

AWS Security 101: 함께 만들어봐요. 안전한 서비스

2화 - DDoS, 침해사고 예방

홍성진



홍성진 aka. nisam

- 샌드버드 Product Security Engineer
- 前 네이버 Security Engineer
- AWS 한국 사용자모임 보안 소모임 운영진
- OWASP Seoul Chapter 운영진
- 비오비 4기

#AppSec #CloudSec #DevSecOps #ThreatModeling #BugBounty #SecureCoding

#☕ #🎾 #🏋️



PREVIOUSLY ...



??? :

성진 씨 우리 기존 서비스 AWS에 올릴거예요.
내일까지 AWS 계정 만들어서 **안전**하게 설정 해주세요!



성진 :

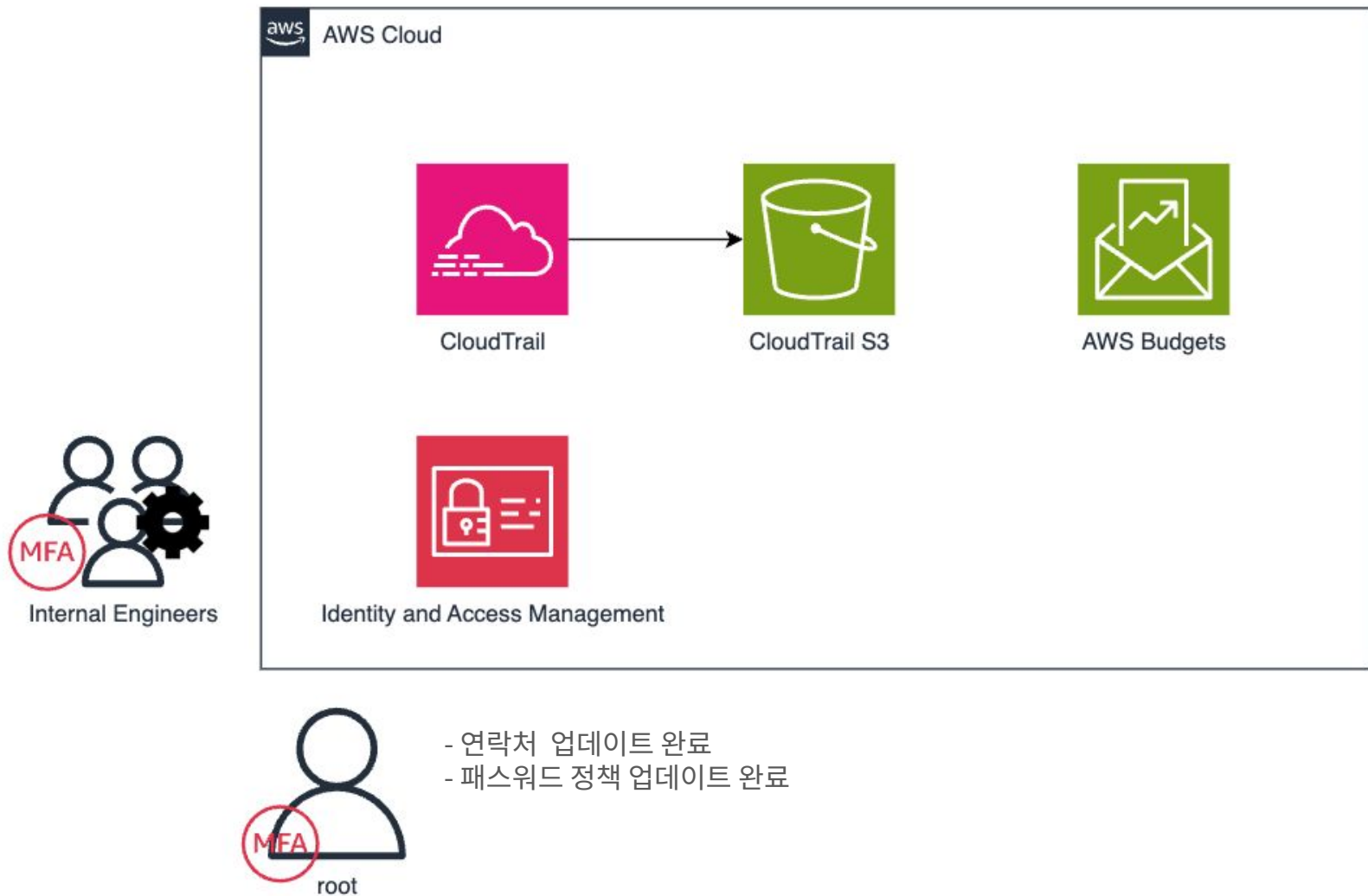
네? 저 AWS 안 써봤는데요?



