CLOUD

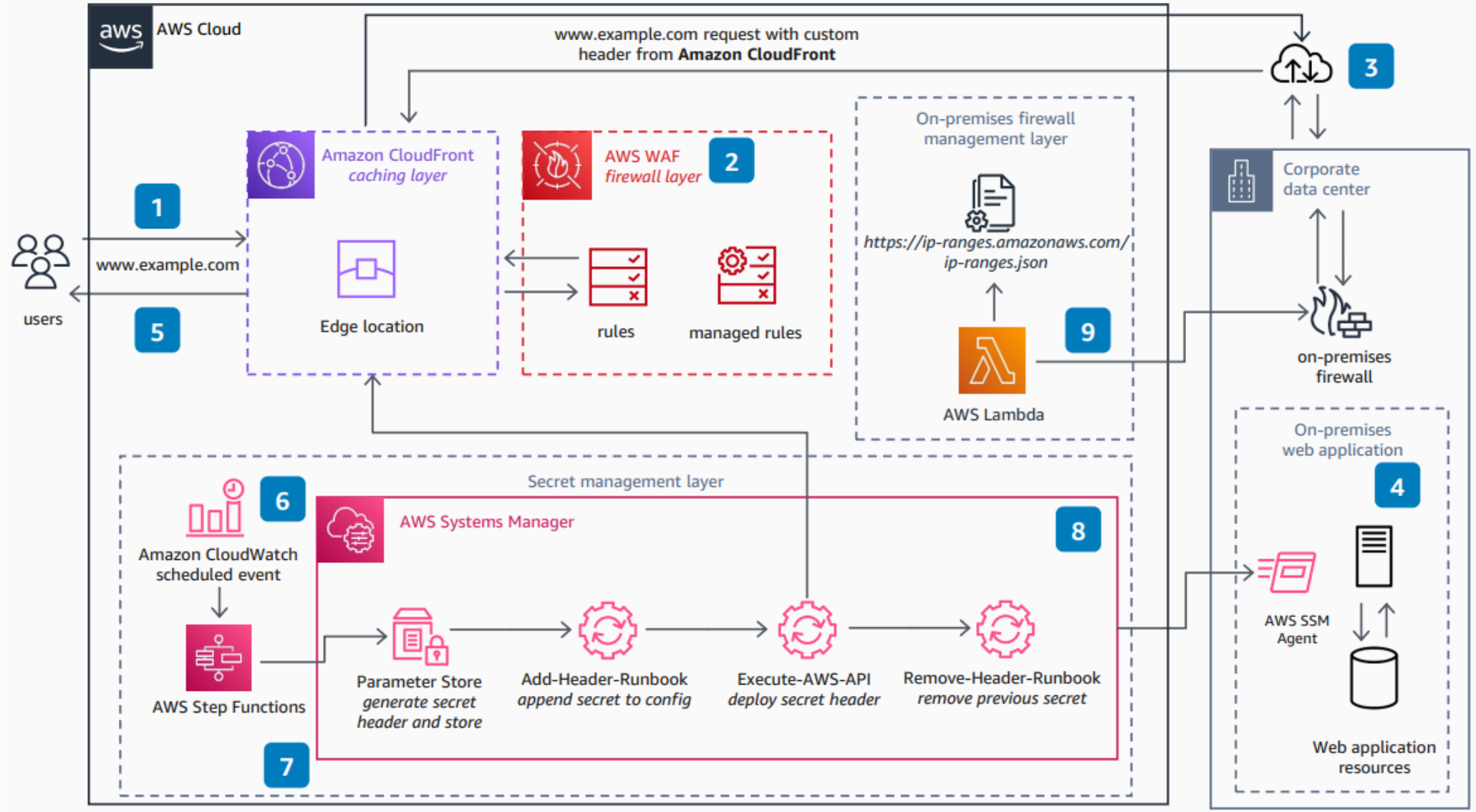
Reference Architecture Review

AWS Security

박경규

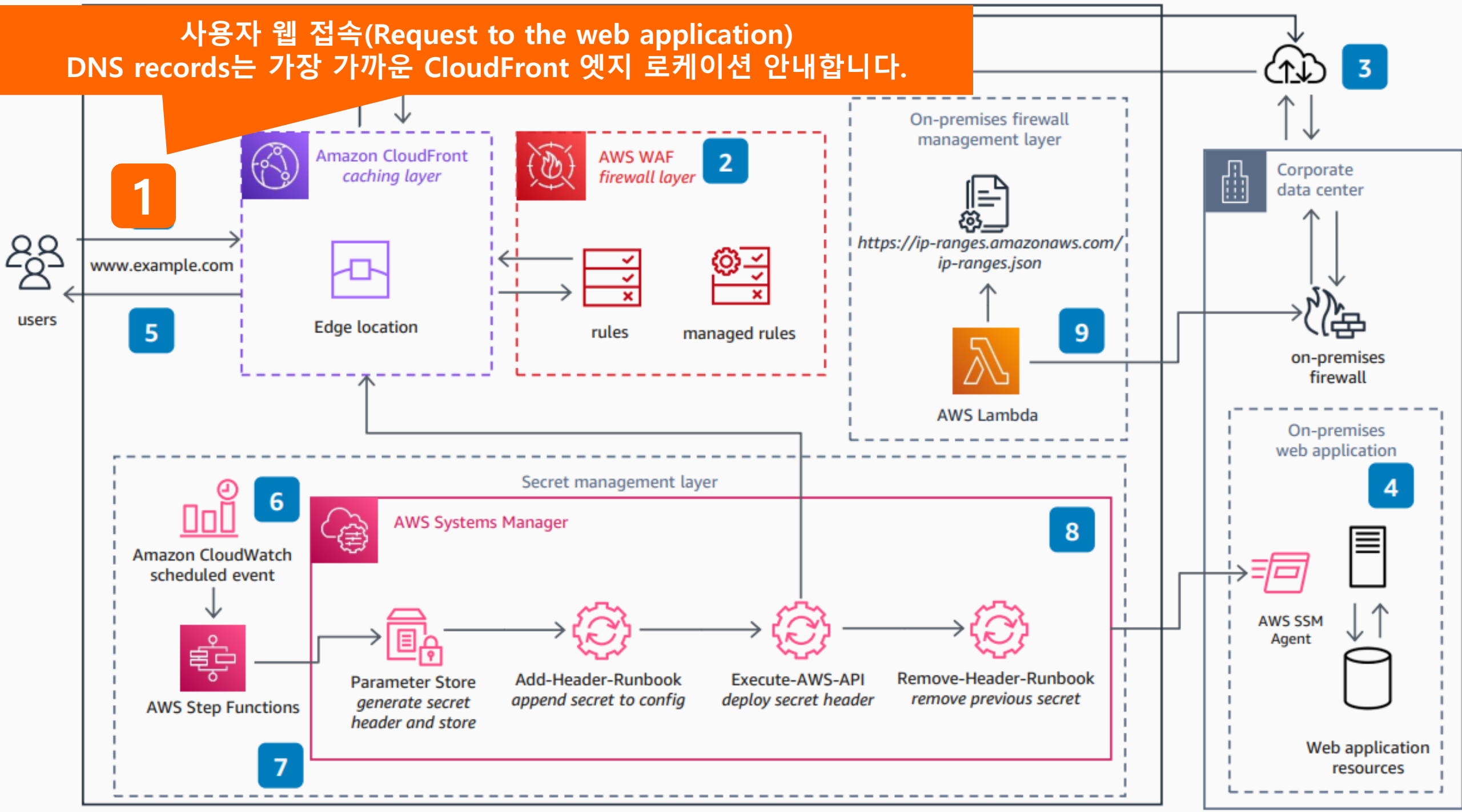
