virus software, Anti-Spam software and Distributed Denial of Service (DDoS). We have proposed a general architecture for a security overlay network that can be deployed over a cloud infrastructure. We have shown a real-world proof-of-concept implementation of our proposed architecture to protect a small-size production network. The implementation was done using today's available cloud technologies. We have discussed and analyzed our cloud-based security overlay network in the context of a small prototype implementation. In particular, we have addressed key aspects related to effectiveness, flexibility, control, costs and performance. We have shown that in general the cloud-based security solution is an attractive option in terms of cost, flexibility, effectiveness. However, future research work needs to be done to quantify the actual performance latency that could be associated with implementing cloud-security solutions.

Acknowledgements

We thank all the anonymous reviewers for their constructive comments which helped us to improve the quality and presentation of this paper. We are also grateful to the Associate Editor whose pertinent remarks also contributed toward further improvements of the paper.

References

[1] Takabi, H., Joshi, J. B. D., Ahn, G.-J.: Security and Privacy Challenges in Cloud Computing Environments. IEEE Security and Privacy. IEEE Computer Society. Vol. 8, Issue 6, pp. 24-31, 2010

[2] Du, P., Nakao , A.: DDoS defense as a network service. IEEE Network Operations and Management Symposium NOMS. pp. 894-897, 2010. Osaka, Japan.

[3] Imperva Inc.: Imperva Cloud DDOs Protection Service. http://www.imperva.com/products/wsc_ cloud-ddos-protection-service.html

[4] McAfee Inc.: McAfee SaaS E-mail protection. http://www.mcafee.com/es/products/saas-email-protection.aspx

[5] Arbor Inc.: Arbor Peakflow SP. http://www.arbornetworks.com/delivering-in-cloud-ddos-attack-protection-services.html

[6] Vieira, K., Schulter, A., Westphal, C.B.: Intrusion Detection Techniques in Grid and Cloud Computing Environment. IT Professional. IEEE Computer Society. Vol. 12, Issue 4, pp. 38-43. 2010.

[7] Roschke, S., Cheng, F., Meinel, C.: Intrusion Detection in the Cloud. Proceedings of IEEE International Conference on Dependable, Autonomic and Secure Computing, pp.729-734, 2009. Chengdu, China

[8] Guan, Y., Bao, J.: A CP Intrusion Detection Strategy on Cloud Computing. Proceedings of International Symposium on Web Information Systems and Applications, pp.084-087, 2009. Nanchang, China.

[9] Yan, W., Wu, E.: Toward Automatic Discovery of Malware Signature for Anti-Virus Cloud Computing. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. Springer. Vol. 4. pp. 724-728, 2009.

[10] Zheng, X., Fang, Y.: An AIS-based cloud security model. Proceedings of International Conference on Intelligent Control and Information Processing (ICICIP), pp. 153-158, 2010. Delian, China.

[11] Oberheide, J., Cooke, E., Jahanian, F.: Rethinking Antivirus: Executable Analysis in the Network Cloud. Proceedings of 2nd USENIX Workshop on Hot Topics in Security. August 2007. Boston, Massachusset.

[12] Feamster , N.: Outsourcing home network security. Proceedings of the 2010 ACM SIGCOMM workshop on Home networks, pp. 37-42, 2010. New Delhi, India.

[13] GFI Software. GFI Email Security Test, Available at http://www.gfi.com/emailsecuritytest/

[14] Duffy Marsan, C.: Verisign to extend cloud-based DDoS protection to SMEs. Computer World UK, Available at http://www.computerworlduk.com/news/security/3278805/verisign-to-extend-cloud-based-ddos-protection-to- smes/