International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Fortifying Electronic Medical Record (EMR) Applications: Advanced Security Controls in Oracle Cloud Infrastructure (OCI)

Velmurugan Dhakshnamoorthy

Lead Technical Architect, Tech Mahindra, Singapore

Abstract: ***This case study presents a comprehensive security framework for Electronic Medical Record (EMR) applications deployed in Oracle Cloud Infrastructure (OCI) (Oracle, 2022). The framework utilizes a Hub & Spoke network design to centralize security management and streamline traffic flow (Oracle, 2022). It integrates advanced security controls, including firewalls and intrusion detection systems, to protect against malicious activities. The framework ensures secure data handling with North - South and East - West traffic inspection and segregation of internet and intranet traffic. Regular security audits and continuous monitoring maintain data integrity, confidentiality, and availability, offering healthcare organizations a secure, scalable, and efficient cloud infrastructure for EMR applications.***

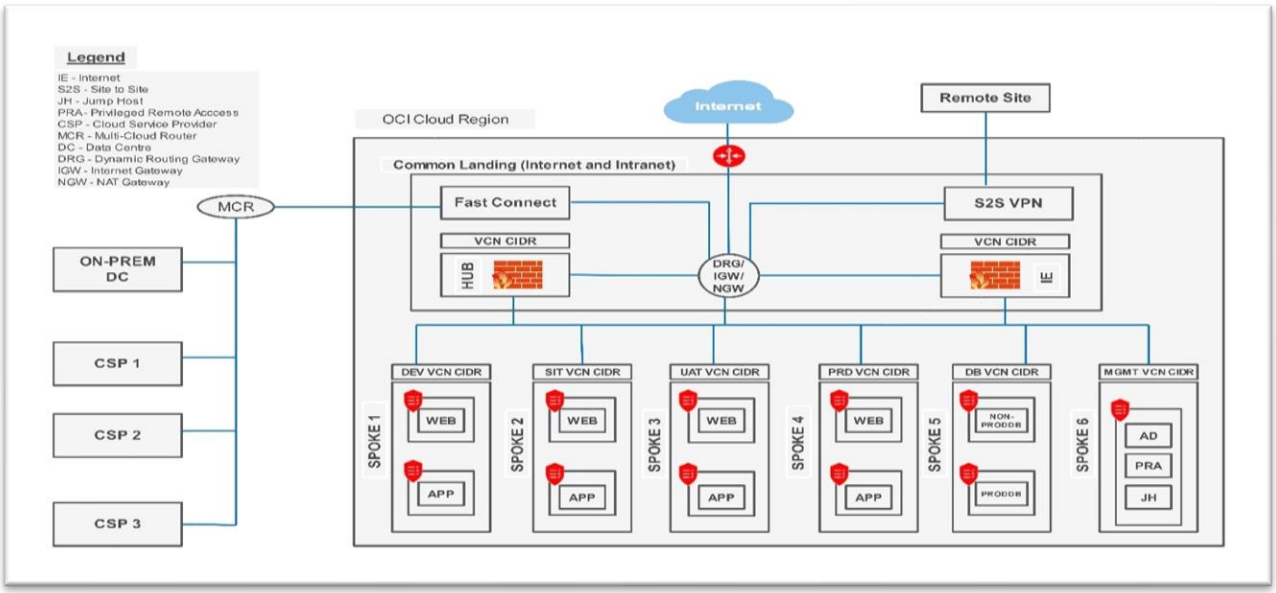
Keywords: Oracle Cloud Infrastructure, Electronic Medical Records, Network Security, Hub & Spoke Model, Healthcare Cloud Security

1. About EMR

An Electronic Medical Record (EMR) system securely manages patient health data throughout their lifecycle, integrating with applications such as labs, radiology, and telehealth software. It is crucial to detect, inspect, and protect against threats, including insider and outsider attacks, Phishing, Fraud, Data Breaches, Malware, Encryption Blind Spots, Cloud Risks, and Human Error. Comprehensive security measures maintain the integrity, confidentiality, and availability of patient data, fostering a secure and efficient healthcare ecosystem.

2. EMR Deployment in OCI:

The EMR application has been meticulously architected and implemented in Oracle Cloud Infrastructure (OCI) to ensure scalability, resilience, fault tolerance, high availability, and security. Utilizing different fault domains within the same region, this deployment guarantees uninterrupted service and optimal performance. The Hub & Spoke networking model enhances security and data flow management, enabling the robust handling and efficient processing of large volumes of sensitive patient information, thus providing a reliable and secure environment for healthcare applications.



