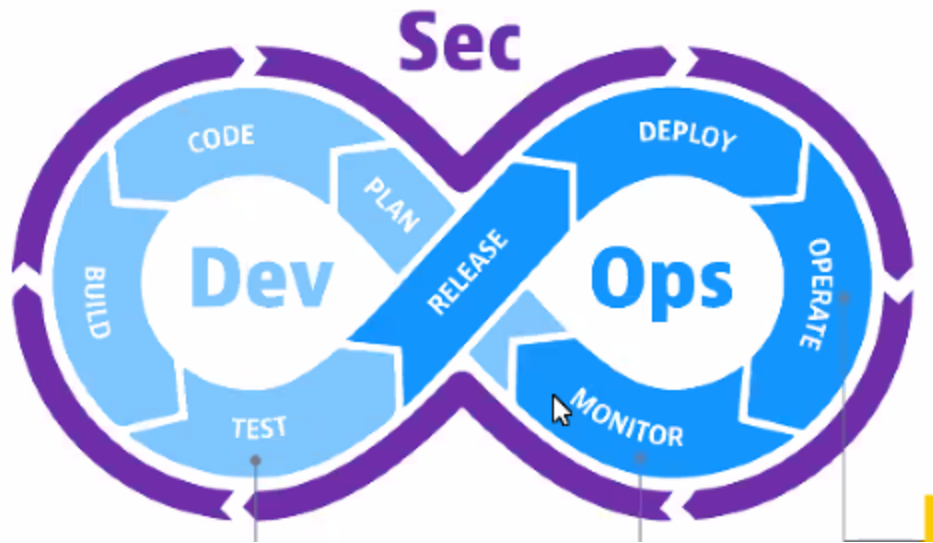


AWS Security

DevSecOps



Güvenliğin 3 sac ayağı

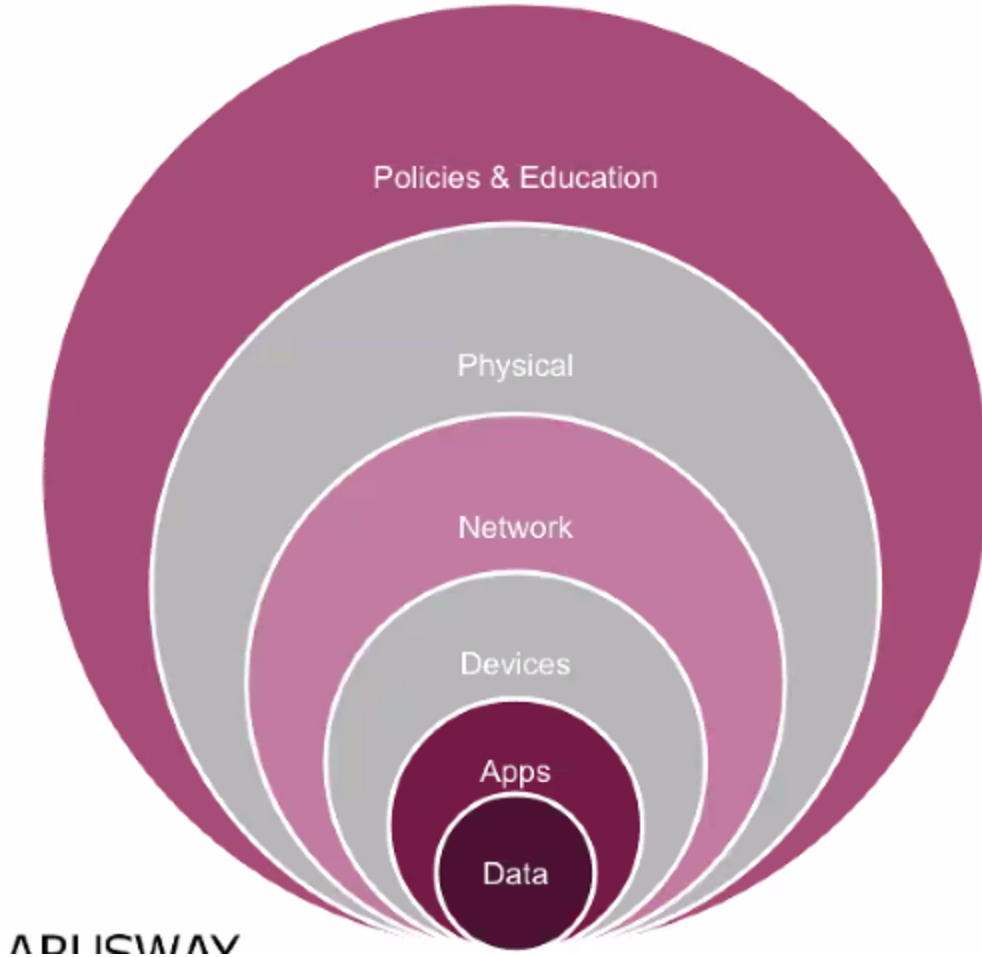


1) Confidentiality: Yetkisiz kişileri engelleme

2) İntegrity: Bütünlük. Dosyayı korumak önemli ancak bunu yaparken datanın bütünlüğünü bozmamak.

