1.3 Configuring Security Group

Network ACLs in AWS

- Network ACL, or NACL, is a defense in depth mechanism that's not being used by default.

What the Network ACL is, it is a stateless or a static packet-filtering firewall that applies to all traffic inbound to a subnet, so we have Inbound Rules and Outbound Rules. And this Network ACL will apply to all the instances, everything in that subnet.

- **Stateless or static**, that means the NACL will actually evaluate each individual packet or datagram one at a time coming into the subnet and going out of the subnet.
- ACL is going to process starting with the lowest number and then go to the next number. **And as soon as it finds a match, okay, it looks at the packet,** it evaluates the headers, and as soon as it finds a match, it will take that Allow or Deny action.

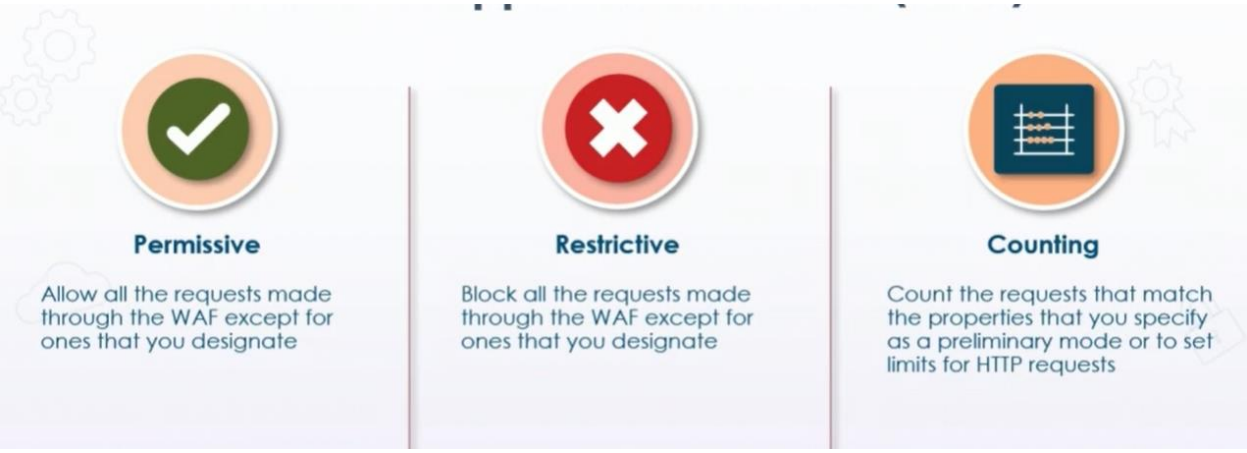
- It's a static packet-filtering firewall. Whatever you allow inbound, you have to also allow outbound. And it applies to everything in the subnet, and you can configure, ALLOW rules or DENY rules.