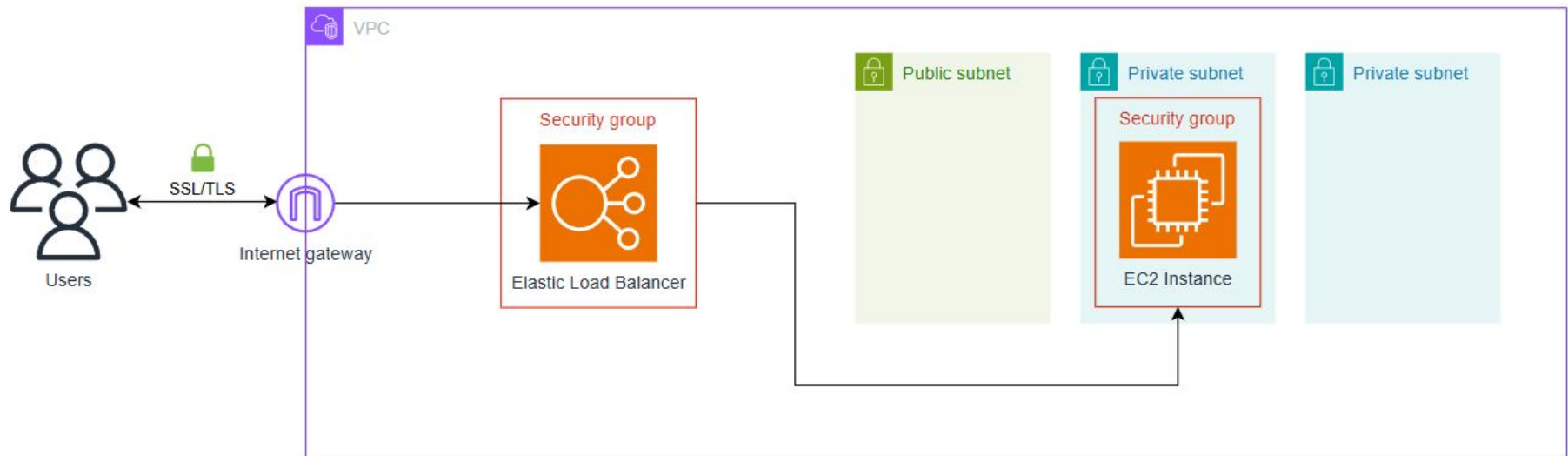


Shared Responsibility Model

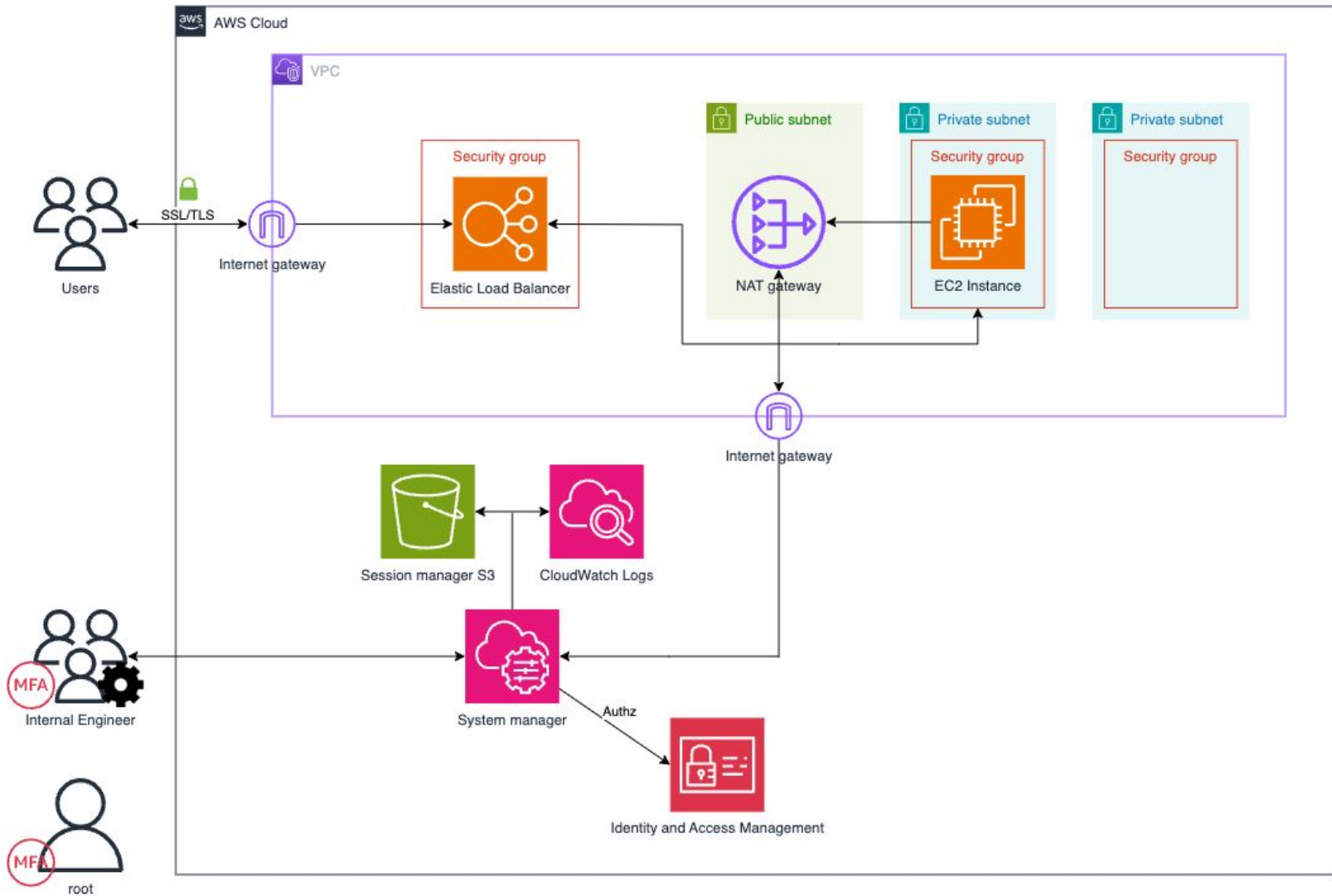
아키텍처 v0.1



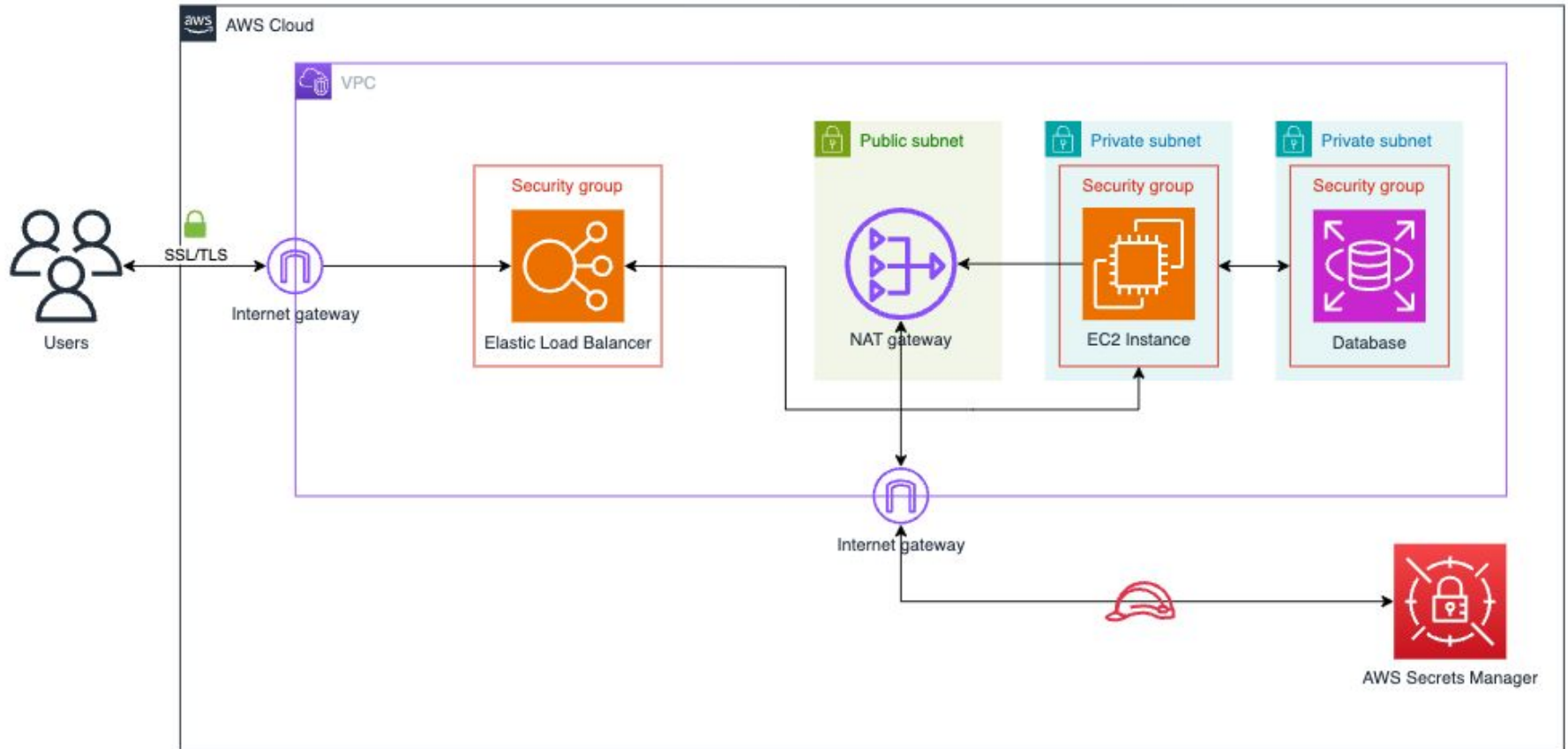
아키텍처 v0.2 (암호화 통신 적용)



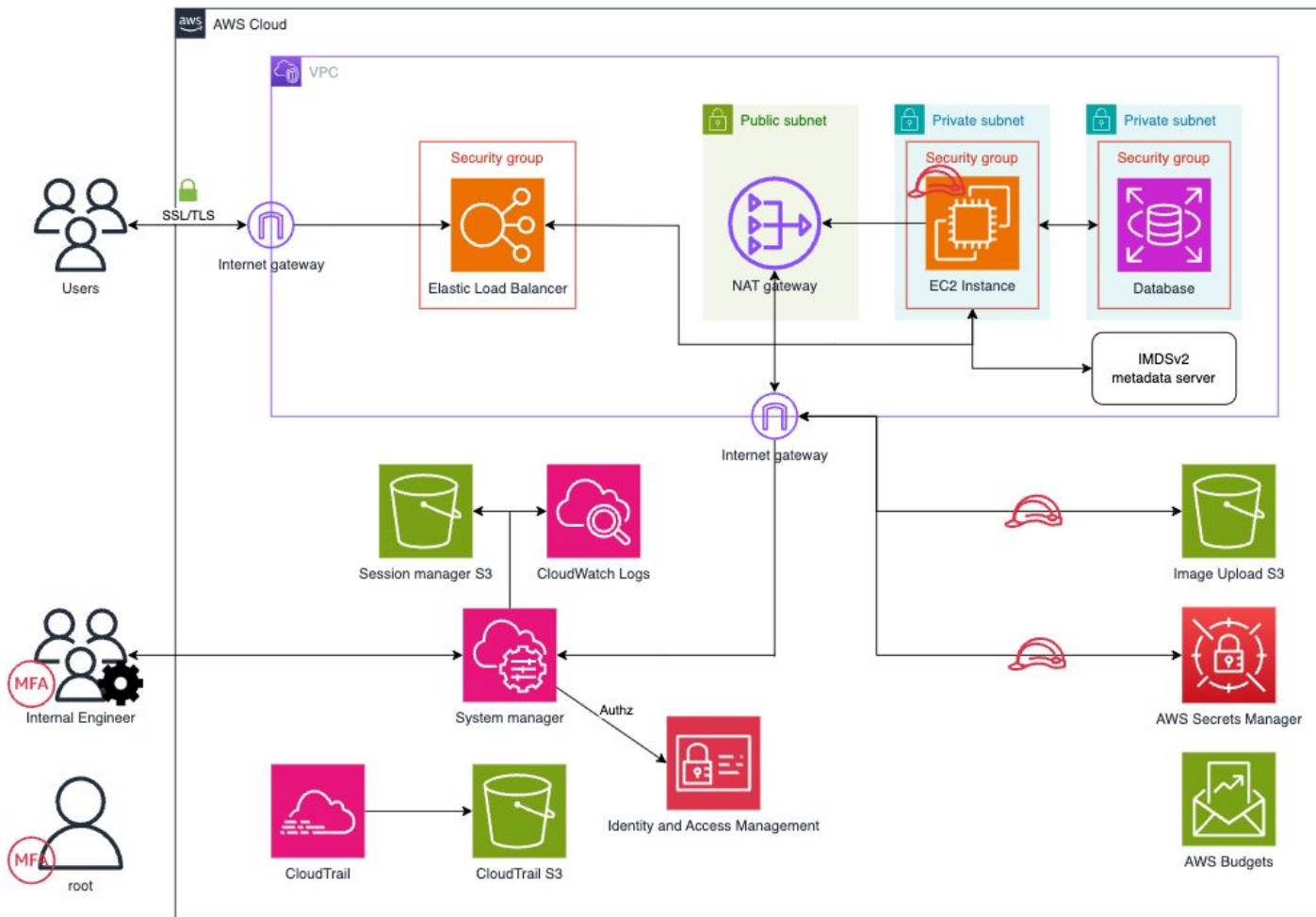
아키텍처 v0.3 (서버 접근 제어 적용)



아키텍처 v0.4 (데이터 베이스)



최종 인프라 구성도 v1.0





성진 :

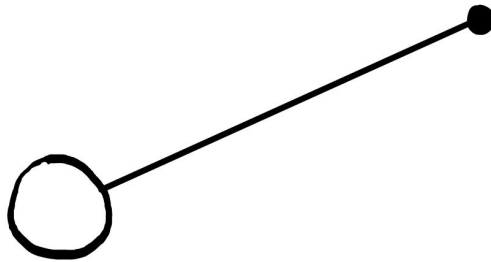
우선 이정도면 오늘은 퇴근해도 되겠지…?



??? :

성진씨! 잠시 제 자리로 와주시겠어요?

여러분들은 이제 ...





??? :

성진씨, 요즘 보안 사고가 끊이지 않던데 우리는 DDoS나 침해사고가 발생해도 대응에 문제가 없나?



성진 :

아.. 네! 한번 알아보겠습니다!



1. 클라우드 보안의 이해

공동 책임 모델

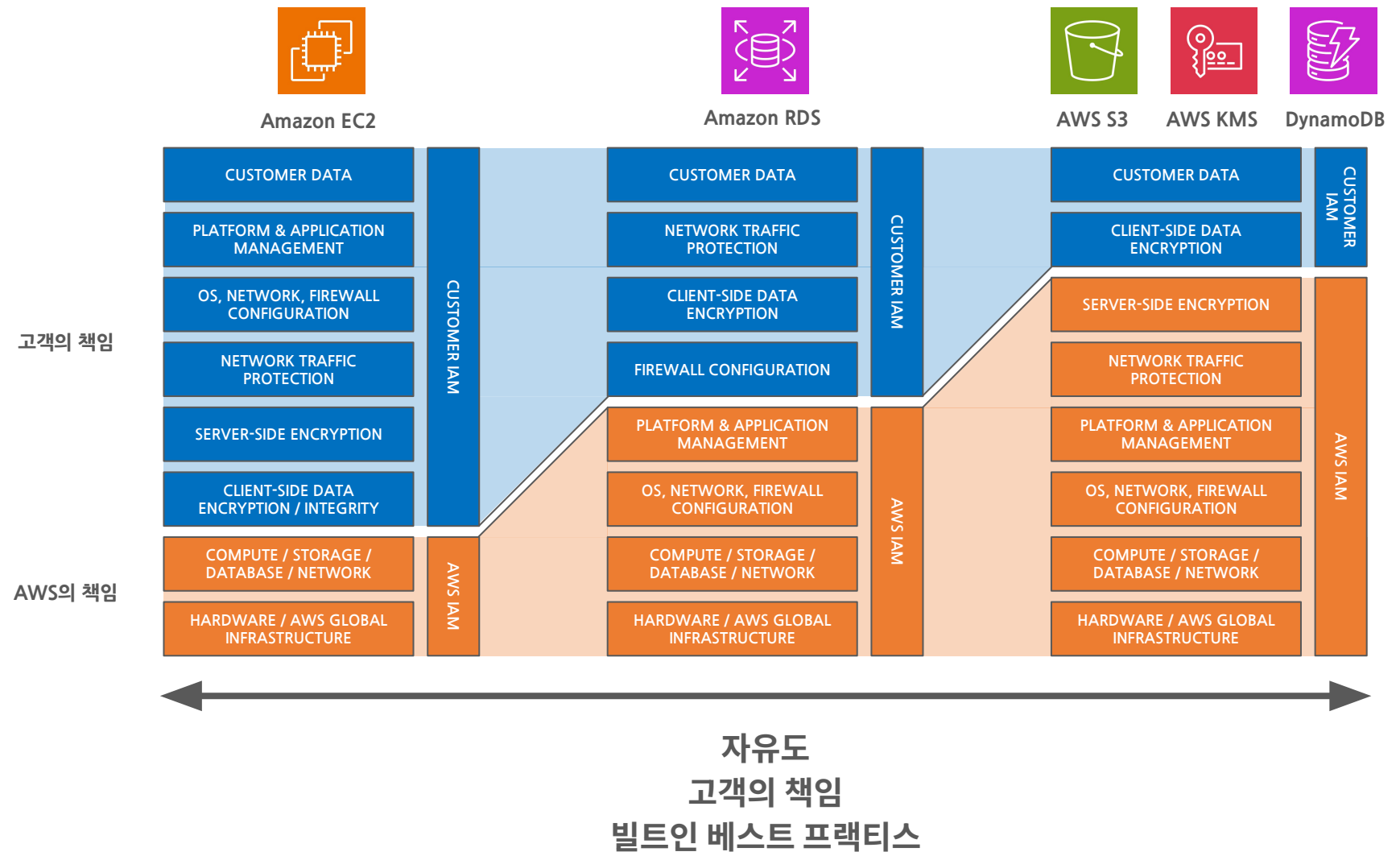


어떻게 길거리로
나오시게 되셨나요?
도박? 마약?

EC2 서버를 실수로
안 꺾어요...