Reference Architecture

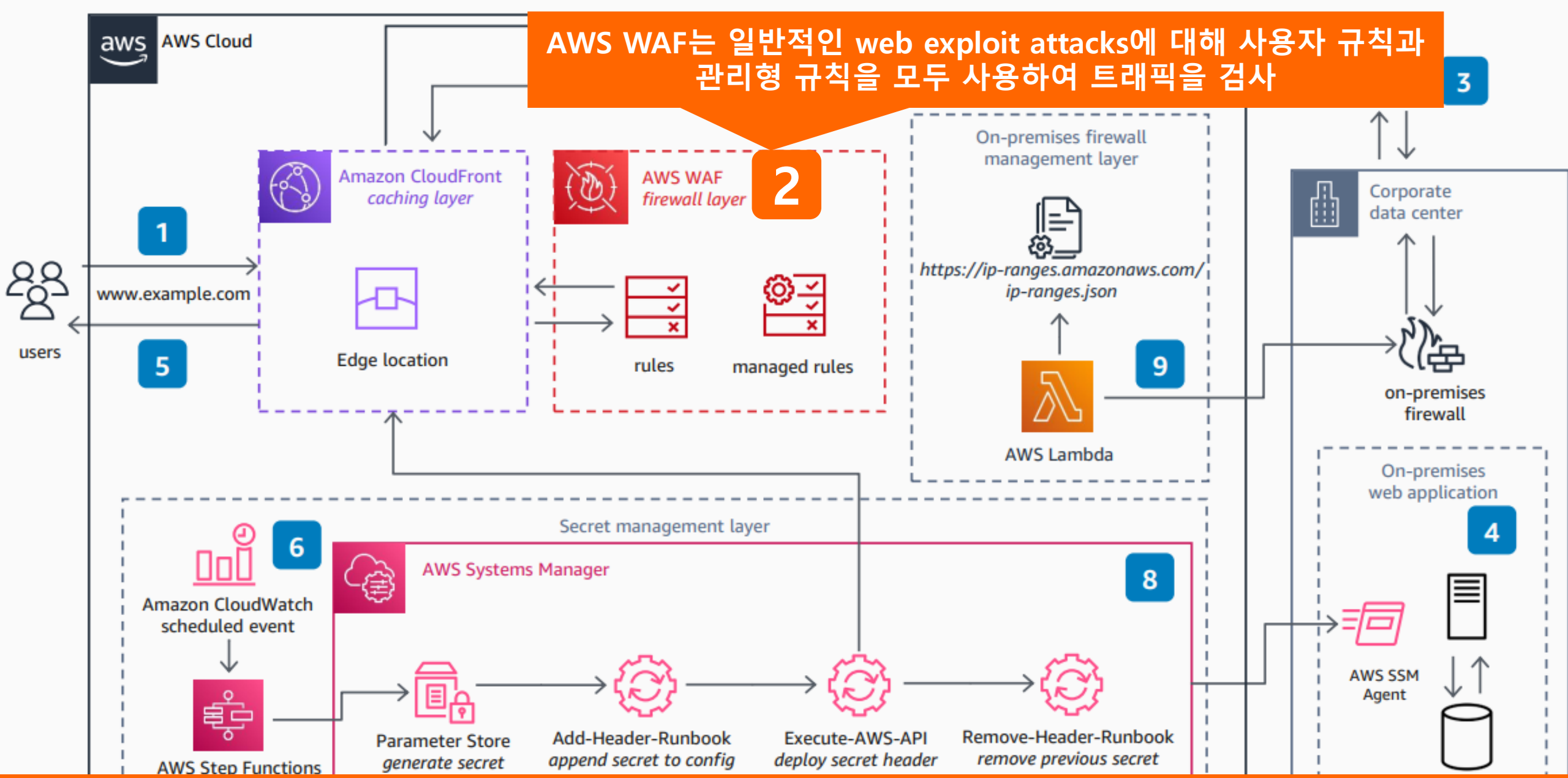
Cloud Front의 사용자 지정 오리진 및 사용자 지정 암호 헤더를 활용하여, 일반적인 웹 취약점으로부터 