SJIF Impact Factor: 7.001| ISI I.F.Value:1.241| Journal DOI: 10.36713/epra2016 ISSN: 2455-7838(Online)

EPRA International Journal of Research and Development (IJRD)

Volume: 5 | Issue: 5 | May 2020 - Peer Reviewed Journal

MONITORING AND ANALYSING SECURITY STATE OF IAAS AGAINST CYBER THREATS

Miss Pratiksha Bhagawati

MCA Scholar, School of CS & IT, Dept of MCA,Jain(Deemed-to-be) University,
Bangalore, India.

Article DOI: https://doi.org/10.36713/epra4369

ABSTRACT

Considering the sensitivity and damage of data that can be caused by cyber-threats in a cloud computing model, this work is proposed to studythe impact of various cyber threats and methods to minimize them. A comprehensive SIEM architecture to detect cyber-threatsand create immediate reports to mitigate them has been proposed. SIEM shall thus provide analysis of security alerts, review logs and perform auditing.

The proposed methodology will continuously monitor the security state against compute, networking, storage, data and application. It shall extend security posture management and threat protection to on-premises VMs. Another great advantage is that it shall provide global HTTP load balancing with instant failover.

KEYWORDS- *SIEM, cyber-threats, security alerts, logs, auditing, on-premises, global HTTP load balancing, instant failover.*

I. INTRODUCTION

Since the invention of cloud computing, large scale industries having been using it in order to take the advantage of quicker deployment, greater scalability, and cost saving of services. Enhancement of existing security features and addition of new features have led to the growth of cloud computing.In this era of rapid growth of IT industry, a cloud provider must keep track of consumer demands and requirements in order to keep up with the pace.

This project provides insights into some of the latest cloud practices and technologies information security practitioners must be aware of as IT and sensitive data extends beyond the traditional corporate perimeter. Providers, regulators, and the enterprise must cooperate to establish baseline security requirements across these services.

Understanding the use of cloud and related technologies along with the roles and responsibilities of data security and ownership up front will improve the procurement and long term management of these services.

The SIEM architecture here focuses on detecting cyber-threats and putting on a timely action thus by providing immediate incident response and creating reports which helps to meet compliance requirements. This is nothing but log analysis and auditing.

An analytical engine analyses the data and machine learning synthesizes it. This engine shall thus provide recommendations and threat alerts for protecting our workloads. We will know right away if there's been an attack or anomalous activity.

A secure endpoint service will provideHTTP load balancing and path-based routing rules for applications which are distributed across the globe. It will try to reach the destination using the fewest hops amongst the other routes available.

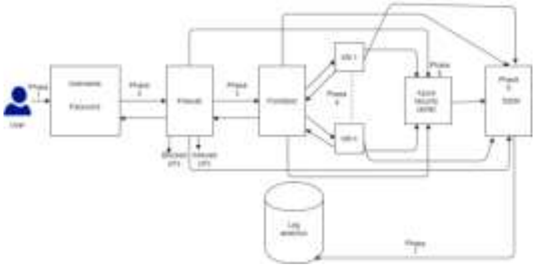


Figure 1. Architecture flow

II. LITERATURE REVIEW

[1]In this paper author proposed a safety protection framework for VMs to eliminate partial security risks, which contained access control, network abnormality detection, memory and files scanner for VM. The problem of VM information security monitoring in the cloud environment was studied, a VM monitoring method was proposed by online analyzing VM security state, networks, applications and data in the virtualization layer.

[2]The main contribution of this paper is the configuration of VMs with security tools for security-aware allocation of VMs in cloud systems. Based on the security analysis and evaluation of the virtual machine state, we have developed an architecture where the VMs can be placed following the best practice in security-aware manner. With the help of this the cloud platform can be secured ensuring reduction of security risks.

[3]IaaS cloud platform requires new virtualization-aware security solutions that have the ability to externally monitor and protect the hosted VMs externally. In this paper, we presented some CloudSecurity tools, a solution that provides active, transparent and real-time security monitoring for multiple concurrent VMs hosted on a cloud platform. CloudSecurity tools utilizes VMI techniques to monitor the hosted VM's memory externally, without installing any monitoring code inside the hosted VMs.

III. PROBLEM STATEMENT

The privacy of sensitive data and security of shared websites have become two major issues of cloud computing.The Infrastructure-as-a-Service (IaaS) landscape is dominated by the three major providers and their services often overlap with Platform-as-a-Service (PaaS) offerings. New capabilities further decouple hardware and software capabilities.

No matter how scaled the industry is and how many parties took the advantage of cloud services, but the cloud providerstill cannot be trusted as a third party. Cloud provider possesses a semi-trust nature because of which the traditional security models cannot be directly headed onto acloud based security framework.Traditional Security usually leads to zero-day vulnerability.

IV. SOLUTION

The proposed method will help cloud administrators to handle the cyber-threats flawlessly, check on network issues and to keep track on consumer requirements.