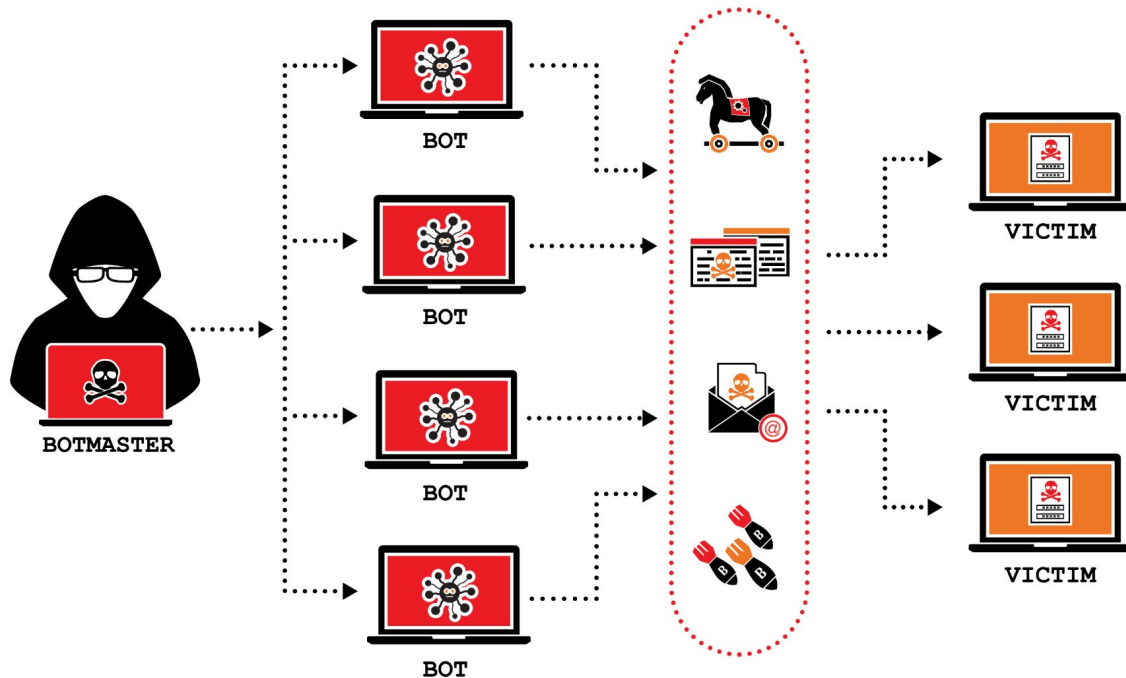
공유 책임 모델 - 서비스 별 차이



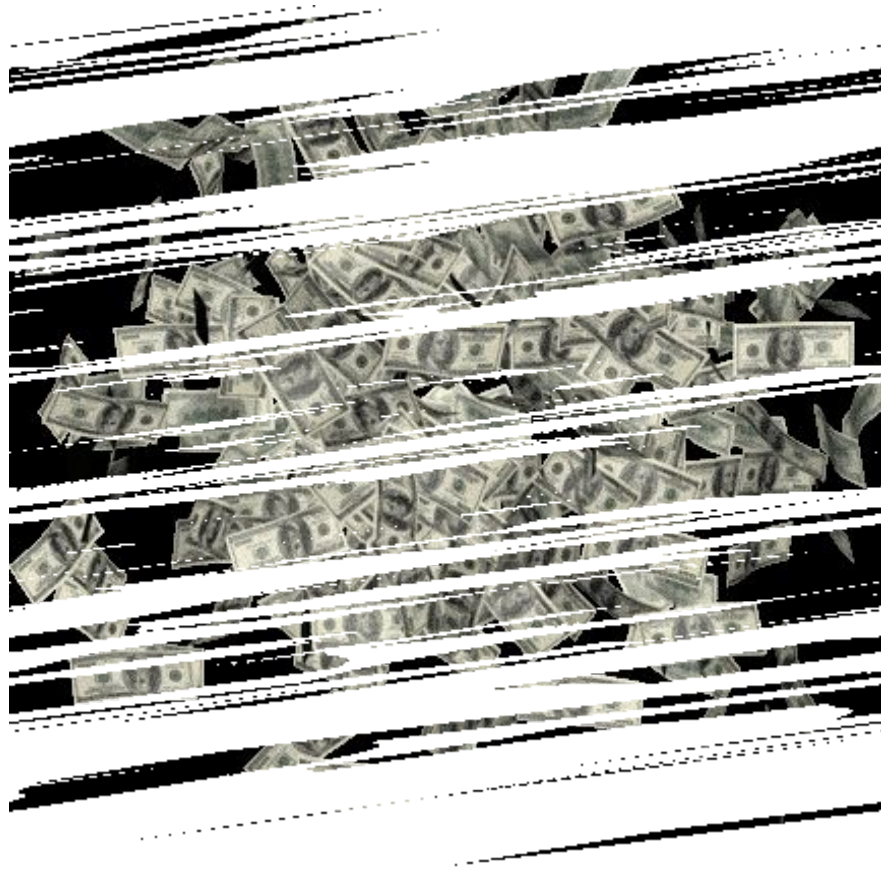
2. DDoS 예방

DDoS의 이해

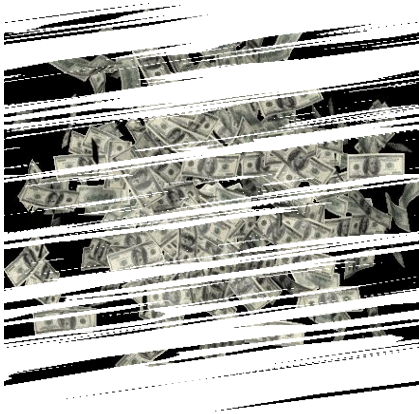
DDoS(Distributed Denial of Service Attack)란 여러 개의 장치를 이용하여 컴퓨터 서버나 네트워크 장비를 대상으로 처리할 수 없을 정도의 과도한 트래픽을 발생시켜 정상적인 데이터 전송에 장애를 일으키는 공격



DDoS의 목적



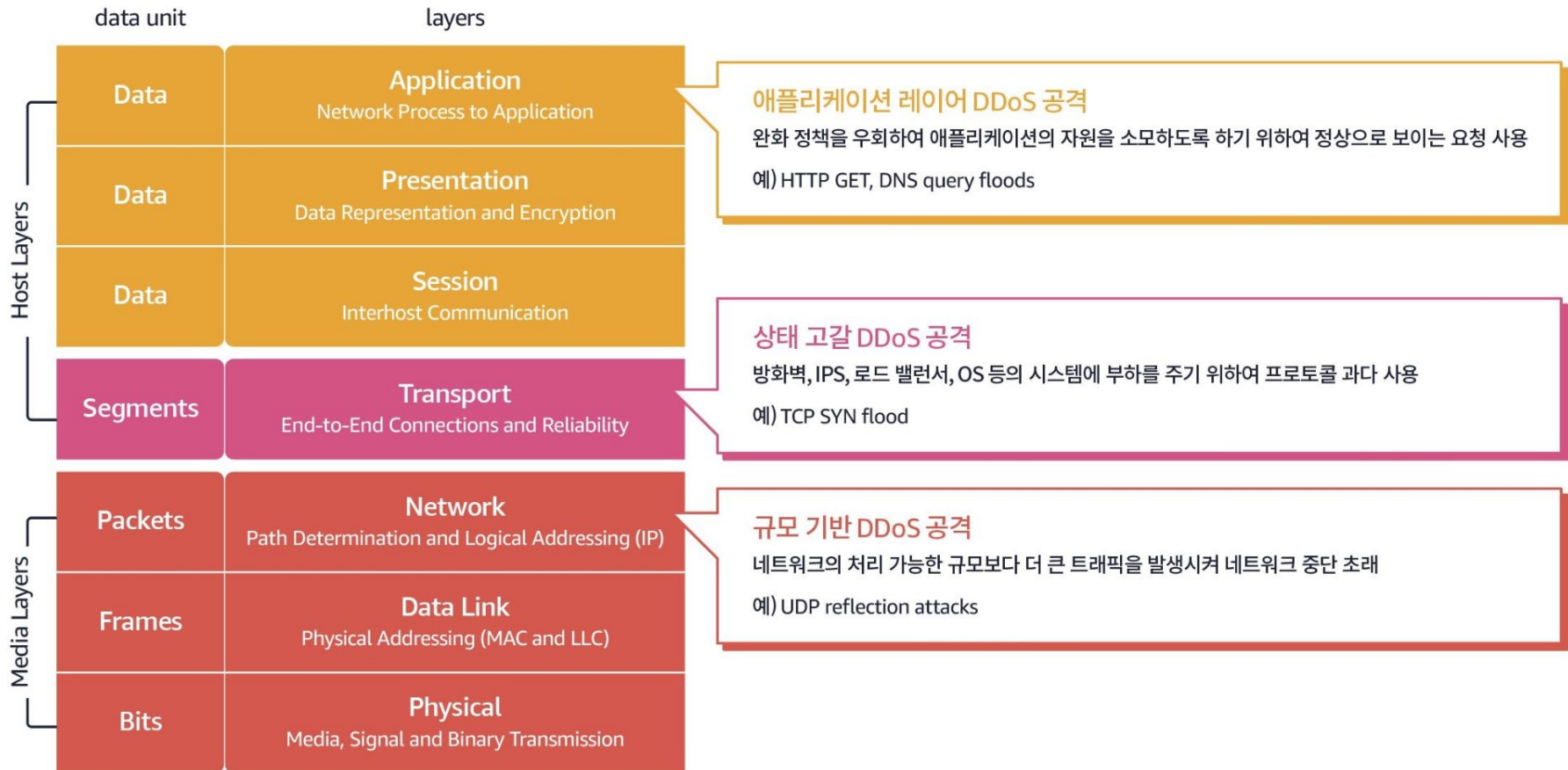
DDoS의 목적



>

ROI
(return on investment)

공유 책임 모델 - DDoS



공유 책임 모델 - DDoS



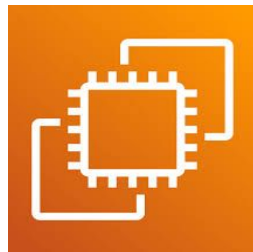
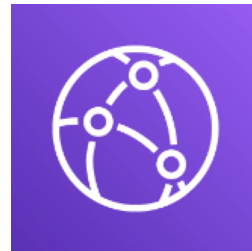
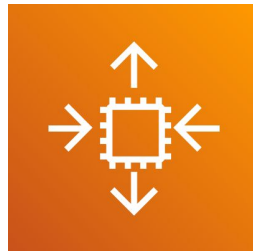
AWS Shield



AWS Shield는 분산 서비스 거부(DDoS) 공격으로부터 웹 애플리케이션을 보호하는 관리형 서비스입니다. 무료 서비스이며 3/4 계층의 공격을 자동으로 방어합니다.

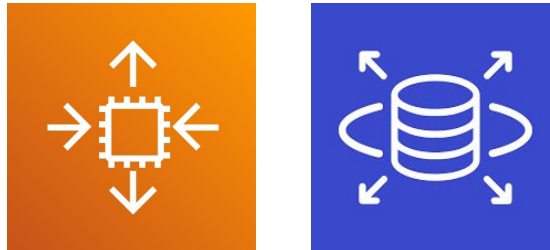
여러분들의 선택은..!?

aws AWS Cloud



Amazon EC2/Aurora Auto Scaling

DDoS로 인해 발생하는 인프라 리소스 부족을 해결하기 위해 스케일링을 고민해 볼 수 있으나, 일반 트래픽과 공격 트래픽을 구분하지 못하고 발생하는 비용적인 부분과 스케일 아웃까지 소요되는 걸리는 시간 때문에 한계점이 존재함



AWS WAF



웹 애플리케이션 방화벽 서비스로, 7계층에서 발생하는 웹 공격과 **DDoS 공격**을 탐지하고 차단하는 역할을 합니다.

- 7계층의 공격은 기본적인 AWS Shield로 방어가 불가능 함.
- WAF가 제공하는 Rate Limit 활용하여 DDoS 예방 가능.
- AWS가 제공하는 룰 및 사용자 정의 규칙 사용 가능.
- Amazon CloudFront, API Gateway REST Application Load Balancer 등의 리소스에 설정가능

WAF - Rate Limit 설정

[AWS WAF](#) > [Web ACLs](#) > Create web ACL

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5
Review and create web ACL

Add rules and rule groups [Info](#)

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (0)

Edit Delete

Add rules ▲

Add managed rule groups

Add my own rules and rule groups

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

	Name	Capacity	Action
No rules. You don't have any rules added.			

Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. [AWS WAF Pricing](#)

0/5000 WCUs

Rule Validate

Name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Type

☐ Regular rule

☒ Rate-based rule

Limits request rates for requests that match your criteria. Applies the action to matching requests when the limit is reached, and removes the action when the rate falls below the limit.

WAF - Rate Limit 설정

Rate-limiting criteria [Learn more](#)

Rate limit
The maximum number of requests to allow during the specified time window that satisfy your criteria. You can narrow the scope of the requests using a scope-down statement. You can group requests by component types for count aggregation. You must provide at least one aggregation component or a scope-down statement.

Rate limit must be between 10 and 2,000,000,000.

Evaluation window
The amount of time to use for request counts.

The default time span is 5 minutes. Valid values are 1, 2, 5, and 10 minutes.

Request aggregation
Select the web request components to use for request aggregation. AWS WAF groups, counts, and rate limits requests based on this criteria.

☒ **Source IP address**
Use only the IP address from the web request origin. If a web request goes through one or more proxies or load balancers, this will contain the address of the last proxy, and not the originating address of the client.

☐ **IP address in header**
Use only a client address in an HTTP header. Use caution with this option, as headers can be handled inconsistently by proxies and they can be modified to bypass inspection.

☐ **Custom keys**
Create an aggregation key using one or more component types, selected from a list. You can combine an IP address option with other components, and you can create keys that don't use an IP address.

☐ **Count all**
Count and rate limit all requests that match the rule's scope-down statement.

Evaluation Windows는 체크할때 n분 전이라는 의미를 가짐

WAF - Rate Limit 설정(action)

- Block: 특정 조건을 충족하는 요청을 바로 차단합니다.
- Count: 요청을 감지하되 차단하지 않고, 로그로만 기록하는 용도입니다.
- CAPTCHA: 사용자가 인간임을 증명하기 위해 CAPTCHA를 해결하도록 유도합니다. \$4, 1000회 분석당
- Challenge: JS 기반으로 봇 검증을 진행하는 정책입니다. \$0.4, 리스폰스당


Action

Action
Choose an action to take when a request matches the statements above.

☐ Allow

☐ Block

☒ Count

☐ CAPTCHA [customize](#) 

☐ Challenge

► Custom request - optional

► Add label - optional
Add labels to requests that match this rule. Rules that are evaluated later in the same web ACL can reference the labels that this rule adds.

WAF - Rule 우선순위

Set rule priority [Info](#)

Rules (4)

▲ Move up

▼ Move down

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

	Name	Capacity	Action
<input type="radio"/>	test1	1	Allow
<input type="radio"/>	test	2	Block
<input type="radio"/>	AWS-AWSManagedRulesAnonymousIpList	50	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesAmazonIpReputationList	25	Use rule actions

Cancel

Previous

Next

WAF - Managed rules for DDoS Protection

Rate limit 외에도 DDoS를 보호할 때 사용할 수 있는 각종 유/무료 룰을 사용 가능. 상세 룰이 없기 때문에 적용시 발생하는 문제점을 알 수 없으므로, 꼭 Count로 설정 후 로깅 후 사용이 권장

Step 1

[Describe web ACL and associate it to AWS resources](#)

Step 2

Add managed rule groups

Step 3

Set rule priority

Step 4

Configure metrics

Step 5

Review and create web ACL

[AWS WAF](#) > [Web ACLs](#) > Create web ACL

Add managed rule groups [Info](#)

Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers. Any fees that a managed rule group provider charges for using a managed rule group are in addition to the standard service charges for AWS WAF. [AWS WAF Pricing](#)

▼ AWS managed rule groups

Paid rule groups

AWS WAF charges subscription and usage fees for paid managed rule groups. These are in addition to the standard service charges for AWS WAF. [AWS WAF Pricing](#)

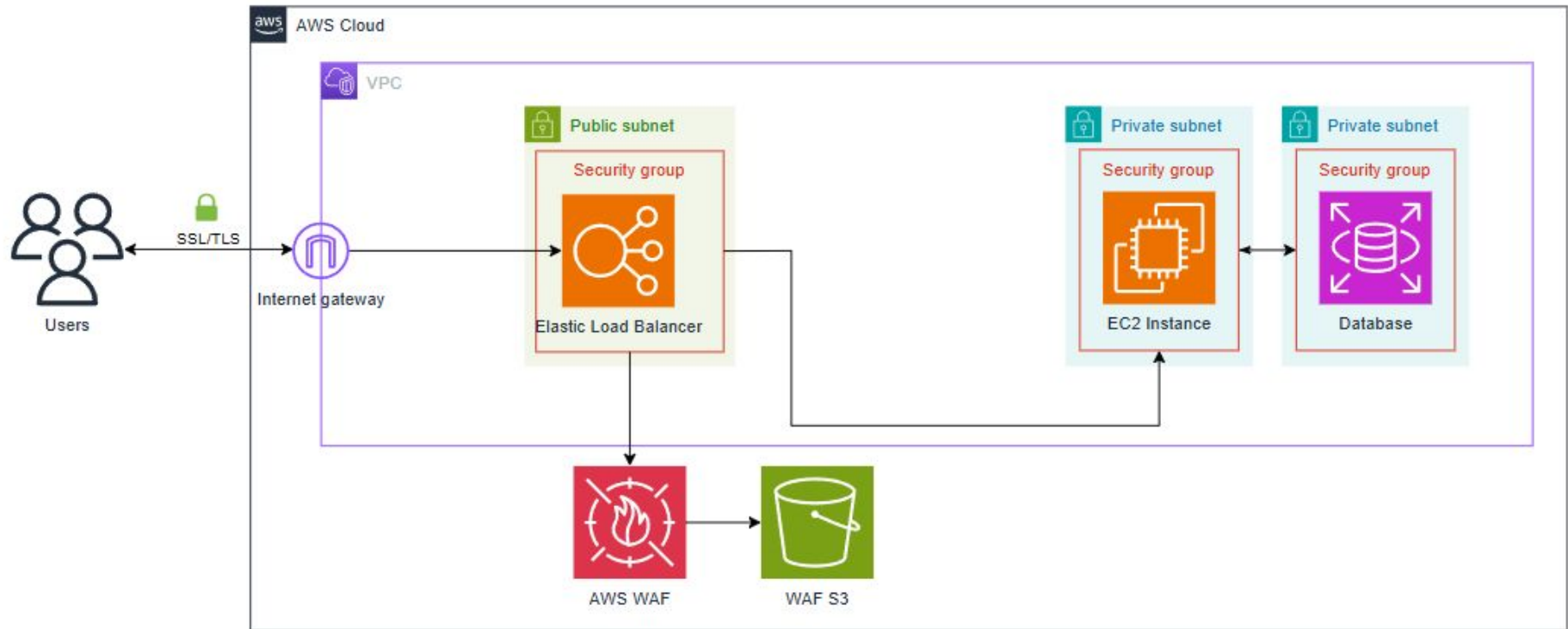
Name	Capacity	Additional fees	Action
Account creation fraud prevention - new Provides protection against the creation of fraudulent accounts on your site. Fraudulent accounts can be used for activities such as obtaining sign-up bonuses and impersonating legitimate users. Learn More	50	<ul style="list-style-type: none">\$10 per month (prorated hourly).Tiered fee model for requests analyzed AWS WAF Pricing	<input checked="" type="radio"/>
Account takeover prevention Provides protection for your login page against stolen credentials, credential stuffing attacks, brute force login attempts, and other anomalous login activities. With account takeover prevention, you can prevent unauthorized access that may lead to fraudulent activities, or inform legitimate users to take a preventive action. Learn More	50	<ul style="list-style-type: none">\$10 per month (prorated hourly).Tiered fee model for requests analyzed AWS WAF Pricing	<input checked="" type="radio"/>
AntiDDoS Protection for Layer 7 attacks Provides protection against DDoS attacks targeting the application layer, also known as Layer 7 attacks.	50	<ul style="list-style-type: none">\$20 per month (prorated hourly).Tiered fee model for requests analyzed AWS WAF Pricing	<input checked="" type="radio"/>

Free rule groups

You can use the free rule groups without any added charges beyond the standard service charges for AWS WAF. [AWS WAF Pricing](#)

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. Learn More	100	<input checked="" type="radio"/> Add to web ACL
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. Learn More	25	<input checked="" type="radio"/> Add to web ACL
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. Learn More	50	<input checked="" type="radio"/> Add to web ACL

아키텍처 v1.1



DNS 서버 - Amazon Route53



Route 53는 전 세계에 분산된 AWS 엣지 로케이션에서 대량의 DNS 트래픽을 흡수할 수 있는 뛰어난 확장성과 복원력을 갖추어 DDoS 공격에 강합니다.

- DNS 공격에 관한 기본 DDoS 방어 기능 탑재(AWS Shield)
- 셔플 샤딩: 각 호스팅 존에 4개의 네임 서버를 할당하되, 256개 이상의 서로 다른 네임 서버 풀에서 무작위로 선택하여 특정 네임 서버가 공격 당해도 다른 호스팅 존에 영향을 주지 않으며고가용성을 보장
- 애니캐스트: 가까운 엣지 로케이션에 질의, 전세계에 분산되어고가용성 보장

도메인 관리업계 1위 [redacted] 디도스로 2시간 48분간 접속장애(종합)

송고 2023-02-24 14:18

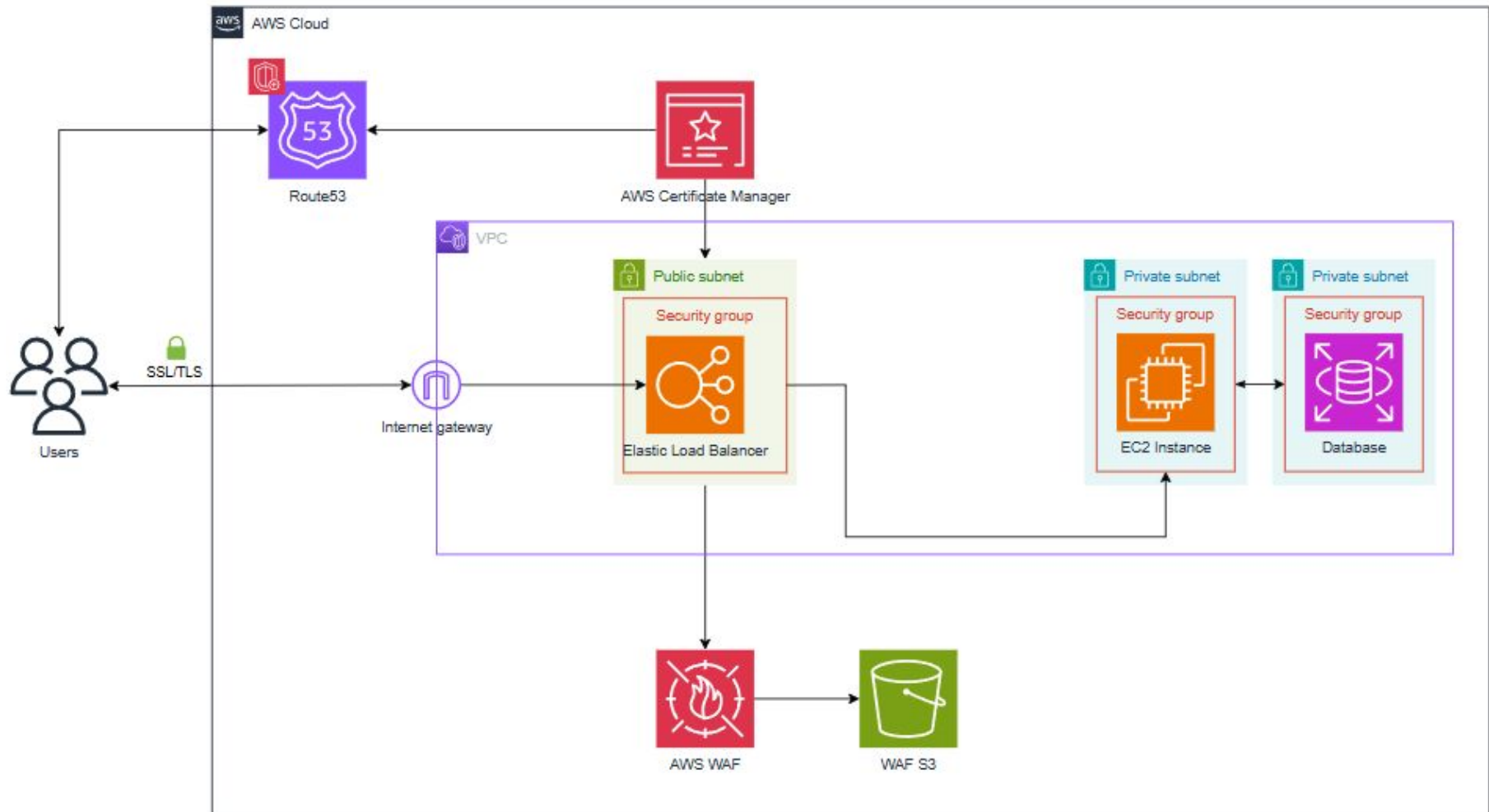


오규진 기자

+ 구독

당국 관계자 " [redacted] 함께 공격 규모 파악 중"

