AWS Solutions Architect Associate

Session 602

Security, Id & Compliance: AWS Shield and WAF

July/2024

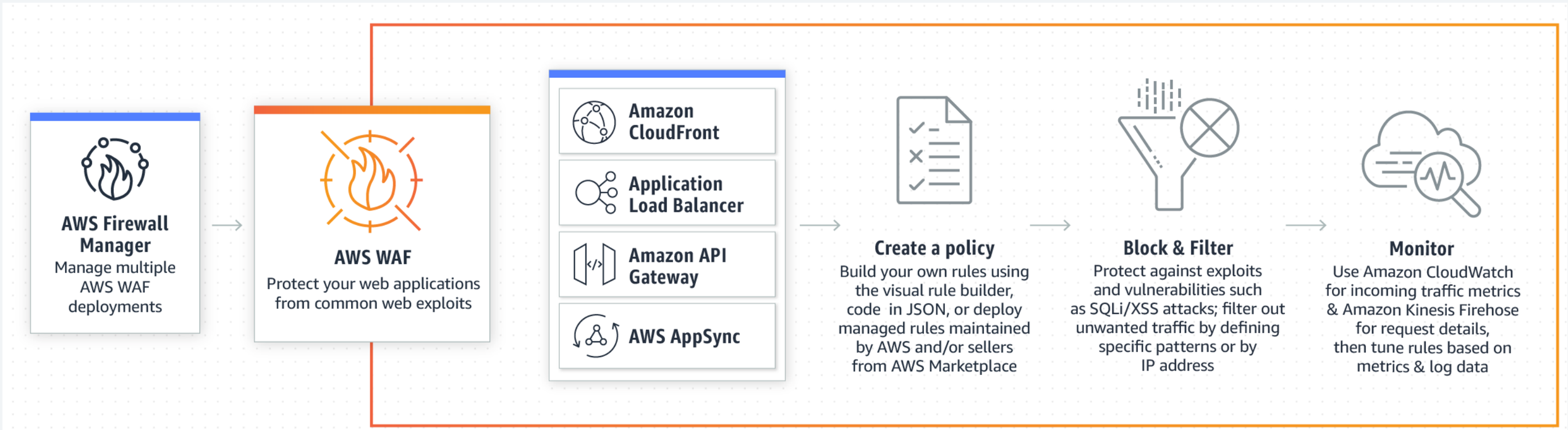
Web Application Firewall

fmorenod.co

Web Application Firewall (WAF) is a special firewall to monitor, inspect and block any HTTP/S traffic from and to Web Application. Commercial examples: F5, Fortinet, Barracuda.

The level of inspection come from source IP or content on the query. The action can be:

- Allow all requests except the ones that you specify
- Block all requests except the ones that you specify. You can block request if there pass a threshold under conditions
- Count the requests that match the properties that you specify