3. Solution Highlights

Hub & Spoke Network Design:
A hub - and - spoke network design connects multiple nodes (spokes) to a central hub, enhancing security and management (Oracle, 2022). As noted by Oracle (2022), this design streamlines security management and enforces consistent policies. It allows efficient traffic inspection, simplifying access control to prevent unauthorized access. This design supports easy scalability and cost - effective security by reducing redundancy. It also facilitates network segmentation, limiting the spread of threats, and enhances monitoring and auditing for a robust security posture. This approach ensures seamless integration and optimal data flow across diverse environments.

Inspection and control of NS (North - South) traffic:
North - South (NS) traffic involves data from various Cloud Service Providers (CSPs), on - premises systems, and hospital locations (Oracle, 2022). According to Oracle's documentation (2022) Incoming traffic initially reaches the Dynamic Routing Gateway (DRG), which routes it to the hub firewall, equipped with Intrusion Detection and Prevention Systems (IDPS) for thorough inspection. Utilizing whitelisting and block listing mechanisms, the firewall ensures only non - malicious traffic proceeds to the spoke Virtual Cloud Network (VCN). Within the VCN, additional security measures like security lists and Network Security Groups (NSGs) are implemented to secure access to workloads. Based on predefined rules and routing, return traffic is directed back to its origin.

Inspection and control of ES (East - West) traffic:
East - West (ES) traffic involves data exchanged within the cloud between spoke Virtual Cloud Networks (VCNs). When initiated from one workload spoke VCN, the egress traffic exits to the Dynamic Routing Gateway (DRG) based on predefined SL and NSG rules. The DRG routes this traffic to the hub firewall, which uses Intrusion Detection and Prevention Systems (IDPS) along with whitelisting and block listing mechanisms for inspection. Once verified as non - malicious, the traffic is allowed to proceed to the target spoke VCN, where additional security controls, such as security lists and Network Security Groups (NSGs), are in place. Return traffic is directed back to the originator based on predefined rules and routing

4. Segregation of Internet and Intranet Traffic:

Internet Traffic:
Internet traffic, initiated from external sources, follows a different route than intranet traffic. It reaches the internet gateway attached to the public subnet and is inspected by a separate firewall in the hub using IDPS, anti - virus, and whitelisting features. Once cleared, it proceeds to the spoke Virtual Cloud Network (VCN), passing through a public load balancer. Backend servers reside in private subnets, and traffic is further inspected by a Web Application Firewall (WAF) to mitigate OWASP top 10 attacks. Internet - based applications may route through a CDN before passing through the public load balancer, WAF, security lists (SL), and Network Security Groups (NSG). Outbound traffic follows predefined rules and routing within the VCN and firewall.

Intranet Traffic:
Intranet traffic is routed via the Dynamic Routing Gateway (DRG), which directs it to the hub firewall. Here, Intrusion Detection and Prevention System (IDPS) features are employed, along with whitelisting and block listing mechanisms, to inspect the traffic. Once verified as non - malicious, the traffic proceeds to the target spoke Virtual Cloud Network (VCN), typically passing through a private load balancer for intranet - based applications. Additional security controls, such as security lists and Network Security Groups (NSGs), are implemented within the VCN. Return traffic follows predefined rules and routing back to the initiator, ensuring secure and efficient communication.

5. Conclusion

This case study highlighted the critical aspects of managing and securing cloud environments. By examining the overall infrastructure and networking landscape, we emphasized the importance of a well - structured foundation. The Hub & Spoke Network Design's role in centralizing security and ensuring efficient traffic flow was showcased, along with detailed inspections and controls for both North - South (NS) and East - West (ES) traffic. Finally, the article discusses the segregation of internet and intranet traffic, illustrating the application of various security protocols. This comprehensive approach provides a clear understanding of achieving a secure and efficient cloud infrastructure.

References

[1] Velmurugan Dhakshnamoorthy, "Technical Architect, Lead, " *Fortifying Electronic Medical Record (EMR) Applications: Advanced Security Controls in Oracle Cloud Infrastructure (OCI)*, vol.13, no.11, p.3, 2024.
[2] Oracle. (2022). Hub & Spoke Network. Retrieved from (https: //docs. oracle. com/en/solutions/hub - spoke - network/index. html)
[3] Oracle. (2022). Dynamic Routing Gateway. Retrieved from https: //docs. oracle. com/en/solutions/hub - spoke - network - drg/index. html