International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

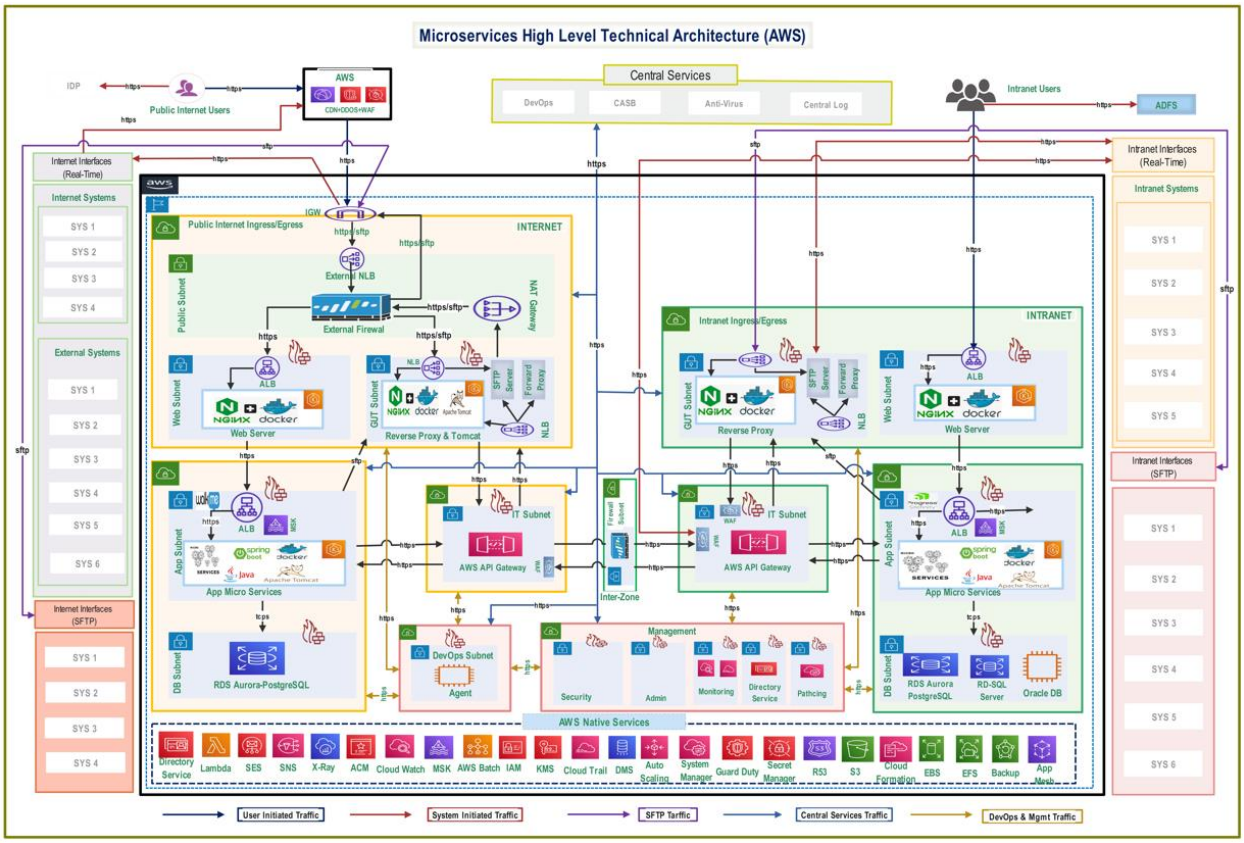
Architecting Secure Microservices Deployments on AWS

Velmurugan Dhakshnamoorthy

Lead Technical Architect, Tech Mahindra, Singapore.

Abstract:
In the rapidly evolving digital era, microservices deployments have become indispensable for businesses aiming for enhanced scalability, flexibility, and resilience. By fragmenting applications into smaller, autonomous services, organizations can scale individual components, optimize performance with specific technology stacks, and improve fault isolation, thereby minimizing the risk of comprehensive system failures. However, ensuring robust security is of utmost importance. This article delves into key security frameworks and architectural designs employed in AWS to provide comprehensive protection for microservices deployments, safeguarding them from potential threats and vulnerabilities.