3) Availability: İstediğimiz zaman ulaşabilmek.

Defense-in-Depth:



Çok katmanlı bir güvenlik sağlar. En dışta personelin eğitimi, şifre güvenliği vs. Daha sonra fiziksel güvenlik gelir. Server odalarının kilitleri, etraftaki kameralar vs. Sonra network katmanı gelir. Yani datayı sakladığımız yeri bir networke alarak belirli giriş protokolleri belirleriz. NACL gibi. Bu sayede herkes bizim verilerimize ulaşamıyor.

Sonra Device katmanı gelir. Bu da sisteminizde kullanılan cihazların bilgisayarların güvenlik açığının olmaması. Bu nedenle gerekli güncellemeler yapılmalı. Bir sonraki

katman application katmanı. Webde yapılan korumalar. Örneğin bir siteye girerken çift katmanlı koruma vs.

Son katman data. Bu katmanda herhangi bir gizli veri tutulmaz. Şifreye vs ihtiyaç duyulduğu zaman ilgili kasaya (vault) gidip şifreyi alıp kullanır. DATA bir şekilde ele geçirilirse şifreler ele geçirilemez. Hardening(sıkılaştırma)

Preventative and Detective Controls

Detective

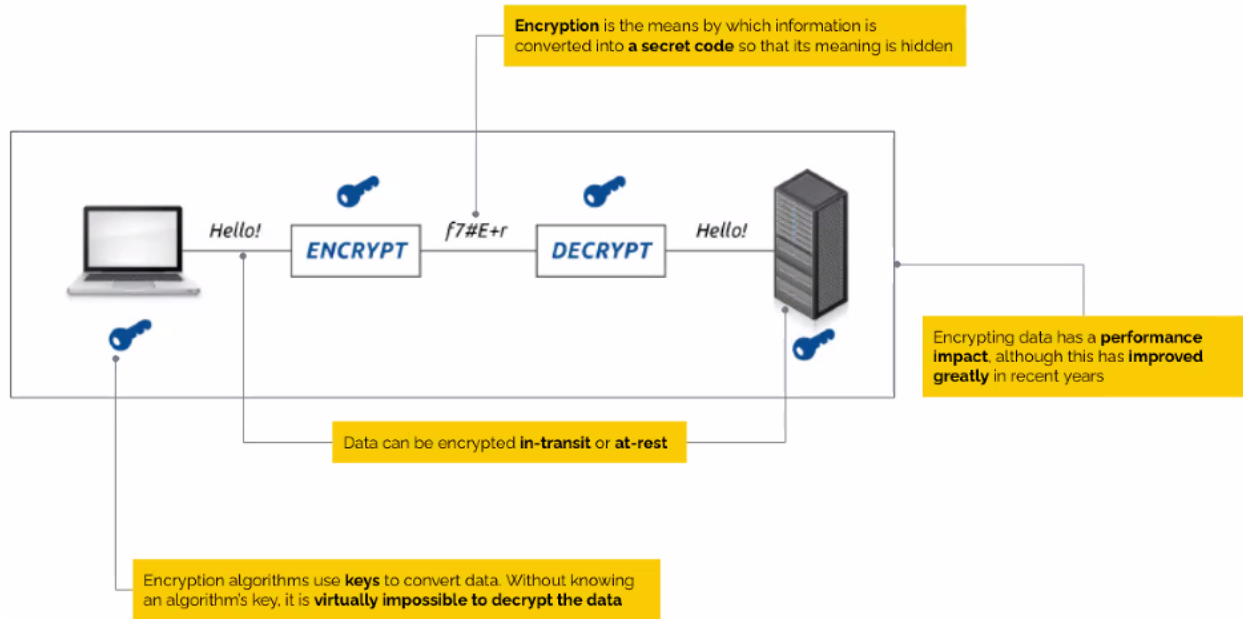
- **Identifies** threats, **logs** events and sends **alerts**
- Requires **manual or automated remediation**

Preventative

- Automatically **disallows** actions
- Can lead to **stopping legitimate** behavior

