



NETWORK ASSAILABLE ANALYSIS THROUGH LOG RETRIEVAL AND DEPLOYING SECURITY MECHANISMS OFF PREMISES

Mr. P R Kuber Gupta

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

Article DOI: <https://doi.org/10.36713/epra4306>

ABSTRACT

The model that is proposed in this article helps in securing both on and off premises networks of any organization without any ambiguity. Usage of SIEM tool for log retrieval and analysis, firewalls and other security mechanisms to protect environment from intruders helps in achieving a secured network platform. The proposed methodology helps in protecting organization's network from attackers or intruders through lateral movement detection.

KEYWORDS- *SIEM, firewall, security mechanisms, on premises, off premises, lateral movement.*

I. INTRODUCTION

Currently organizations are going through major industry transformation, one such is migrating from on premises to off premises. Here, on premises refers to traditional datacenter approach to house data and off premises refers to hosting data in cloud, which makes data available anywhere, anytime because of the nature of the technology.

Since, data is getting stored in cloud and as we know data is so precious in the current circumstances, we need to secure it from vandalizers or trespassers etc. The proposed methodology assists in providing security for data that is hosted in cloud as well as data that is stored in traditional datacenters. The architecture deals with deployment of security mechanisms and deployment of SIEM tool for log analytics. This helps in detecting lateral movement of attacker. Lateral movement refers to the process where the hacker get unauthorized access over one asset in the network and through that one asset he is capable of gaining access over other available assets

in the network, which is a serious threat to the entire network integrity, this can lead to compromise of entire network of an organization.

Firewall helps in tracking traffic movement of the network both inbound and outbound directions and also it filters the data packets and allows to reach network one which are legitimate and discards other which are not authorized to enter network.

WAF is another mechanism which stands for web application firewall that works solely for website or web application. It can prevent any attack (OWASP top 10 vulnerabilities) that leads to compromising of website or web application.

SIEM tool is used to gather logs from all the networking devices available in the network as wells as from the devices that are hosted on premises. This provides one single platform for log analysis of both on and off premises networking devices. Networking devices can be a virtual instance or a firewall or a WAF or routers or switches etc.

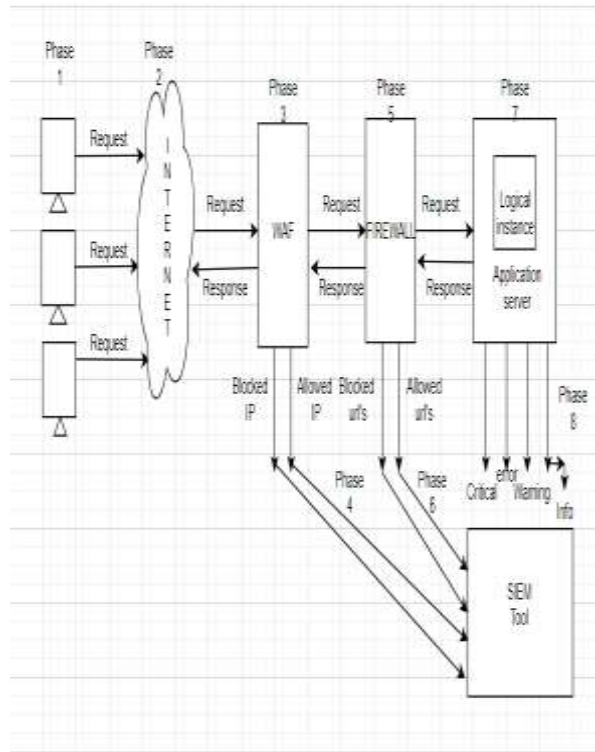


Fig 1. Architecture flow

II. LITERATURE REVIEW

^[1] In this paper author proposed a framework that helps in detecting lateral movement in network and also author stated that this framework can be prolonged to all the devices in network. And the paper also deals with event management by the means of SIEM usage.

^[2] Author in this paper stated that due to data migrating to cloud and security mechanisms are also getting transferred to cloud environment SIEM tool helps in gathering events that are occurring in the network and helps in securing the cloud environment effectively.

III. PROBLEM STATEMENT

Data stored on premises is bound to certain physical location but when data is migrated to cloud

that is off premises data can be distributed among multiple server instances this involves some serious security threats. And analysing logs from on premises and off premises separately increases workload on administrators.