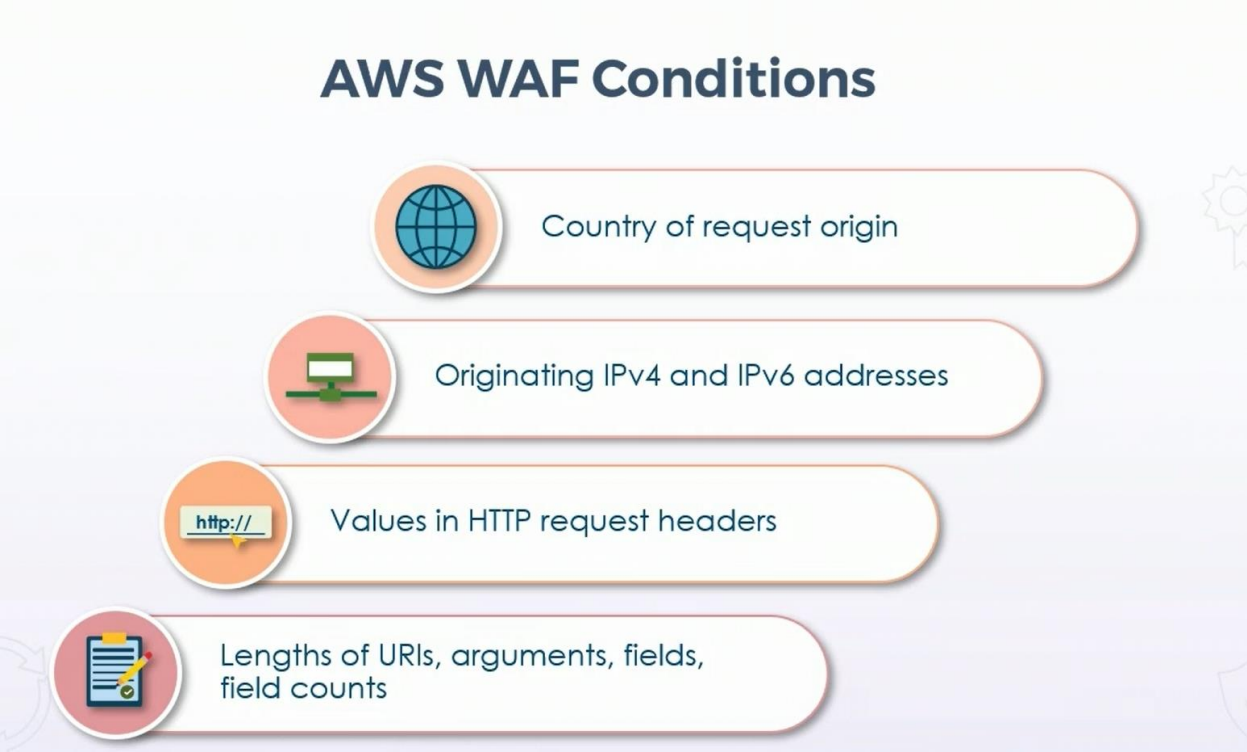
Security Groups in AWS

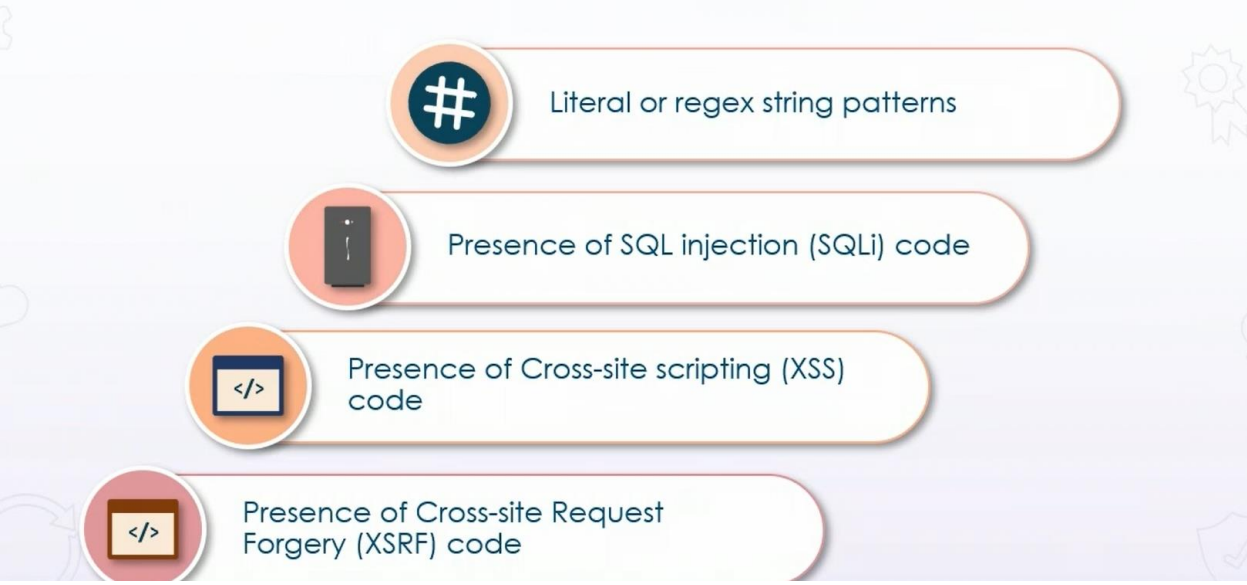
- The security group applies to all traffic inbound and outbound from a specific instance.
- Default security group: ending with afb
- It basically just has a set of whitelisting rules for you to allow traffic to the instance and from the instance.
- Security group does not have a deny rule.
- you can see the inbound rule, by default, basically going to allow All traffic into this instance if it's another instance using the default security group. In other words, no traffic will be allowed to this instance by default, for example, from the Internet.
- Outbound however, by default, we're going to allow All traffic on All protocols, on All port ranges, to any destination.
- security group is a stateful, packet-filtering firewall.
- Stateful firewall: It tracks the TCP connection, or UDP flow, and automatically allows the traffic back into the instance, if it was generated from the instance.
- security group is a stateful packet-filtering firewall that's applied to the instance. It has no deny rules. It's a whitelisting firewall and you have an inbound rule and an outbound rule, and you have a default security group that you can apply, or you can create your own security groups.