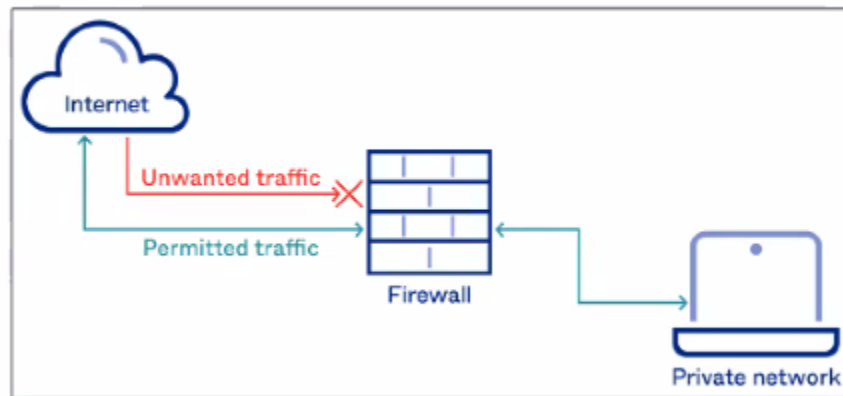
Security Solutions

Encryption

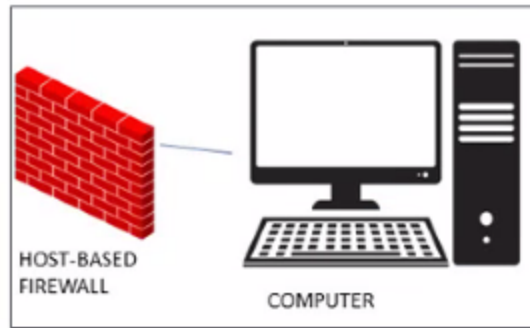


Bilgiyi okuması açması şifrelemesi zaman alıyor.

FireWall

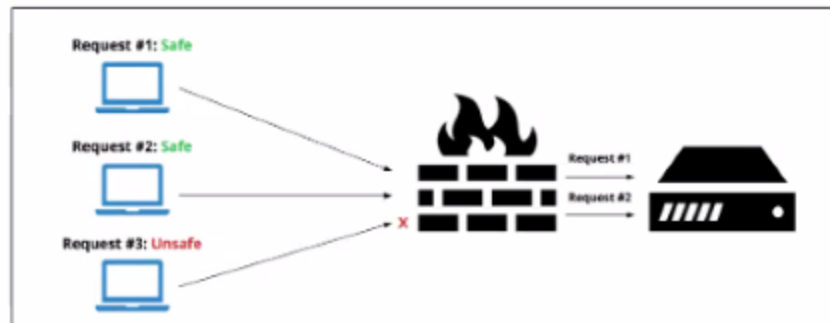


Hardware ya da Software olarak kullanılabilir. Software Firewall, Network Firewall olarak da bilinir. Bir de Host-Based var. Bu da bilgisayarın içine kurulur. Layer 3-4 te çalışır.



Web Application Firewall (WAF): Bu artık Layer 7 de çalışır. Web application üzerinden nasıl engelleyebiliriz. Onu gösterir. Aşağıda bazı saldırı yöntemleri gösterilmiştir. Firewall ile bunlar engellenir.

- Typically protects web applications against specific attacks:
 - **cross-site forgery**
 - **cross-site-scripting (XSS)**
 - **SQL injection**
 - **distributed-denial-of-service (DDOS)**



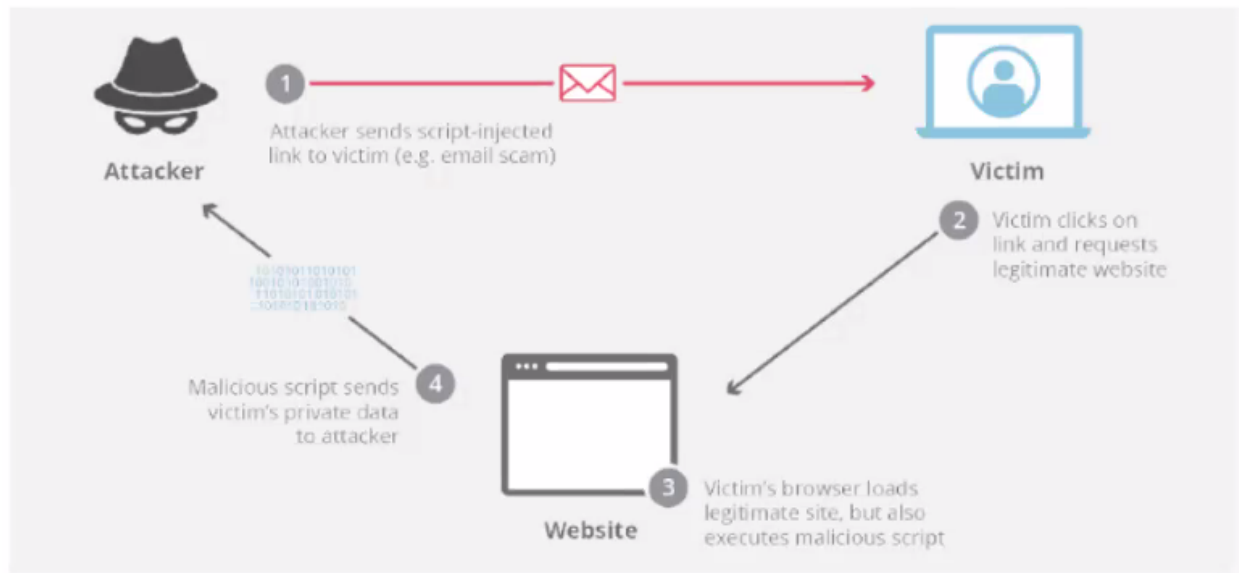
Cross site Forgery: Session bilgileri çalınır.

CROSS SITE REQUEST FORGERY (CSRF)



Cross Site Scripting: Bir mail geliyor. Tıklayınca senin güvendiğin bir siteye yönlendiriyor. Örneğin Onun linkiyle Garanti'ye gidersen senin bilgilerini çalıyor.