IV. SOLUTION

The proposed method overcomes the snags that are faced by the administrators during the maintenance phase of network that can be either physical datacentre or cloud environment.

In the proposed model all the logs get stored in log analytics workbook and we can retrieve them whenever we need to analyse them.

Storing logs that are generated from all the devices that are present in network helps in avoiding lateral movement and effectively generate security policies.

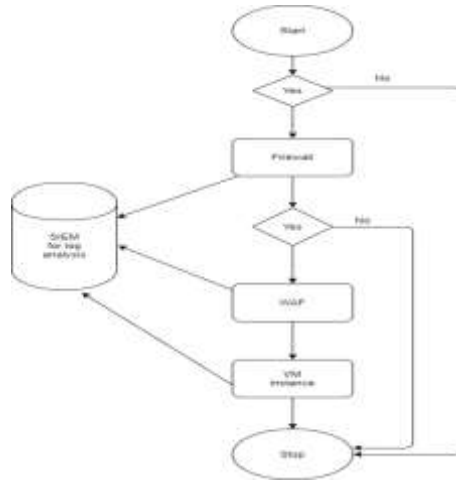


Fig 2. Flow chart

Flow chart above depicts that when a user from public network tries to access resources that are hosted in private network, first the request is traversed through firewall and if the firewall doesn't block the traffic the request further travels towards WAF and here request undergoes inspection once again, if request is found legitimate then access is

granted to the resources that are hosted in intranet, if the request is found malicious then traffic is discarded in the mid-way without reaching the resources. Resource here can be a VM that is configured as web server etc. and finally all these movement made by the traffic will be stored / logged in workbook using SIEM mechanism.

V. IMPLEMENTATION

5.1 working

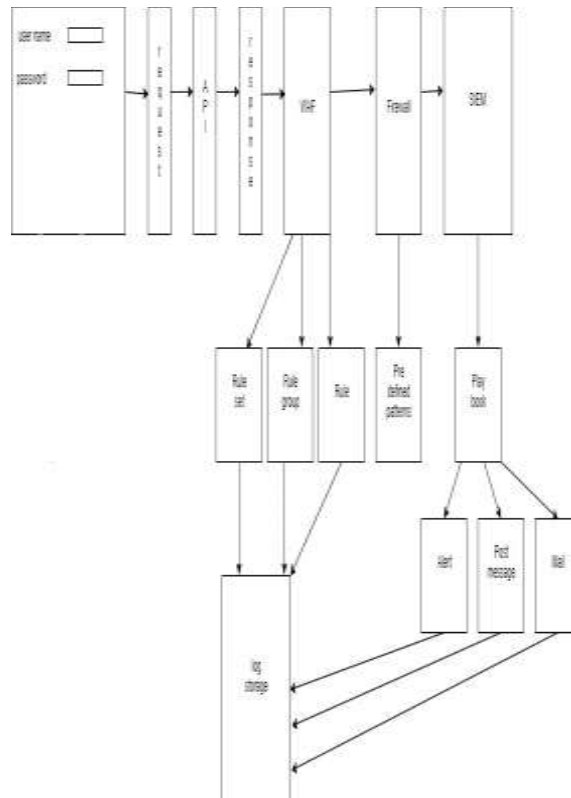


Fig 3. Model representation



The above figure represents how each and every entity is dependant on each other and how data traffic is travelled through out 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. Now WAF checks the request pattern that is if any malicious payload which leads to website comptonization is detected and dropped. It basically deals with OWASP top 10 vulnerabilities like XSS scripting attack, SQL injection attack, broken access control, sensitive data exposure etc. 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 WAF logs and WAF logs are separated from vm logs etc. which results in easy maintenance and analysis of logs. To gather logs from the devices that are hosted in traditional datacentre we can make use of connector that connects SYSLOG server that resides in datacentre with SIEM that is configured in cloud premises. Usually SYSLOG server is used to store all events using syslog mechanism from all the networking devices. 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

Azure sentinel

Microsoft Azure Sentinel is a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution. Azure Sentinel delivers intelligent security analytics and threat intelligence across the enterprise, providing a single solution for alert detection, threat visibility, proactive hunting, and threat response.

Azure Sentinel is your birds-eye view across the enterprise alleviating the stress of increasingly sophisticated attacks, increasing volumes of alerts, and long resolution timeframes.