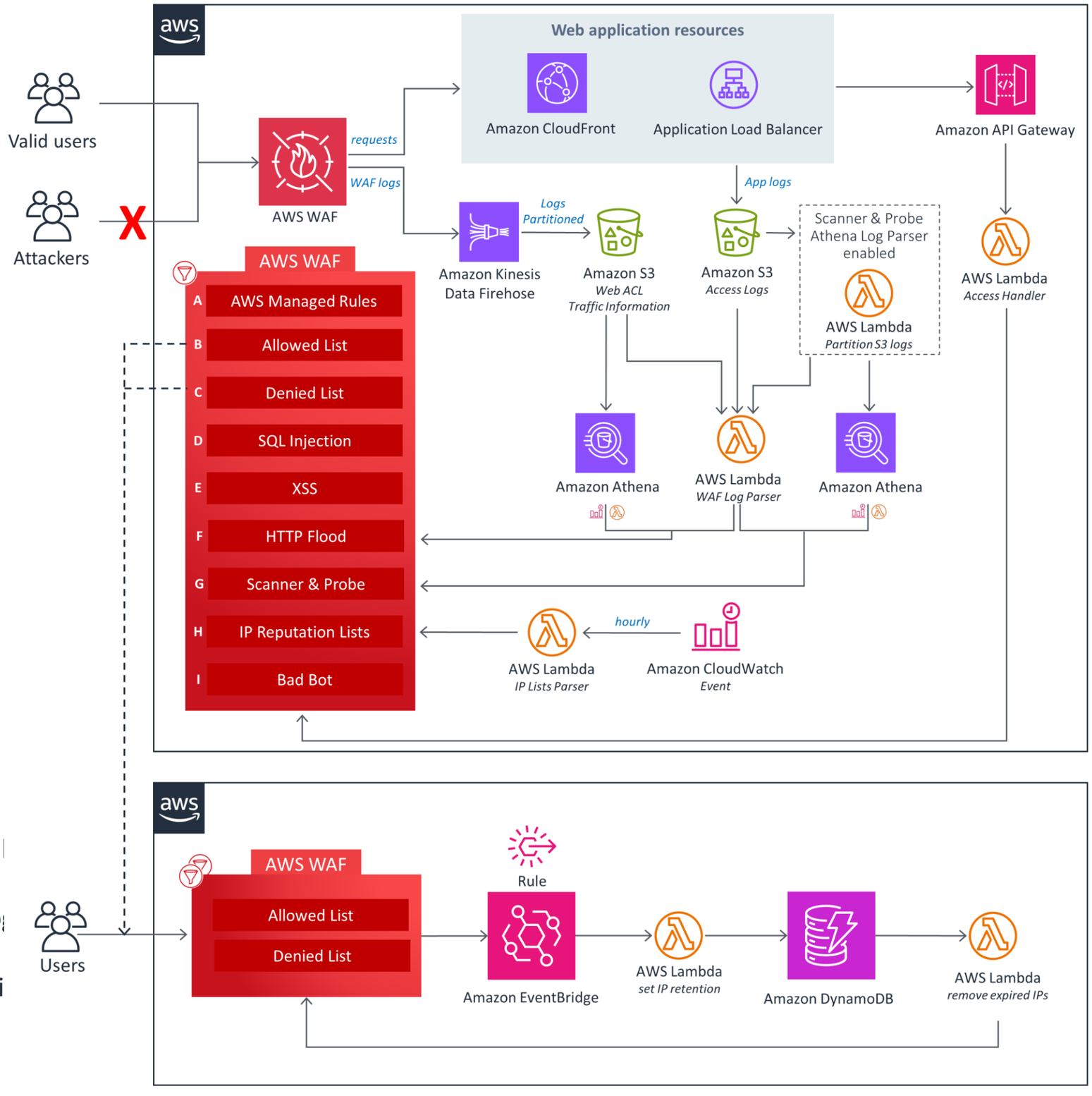


- Agile protection against web attacks
- Save time with managed rules: Rules Marketplace.
- Improved web traffic visibility; provided real-time metrics and sampled requests.
- Ease of deployment & maintenance: Reuse in several targets.
- Easily monitor, block, or rate-limit bots: AWS WAF Bot Control.
- Security integrated with how you develop applications

Taken from https://aws.amazon.com/waf/?nc=bc&pg=gs and https://aws.amazon.com/waf/getting-started/ (18/07/2024)

WAF - Benefits

- Web traffic filtering. Using:
  - ❖ IP addresses that requests originate from.
  - ❖ Country that requests originate from.
  - ❖ Values in request headers.
  - ❖ Strings that appear in requests, either specific strings or strings that match regular expression (regex) patterns.
  - ❖ Length of requests.
  - ❖ Presence of SQL code that is likely to be malicious (known as *SQL injection*).
  - ❖ Presence of a script that is likely to be malicious (known as *cross-site scripting*).



Example of WAF using Cloudformation:

HTTP Flood: web-layer DDoS attacks or a brute-force l
attempt.

Scanners and Probes (G): parses application access lo
detect abnormal requests and block it.

Bad Bots (I): honeypot to avoid attack overpass your i

Taken from https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html and https://aws.amazon.com/solutions/implementations/aws-waf-security-automations/ (18/07/2024)

AWS WAF Components

Conditions

Conditions

IP set - list of ip addresses or Cidr range string match set - list of http field strings to check in a request

IP Set : Internal IP address

101.21.23.32/24

101.21.23.32/24

IP Set : Beta users IP address

121.25.36.35

121.36.54.25

String match Set : Beta user auth

Authorization matches Basic Qqwerlkjou

Authorization matches Basic qiuojl34987

Rules

Rules

Create rules using a combination of conditions ie IP addresses, string match sets

Rule : Internal Users

IP Set
Internal IP address

Rule : Beta Users

IP Set
Beta users IP address

And

String match set
Beta user auth

Web ACL

Web ACL

Add rules to Web ACL & define actions.

