

1.3 Configuring Security Group

In this course, we will:

- Explore core security support services
 - Network ACLs
 - Security groups
 - Advanced web application firewall
- Look at anti denial-of-service and Anti-DDoS with AWS Shield standard and AWS Shield advanced
- Wrap up with Amazon Inspector, GuardDuty and AWS key management services (KMS)

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.

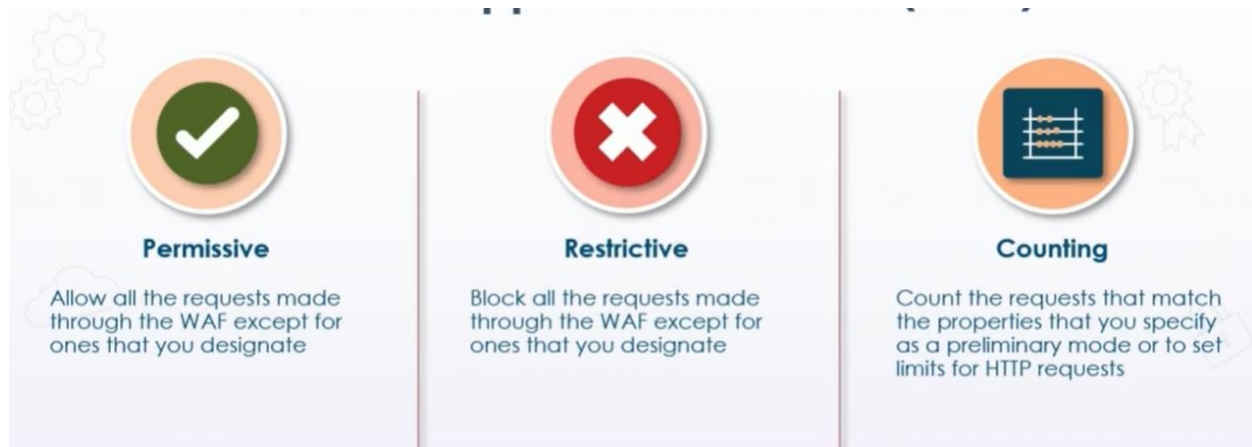
Security Groups in AWS

- The security group applies to all traffic inbound and outbound from a specific instance.
- Default security group: ending with `sg-`
- 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 AWS Web Application Firewall (WAF) lets you control and monitor the HTTP and HTTPS requests forwarded to Amazon CloudFront (CDN), Application Elastic Load Balancer (ELB), or API Gateway

- 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



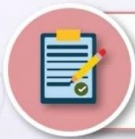
Country of request origin



Originating IPv4 and IPv6 addresses



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

AWS Shield



DoS and DDoS protection provided at no extra cost

Basic protection against common DoS floods and exploits

Additional protection from known DDoS attacks

Most common DDoS comes from botnet servers

Combined with NACLs, SGs, and WAF for layered defense

AWS Shield Advanced



Expanded DDoS attack protection for a price



For ELBs, CloudFront distributions, and Route 53 hosted zones



24x7 DDoS response team (DRT) assistance



Must have a Business or Enterprise Support Plan



Access to advanced, real-time metrics and deep visibility reporting

Amazon Inspector

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

Amazon Inspector

Vulnerability assessment



- Amazon Inspector is an automated security assessment service that enhances security and compliance of applications running on AWS
- Inspector automatically evaluates applications for vulnerabilities and nonconformity with best practices

Inspector automatically evaluates applications for vulnerabilities

Amazon Inspector



AWS discourages running assessment tools



Produces a detailed list of security findings



Results available through console or API



Includes knowledgebase of 100's of rules



Generates various meaningful reports

Amazon GuardDuty

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

Amazon GuardDuty

Fully-managed threat detection service

Looks for attacks, anomalies, and unauthorized actions

Based on well-defined "findings" categories

Monitors flow logs, CloudTrail, S3 data events, and DNS log activities

It is a regional service with prices based on quantity of events and log volumes



AWS Key Management Service (KMS)

Key type [Help me choose](#)



Symmetric

A single encryption key that is used for both encrypt and decrypt operations



Asymmetric

A public and private key pair that can be used for encrypt/decrypt or sign/verify operations

Key usage [Help me choose](#)



Encrypt and decrypt

Key pairs for public key encryption

Uses the public key for encryption and the private key for decryption.



Sign and verify

Key pairs for digital signing

Uses the private key for signing and the public key for verification.

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.

Secure

KMS uses FIPS 140-2 validated hardware security modules to generate and store your keys. Your keys can only be used inside these devices and can never leave them.

Reliable

KMS uses highly durable storage and a resilient architecture to ensure that your keys are always available and are never lost.

Compliance

The security and quality controls in AWS KMS have been certified by multiple compliance schemes to simplify your own compliance obligations.

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