Cross Site Scripting (XSS)



SQL INJECTION: Bir dataBase'imiz var. Buna gi,riş yapabilmek için belirli sorgular atıyoruz ve kullanıcı adı/ şifreyi giriyoruz. Bizim SQL düzenimiz düzgün değilse adam bizim yaptığımız standart sorgunun arasına kendi sorgusunu inject ederek tüm kullanıcıların bilgisini alır. Aşağıdaki kırmızılar kötü niyetli.

SQL INJECTION

```
"SELECT *  
FROM users  
WHERE login=$name  
AND password = $pwd"
```

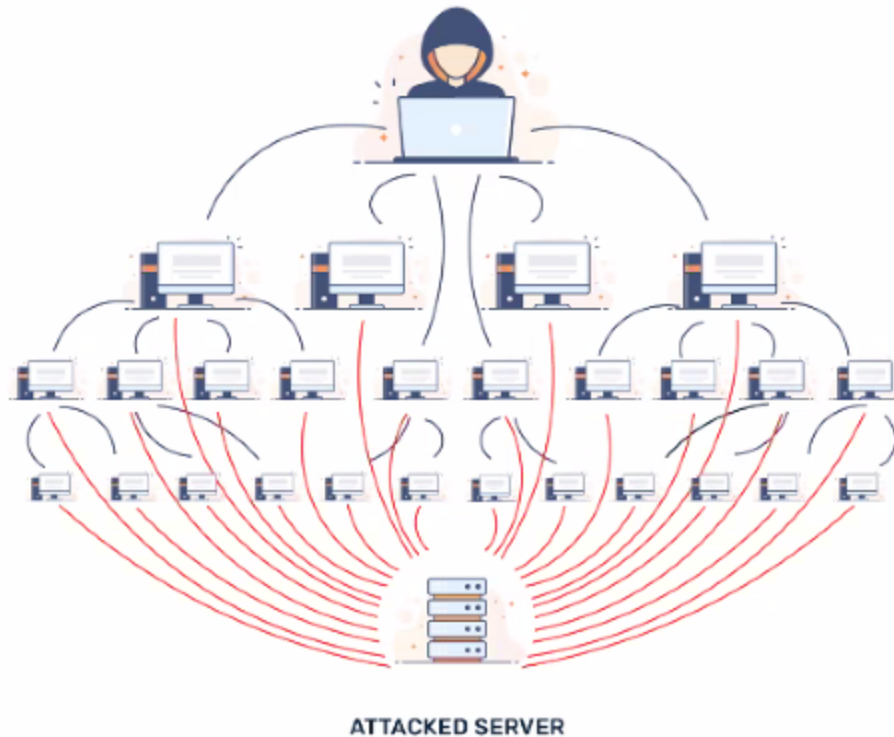
```
SELECT * FROM USERS WHERE username = 'osvaldo' and password = 'PI1234'
```

```
SELECT * FROM USERS WHERE username = 'administrator' -- and password = ''
```

```
UNION SELECT username, password--
```

DDOS Attack: Bunlar dışında sizin sitenize random saldırılar olabilir. Örneğin normalde günlük 10-20 giriş varsa adam bir anda 10bin-20bin giriş isteğinde bulunur. Site bunları kaldıramaz ve çöker.

DDOS Attack



Intrusion Detection and Prevention (Next Generation Firewall (NGFW))

Belirli yapay zeka algoritmaları ile çalışır.

- Typically use 4 types of algorithms:
 - **signature-based** detection
 - **anomaly-based** detection
 - **stateful protocol** analysis
 - **reputation** analysis

Signature: senin belirlediğin kriterlere göre yasaklama yapıyor. Örneğin bir suçlu profilki belirleriz onları yasaklar.

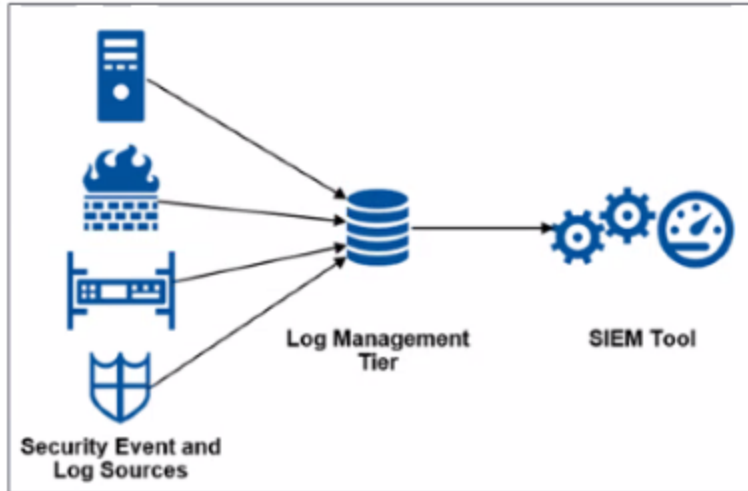
Anomaly: Normal davranış kriteri belirleriz buna uymazsa yasaklar.