Web ACL : Beta app Accesslist

If

Rule:
Internal Users - Allow

Or

Rule:
Beta Users - Allow

Else

Block all requests

Apply

Elastic Load Balancing

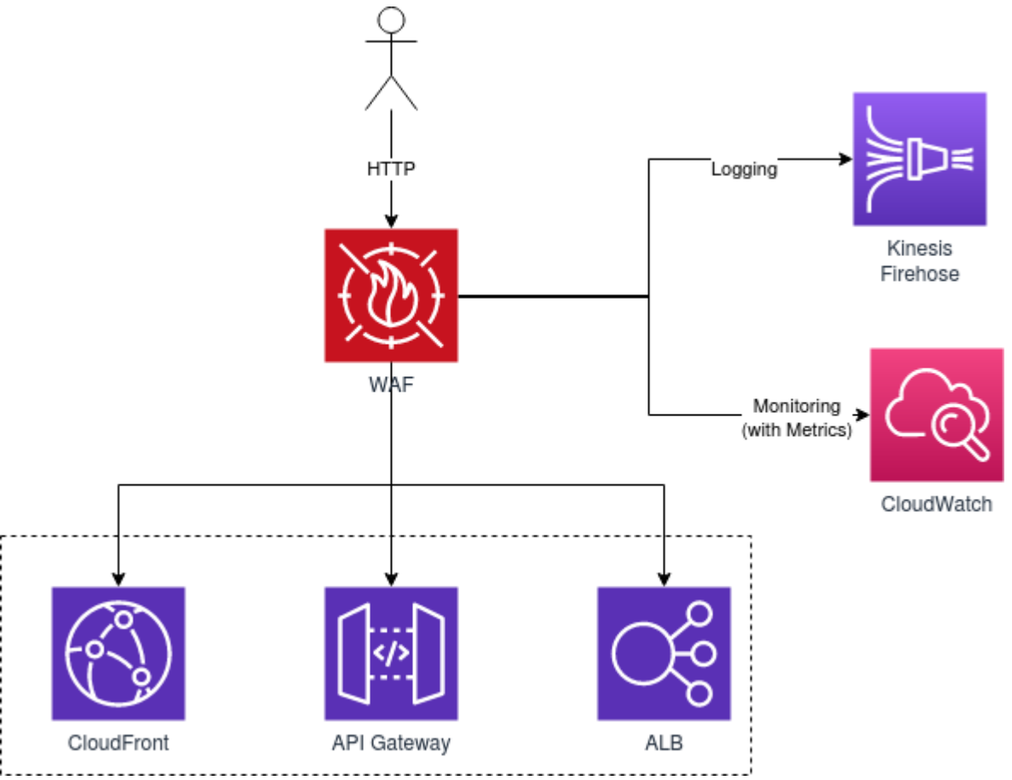
Amazon CloudFront

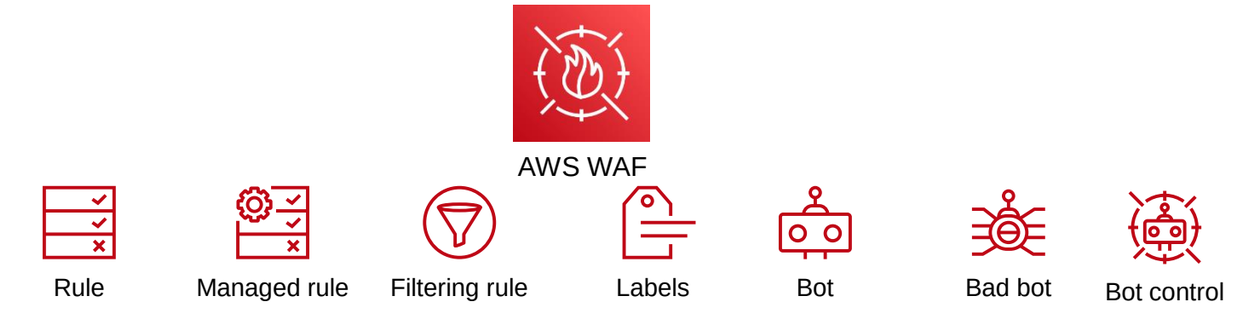