An analytical engine shall thus collect logs which can be very useful while at the time of analysis. These logs can be reviewed and further processed for auditing purpose.

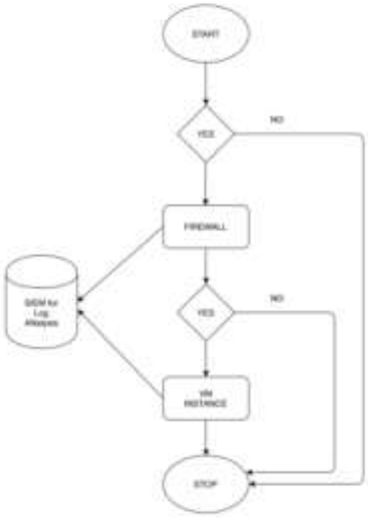


Figure 2. Flow Chart

In the above flowchart, initially users from internet tries to access the services that are provided by the VM instance that is hosted in private network using its public IP address. Later firewall filters the request whether the concern request is legitimate or not and allows the packet if it is authorized. If the data packet is trust worthy then access is provided to the services that are hosted in VM and all these logs are stored in SIEM for log analysis which can be used in future.

V. IMPLEMENTATION

5.1 Working

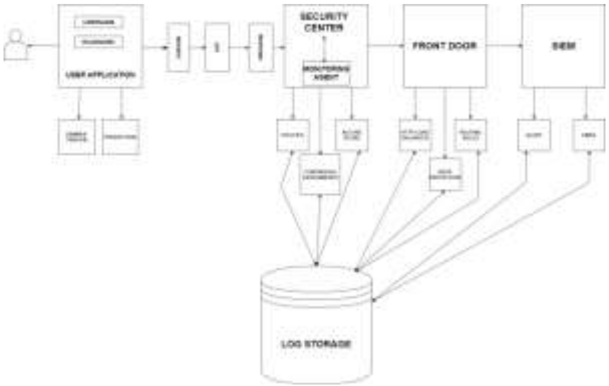


Figure 3. Model representation

The above figure represents how each and every entity is dependent on each other and how data traffic is travelled throughout the architecture. When user tries to access the website firstly the request is being inspected by firewall and firewall checks for the rules that are inculcated in it that is both inbound and outbound rules that are configured in it. If request is free from all these vulnerabilities website will be available for access to the internet user. Now finally, all these request movement is logged using SIEM and further can be used to examine the logs in order to escalate any issue before it persists. Logs are collected from all the available devices in the network that are configured to SIEM and this tool stores logs in segregated manner that is like firewall logs are kept isolated from vm logs and vm logs are isolated from firewall logs etc. which results in easy maintenance and analysis of logs.

When we activate Security Center, a monitoring agent is deployed automatically into Azure virtual machines. For on-premises VMs, you manually deploy the agent. Security Center begins assessing the security state of all your VMs, networks, applications and data.

An analytical engine analyzes the data and machine learning synthesizes it. Security Center provides recommendations and threat alerts for protecting your workloads. We will know right away if there's been an attack or anomalous activity.

When we activate Azure Front door, it shall provide global HTTP load balancing for applications which are globally distributed among various regions. The way this works is that it caches the static content of an application which it returns when an user tries to access the application without the need to do a server trick. It uses AnyCast, which means it will try to reach the destination using the fewest hops amongst the other routes available. So there can be multiple routes, but AFD(Azure Front Door) chooses the shortest and the fewest hops. User accesses applications, it goes to Azure Front Door Services and there it decides which region the request should be routed to.

This can be connected to SIEM and logs from both on and off premise can be made available in one centralized platform which reduces the workload on administrators by avoiding log management separately.

5.2 Software required

Virtual machine: A virtual machine is a virtual representation, or emulation, of a physical computer which provides the functionality similar to the physical computers i.e. they run operating system and applications on top of it and the fact that they are computer files, known as an images which runs on top of physical computers using the hypervisor, due to this the user has the liberty of running multiple operating systems on top of the main operating system without the need of buying additional physical resource. Just as the physical machine has two modes, however so must the virtual machine. Consequently, we must have:

- A virtual user mode
- A virtual kernel mode

Both of which run in a physical user mode.

The software inside a virtual machine cannot escape or tamper with the computer itself.

Hence virtual machine provides a computing environment which is ideal for testing and developing softwares, other operating systems including beta releases, creating operating system backups etc. It provides a faster booting process as well.

Microsoft Azure Security Center: Security Center provides security posture management for our cloud workloads.In Azure, it is important to understand that there are some sort of security within the workload that you put in azure on your side as a consumer. When it comes to security of the workload you put in, it is shared responsibility between customer and azure. These responsibilities include storage, virtual machines, application etc. So, the purpose of Azure security center is to monitor those security scenarios within the azure environment and then highlight any vulnerabilities identified. Thereby, this helps us to ensure that we are following best practices and fix common misconfigurations for Azure infrastructure as a service (IaaS) and platform as a service (PaaS) resources that may include:

- Failure to deploy system updates on virtual machines (VMs).
- Unnecessary exposure to the Internet through public-facing endpoints.
- Unencrypted data in transit or storage.

