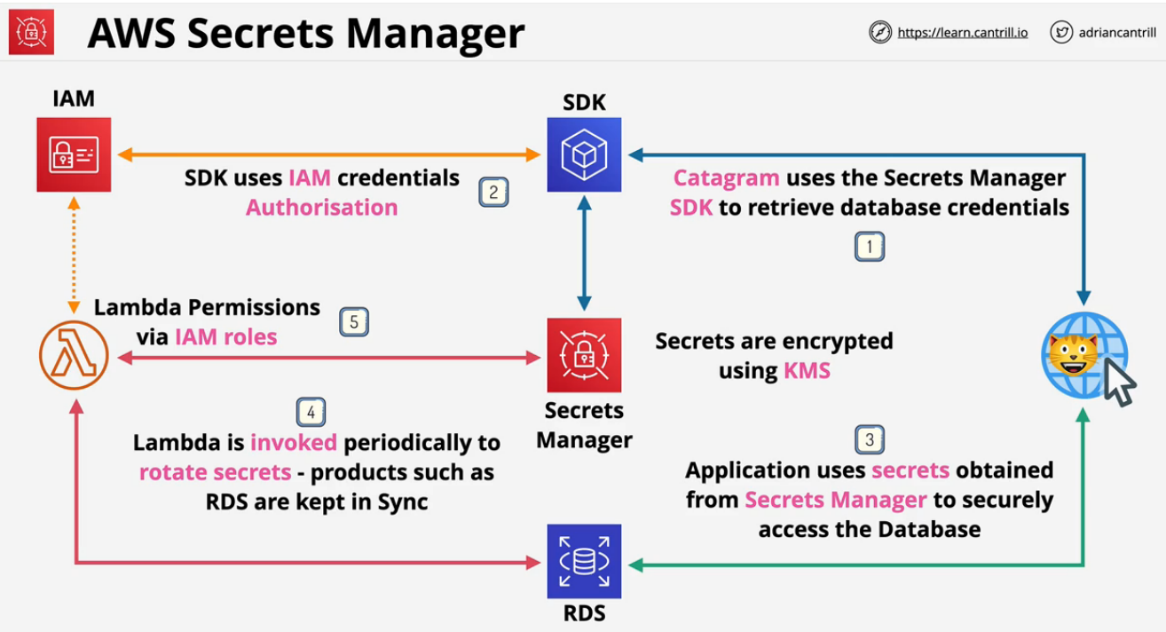
**Security-Deployment-Operations**

**AWS Secrets Manager**

* Share functionality with parameter store. Sometimes both are appropriate.
* Designed specifically for secrets, passwords, API keys.
* Usable via Console, CLI, API, or SDK (integration)
* Supports the **automatic rotation of secrets using Lambda.**
* Directly **integrates with RDS and a limited set of AWS products.** If **lambda is invoked and changes a secret, the password can automatically change in RDS.**
* Secrets are **encrypted at rest.**
* Integrates with **IAM, can use IAM permissions to control access to secrets.**

**Secrets Manager Example**

1. The Secrets Manager SDK retrieves database credentials.
2. SDK uses IAM credentials to retrieve the secrets.
3. Application uses the secrets to access the database.
4. Periodically, a lambda function is invoked to rotate the secrets.
5. The Lambda uses an execution role to get permissions.

Secrets are secured using KMS so you never risk any leakage via physical access to the AWS hardware and KMS ensures role separation.

**Keyword Analysis for exam:**

* Rotation, Integration, RDS, Secrets -> Secret Manager
* Other -> Parameter Store

**AWS Shield and WAF (Web Application Firewall)**

**AWS Shield:**

Provides protection against DDoS attacks with AWS resources. This is a denial of service attack. Normally not possible to block them by using individual IP addresses. Without detailed analysis, the traffic looks like normal requests to your website.

* **Shield Standard**
  + Free with **Route53 and CloudFront** as default
  + Provides **layer 3 and layer 4** protection against DDoS attacks.
* **Shield advanced**
  + $3000 per month
  + Includes **EC2, ELB, CloudFront, Global Accelerator and R53**
  + Provides access to **DDoS advanced response team and financial insurance against increased costs.**
* **WAF (web application firewall)**
  + Layer 7 firewall (HTTP/s) firewall
  + Protects against complex application layer 7 attacks:
    - **SQL injections**
    - **cross-site scripting**
    - **geo blocks**
    - **rate awareness**
  + **WEBACL** integrated with **ELB, “API gateways”, and CloudFront.**
    - Rules are added to WEBACL and evaluated when traffic arrives.

**Example of Architecture**

Shield standard automatically looks at the data before any data reaches past Route53. The user is directed to the closest CloudFront location. Again, shield standard looks at the data again before it moves on.