Endpoint를 보호하는 아키텍처



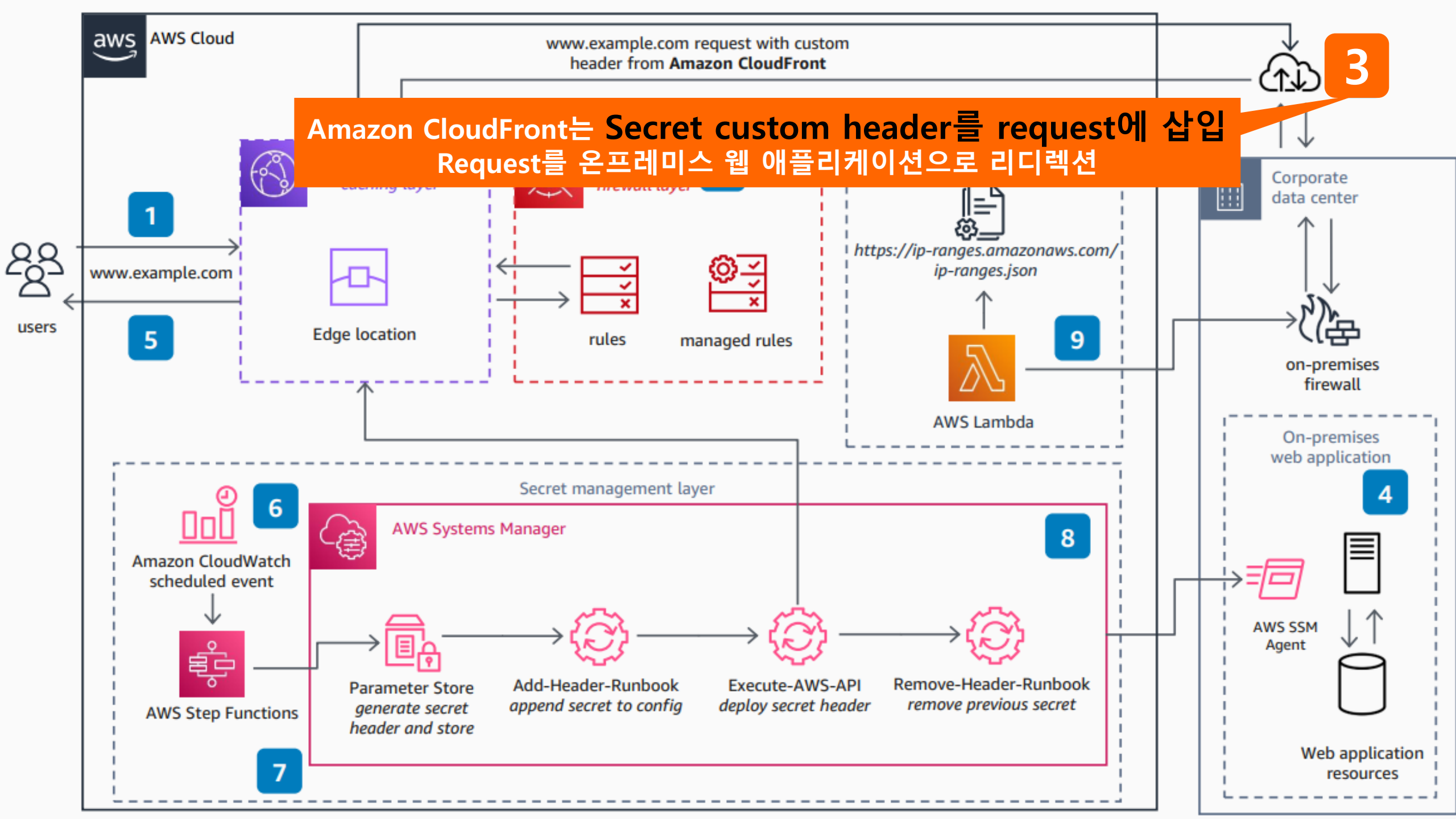
https://d1.awsstatic.com/architecture-diagrams/ArchitectureDiagrams/