아키텍처 v1.2



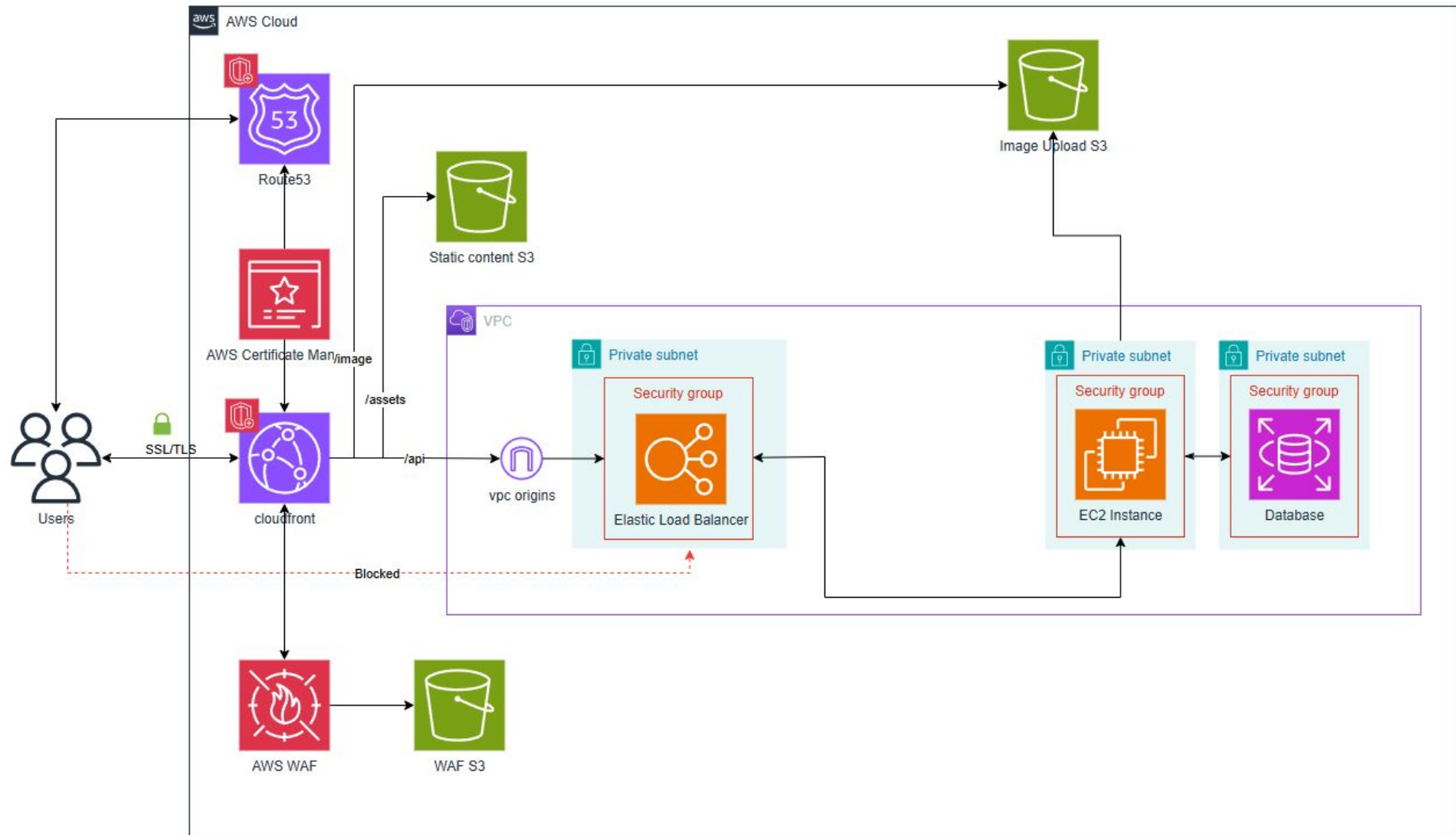
CloudFront



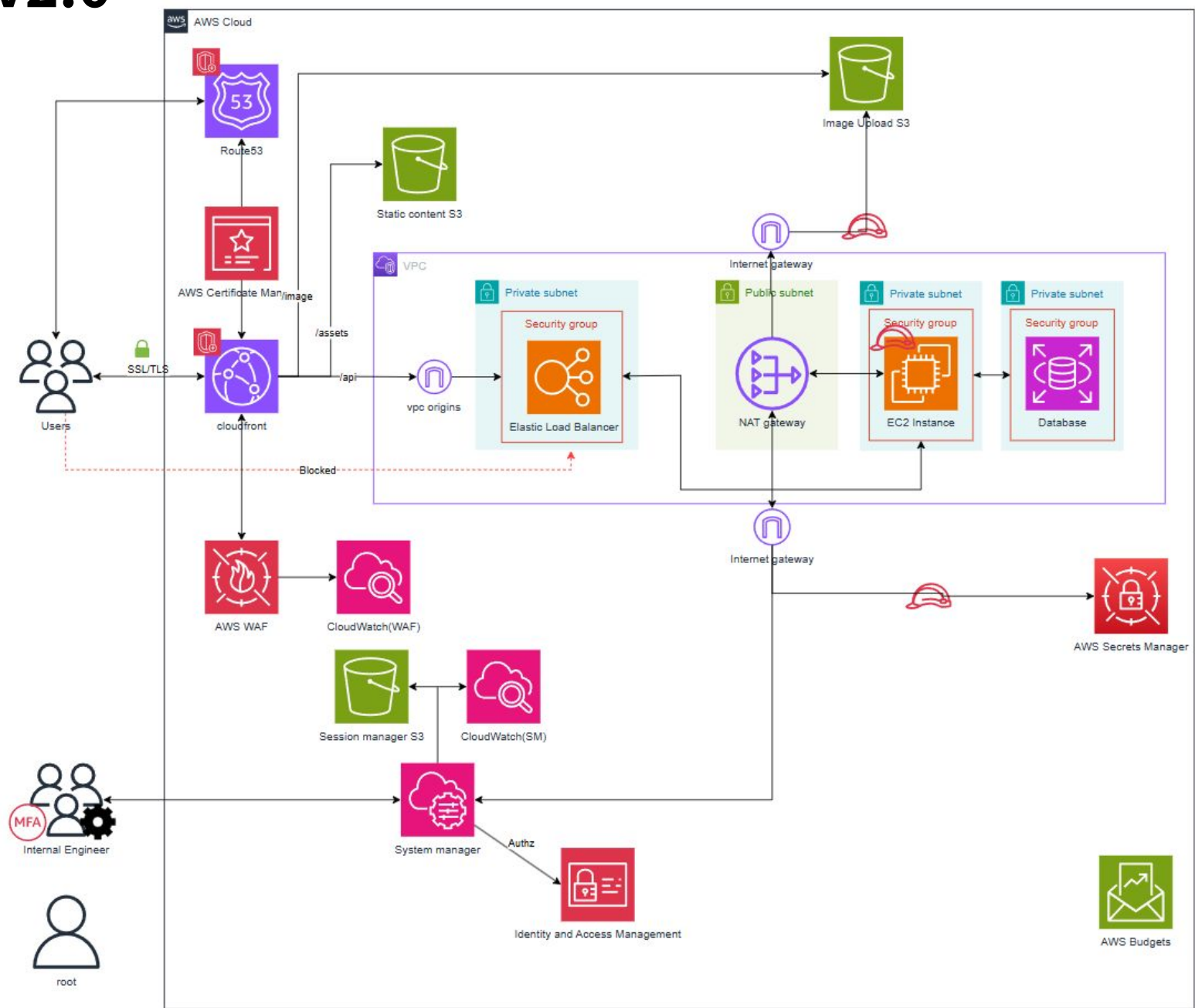
CloudFront는 전 세계에 분산된 엣지 서버를 통해 콘텐츠를 제공할 수 있는 CDN 서버. 트래픽을 분산시켜 공격 트래픽이 원본 서버에 직접 닿지 않게 하여 공격 완화 가능.

- 정적, 동적 콘텐츠를 분리하여 네트워크 트래픽 분산
- 엣지 서버를 통해 대량 트래픽을 분산
- 캐싱 기능을 이용해 부하 감소
- WAF 연결 제공

아키텍처 v1.3



아키텍처 v2.0



DDoS 테스트시 유의점

- 모든 테스트는 [AWS 고객 계약](#) 또는 Amazon Web Services 구매 및 사용을 규정하는 기타 계약의 약관을 따릅니다.
- DDoS 시뮬레이션 테스트는 AWS에서 DDoS 시뮬레이션 테스트를 수행하도록 사전 승인받은 [AWS 파트너 네트워크\(APN\) 파트너](#) (AWS DDoS 테스트 파트너)가 수행해야 합니다.
- DDoS 시뮬레이션 테스트의 대상은 AWS Shield Advanced에 가입한 본인이 소유한 AWS 계정의 보호된 리소스로 등록되어 있거나, AWS Shield Advanced에 가입한 본인이 소유한 계정에 있는 Amazon API Gateway 에지 최적화 API 엔드포인트로 등록되어 있어야 합니다.
- DDoS 시뮬레이션 테스트의 비트 볼륨은 초당 20기가비트를 초과할 수 없습니다.
- Amazon CloudFront 배포를 테스트할 때 DDoS 시뮬레이션 테스트의 패킷 볼륨은 초당 500만 패킷을 초과할 수 없으며, 다른 유형의 AWS 리소스를 테스트할 때는 초당 50,000 패킷을 초과할 수 없습니다.
- DDoS 시뮬레이션 테스트의 요청량은 초당 50,000건을 초과할 수 없습니다.
- DDoS 시뮬레이션 테스트는 AWS 리소스에서 시작될 수 없으며, 증폭 공격을 시뮬레이션하기 위해 AWS 리소스를 사용할 수 없습니다.
- 귀하는 모든 DDoS 시뮬레이션 테스트의 위험을 감수하고 테스트 공급업체의 조치에 대한 책임을 져야 합니다.
- AWS는 언제든지 테스트 공급업체에 시뮬레이션 테스트를 종료하도록 지시할 수 있습니다.
- 테스트 수행 및 테스트 결과는 AWS 고객 계약에 정의된 대로 AWS 기밀 정보입니다.