Report/Logs

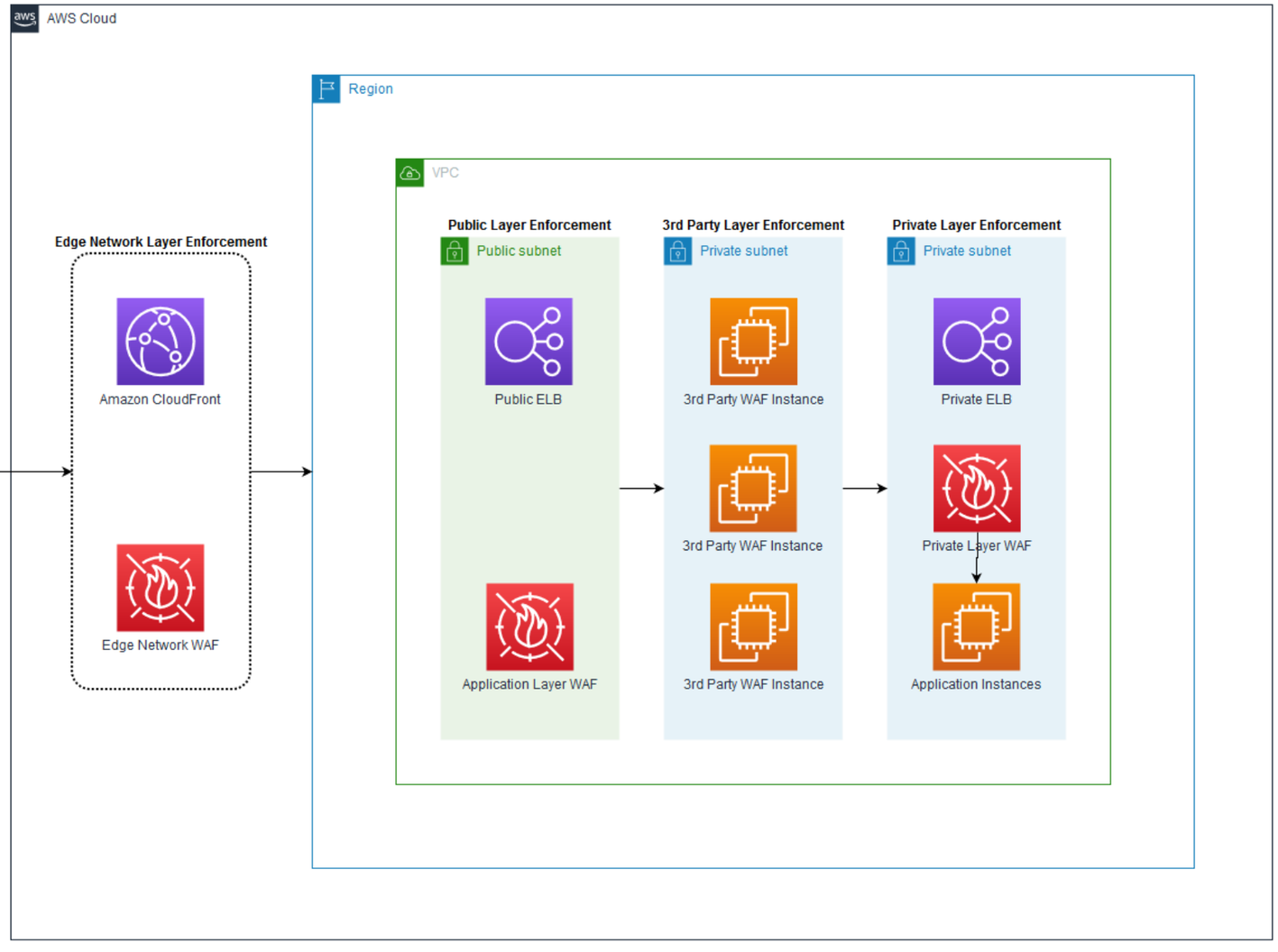
Amazon CloudWatch

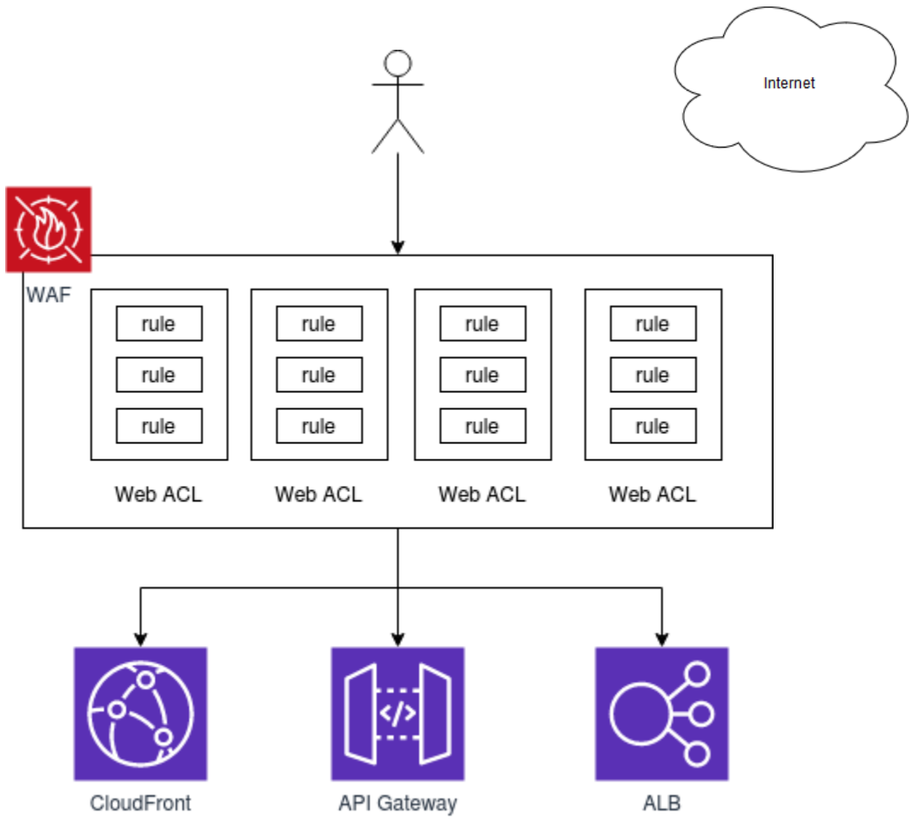
Taken from https://www.slideshare.net/AmazonWebServices/aws-web-application-firewall-and-aws-shield-webinar , slide 13/41 (18/07/2024)