securing-custom-origins-with-aws-waf-ra.pdf?did=wp_card&trk=wp_card

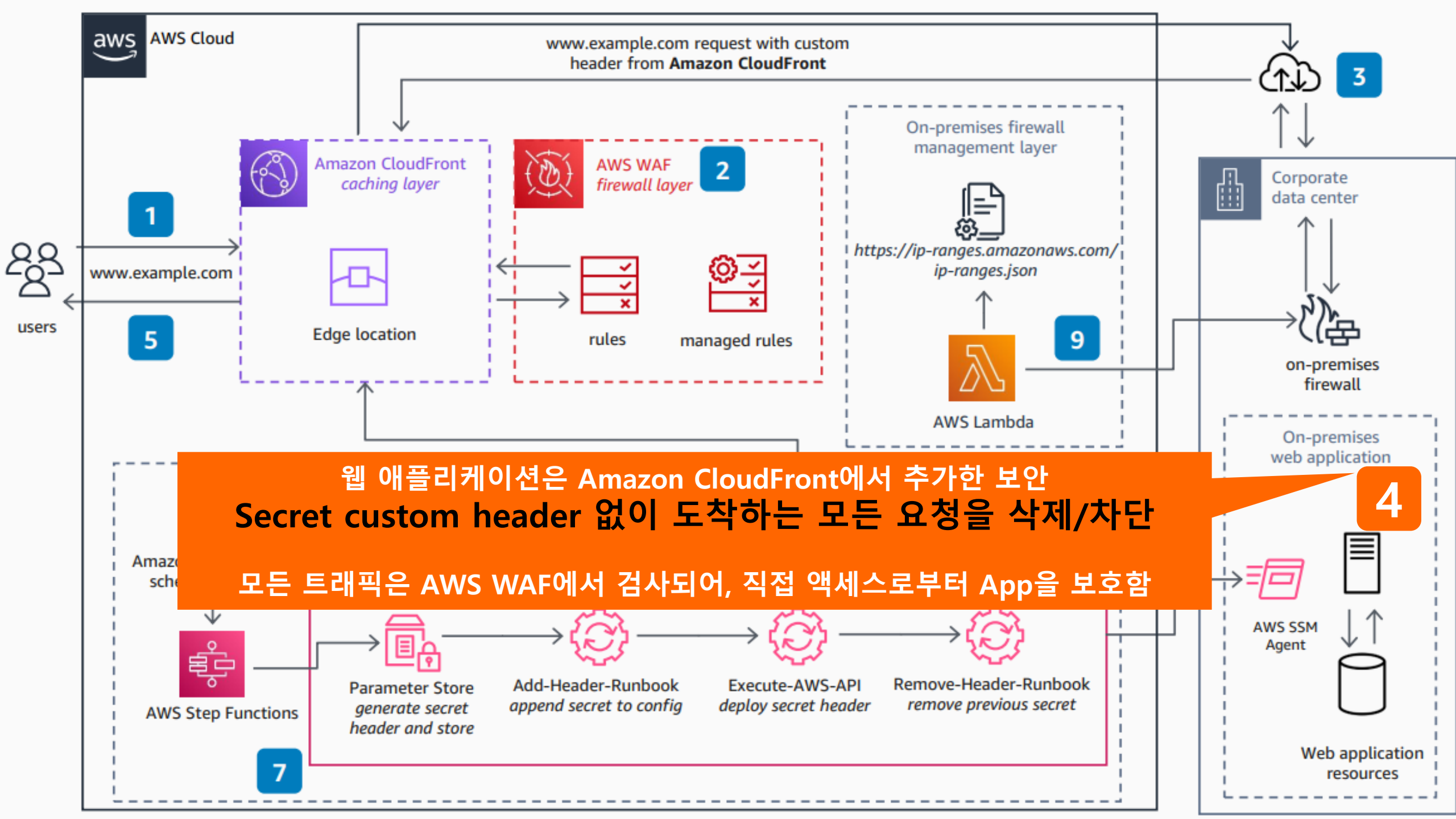
사용자 웹 접속(Request to the web application)
