International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2020): 7.803

Ideal Architecture for Security Operation Center Complementing Data Centers: An Overview

Ankit Srivastava[1], Jatin Nagpal[2]

[1]Senior Manager

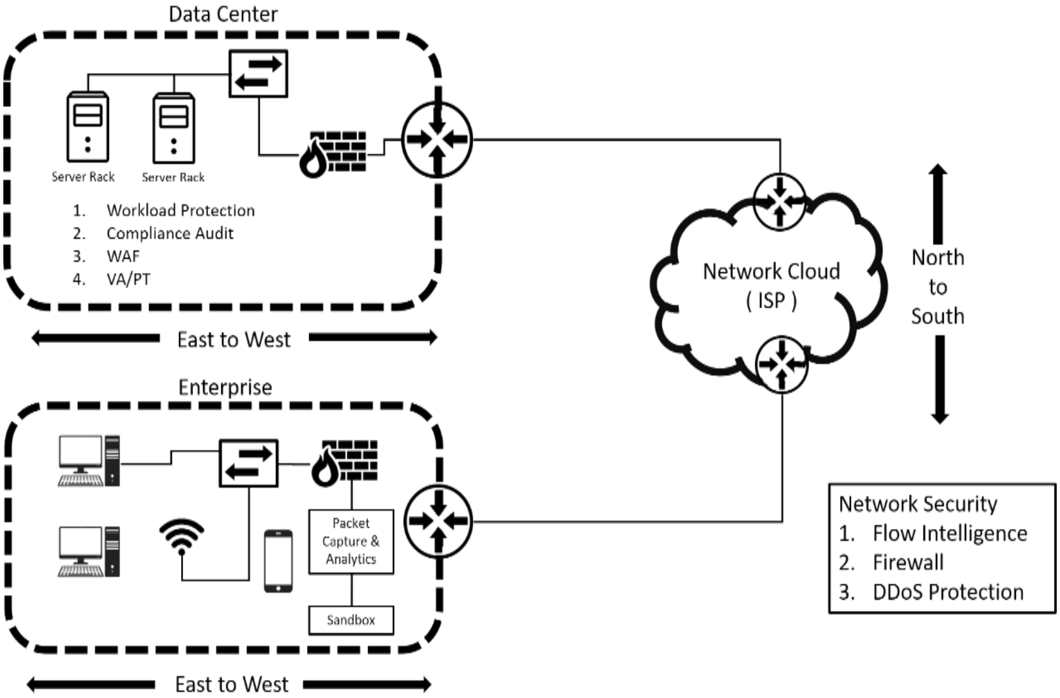
[2]Manager

Abstract: ***In today's cyber world every bit of information is precious and the attempt to exploit this is unprecedented. From script kiddies to state - sponsored hacking groups, all are continuously attempting to breach into the systems for various reasons including complete service disruption. Directly or indirectly all sorts of data are stored in data centers whether it is for cloud service or for on - premises solutions. Security operation centers compliment data centers by providing required security measures. To ensure the security of Data Centers lots of security features are required to be implemented which can be ensured by establishing a security operation center (SOC).***

Keywords: Security Operation Center, Multi - Layered Network, End to End Encryption, DDoS Mitigation, DNS Security Solution, SIEM, WAF, Workload Security, Network Behavior Analysis

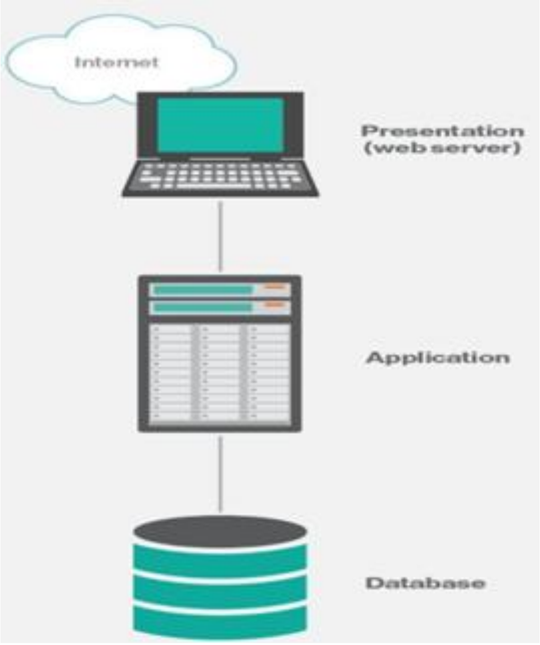
1. Introduction

In today's cyber world every bit of information is precious and the attempt to exploit this is unprecedented. From script kiddies to state sponsored hacking groups, all are continuously attempting to breach into the systems for various reasons including complete service disruption. Directly or indirectly all sort of data is stored in data centers whether it is for cloud service or for on - premises solution. Security operation centers compliments data centers by providing required security measure. To ensure the security of Data Centers lots of security features are required to be implemented which can be ensured by establishing a security operation center (SOC).