AWS Web Application Firewall (WAF)

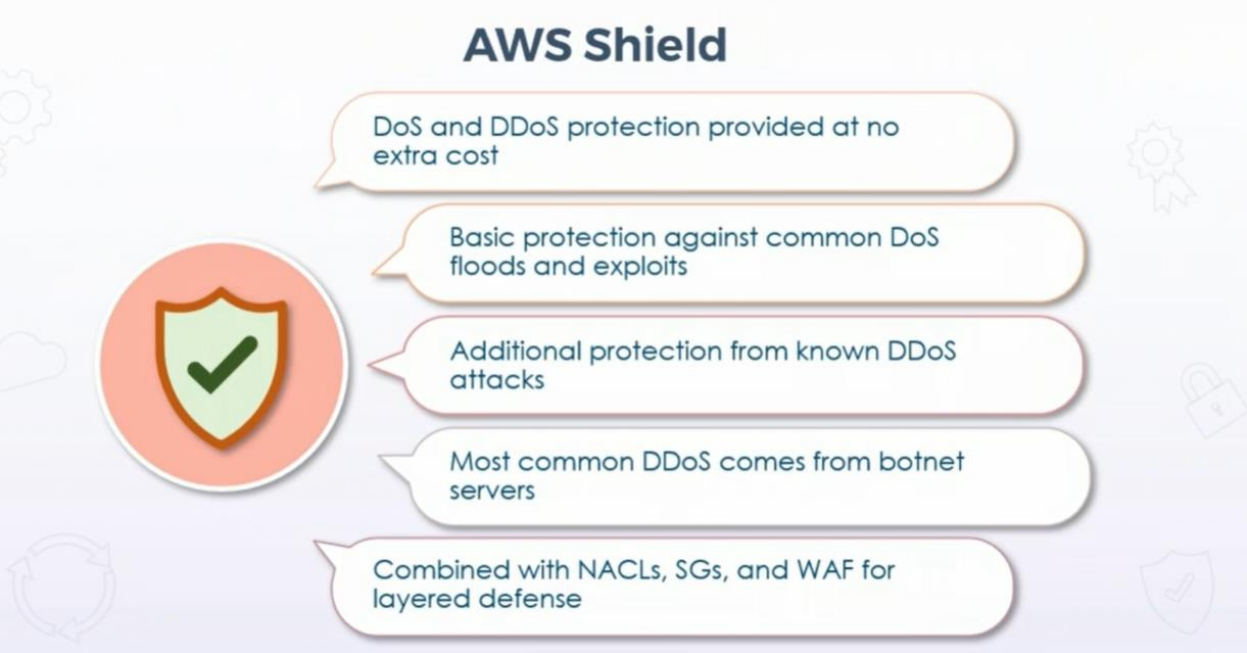
- the WAF can run on the Application Elastic Load Balancer,not the Network Elastic Load Balancer.
- it operates on the application layer of the TCP IP model.

