**SECURING APPLICATION ENDPOINTS IN AWS CLOUD**

This document refers to the Data Encryption tasks and steps for the application endpoints which are exposed to the Internet in AWS Cloud. Please follow through the reference in this document for a detailed level of implementation.

| **Task** | **Description** | **Detailed Steps** |
| --- | --- | --- |
| **Secure Network Architecture** | Deploy application endpoints within a VPC with appropriate subnets and security groups. | 1. Create a VPC with desired IP range and subnets.  2. Configure route tables for subnets.  3. Create security groups for the application. |
| **Access Control** | Implement secure authentication mechanisms and IAM roles for access control. | 1. Set up IAM users and groups.  2. Create IAM roles with appropriate permissions.  3. Enable MFA for IAM users. |
| **Encryption** | Configure SSL/TLS encryption for data in transit and obtain valid SSL/TLS certificates. | 1. Generate or import an SSL/TLS certificate.  2. Configure SSL/TLS on load balancers or application servers. |
| **Web Application Firewall (WAF)** | Deploy AWS WAF to protect against common web attacks and configure security rules. | 1. Create a WAF WebACL.  2. Define and add rules to block or allow specific traffic. |
| **Monitoring and Logging** | Enable logging and monitoring using CloudTrail, CloudWatch, and other logging services. | 1. Enable CloudTrail to log API activity.  2. Set up CloudWatch alarms for monitoring key metrics. |
| **Regular Review and Updates** | Periodically review and update security configurations based on best practices and vulnerability assessments. | 1. Conduct regular vulnerability assessments.  2. Stay informed about security best practices and updates. |
| **Employee Awareness and Training** | Provide training and awareness programs on secure configuration and best practices for application endpoints. | 1. Develop training materials on secure configuration.  2. Conduct training sessions for employees. |

Please refer to the appropriate AWS documentation for detailed step-by-step instructions for each task:

* [Amazon VPC Documentation](https://docs.aws.amazon.com/vpc/index.html)
* [AWS Identity and Access Management (IAM) Documentation](https://docs.aws.amazon.com/iam/index.html)
* [AWS Certificate Manager Documentation](https://docs.aws.amazon.com/acm/index.html)
* [AWS WAF Documentation](https://docs.aws.amazon.com/waf/index.html)
* [AWS CloudTrail Documentation](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)
* [Amazon CloudWatch Documentation](https://docs.aws.amazon.com/cloudwatch/index.html)
* [AWS Security Best Practices](https://aws.amazon.com/security/best-practices/)
* [AWS Well-Architected Framework](https://aws.amazon.com/architecture/well-architected/)