- Collect data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- Detect previously undetected threats, and minimize false positives using Microsoft's analytics and unparalleled threat intelligence.
- Investigate threats with artificial intelligence, and hunt for suspicious activities at scale, tapping into years of cyber security work at Microsoft.
- Respond to incidents rapidly with built-in orchestration and automation of common tasks.

Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

Web Application Firewall

Azure WAF is a web application firewall that helps protect your web applications from common threats such as SQL injection, cross-site scripting, and other web exploits. You can define a WAF policy consisting of a combination of custom and managed rules to control access to your web applications.

Virtual instance

A VM is a simulation of a physical machine, such as a workstation or a server, that runs on a host that supports virtualization. Many VMs can run on the same host, sharing its resources.

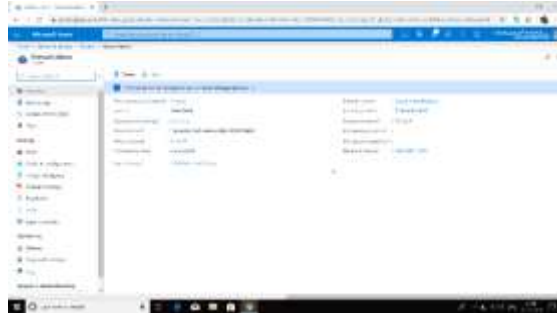
VI. EXPERIMENT

- Firewall for packet inspection.
- WAF for protecting web application or website.
- SIEM for log analytics.
- Vm to host webserver.

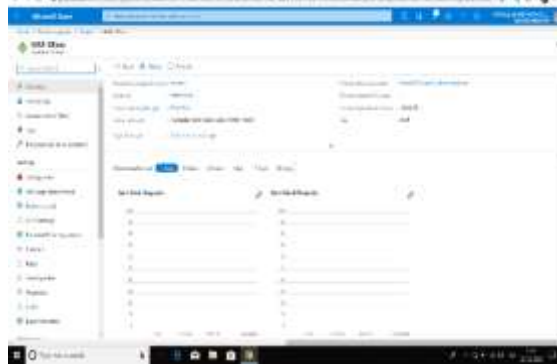


VII. RESULT ANALYSIS

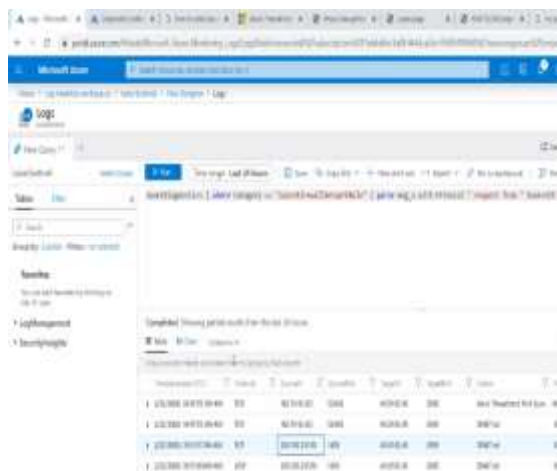
- Firewall to secure the infrastructure.



- WAF to protect web application or website from unauthorized access.



- SIEM for log analysis and storage.



VIII. CONCLUSION AND FUTURE ENHANCEMENT

Securing data (web application/ data/ CRM application/ financial information etc.) that is stored in cloud premises by utilizing efficient security mechanisms such as firewall for packet inspection, WAF for protecting web server from different attacks that can have huge impact on the business, SIEM for log analysis. This model helps in tracking users who

are trying to access the services that are available in the intranet of an organization this assists in securing the environment even more efficiently.

We can use the same SIEM for log analysis of the devices that are present on premises. This approach can make all the logs i.e. both cloud level and physical level logs centrally available in a single platform which reduces administrator’s workload. To achieve this, financial aid is required.



IX. REFERENCES

1. **Author:** *Airull Azizi Awang Lah, Rudzidatul Akmam Dziauddin, Marwan Hadri Azmi* Proposed Framework for Network Lateral Movement Detection Based On User Risk Scoring in SIEM, 2018.
2. **Author:** *Jong-Hoon Lee, Young SooKim, Jong Hyun Kim, Ik Kyun Kim* Toward the SIEM Architecture for Cloud-based Security Services, 2017.