DNS records는 가장 가까운 CloudFront 엣지 로케이션 안내합니다.

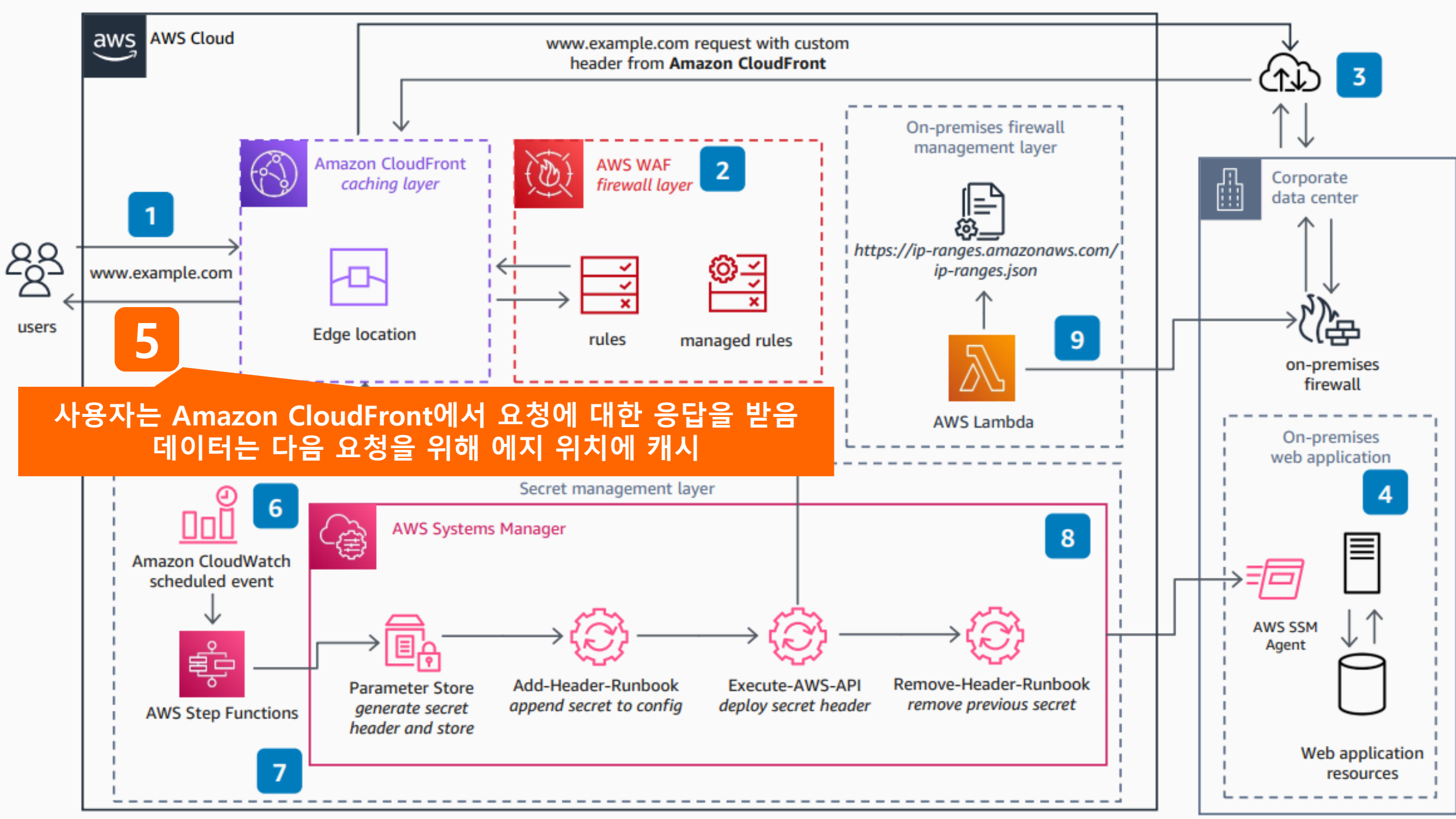


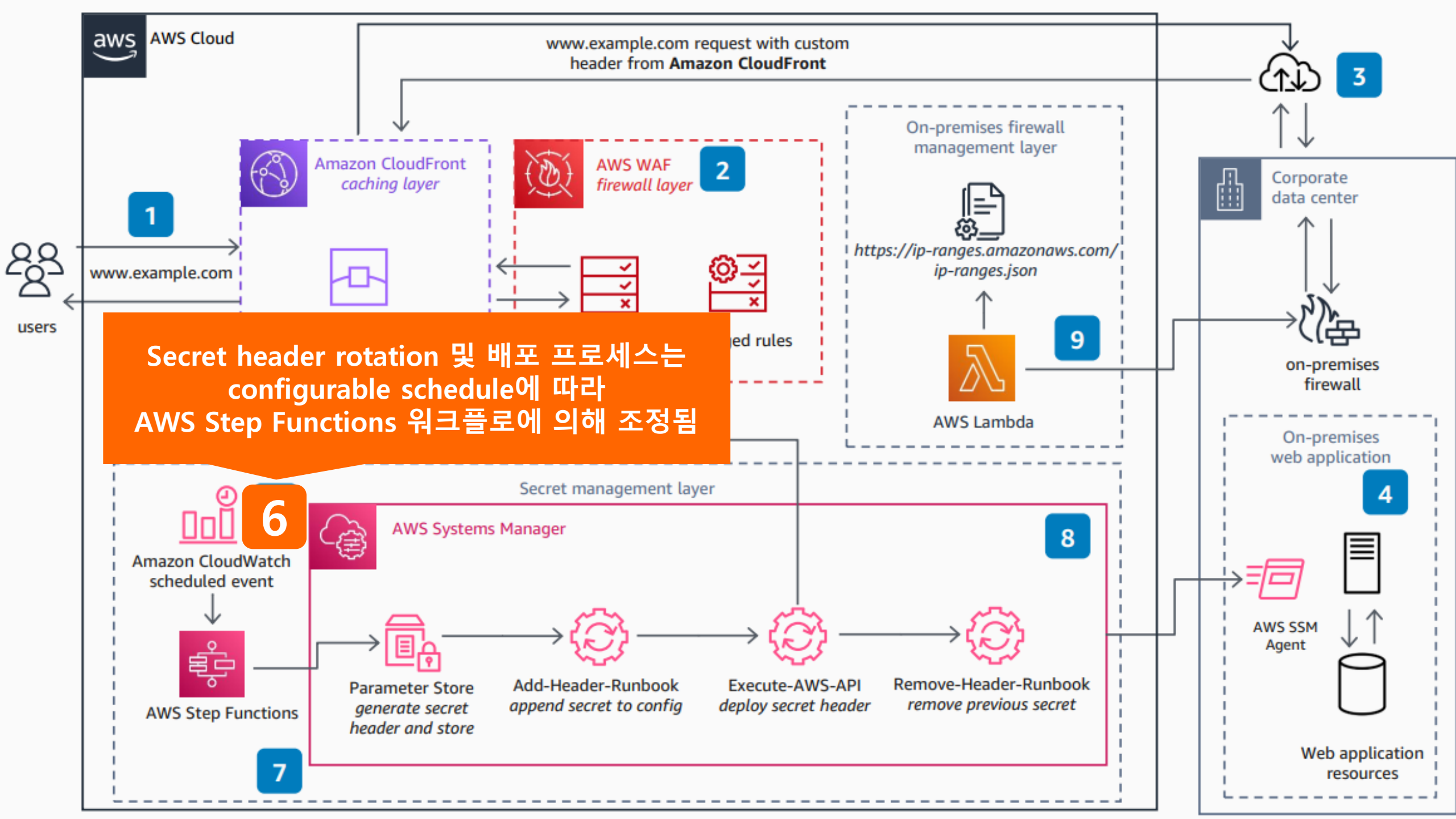