<https://aws.amazon.com/ko/security/ddos-simulation-testing/>

Serverless 환경의 신규 위협

Serverless의 특징 때문에 많은 트래픽이 서비스의 장애로 연결되지는 않지만 비용을 증가시키는 Denial-of-Wallet 공격과 같은 신규 위협이 발생





성진 :

우선 이정도면 DDoS는 예방이 되었겠지?



성진 :

우선 이정도면 DDoS는 예방이 되었겠지?



??? :

아참! 요즘 보니까 사고가 잦던데... 저희는 사고 발생해도 문제 없죠?

3. 침해사고 예방

침해사고의 책임 공유모델

물리적으로 침입당해 서버가 도난당한 경우

내부 시스템이 해킹당해 고객 계정 정보 유출

하이퍼바이저나 호스트 OS의 취약점으로 인한 데이터 유출

네트워크 인프라의 결함으로 인한 데이터 유출

계정 관리 소홀

액세스 키 노출

IAM 권한 설정 오류

S3 버킷 공개 설정

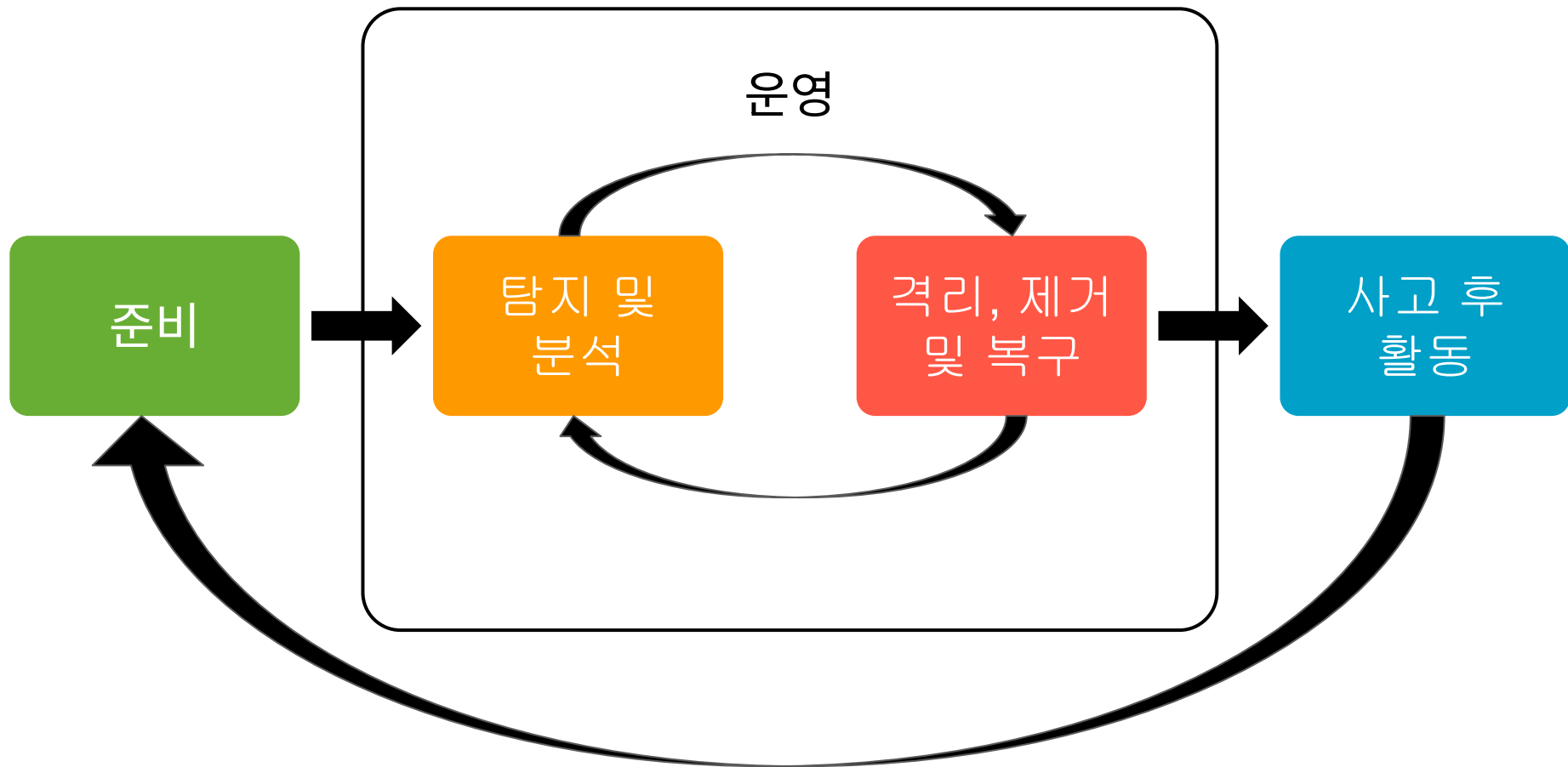
보안 그룹 설정 미흡

OS 패치 누락

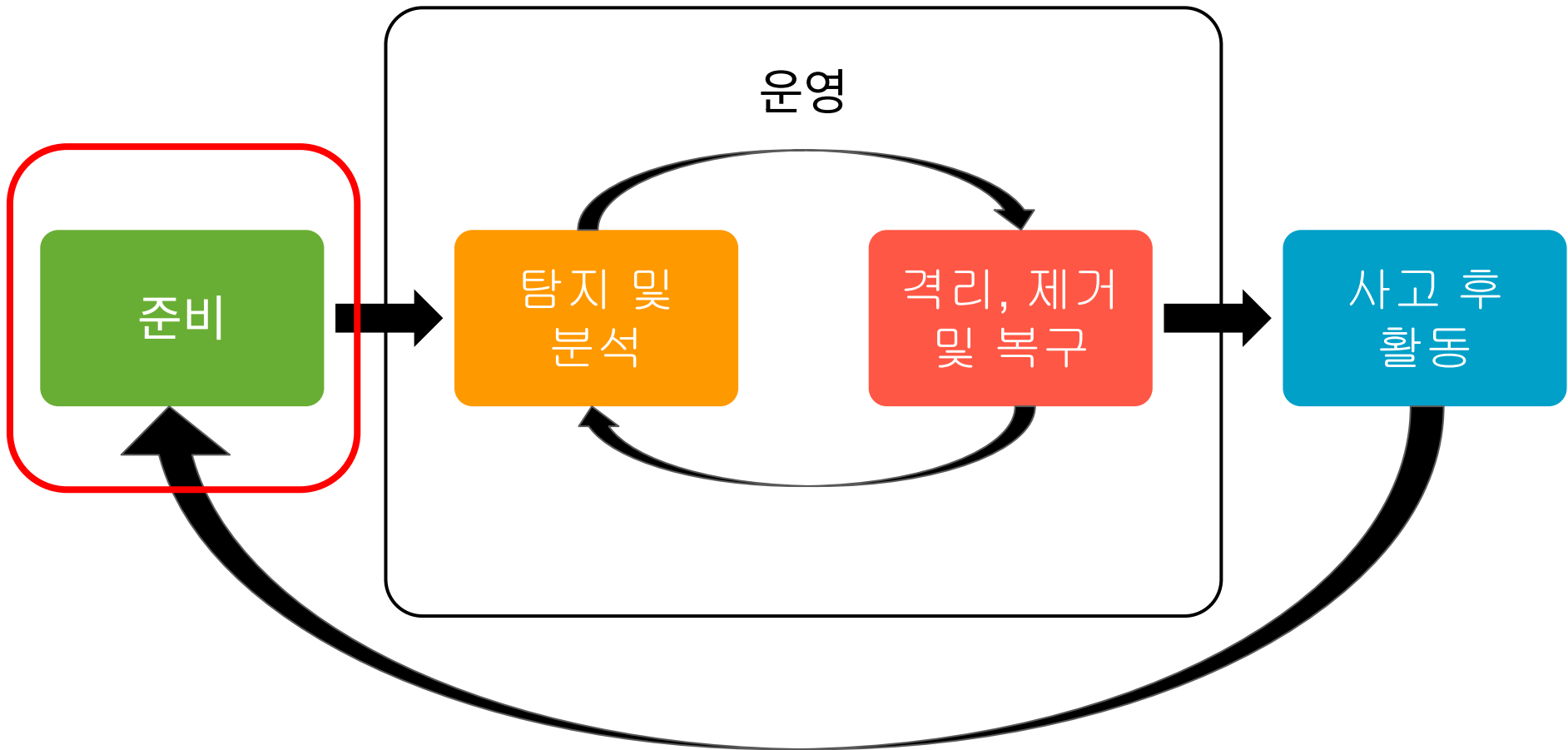
애플리케이션 취약점

데이터 암호화 미적용

침해 대응 라이프 사이클



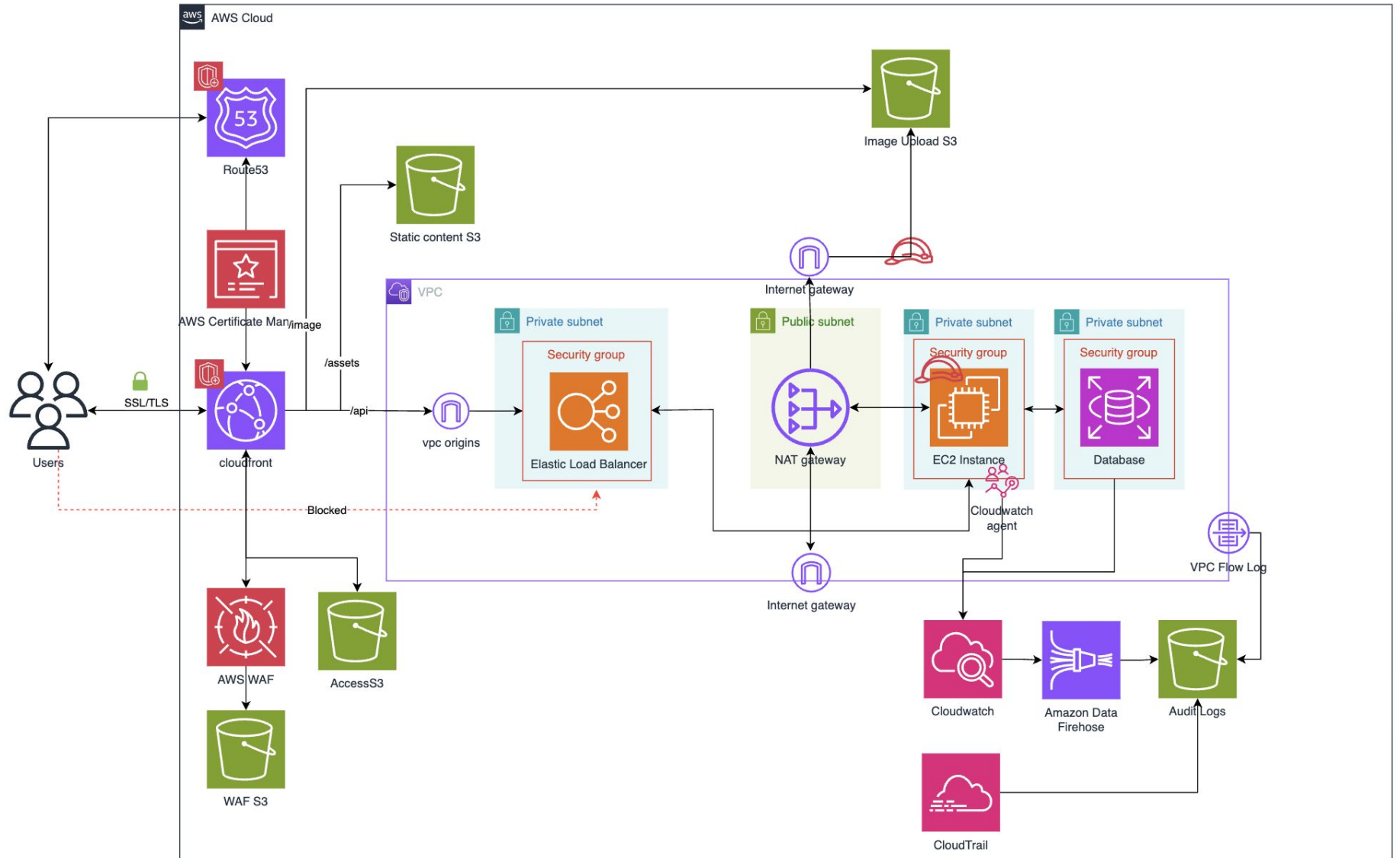
침해 대응 라이프 사이클



준비 - 로그 수집

- AWS Cloudtrail
- 운영체제 및 애플리케이션 로그
- 데이터베이스 로그
- WAF 로그
- 네트워크 로그(VPC 로그)
- 액세스 로그