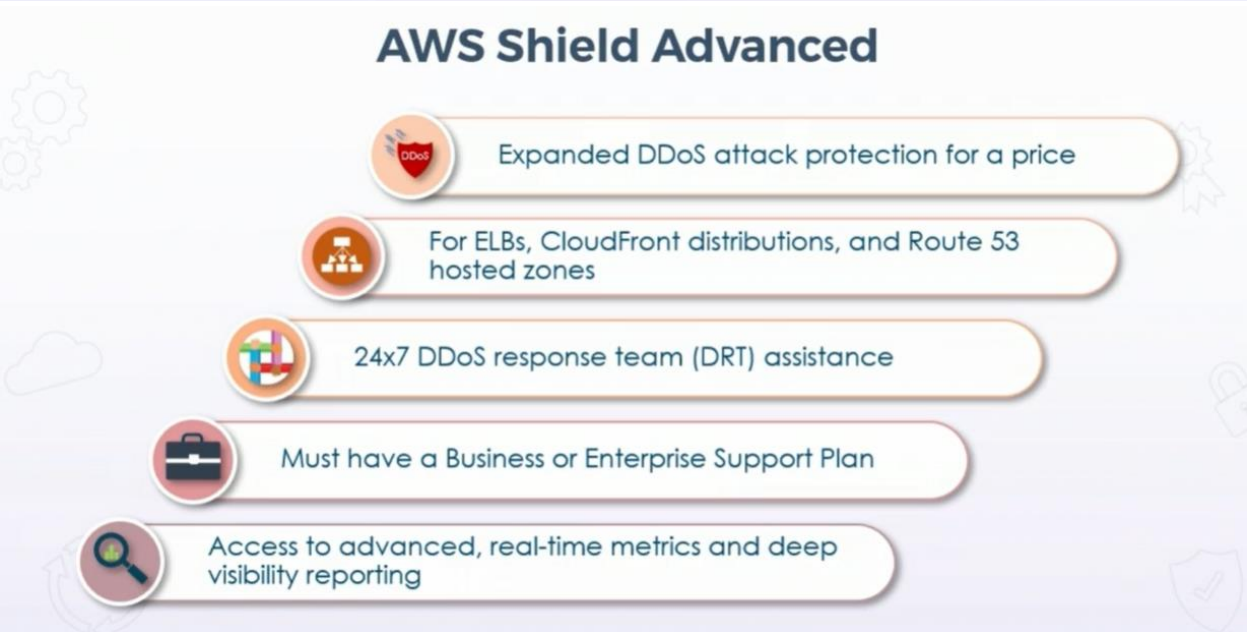



AWS WAF Conditions
Country of request origin
Originating IPv4 and IPv6 addresses
http://
Values in HTTP request headers
Lengths of URIs, arguments, fields, field counts


Literal or regex string patterns
Presence of SQL injection (SQLi) code
</>
Presence of Cross-site scripting (XSS) code
</>
Presence of Cross-site Request Forgery (XSRF) code