Stateful protocol: Güvendiğiniz belirli kişiler belirleriz bunlardan gelenleri kabul et deriz.

Reputation: Genelde kötü nam salmış yerlerden gelenleri engelle. Örneğin rusyaadan gelen istekleri engelle. Ya da belirli CIDR bloklarından gelen istekleri reddeder.

ISPS

Security Information and Event Management (SIEM)



Networkte değil de log kayıtlarına odaklanmış. örneğin istanbulda yaşıyosun G.Africa dan giriş yapmışsın. Şüpheli durum. İzin vermez.

Vulnerability Scanner

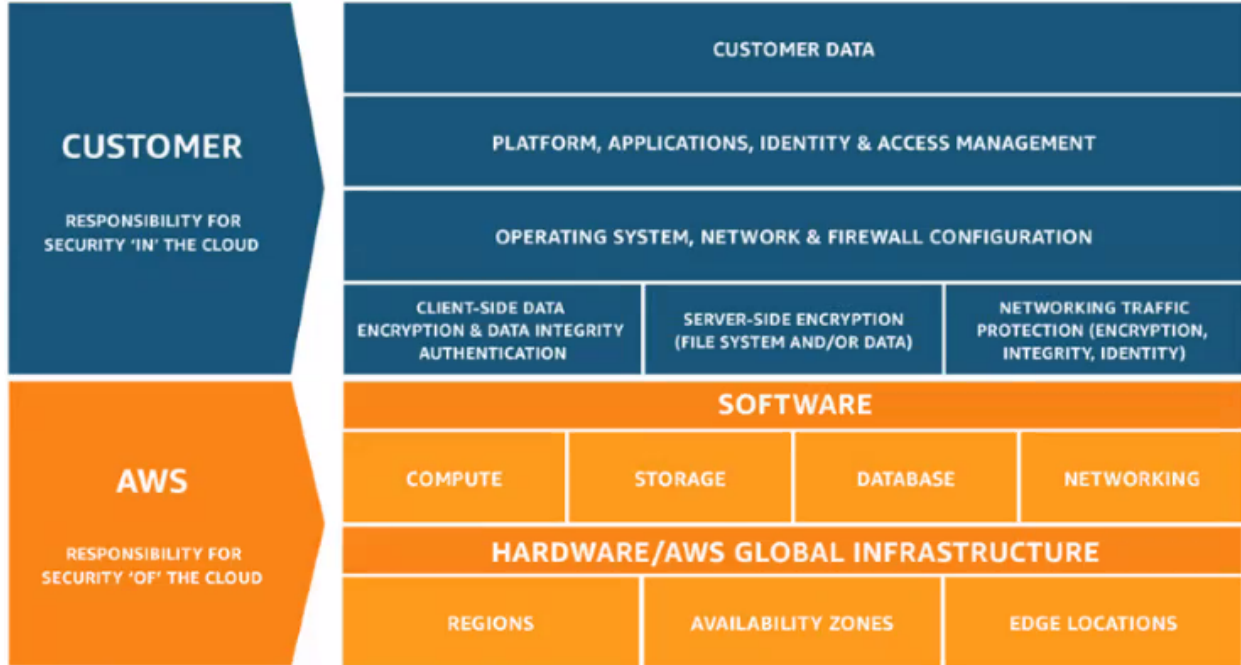
Antivirus programlarının sunduğu ücretsiz scan'leri buna dahil edebiliriz. Tamam bu taramalar önemli ve belirli periyotlarda yapılması gerekir ancak bunu senin yetkilendirdiğin birinin yapması gerek. Senden bağımsız ücretsiz bir firmaya kendi

sistemini taratırsan tüm açıklarını ona söylemiş olursun. Bunu kötü niyetli biri ile paylaşmayacağının garantisi yok.

AWS'in SORUMLULUKLARI

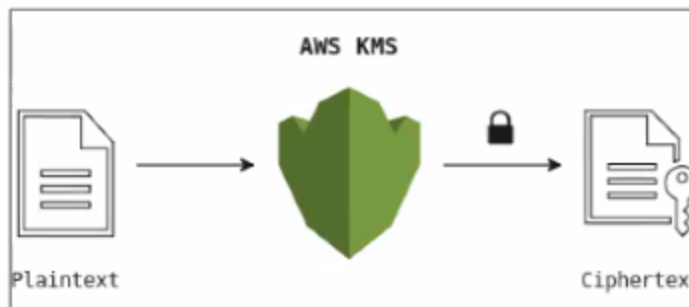
Shared Responsibility model

Burası artık AWS'nin ve bizim sorumluluklarımızı gösteriyor. Sınavlarda çıkabilir.