Security Center has the ability to both detect and help protect against threats. This tool alerts us against threats such as remote desktop protocol (RDP) brute-force attacks and SQL injections. And it provides actionable recommendations for mitigating these threats.

Microsoft Azure Front Door: Azure Front door service ensures application availability and maximize performance.

It provides the following features:

- Application and API acceleration.
- Global HTTP load balancing.
- SSL offload.
- WAF at the edge.

It additionally provides better performance and instant failover. Users experience better performance because it uses AnyCast and split DCP which provides lower latency thereby providing higher performance. Also it provides global HTTP load balancing enabling us to create applications that are globally distributed. One of the other features is that it provides SSL offload. This in turn takes that load off the web contents which do not have to encrypt or decrypt the request and that overhead is thus taken over by Azure Front Door. Finally it provides WAF(Web Application Firewall) for applications to provide security from DDoS attacks.

VI. EXPERIMENT

Things to configure:

- .VMs for hosting webserver
- Azure Security Center for monitor those VMs.
- Azure Front Door for global HTTP load balancing and WAF.

VII. RESULT ANALYSIS

1. Security Center

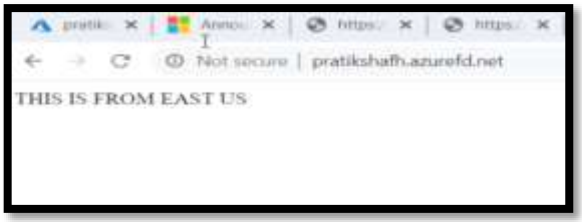
It shows the resource security hygiene of all the VMs such as which resources are under high security, medium security and low security and so on. It also detects networking issues with healthy and unhealthy resources, shows an overall Security Score etc.

2. Front Door

Considering an application which is distributed across two different regions, say, Central US and East US, Azure Front Door shall perform global HTTP load balancing using AnyCast. When the User tries to access this application, it goes to Azure Front Door Service and there it decides which region the request should be routed to.

Scenario I:

If the user tries to access the application and the region East US contains less hops (this is done through AnyCast) , then it shall load the one in East US.

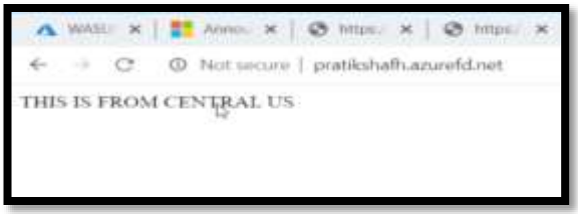


Not secure | pratikshafh.azurefd.net

THIS IS FROM EAST US

Scenario II:

If the user tries to access the application and the region Central US contains less hops (this is done through AnyCast) , then it shall load the one in Central US.



THIS IS FROM CENTRAL US

Here Azure Front Door (AFD) has performed HTTP load balancing for applications which are globally distributed. When the application at one region has gone down or has more hop count, the application from the other region has been put into play thus by caching the static content of an application which it returns when an user tries to access the application without the need to do a server trick.

VIII. CONCLUSION AND FUTURE ENHANCEMENT

We can implement a tool which should be able to show the virtual machines which do not have endpoint protection and then we should be able to install endpoint protection immediately with just a click away.

Apart from visibility, I would also like to add a feature where I can add Just in Time access configuration for VMs for maintenance purpose because it requires most protection from severe threats than some others. It will be done either through the graphical console or through powershell. It will basically work by selecting a management port that I want and selecting the maximum time that I want it to be open and then activate it. So after 20 minutes when we are down with our maintenance it will automatically lock those ports.

IX. REFERENCES

1. ***Author:**Xueyuan Yin; Xingshu Chen ; Lin Chen ; Guolin Shao ; Hui Li ; Shusong Tao College of Computer Science, Sichuan University, Chengdu, China Security as a Service for IaaS platforms, 2018*
2. ***Author:**Xuebiao Yuchi1, and Sachin ShettyEnabling Security-Aware Virtual Machine Placement in IaaS Clouds, 2015*
3. *Electrical and Computer Engineering, Tennessee State University, Nashville, TN 37209, USA*
4. *China Internet Network Information Center, National Engineering Laboratory for Naming and Addressing, Beijing, China*
5. ***Author:** Amani S. Ibrahim, James Hamlyn-Harris, John Grundy and Mohamed Almorsy Centre for Computing and Engineering Software SystemsCloudSec: A Security Monitoring Appliance for Virtual Machines in the IaaS Cloud Model, 2011*