Traditional implementation of Security: In traditional implementation of security North to south traffic was usually protected by implementing firewall solution while for east to west traffic mostly end point protection solutions were used Components of SOC which should be implemented to protect data center, servers, services, network and customers infrastructure from any type of cyber - attack by using state of art technologies are mentioned below:

Multi - Layered Network: Layered deployment approach of the data centre design provides resiliency scalability and increases performance. From network perspective it may be divided into core layer, aggregation Layer and Access layer.



From application perspective also a three - tier deployment has been proven to be really effective. In this model architecture is bifurcated into web layer, application layer and database layer. Web layer is presentation tier which communicates with other two tiers. Logic part of the application is termed as application tier while the information is stored in data base tier. Though this implementation is logical but physical implementation is also feasible and makes the deployment more secure. To enhance security each of these layers may be applied with certain checks like whitelisting of IPs and authentication so that even these layers can not communicate with each other without authentication. Now if a hacker gets into web tier even then he will not be able breach into other layers.

End to End Encryption: A 100% protection against cyber threats cannot be ensured but end to end encryption makes attempts to misuse the information futile. Often, the motive of hackers is to steel the information but in case the data is encrypted then the encrypted data is useless for the hackers. So, the data should be encrypted in transit as well as at rest.

Security Solutions recommend to be implemented in Data Centers/NOCs for Protection Against Threats:

DDoS Mitigation: Distributed denial of service (DDoS) attacks are a subclass of denial of service (DoS) attacks in which multiple connected online devices also known as botnet exhaust resources of a legitimate website or application by flooding with fake traffic and the website become unavailable to the legitimate users.

1) Application (layer 7) attacks: DOS or DDOS attack that overloads a server by sending a large number of requests which are resource exhaustive. Some of the examples are DNS query flood, HTTP floods, slow attacks (e. g., Slowloris or RUDY).
2) Network layer (Layer 3/Layer 4) attacks: These are DDOS attacks which intends to choke the network by clogging the pipelines. Attack vectors in this category include NTP amplification, SYN flood, DNS amplification and UDP flood attacks.

A proven DDoS detection and mitigation solution must be implemented with a certain guaranteed clean pipe availability to mitigate the DDOS attack. For eg. If an organization has a traffic connectivity of 10G then it could procure at least 10G of on - premises clean pipe for volumetric attack. If the attack has more traffic than the guaranteed on - premises clean pipe then organisation should also opt for cloud - based mitigation. Certain organizations use on premises DDOS mitigation while some uses cloud based DDOS protection but best method is to opt for a hybrid model where on premises DDOS protection should be used primarily but in case the capacity of on - premises solution exhausts a switch over to on - cloud solution should be available.

DNS Security Solution: While DNS is invaluable to the Internet community, it isn't without vulnerability. When it was created, the Internet was significantly smaller and safer place, so there was little security in mind. A secure DNS is essential because it links the domain name to the IPDNS Security Solution ensures data integrity and authentication to security aware resolvers and applications through the use of cryptographic digital signatures. These digital signatures are included in secured zones as resource records. This happens at every step in the domain name translation process to ensure proper security. Through DNS Security Solution, organizations can block or redirect DNS requests to known malicious domains – based on threat intelligence – to stop users from visiting dangerous sites or malware from communicating with its operator. To have this visibility into this DNS traffic for analysis and redirecting, as an alternative to encrypting the full network path between the device and the external DNS resolver, we can use unencrypted DNS between devices and the gateway of the local network, but encrypt all DNS traffic between the gateway router and the external DNS resolver. Some of the most common Some of the most common DNS Security extensions added to the DNS RFC by IETF to help secure the DNS are listed below:

1) Cryptographic authentication of DNS data, usually with a symmetric key, since it consumes fewer network resources as compared to using asymmetric cartography.
2) Authenticated DoE (Denial of Existence), which allows the DNS resolver to tell whether or not a domain exists. At the same time, it can confirm that the yet - to - be - resolved domain does, indeed, exists.
3) Data integrity and authentication, ensured by binding crypto - generated digital signatures to the corresponding Domain Name Systems RR sets. Quick clarification – as Microsoft’s DNS documentation eloquently puts it, RR (resource records) are the “building blocks of host - name and IP information and are used to resolve all DNS queries”. Furthermore, DNNSEC also covers origin authentication – provides an extra security boost.
4) Response Policy Zones, which consist of laying down a set of rules regarding what your DNS queries can look and cannot look when interrogating a recursive DNS server. It is very useful in decreasing the chances of querying domain names that could be linked to malicious servers.