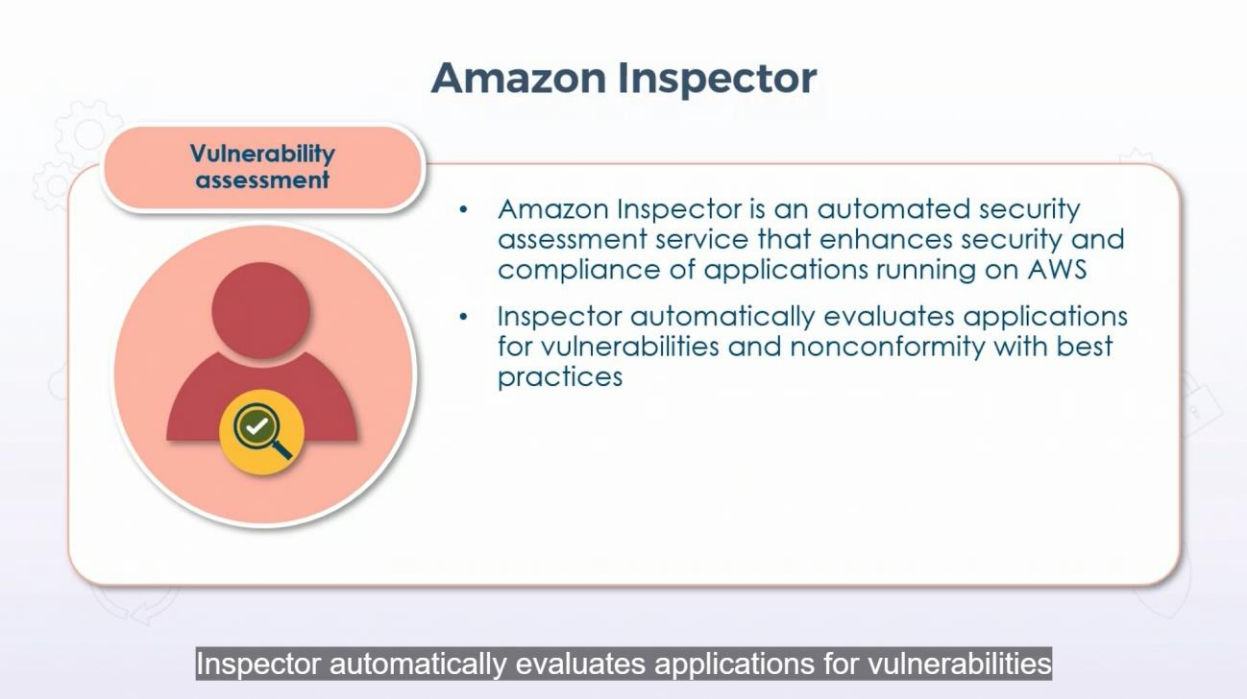
AWS Shield





Amazon Inspector

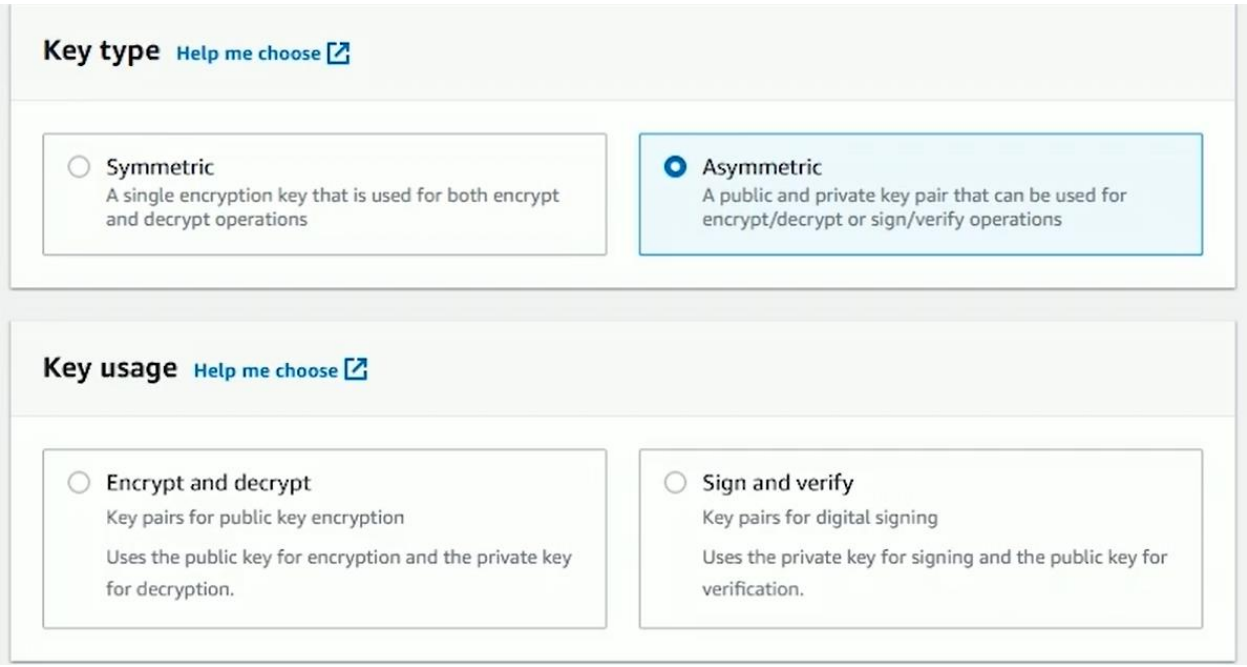
service that enhances security and compliance of applications running on AWS by evaluating applications for vulnerabilities and nonconformity with best practices



Amazon GuardDuty

service monitors flow logs, CloudTrail, S3 data events, and DNS log activities for advanced threat management

AWS Key Management Service (KWS)



AWS KMS helps you centrally manage and securely store your keys. You can generate keys in AWS KMS or import them from your own key management infrastructure. You can submit data directly to AWS KMS to be encrypted, or decrypted. Other AWS services can use your keys on your behalf to protect data encryption keys that they use to protect your data.

Your keys never leave AWS KMS and you are always in control of your keys. You can set usage policies that determine which users can use your keys and what actions they can perform. All requests to use these keys are logged in AWS CloudTrail so that you can track who used which key, how and when.

Benefits and features

Fully managed

You can focus on your use of encryption while AWS handles durability, physical security, and policy enforcement to ensure that your keys are always available and safe.

Centralized key management

KMS presents a single control point to manage keys and define policies consistently across integrated AWS services and your own applications.

Integrated with AWS services

KMS is integrated with all major AWS services to simplify the use of encryption and to protect stored data through a common set of tools for controlling access.

Encryption for all your applications

KMS is integrated with the AWS Encryption SDK to help you build encryption and key management into your own applications.

Built-in auditing

KMS is integrated with AWS CloudTrail to provide a consolidated record of all key management activities and any attempt to use your keys.

No commitment

There is no commitment and no upfront charges. You only pay for the keys that you create and when you use them.

type of encryption does AWS KMS use to protect an Elastic Block Store volume or S3 bucket: **AES-256**