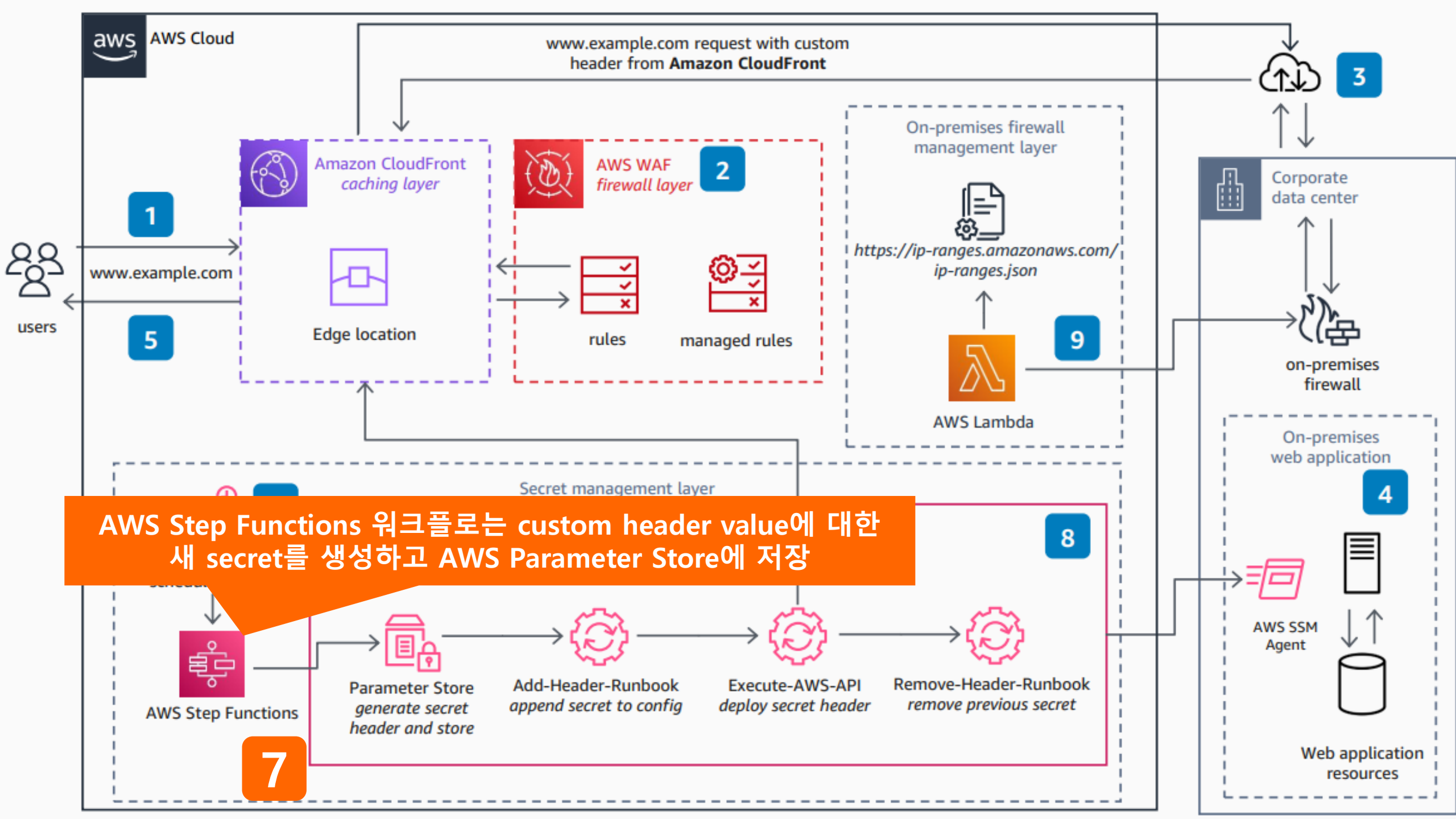
- **Web exploitation :** 웹 기반 애플리케이션의 취약점을 악용하여 민감한 데이터에 액세스하거나 앱을 제어하는 프로세스임