WAF Examples









Taken from https://aws.amazon.com/blogs/security/defense-in-depth-using-aws-managed-rules-for-aws-waf-part-1/ (18/07/2024)

3rd Party WAF Dashboard

Taken from https://help.sumologic.com/07Sumo-Logic-Apps/01Amazon_and_AWS/AWS_WAF/Install_the_AWS_WAF_App_and_View_the_Dashboards (18/07/2024)

WAF - Pricing

Region
US East (Ohio)

Resource Type	Price
Web ACL	$5.00 per month (prorated hourly)
Rule	$1.00 per month (prorated hourly)
Request	$0.60 per 1 million requests (for inspection up to 1500 WCUs and default body size*)
Bot Control and Fraud Control	Additional cost as per tabs above

Region
US East (Ohio)

AWS WAF Bot Control*	Request Fee	Captcha	Challenge
Common	$1.00 per Million requests inspected	$4.00 per 10k captcha attempts analyzed	$0.40 per million responses served
Targeted	$10.00 per Million requests inspected	Included	Included

Taken from https://aws.amazon.com/waf/pricing/ (18/07/2024)

Case A: No managed rule group and 19 rules written by you

Web ACL charges = $5.00 * 1 = $5.00
Rule charges = $1.00 * (19 rules) = $19.00
Request charges = $0.60/million * 10 million = $6.00
Total combined charges = $30.00/month

Case B: One managed rule group from AWS Marketplace seller and 9 rules written by you

Web ACL charges = $5.00 * 1 = $5.00
Rule charges = $1.00 * (1 managed rule group + 9 rules) = $10.00
Request charges = $0.60/million * 10 million = $6.00
Total AWS WAF charges = $21.00/month

Managed rule group charges = $20.00
Managed rule group request charges = $1.20/million * 10 million = $12.00
Total AWS Marketplace charges = $32.00/month

Total combined charges = $53.00/month

Case E: Bot Control with scope down statement enabled on web ACL and 7 rules written by you

Web ACL charges = $5.00 * 1 = $5.00
Rule charges = $1.00 * (1 managed rule group + 7 rules) = $8.00
Request charges = $0.60/million * 20 million = $12.00
Total WAF charges = $25.00/month

Bot Control charges = $10.00 * 1 = $10.00
Bot Control request charges = $1.00/million * (20 million requests * 50% - 10 million free requests) = $0
Total Bot Control charges = $10.00/month

Total combined charges = $35.00/month

Case F: Targeted Bot Control enabled on 3 WebACLs and 21 rules written by you processing 35 million requests

Web ACL charges = $5.00 * 3 = $15.00
Rule charges = $1.00 * (3 managed rule group + 21 rules) = $24.00
Request charges = $0.60/million * 35 million = $21.00
Total WAF charges = $60.00/month

Bot Control charges = $10.00 * 3 = $30.00
Bot Control request charges = $10.00/million * (35 million requests - 1 million free requests) = $340.00
Total Bot Control charges = $370.00/month

Total combined charges = $430.00/month

DDoS Attack

DoS is the acronym of Denial of Service, and it is generating multiple packets to overwhelm (overpass) the current capacity of the server/service to attend legitimate requests.
DDoS is Distributed DoS, which use multiple source: attackers or compromised hosts (zombies).

Open Systems Interconnection (OSI) Model:

Difficult to detect, specific and specialized attacks. i.e. Login form

#	Layer	Application	Description	Vector Example
7	Application	Data	Network process to application	HTTP floods, DNS query floods
6	Presentation	Data	Data representation and encryption	SSL abuse
5	*Session*	*Data*	*Interhost communication*	*N/A*
4	Transport	Segments	End-to-end connections and reliability	SYN floods
3	Network	Packets	Path determination and logical addressing	UDP reflection attacks
2	*Datalinks*	*Frames*	*Physical addressing*	*N/A*
1	*Physical*	*Bits*	*Media, signal, and binary transmission*	*N/A*

Easier to detect

Techniques to mitigate:
Reduce Attack Surface Area: CDN, ELB and WAF or ACL.
Plan for Scale: Transit Capacity (CDN and Smart DNS) and Server Capacity (Elastic servers).
Know what is normal and abnormal traffic
Deploy Firewalls for Sophisticated Application attacks: WAF.