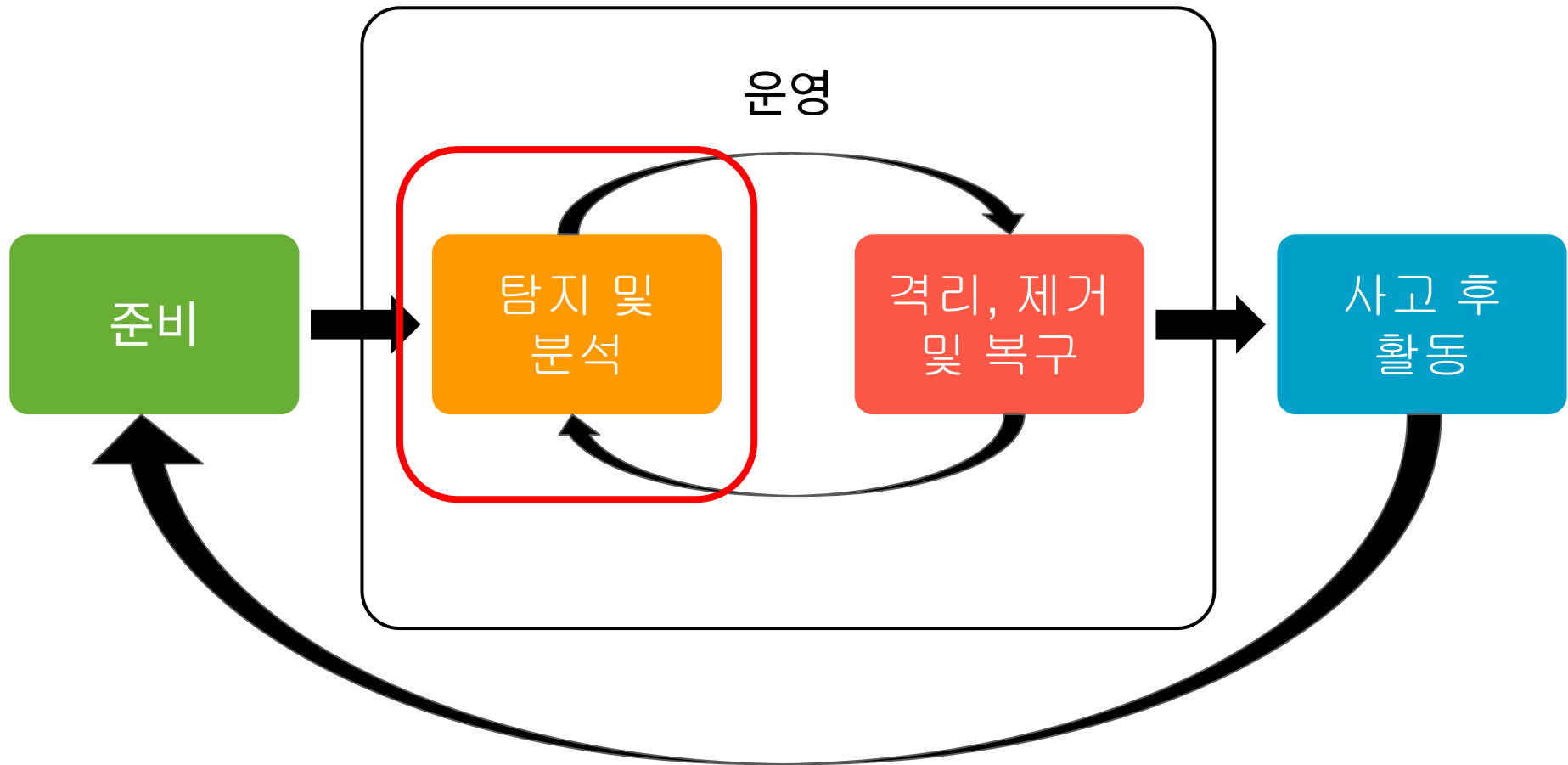
아키텍처 v2.1



로그 저장소 S3 설정

- 보관기간(내부 규정 및 컨플라이언스 요구사항)
 - 비용(Tier 설정)
- 무결성(S3 Object Lock, Tier 전환은 제한하지 않음)

침해 대응 라이프 사이클



탐지 - GuardDuty



Amazon GuardDuty는 AWS 계정, 워크로드 및 데이터를 보호하기 위해 악의적인 활동과 **비정상적인 동작**을 모니터링하고 탐지하는 지능형 위협 **탐지** 서비스입니다.

- 별도의 아키텍처 개선 없이 사용할 수 있는 매니지드 서비스
- VPC 흐름 로그, AWS CloudTrail, DNS 쿼리 로그, AWS CloudTrail S3 데이터 이벤트 로그, EKS 감사 로그, Lambda 네트워크 활동 로그, 및 RDS 로그인 활동 로그를 수집
- 발견된 이벤트 알람을 다른 곳에 연동 가능
- 제공되는 룰셋을 조정하여 오탐 제어 가능 (다만 새로운 룰은 추가할 수 없음)
- S3 멀웨어 찾는 기능을 옵션으로 제공
- 기본 90일동안 로그 저장

Findings (368) Info

Actions ▾

Saved rules

Apply saved rules ▾

Filter findings

Status





















Current ▾

Threat type

All findings ▾

< 1 ... >

<input type="checkbox"/>	Title	Severity ▾	Finding type ▾	Resource ▾	Count
<input type="checkbox"/>	[SAMPLE] A container escape via cgroups was detected in EC2 instance i-99999999.	High	PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	Kubernetes Cluster:	1
<input type="checkbox"/>	[SAMPLE] The resource discovery API GeneratedFindingAPIName was invoked from a Tor exit node.	Medium	Discovery:S3/TorIPCaller	S3 Bucket: example-bucket1	1
<input type="checkbox"/>	[SAMPLE] The user GeneratedFindingUserName successfully logged into RDS database generatedfindingdbinstanceid from a public IP address in an unusual way after a consistent pattern of unusual failed login attempts.	Low	CredentialAccess:RDS/AnonymousBehavior.SuccessfulBruteForce	RDS DB Instance: generatedfindingdbinstanceid	1
<input type="checkbox"/>	[SAMPLE] The EC2 instance i-99999999 has executed an in-memory or shared file.	Medium	A container escape via cgroups was detected in EC2 instance i-99999999. <div>High First seen a minute ago, last seen a minute ago Info</div> <p>The process GeneratedFindingProcessName in EC2 instance i-99999999 has modified the cgroup release agent located at GeneratedFindingPath.</p> <div>Investigate with Detective</div> <div>This finding is <div>Useful</div> <div>Not useful</div></div>		
<input type="checkbox"/>	[SAMPLE] The EC2 instance i-99999999 has loaded a kernel module.	Low			
<input type="checkbox"/>	[SAMPLE] The reconnaissance API GeneratedFindingAPIName was invoked from a known malicious IP address.	Medium			
<input type="checkbox"/>	[SAMPLE] A malware scan on your S3 object EXAMPLE-OBJECT has detected a security risk EICAR-Test-File.	High			
<input type="checkbox"/>	[SAMPLE] The EC2 instance i-99999999 is probing a port on a large number of publicly routable IP addresses.	High			
<input type="checkbox"/>	[SAMPLE] A Bitcoin-related domain name was queried by EC2 instance i-99999999.	Medium			

Overview			
	Finding ID	00976361001e41188f99a7721a0332be	 
	Type	PrivilegeEscalation:Runtime/CGroupsReleaseAgentModified	 
	Severity	HIGH	 
	Region	us-east-1	
	Count	1	
	Account ID	242864343139	 
	Resource ID	GeneratedFindingKubernetesWorkloadName	
	Created at	10-23-2025 14:03:03 (a minute ago)	
	Updated at	10-23-2025 14:03:03 (a minute ago)	
Resource affected			
	Resource role	TARGET	 
	Resource type	KubernetesCluster	 
Kubernetes workload details			
	Name	GeneratedFindingKubernetesWorkloadName	 
	Namespace	GeneratedFindingKubernetesWorkloadNamespace	 
	Type	Pods	
	UId	00112233-4455-6677-8899-aabbccddeeff	
Container details			
	Container runtime	GeneratedFindingContainerRuntime	
	ID	GeneratedFindingContainerId	 
	Image	GeneratedFindingContainerImage	 
	Image prefix	GeneratedFindingContainerImagePrefix	
	Name	GeneratedFindingContainerName	

분석 - Amazon Detective



AWS 리소스의 로그 데이터를 자동으로 수집하고, 머신러닝 및 통계 분석 기술을 사용하여 보안 조사를 더 빠르고 효율적으로 수행하도록 돕는 서비스

- GuardDuty가 필수적으로 활성화 되어 있어야 사용가능
- GuardDuty와의 추가 설정 및 변경 없이 작동하는 매니지드 서비스
- 다른 보안 도구와 연동 지원

Backdoor:EC2/C&CActivity.B!DNS

Finding ID: [04c0a4edacec98b5466abc81ab184da8](#)

High EC2 instance [i-031b41fdb56911b89](#) is querying a domain name Command & Control server. [Info](#)

[Investigate with Detective](#)

This finding is

Useful

Not useful

Overview

Severity	HIGH
Region	us-east-1
Count	136978
Account ID	[REDACTED]
Resource ID	i-031b41fdb56911b89
Created at	06-09-2022 15:05:21 (a year a
Updated at	08-11-2023 09:14:29 (2 minut



Investigate with Detective

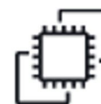
Detective visualizes the CloudTrail, VPC flow data and EKS audit logs for the resources affected by this finding.



GuardDuty finding

[04c0a4edacec98b5466abc81ab184da8](#)

Investigate trends, new behaviors, and relationships involving the resources and actors present within the finding.



EC2 instance [i-031b41fdb56911b89](#)

Investigate VPC flow traffic trends or view the activity details. Analyze CloudTrail activity associated with the EC2 Instance and quickly identify any new behavior.



AWS account [\[REDACTED\]](#)

Investigate account level CloudTrail activity to identify unusual trends in volume, new activity, and location access patterns.