- Key Management Service (KMS)

Herhangi bir servise girerken bu anahtarlar ile giriş yaparız

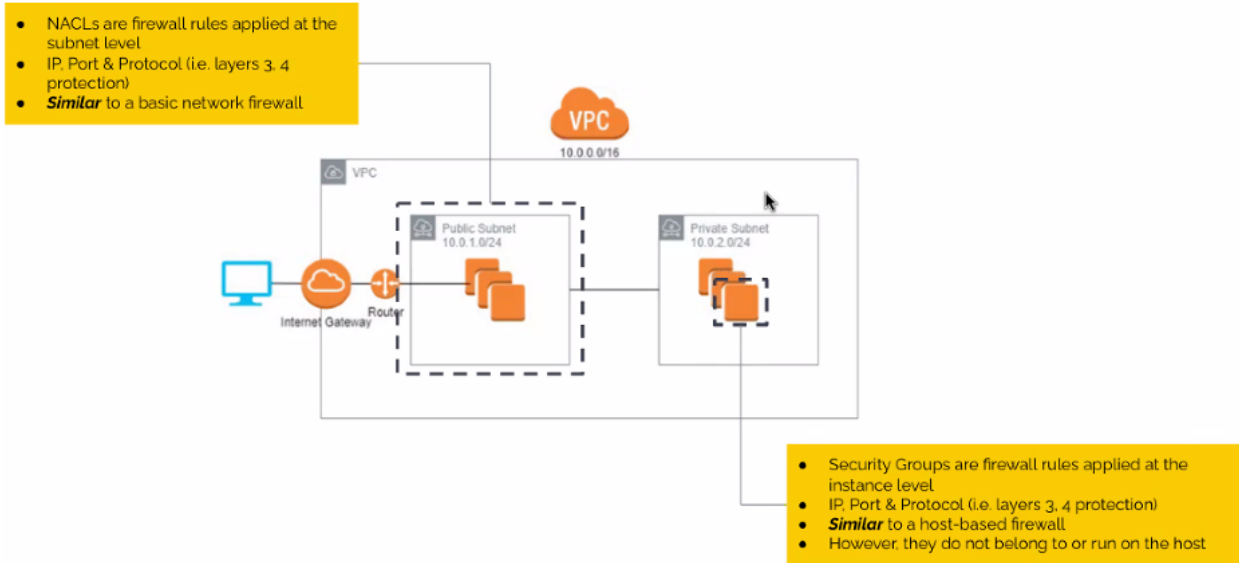


Üç tip vardır. Biz oluşturup saklarız. Ya da AWS oluşturup saklama işini o yapar. Rotation dediği şifre değiştirme olayı.

Type of KMS Key	Specific to Account?	Customer Manages?	Automatic Rotation	Key Policy Possible?
Customer Managed Key	Yes	Yes	Optional	Yes
AWS Managed Key	Yes	No	Every 3 yrs.	No
AWS Owned Key	No	No	AWS Dependent	No

- Security Groups and NACLs

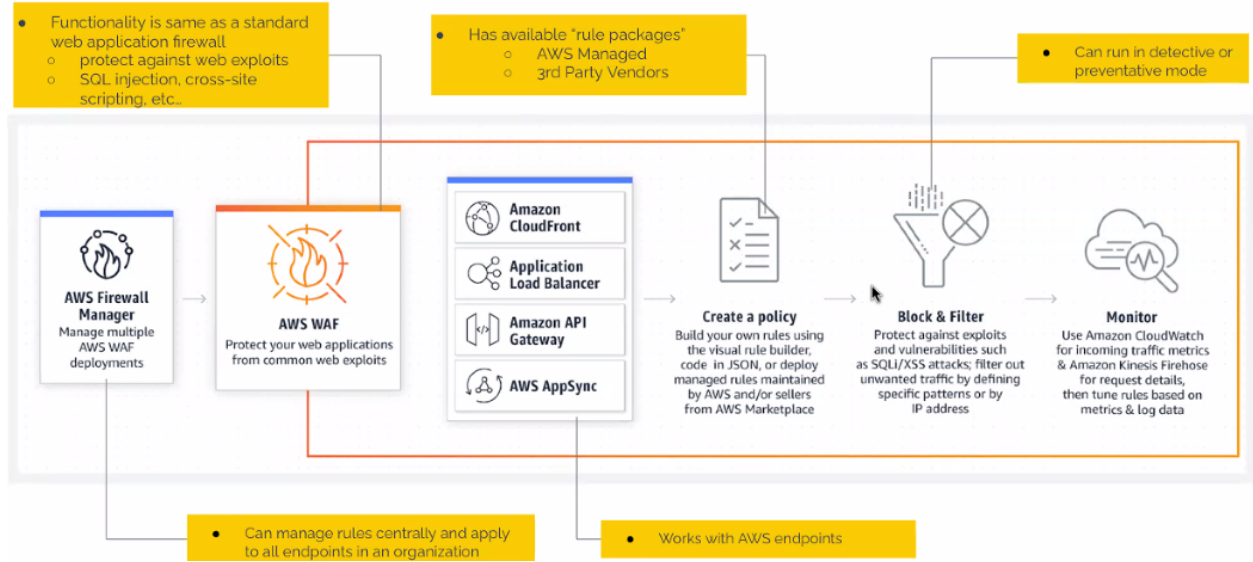
NACL, Network Firewall'un AWSteki karşılığıdır.