Taken from https://aws.amazon.com/shield/ddos-attack-protection/?nc1=h_ls (18/07/2024)

AWS Shield

Feature	AWS Shield Standard	AWS Shield Advanced*
Active Traffic Monitoring		
Network flow monitoring	Yes	Yes
Automatic always-on detection	Yes	Yes
Application traffic monitoring	x	Yes
Attack Mitigations		
Protection from common DDoS attacks (e.g. SYN floods, ACK floods, UDP floods, Reflection attacks)	Yes	Yes
Automatic inline mitigation	Yes	Yes
Additional DDoS mitigation capacity for large attacks	x	Yes
Automatic application layer (L7) DDoS mitigations	x	Yes
Self-service application layer (Layer 7) mitigations	Yes, using AWS WAF	Yes, using AWS WAF
SRT-driven application layer (Layer 7) mitigations	x	Yes, with Shield Response Team
Instant rule updates	Yes, using AWS WAF	Yes, using AWS WAF
AWS WAF for app vulnerability protection	Yes, using AWS WAF	Yes, using AWS WAF
Visibility and Reporting		
Layer 3/Layer 4 attack notification	x	Yes
Layer 7 attack notification	x	Yes
Layer 3/Layer 4/ Layer 7 attack historical report	x	Yes
Shield Response Team and Support		
DDoS protection best practices/architecture review	Yes, self-service	Yes
Custom mitigations during attacks	x	Yes, with Enterprise or Business support
Post attack analysis	x	Yes, with Enterprise or Business support
DDoS Cost Protection (Service credits for DDoS scaling charges)		
Amazon Route 53	x	Yes
Amazon CloudFront	x	Yes
Elastic Load Balancing (ELB)	x	Yes
Amazon Elastic Compute Cloud (EC2)	x	Yes
Note: AWS Shield Advanced benefits, including DDoS cost protection, are subject to your fulfillment of the 1-year subscription commitment.		

Web Application Firewall (WAF)		
Self-service	Yes	Yes
API access/integration	Yes	Yes
Flexible rules engine	Yes	Yes
Fast rule propagation	Yes	Yes
Pricing	See Pricing	Included at no additional charge with AWS Shield Advanc protected in AWS Shield Advanced
Cost		
Monthly	x	Yes, see Pricing (Subject to 1-year subscripti
Usage based	x	Yes, see Pricing
SLA	x	Yes

AWS Shield is a managed Distributed Denial of Service (DDoS) protection.

AWS Shield Standard, at no additional charge, bring support to Cloudfront and Route 53. It specialized on Layer 3 and 4.

AWS Shield Advanced bring all services of Standard plus EC2, ELB and Global Accelerator. In addition, it is integrated with WAF. Full support managed.

AWS Shield

AWS Shield Advanced

Taken from https://aws.amazon.com/shield/ddos-attack-protection/?nc1=h_ls
https://docs.aws.amazon.com/waf/latest/developerguide/ddos-overview.html
https://aws.amazon.com/shield/pricing/ (18/07/2024)

Shield - Pricing

Pricing	AWS Shield Standard	AWS Shield Advanced
Subscription Commitment	None	1 Year*
Monthly Fee (See note 1)	No additional cost	$3,000.00
Data Transfer Out Usage Fees (See note 2)	No additional cost	AWS Shield Advanced Data Transfer Usage fees apply as per table below.

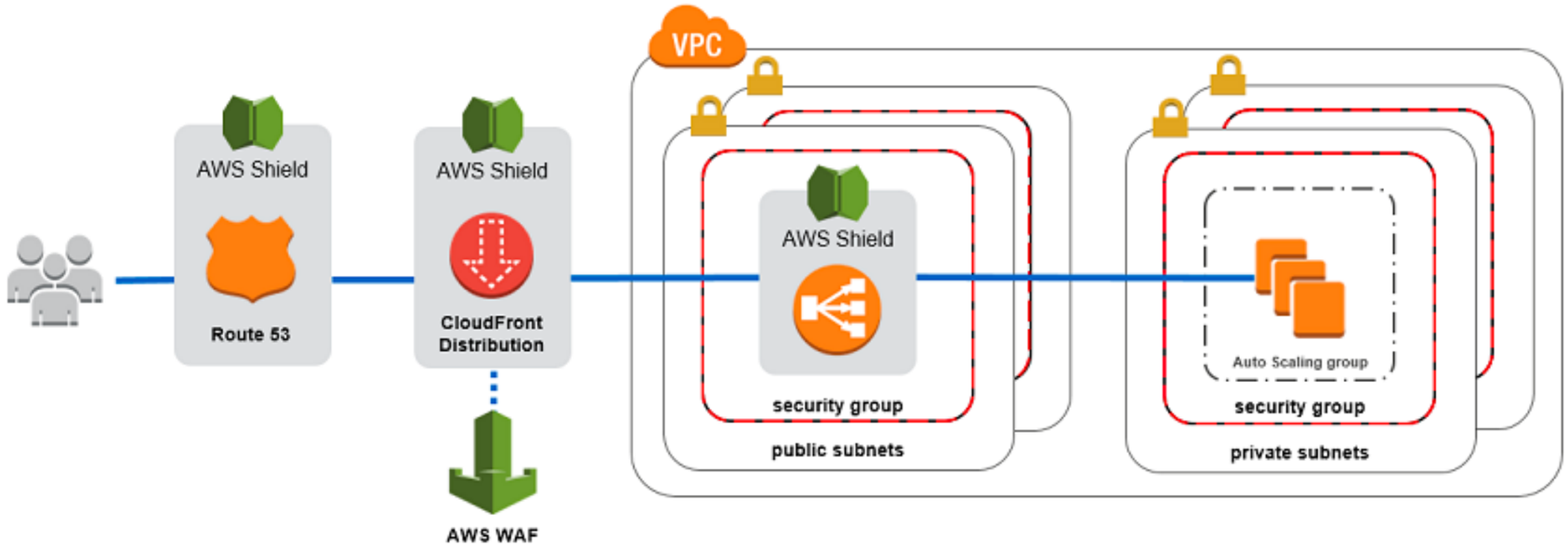
AWS Shield Advanced Data Transfer Out Usage Fees (per GB)