IP address [54.160.248.125](#)

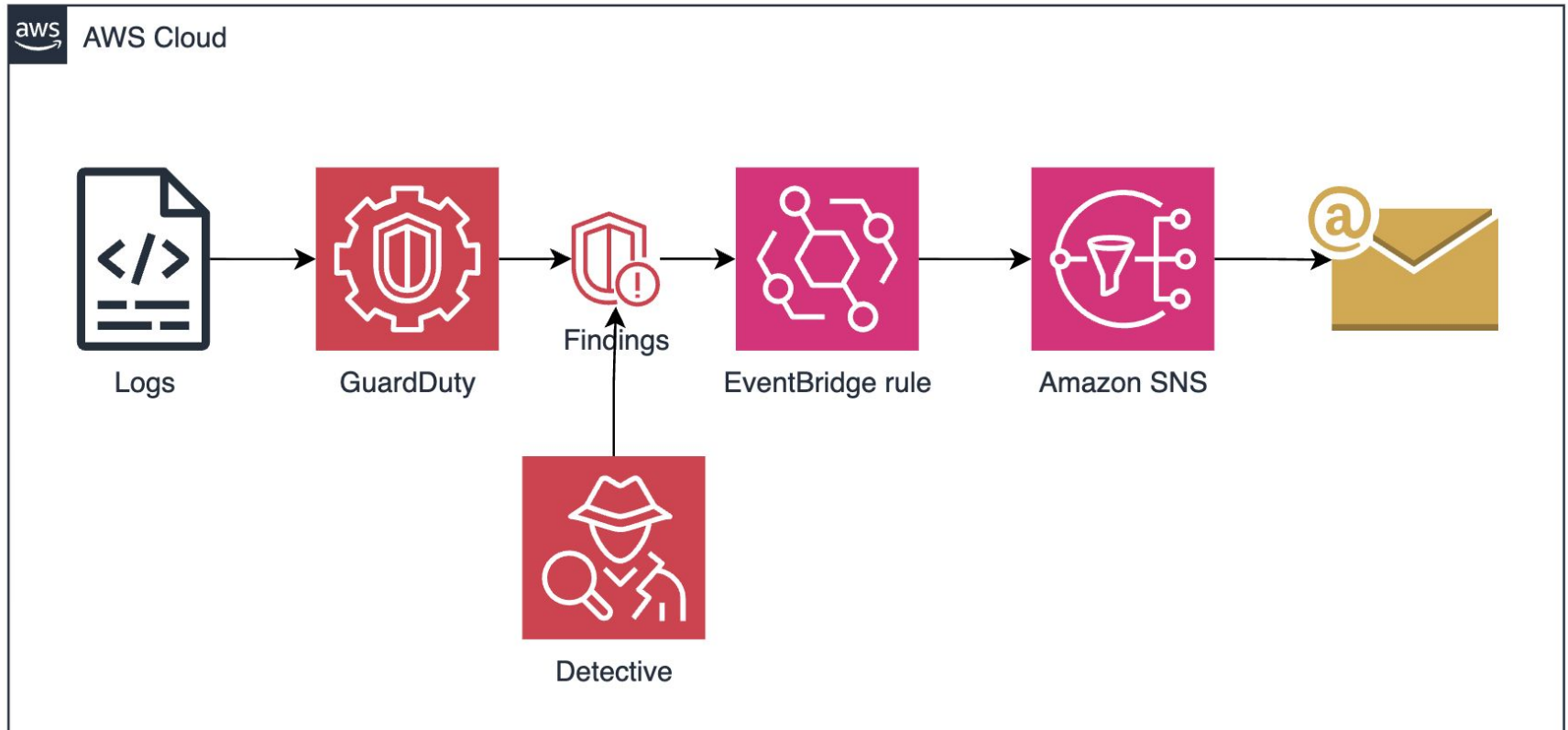
Investigate CloudTrail activity originating from the IP address to see unusual trends in volume, new activity from this IP address, and determine which resources have used the IP address.



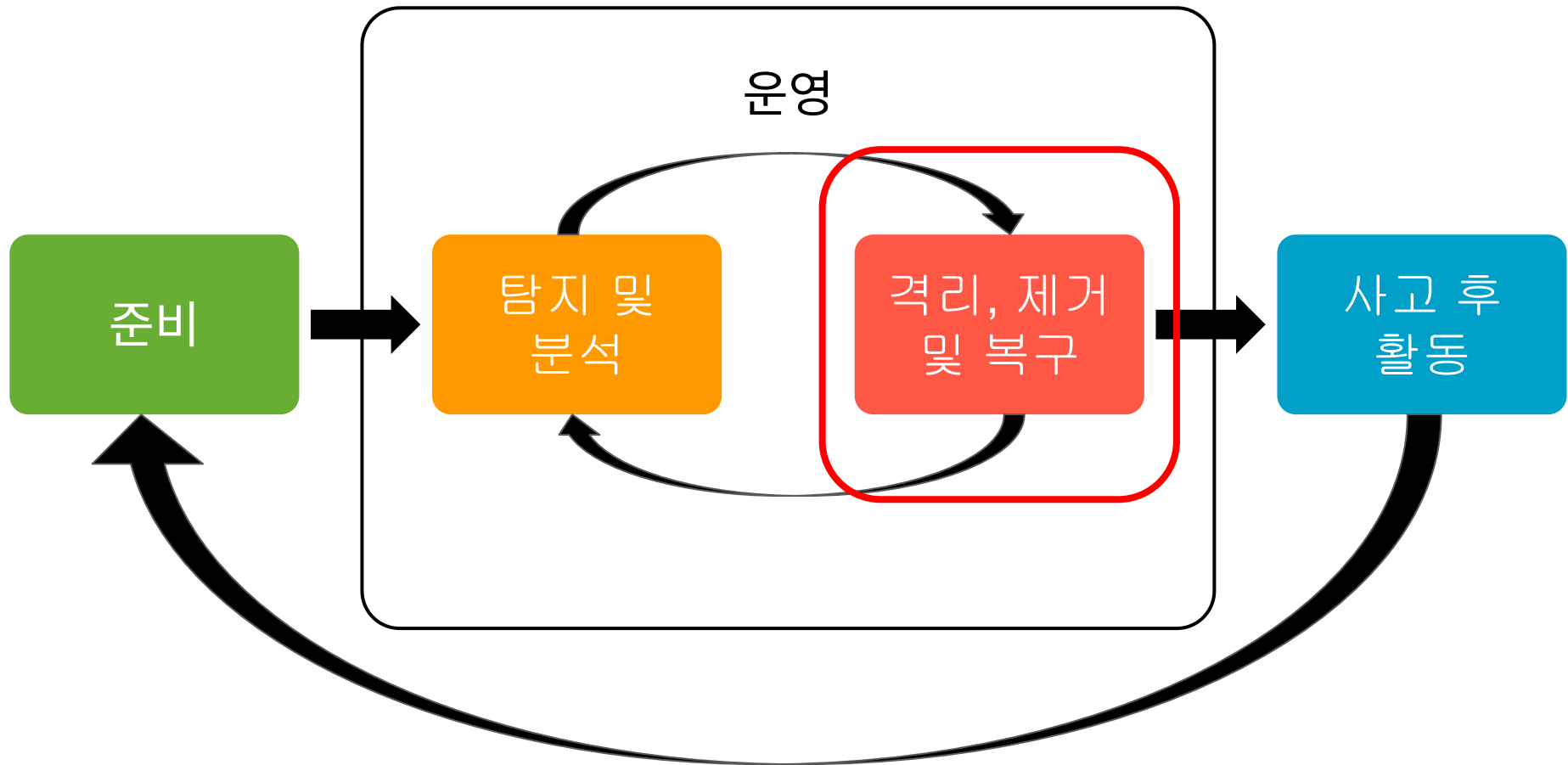
IP address [10.0.1.95](#)

Investigate CloudTrail activity originating from the IP address to see unusual trends in volume, new activity from this IP address, and determine which resources have used the IP address.

아키텍처 v2.2



침해 대응 라이프 사이클



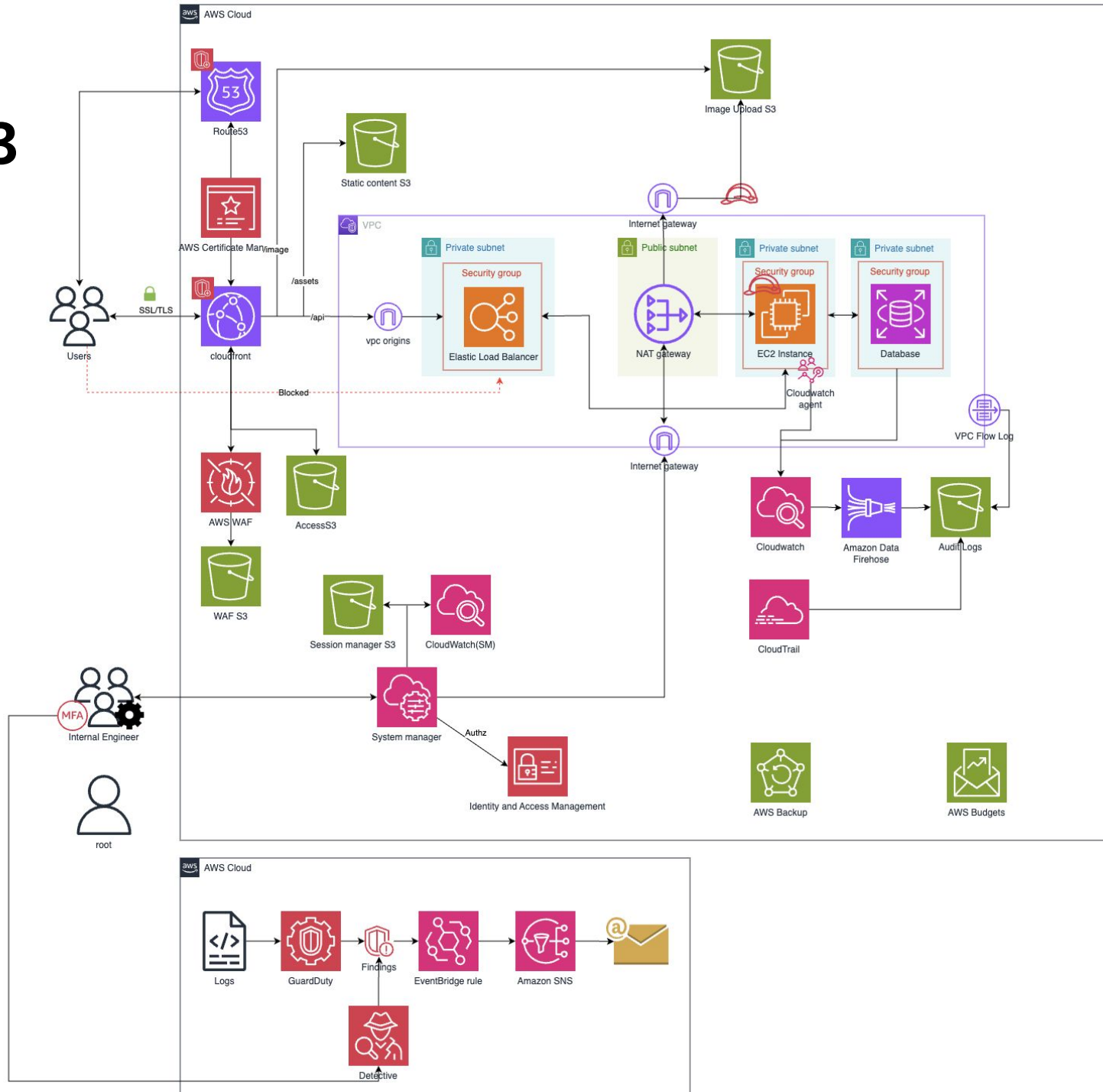
복구 - AWS Backup



AWS 서비스의 대부분의 저장소를 백업하고 중앙에서 통합하고 자동화하는 완전관리형 서비스

- 자동화를 통해 지정된 주기, 보존, 대상 설정 가능
- 백업 복원 기능 지원
- 불변 백업 설정: 통해 백업본을 일정기간 동안 삭제 방지 할 수 있음
- 다중 리전 저장, 무결성, 자체 백업 지원

아키텍처 v3



Thank you!

Q & A

Next Episode Preview

- 컴플라이언스 심사
- DevSecOps

참고자료

- <https://www.thesslstore.com/blog/what-is-a-ddos-attack/>
- <https://docs.aws.amazon.com/security-ir/latest/userguide/introduction.html>
- <https://aws.amazon.com/ko/blogs/korea/anti-ddos-for-game/>
- <https://aws.amazon.com/ko/blogs/tech/security-logging-strategies-for-security-incident-response/>
- <https://dev.classmethod.jp/articles/amazon-detective-explained-korean/>
- <https://aws.github.io/aws-security-services-best-practices/guides/detective/#investigating-a-finding>