Security groups ise Host Based Firewall'a benzer. Yani networkümün içine girdikten sonra devreye girer.

- AWS WAF

Web Application Firewall AWSYe özel değil ancak AWS De kendi uygulamasını çıkarmış.



Kendim oluşturabilirim. 3. parti yazılımcılardan alabilirim (çoğu paralı) ya da AWS'nin hazırlarından alabilirim (bir kısmı paralı)

- AWS Network Firewall



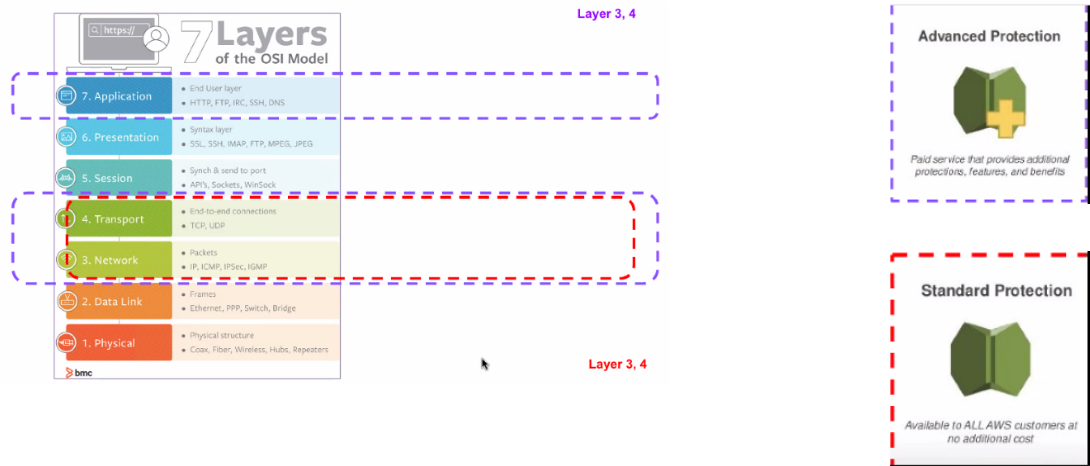
IPS daha çok niyet okuyup saldırıları engelliyor.

- AWS Inspector: Vulnerable Scanner gibi çalışır. Bizim sistemi inceler ve açıkları düzeltmek için önerilerde bulunur bize.
- AWS Guard Duty: DAha çok log kayıtlarını inceler. Anormal durum yakalarsa engeller. Ör. afrikadan alışveriş yapma gibi. AWS haricindeki karşılığı **SIEM**'dir

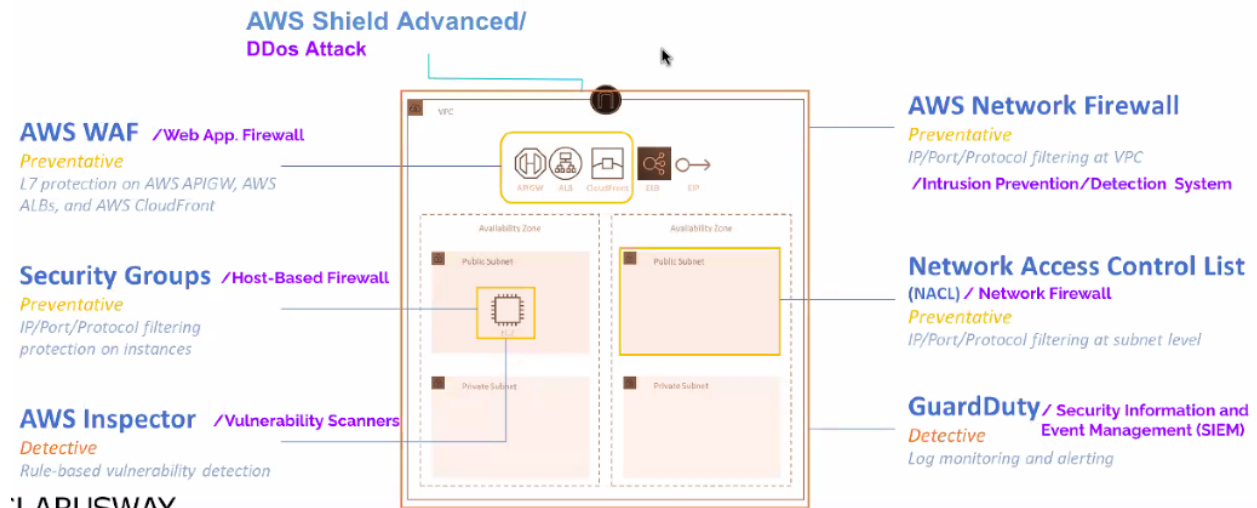
- AWS Security Hub: Daha çok dashboard gibidir.
- AWS Shield: Daha çok DDOS ataklara yönelik uzmanlaşmış. Tamam WAF DDOSları engelliyor ancak Shield direk bu konuya yönelmiş.

Standart Protection: sadece Layer 3-4 te koruma sağlar. Her kullanıcıya bu korumayı sağlar.