Region: US East (Ohio)

	Amazon CloudFront	Elastic Load Balancing (ELB)	AWS Elastic IP (EC2 and Network Load Balancer)	AWS Global Accelerator	Amazon Route 53
First 100 TB	$0.025	$0.05	$0.05	$0.025	No additional cost
Next 400 TB	$0.02	$0.04	$0.04	$0.02	No additional cost
Next 500 TB	$0.015	$0.03	$0.03	$0.015	No additional cost
Next 4 PB	$0.01	Contact Us	Contact Us	$0.01	No additional cost
Above 5 PB	Contact Us	Contact Us	Contact Us	Contact Us	No additional cost

Taken from https://aws.amazon.com/shield/pricing/?nc1=h_ls (18/07/2024)

Shield - Use Cases



Global activity detected by AWS Shield

The following is a summary of events detected by AWS Shield across all applications running on AWS. With AWS Shield Advanced, you also receive a dashboard that's specific to your applications.

Last two weeks summary

Largest packet attack	223 Mpps
Largest bit rate	448 Gbps
Most common vector	UDP traffic
Threat level	Normal
Total number of attacks	74,588

Taken from https://aws.amazon.com/es/blogs/aws-spanish/usando-aws-para-ejecutar-cargas-criticas-en-sector-publico-consulta-de-resultados-a-elecciones-nacionales-o-estatales/ (18/07/2024)

AWS Firewall Manager

AWS Firewall Manager simplifies your administration and maintenance tasks across multiple accounts and resources for WAF (rules), AWS Shield Advanced (protections), and VPC (security groups: EC2 and ENI) in accounts due to AWS Organizations.
Protect resources (specific types or tagged resources, as you wish) on associated accounts (new members and its resources).
Benefits:
Centralized firewall rules
Security policies across AWS Accounts in your organization.
Coherence (Audit for current and new resources) and Hierarchy.

Pre-requisites

- Step 1: Join and configure AWS Organizations
- Step 2: Set the AWS Firewall Manager administrator account
- Step 3: Enable AWS Config
- Step 4: For Network Firewall and DNS Firewall policies, enable resource sharing
- Step 5: To use AWS Firewall Manager in Regions that are disabled by default

Taken from https://docs.aws.amazon.com/waf/latest/developerguide/fms-prereq.html (18/07/2024)

Firewall Manager - Pricing

For AWS Network Firewall protection policies, AWS Firewall Manager has these main pricing components:

- AWS Firewall Manager protection policy - Monthly fee per Region.
- AWS Network Firewall endpoints - Those created by Firewall Manager will be charged based on current pricing. For more details, see AWS Network Firewall pricing.
- AWS Config Rules - Those rules created by Firewall Manager to monitor changes in resource configurations are charged based on current pricing. For more details, see AWS Config pricing.

You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.

For AWS WAF protection policies, AWS Firewall Manager has these main pricing components:

- AWS Firewall Manager protection policy - Monthly fee per Region.
- AWS WAF WebACLs or Rules - Those created by Firewall Manager will be charged based on current pricing. For more details, see AWS WAF pricing.
- AWS Config Rules - Those rules created by Firewall Manager to monitor changes in resource configurations are charged based on current pricing. For more details, see AWS Config pricing.

If you are an AWS Shield Advanced customer:

For AWS Shield Advanced customers, AWS Firewall Manager protection policy is included at no additional charge. Shield Advanced customers will be charged for the AWS Config rules created to monitor any changes in resource configurations. For more details, check the AWS Shield pricing and AWS Config pricing.

AWS Shield protection policies can be created using AWS Firewall Manager only for Shield Advanced users. The price is included in the AWS Shield Advanced subscription at no additional cost. In addition, the pricing components are as follows:

• AWS Shield Advanced Data Transfer Out Usage Fees: For more details, see AWS Shield pricing

• AWS Config Rules - Those rules created by Firewall Manager to monitor changes in resource configurations are charged based on current pricing. For more details, see AWS Config pricing

For Amazon VPC security group protection policies and network access control lists (ACLs), AWS Firewall Manager has these main pricing components:

• AWS Firewall Manager protection policy - Monthly fee per Region.