WAF Rules are defined and included in a WEBACL which is associated to a cloud front distribution and deployed to the edge.

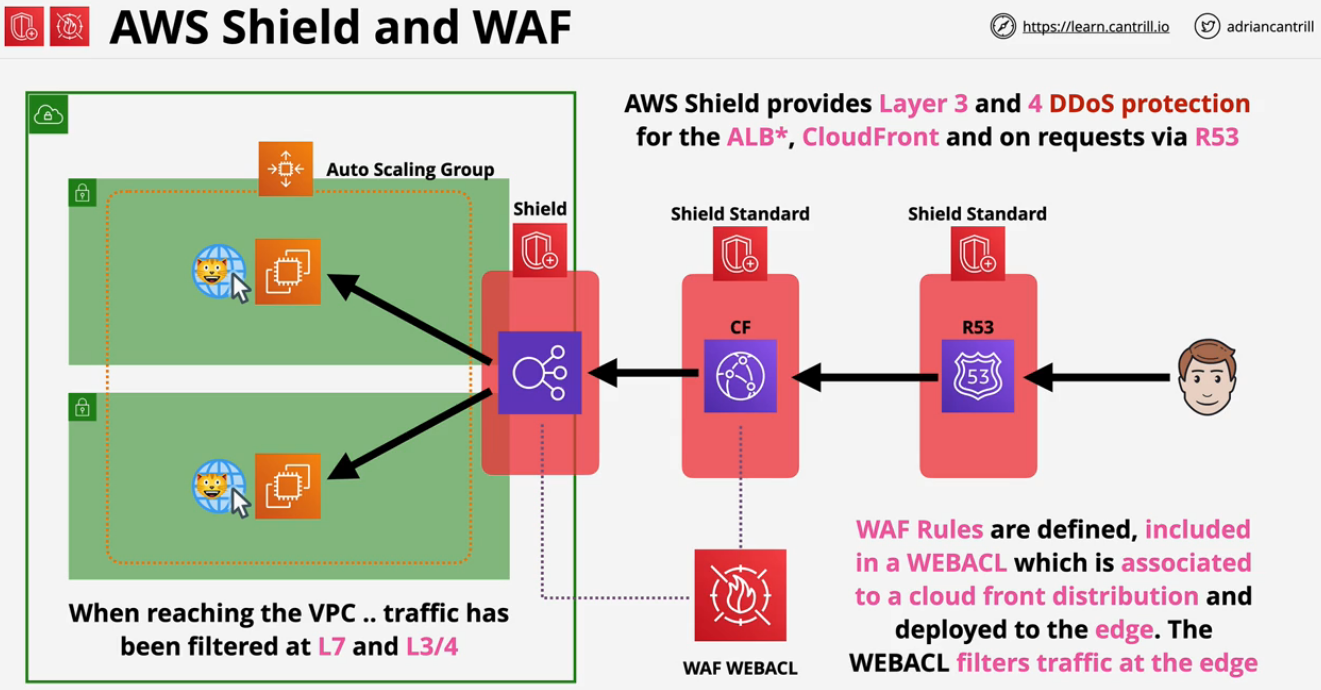
Shield advanced can then intercept traffic when it reaches the load balancer. Once the data reaches the VPC, it has been filtered at Layer 3, 4, and 7 already.

Layer 7 filtering is only provided by WAF.

**Keyword Analysis for exam:**

DDoS -> **Shield Standard(Cloudfront, Route53), Shield Advanced (ALB)**

Layer 7 filtering, http, https filtering -> **WAF (Cloudfront, Route53)**



**CloudHSM**

KMS is the key management service within AWS. It is used for encryption within AWS and it integrates with other AWS products. Can generate keys, manage keys, and can integrate for encryption. The problem is this is a shared service. You're using a service which other accounts within AWS also use. Although the permissions are strict, AWS still does manage the hardware for KMS. KMS is a hardware security module or HSM. **These are industry standard pieces of hardware which are designed to manage keys and perform cryptographic operations.**

You can run your own HSM on premise. Cloud HSM is a true "single tenant" hardware security module (HSM) that's hosted within the AWS cloud. AWS provisions the HW, but it is impossible for them to help. There is no way to recover data from them if access is lost.

Fully **FIPS 140-2 Level 3 (KSM is L2 overall, but some is L3)** IF you require level 3 overall, you MUST use CloudHSM.