Keywords: Microservices, AWS Security, Network Isolation, Traffic Management, Granular Controls



Internet and Intranet Isolation:

To ensure stringent security measures, the architecture employs distinct Virtual Private Clouds (VPCs) for

both internet and intranet applications. This separation, achieved via dedicated subnets, Network Access Control Lists (NACLs), and Network Security Groups (NSGs), minimizes the attack surface and enhances traffic flow control. This segmentation not only isolates different types of traffic but also ensures that any security breach in one VPC does not affect the other, thus fortifying the overall security posture.

Integration VPC with API Gateway:
A critical aspect of this architecture is the Integration VPC, which houses the API Gateway. This gateway is pivotal in managing authentication, authorization, and payload inspection for all API traffic, ensuring that all communication between the internet and intranet is centralized and securely regulated. By leveraging API Gateway, organizations can enforce strict security policies and monitor API traffic for any suspicious activities, thereby enhancing the security of the communication channels.

Granular Traffic Controls:
The architecture implements stringent communication controls, allowing specific flows between services. Web services exclusively interact with application services, which in turn communicate solely with databases and integration components. This approach enforces meticulous control over traffic across various VPCs and subnets, reducing the risk of unauthorized access and data breaches. Such granular traffic management ensures that only authenticated and authorized requests are processed, maintaining the integrity and confidentiality of the data.

Human Traffic Channels:
Human traffic is meticulously directed through Internet and Intranet Web services, establishing a structured entry point for users. System-level inbound and outbound traffic strictly adheres to designated gateway services for both internet and intranet scenarios, ensuring secure and organized traffic flow. This segregation of human traffic channels helps in monitoring user activities and preventing unauthorized access to sensitive resources.

Centralized Management VPC:
A dedicated management VPC serves as the central hub for essential services such as security, patching, monitoring, logging, administration, and directory services. This shared resource optimizes efficiency and consistency across both internet and intranet components, ensuring that security policies and updates are uniformly applied. Centralizing management functions also simplifies compliance and audit processes, enhancing the overall security governance.

DDoS Protection and WAF:
To protect against Distributed Denial of Service (DDoS) attacks, a strategically integrated Content Delivery Network (CDN) is deployed. Additionally, a Web Application Firewall (WAF) is used to defend against top OWASP attacks, thereby bolstering the security of internet-facing services. These tools not only mitigate the risk of DDoS attacks but also filter out malicious traffic, ensuring that legitimate traffic reaches the intended services without any disruption.

Microservices Deployment with EKS:
Microservices are deployed within application subnets, encapsulated in Docker containers, and orchestra-

ted using Amazon's Elastic Kubernetes Service (EKS). Network Load Balancers (NLBs) and Application Load Balancers (ALBs) are strategically placed across different VPCs and subnets to ensure optimal load distribution and fail-over capabilities. By leveraging EKS, organizations can benefit from advanced security features such as network policies, IAM roles for service accounts, and encrypted secrets management, thus enhancing the security of microservices deployments.

Holistic AWS Native Services:

The architecture seamlessly incorporates various AWS native services, spanning Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), resulting in a well-integrated and comprehensive solution stack. By leveraging AWS-native security services such as AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), and AWS CloudTrail, organizations can ensure end-to-end security for their microservices deployments.

Real-time and SFTP Communications:

Both internet and intranet VPCs are equipped to facilitate seamless communication with real-time and SFTP services, supporting diverse functionalities across the ecosystem. By implementing secure protocols and encryption mechanisms, the architecture ensures that data in transit is protected against interception and tampering.

Conclusion:

In conclusion, architecting a secure network for microservices deployments on AWS is crucial for modern businesses aiming to maintain robust security while achieving scalability, flexibility, and resilience. By implementing stringent security controls through distinct VPCs, utilizing a centralized API Gateway for secure communication, and enforcing granular traffic management, organizations can significantly reduce their attack surface and enhance overall security. Moreover, integrating advanced tools like DDoS protection, Web Application Firewalls, and Kubernetes orchestration within AWS ensures that each microservice is shielded against potential threats and vulnerabilities. By leveraging AWS native services and dedicated security frameworks, businesses can deploy microservices with confidence, ensuring that their digital infrastructure remains secure, scalable, and efficient in an ever-changing digital landscape.

Bibliography

1. Velmurugan Dhakshnamoorthy, "Technical Architect, Lead," *Architecting Secure Microservices Deployments on AWS*, p. 3, 2024. https://docs.aws.amazon.com/whitepapers/latest/microservices-on-aws/microservices-on-aws.html