
# How do you provide API security on Kubernetes?

| Security Area | Concept | Explanation | AWS Implementation |
|---|---|---|---|
| **Network-Level Security** | | | |
| Network Policies | Controls pod-to-pod traffic | Creates digital boundaries between services | Requires manual implementation (e.g., Calico); EKS doesn't apply them by default |
| Service Meshes | Encrypts service-to-service communication | Adds observability and mTLS between microservices | Use AWS App Mesh or Istio; manual deployment & config required |
| Ingress Controllers | Manages external traffic securely | Acts as a controlled gateway into the cluster | Use AWS ALB or NGINX ingress; needs manual setup |
| **Authentication & Authorization** | | | |
| Kubernetes RBAC | Role-based access control | Grants permissions to users/services | Enabled by default; you must define roles, bindings, policies |
| API Gateways | Authenticates, routes, and limits external calls | Protects and manages API exposure | AWS API Gateway available; requires integration effort |
| OAuth/OIDC | Standard login protocol for identity | Used for single sign-on and external user access | Use AWS Cognito or integrate external OIDC provider; config required |
| mTLS | Verifies both sides of communication | Ensures identity validation between services | Requires setup via AWS Certificate Manager + service mesh |
| **API-Specific Security** | | | |
| Rate Limiting | Throttles excessive | Prevents abuse or | Use AWS WAF/API Gateway; |

| Security Area | Concept | Explanation | AWS Implementation |
|---|---|---|---|
| | API calls | DoS-style spikes | Kubernetes-specific rate limits need custom setup |
| Input Validation | Sanitizes and validates user input | Prevents injection, malformed requests | Must be implemented in app logic or gateways |
| JWT Validation | Validates bearer tokens for identity | Ensures that the requestor is verified | Use AWS Cognito or custom middleware; integration needed |
| API Keys | Token-based access for apps/services | Simple access control with revocation | Store in Secrets Manager or Parameter Store; manual injection into pods |
| **Secure Configuration** | | | |
| Pod Security Policies | Controls pod capabilities | Blocks privileged containers, hostPath, etc. | Use Pod Security Standards (PSS); not enforced by default, needs configuration |
| Secret Management | Secures credentials, tokens, keys | Prevents sensitive data from being exposed | Use AWS Secrets Manager/Parameter Store; needs integration in Kubernetes apps |
| CIS Benchmarks | Best practices for security hardening | Industry-vetted checklists and configuration guidelines | Use AWS Security Hub; alerts generated but remediation is your responsibility |
| Resource Isolation | Prevents noisy neighbors | Ensures fair use of CPU, memory, etc. | EKS supports it; you must configure resource quotas and limits manually |
| **Monitoring & Incident Response** | | | |
| API Logging | Tracks every call made to the API | Helps in audits and forensic analysis | Use CloudWatch for basic logs; deeper audit logging requires extra setup |
| Runtime Security | Monitors running containers for threats | Detects anomalies during execution | Use AWS GuardDuty for EKS; deeper runtime checks need tools like Falco, Sysdig |
| Security Scanning | Checks containers and manifests | Prevents vulnerabilities before deployment | ECR provides image scanning; manifest/config scans need extra tools (e.g., Trivy, Snyk) |

---

**What is the purpose of Network Policies in Kubernetes?**

A) Encrypt data at rest
B) Define pod-to-pod communication rules
C) Manage user logins
D) Provide access to the Kubernetes Dashboard

✅ **Correct Answer: B**

What is the role of a service mesh in a cloud-agnostic environment?
A) Provision storage volumes
B) Encrypt and manage service-to-service traffic
C) Deploy virtual machines
D) Monitor network egress charges

✅ Correct Answer: B

**What AWS service can be used to manage API rate limiting for services exposed via API Gateway?**
A) AWS WAF
B) AWS CloudWatch
C) AWS IAM
D) AWS Route 53

✅ **Correct Answer: A**