**KSM** all actions are performed with **AWS CLI and IAM roles.**

**HSM will not integrate with AWS by design** and **uses industry standard APIs.**

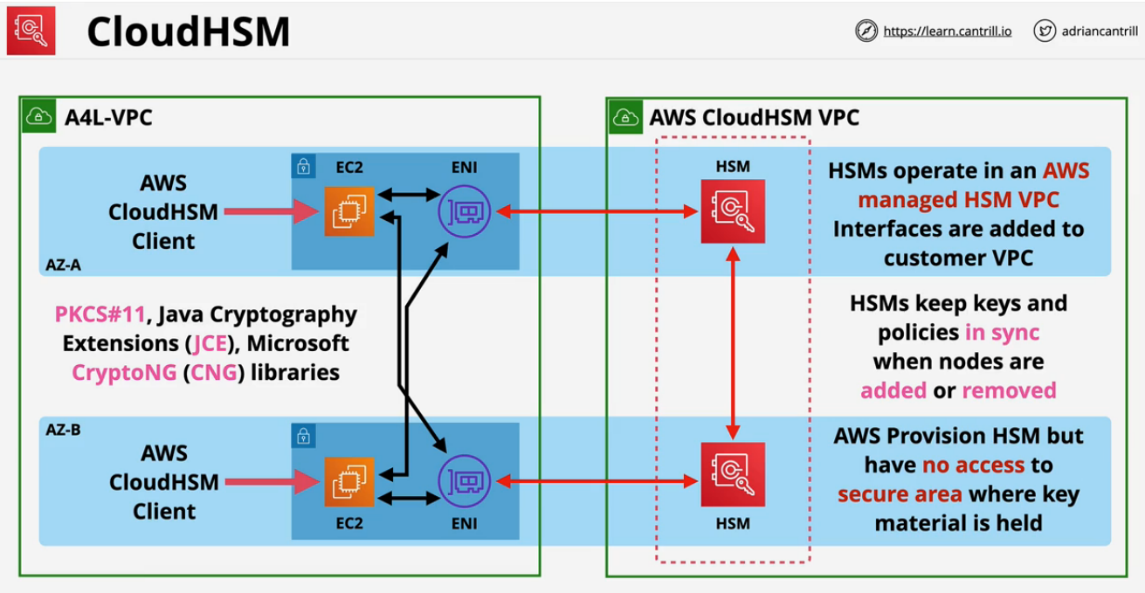
* **PKCS#11**
* **Java Cryptography Extensions (JCE)**
* **Microsoft CryptoNG (CNG) libraries**

KMS can use CloudHSM as a custom key store, CloudHSM integrates with KMS.

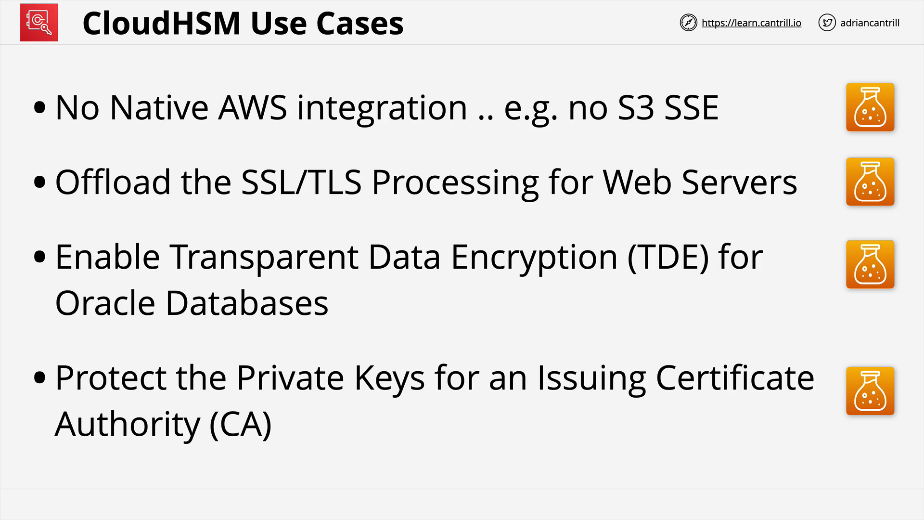


HSM is **not highly available** and **runs within one AZ.** To be **HA, you need at least two HSM devices and one in each AZ** you use. Once HSM is in a cluster, they **replicate all policies in sync automatically.**

HSM needs an endpoint in the subnet of the VPC to allow resources access to the cluster.

AWS has no access to the HSM appliances which store the keys.

**Cloud HSM Use Cases**

* **No native AWS integration with AWS products.** You can't use S3 SSE with CloudHSM.
* **Can offload the SSL/TLS processing** from webservers. CloudHSM is much more efficient to do these encryption processes.
* Oracle Databases can **use CloudHSM to enable transparent data encryption (TDE)**
* Can **protect the private keys an issuing certificate authority.**
* Anything that needs to **interact with non AWS products.**