• AWS Config Rules - Those rules created by Firewall Manager to monitor changes in resource configurations are charged based on current pricing. For more details, see AWS Config pricing.

You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.

For Amazon Route 53 Resolver DNS Firewall protection policies, AWS Firewall Manager has these main pricing components:

- AWS Firewall Manager protection policy - Monthly fee per Region.
- Route 53 Resolver DNS Firewall charges- Rule groups created by Firewall Manager will be charged based on current pricing. For more details, see Route 53 Resolver DNS Firewall pricing.
- AWS Config Rules - Those rules created by Firewall Manager to monitor changes in resource configurations are charged based on current pricing. For more details, see AWS Config pricing.

You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.

For Third-party firewall protection policies, AWS Firewall Manager has these main pricing components:

- AWS Firewall Manager protection policy - Monthly fee per Region.
- Third-party firewall charges – Pricing information for Third-Party Firewalls are available on the AWS Marketplace page.
- AWS Config Rules - Those rules created by Firewall Manager to monitor changes in resource configurations are charged based on current pricing. For more details, see AWS Config pricing.

You only pay for what you use, as you use it; there are no minimum fees and no upfront commitments.

Taken from https://aws.amazon.com/firewall-manager/pricing/?nc1=h_ls (18/07/2024)

Firewall Manager - Pricing

AWS Network Firewall protection policy

All public regions

Region: US East (Ohio)

- $100.00 per policy per Region
- AWS Config rules created by Firewall Manager - See AWS Config pricing
- AWS Network Firewall endpoints created by Firewall Manager - See AWS Network Firewall pricing.

AWS WAF protection policy

All public regions

Region: US East (Ohio)

$100.00 per policy per Region

Global (Amazon CloudFront locations)

$100.00 per policy per Region

AWS Shield Advanced protection policy

All public regions

Included for Shield Advanced customers. No charge per policy per Region

Global (Amazon CloudFront locations)

Included for Shield Advanced customers. No charge per policy per Region

- AWS WAF WebACLs or Rules created by Firewall Manager - Included. No additional charge.
- AWS Config rules created by Firewall Manager - See AWS Config pricing
- AWS Shield Advanced - See AWS Shield pricing

Amazon VPC security group protection policy

All public regions

Region: US East (Ohio)

- $100.00 per policy per Region
- AWS Config rules created by Firewall Manager - See AWS Config pricing

Amazon Route 53 Resolver DNS Firewall protection policy

All public regions

Region: US East (Ohio)

- $100.00 per policy per Region
- AWS Config rules created by Firewall Manager - See AWS Config pricing
- Route 53 Resolver DNS Firewall rule groups created by Firewall Manager – See Route 53 Resolver DNS Firewall pricing.

Third-party firewall protection policy

Fortinet

All public regions

Region: US East (N. Virginia)

- $100.00 per policy per Region
- AWS Config rules created by Firewall Manager - See AWS Config pricing
- Third party firewall charges.

Palo Alto

All public regions

Region: US East (Ohio)

- $100.00 per policy per Region
- AWS Config rules created by Firewall Manager - See AWS Config pricing

Amazon VPC Network ACL Policy Support

All public regions

Region: US East (Ohio)

- $100.00 per policy per Region
- AWS Config rules created by Firewall Manager - See AWS Config pricing

Taken from https://aws.amazon.com/firewall-manager/pricing/?nc1=h_ls (18/07/2024)

Firewall Manager – Pricing Example

Pricing example 2: AWS Firewall Manager policy with 7 accounts

Let's assume you created a new protection policy for an Organization not subscribed to Shield Advanced with 7 AWS Accounts.

- AWS Firewall Manager charges are **$100 per month** for (1) policy.
- In addition, AWS Firewall Manager creates (2) AWS Config rules per policy, per account. Let's assume there are a total of 10,000 Config item changes across all accounts, accounting for $30 (10,000 x $0.003). In addition, let's assume there are 10,000 rule evaluations, resulting in $10 (10,000 x $0.001, where the first 10,000 evaluations are $0.001 each).
- The total AWS Config charges are $40 per month ($30 + $10).
- AWS Firewall Manager creates one AWS WAF WebACL and one Rule per account. Each WebACL costs $5 per month and Each Rule costs $1 per month, for a total of **$42 per month** = ($5 WebACL + $1 Rule) X 7 Accounts.
- At the end of the month your charges will be a total of **$182** ($100 for AWS Firewall Manager + $40 for AWS Config + $42 for AWS WAF).

Item	Qty	Accounts	$/month	Monthly total
Protection Policy	1	7	$100.00	$100.00
AWS Config Configuration Item	10,000	7	$0.0030	$30.00
AWS Config rule evaluations	10,000	7	$0.0010	$10.00
WebACL	1	7	$5.00	$35.00
WAF Rule	1	7	$1.00	$7.00
Total				**$182.00 per month**

Taken from https://aws.amazon.com/firewall-manager/pricing/?nc1=h_ls (18/07/2024)