Advanced Protection: Layer 3-4- ve 7'de koruma sağlar. Ücrete tabi



► Summary of AWS Security Services



AWS Security Service	Protects Against	Applies To	Similar To
Security Groups	Unauthorized access to VPC resources	Instance @ Layer 3, 4 (IP, Port, Protocol)	Host-based Firewall
Network Access Control List (NACL)	Unauthorized access to VPC resources	Subnet @ Layer 3, 4 (IP, Port, Protocol)	Network Firewall
AWS WAF	Web attacks e.g. SQL Injection, cross-site scripting	Layer 7 (HTTP)	WAF
AWS Network Firewall	Malicious network intrusion	Layer 3, 4, 7	IPS / IDS
Guard Duty	Malicious network traffic	Log analysis	SIEM
AWS Inspector	Exploitable vulnerabilities	EC2, ECR	Vulnerability scanner
SecurityHub	Provides single pane of glass view	Network, accounts	SIEM
AWS Shield	DDos Attack	Layer 3, 4 (Shield Standard) Layer 7 (Shield Advanced)	WAF

AWS WAF servisi boş olarak bize geliyor. Üzerine ekleyeceğimiz kurallara göre ücretlendirilir.

Security, Identity, and Compliance

AWS WAF

Protect your web applications from common web exploits

AWS WAF is a web application firewall service that lets you monitor web requests that are forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer. You can protect those resources based on conditions that you specify, such as the IP addresses that the requests originate from.

Get started with AWS WAF

Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.

[Create web ACL](#)

Buradan belirli ruleları seçiyoruz. Bir kısmı paralı bir kısmı ücretsiz. İstersek kendi rulelarımızı da oluşturabiliriz.

Add my own rules and rule groups [Info](#)

[Close](#)

Rule type

Rule type

☐ IP set

Use IP sets to identify a specific list of IP addresses.

☒ Rule builder

Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.

☐ Rule group

Use a rule group to combine rules into a single logical set.




Her bir rule'un bir kapasitesi var. Bir web ACL'in max. capacitysi 1500 olabilir. Seçtiğimiz rullar toplanır. 1500 geçmez ise çalıştırılır.

AWS WAF hizmeti, aynı anda birden çok müşterinin farklı web uygulamalarını koruması gerektiği için sınırlı bir kaynak havuzuna sahiptir. Bu nedenle, hizmetin en yüksek performansı ve müşterilere en iyi deneyimi sunması için, AWS WAF kapasitesi belirli bir seviyede tutulur ve bu seviye maksimum 1500'dir.

Bu sınır, aynı zamanda AWS WAF hizmetini kullanan müşterilerin trafiğinin yoğunluğuna ve diğer faktörlere de bağlıdır. AWS, müşterilerinin ihtiyaçlarına göre bu kapasite sınırını değiştirebilir veya artırabilir.

Name	Capacity	Action
Admin protection Contains rules that allow you to block external access to exposed admin pages. This may be useful if you are running third-party software or would like to reduce the risk of a malicious actor gaining administrative access to your application.	100	<input checked="" type="radio"/> Add to web ACL Edit
Amazon IP reputation list This group contains rules that are based on Amazon threat intelligence. This is useful if you would like to block sources associated with bots or other threats.	25	<input checked="" type="radio"/> Add to web ACL Edit
Anonymous IP list This group contains rules that allow you to block requests from services that allow obfuscation of viewer identity. This can include request originating from VPN, proxies, Tor nodes, and hosting providers. This is useful if you want to filter out viewers that may be trying to hide their identity from your application.	50	<input checked="" type="radio"/> Add to web ACL Edit
Core rule set Contains rules that are generally applicable to web applications. This provides protection against exploitation of a wide range of vulnerabilities, including those described in OWASP	700	<input type="radio"/> Add to web ACL

▼ F5 managed rule groups

Name	Capacity	Action
API Security Rules Protects against API attacks, web attacks (such as XML external entity attacks) and server-side request forgery. The rule set includes support for XML and JSON payloads, and common web API frameworks.	1000	Subscribe in AWS Marketplace 
Bot Protection Rules Protect against automated attacks. Bot Protections Rules is a partner managed rule group for AWS WAF that stops a broad range of malicious bots activities such as vulnerability scanners, web scrapers, DDoS tools, and forum spam tools.	1000	Subscribe in AWS Marketplace 
Common Vulnerabilities & Exposures (CVE) Rules Protect against CVEs. CVE Rules for AWS WAF provides protection for high profile CVEs targeting the following: Apache, Apache Struts, Bash, Elasticsearch, IIS, JBoss, JSP, Java, Joomla, MySQL, Node.js, PHP, PHPMyAdmin, Perl, Ruby On Rails, and WordPress.	1000	Subscribe in AWS Marketplace 
Web Exploits OWASP Rules Protect against web exploits. F5 Web Exploits OWASP Rules for AWS WAF, provides protection against web attacks that are part of the OWASP Top 10, such as: SQLi, XSS, command injection, No-SQLi injection, path traversal, and predictable resource.	1000	Subscribe in AWS Marketplace 