Firewall / IPS: A next - generation firewall includes additional features like application awareness and control, integrated intrusion prevention, and cloud - delivered threat intelligence apart from features already provided by existing firewalls like stateful inspection of incoming and outgoing network traffic. An NGFW has IPS integrated into it, hence for full utilization of NGFW, https traffic passing through NGFW must be decrypted for application of IPS rules on it otherwise https attacks would go unnoticed due to NGFW unable to read traffic. It is necessary for data centres to deploy NGFW which can do deep packet inspection, have automation functionality, AI aware and make fine grained distinctions which cannot be done by traditional firewalls.

End Point Protection: Endpoint security must be installed on all the servers (including VMs) and should be centrally monitored and managed. Only the required ports should to be opened and server hardening must be performed before installing the application. There must be regular update check frequency and the updates must be installed on a test server first to avoid any ill impact. The end point solution must be capable of anti - malware, anti - spyware protection, device and application control, intrusion prevention and firewall, memory exploit mitigation, signature less behaviour - based detection.

Security Information and Event Management (SIEM): SIEM can be considered as the brain of SOC. Proper implementation of SIEM saves significant time of SOC analyst to identify a threat. It facilitates analysis of all types of logs (pattern/anomaly in logs) which are forwarded to SIEM e.g. Syslogs, firewall & IPS logs, OS logs, DNS logs, WAF logs, Proxy logs and application logs. It is recommended that SIEM be integrated with a ticketing system so that whenever an event occurs an auto ticket can be opened and assigned to the concerned security analyst. This will help in proper tracking and performing trend analysis on the kind of security events being generated for the organization. This can also help in building a knowledge database.

Web Application Firewall: Web Application Firewall for securing web application and protecting web application against OWASP top 10 vulnerabilities and other possible web application vulnerabilities. WAF can be initially implemented in learning mode where it will learn the behaviour network towards application. Post that WAF can be implemented in enforce mode. WAF can provide

Work Load Security: Some of the features of work load security which are recommended to be implemented are given below:

1) Application and protected whitelisting, Protect servers from zero - day attacks
2) File, system and admin lockdown.
3) File integrity and configuration monitoring
4) Secure unpatched applications and systems running on legacy and end - of - life platforms
5) Monitor and protect physical and virtual data centers using a combination of host - based intrusion detection (HIDS), intrusion prevention (HIPS), and least - privilege access control.
6) Enable application and instance level security
7) Gain continuous monitoring of data center infrastructure for cyber security and compliance
8) Provide visibility, compliance and hardening.
9) Simplified policy creation in learn mode helps build rules via automated sandboxing.
10) Easily identify abnormal event activity and also monitor your key performance indicators.

Network Behavior Analysis (NBA): NBA works on Netflow which is forwarded from L3 device for analysis. Netflow is a standard protocol to send ip flow of connected devices. An IP flow consists of a group of packets that contain the same IP packet attributes. As a packet is forwarded within a router or switch, it is examined for a set of attributes, including IP source address, IP destination address, source port, destination port, Layer - 3 protocol type, class of service and router or switch interface.

2. Conclusion

Above security solutions are recommended to be implemented in data centers for security of application and servers. However, along with the mentioned solutions some additional steps are also required to be taken for enhanced security and monitoring:

1) Security administrators should block the IoCs on all applicable security solutions.
2) Security administrators are strongly recommended to apply the latest security patches for IoT and Router devices from specific vendors.
3) Security administrators should minimize Internet exposure for Linux servers and IoT devices and use a properly configured firewall.
4) Use application whitelisting to allow only approved programs to run on the systems and use Multi - Factor Authentication (MFA) wherever possible.
5) Security administrators should make sure that all applications, databases, servers, and network devices are periodically hardened and are adequately configured.
6) Organizations should conduct a periodic security assessment and architecture review of critical assets exposed over the Internet.
7) Security administrators must change the default ports for critical services and only open the minimum ports required by each device.
8) System administrators should regularly take Backup of the applications, databases, and all critical data.
9) Security administrators should apply the Principle of Least Privilege to all systems and services.
10) Keep AV signatures, operating systems, and third - party applications up to date on all systems, mobile devices, and servers