- 공격자는 취약점을 악용하여 앱을 장악하거나 민감한 데이터를 훔치거나 앱을 사용하여 다른 시스템에 대한 공격을 할수 있음

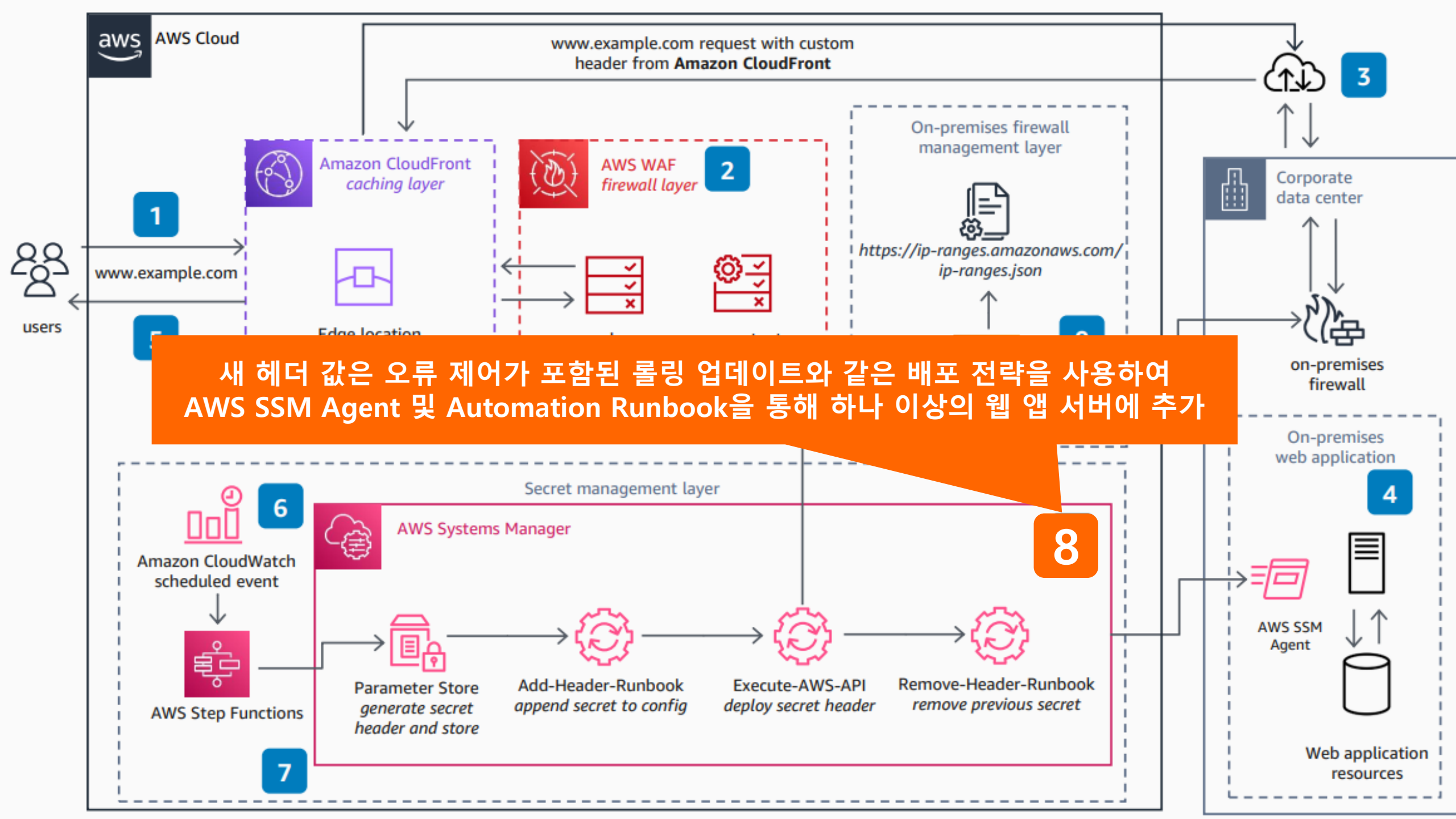

AWS Cloud
www.example.com request with custom header from Amazon CloudFront
3
Amazon CloudFront는 Secret custom header를 request에 삽입
Request를 온프레미스 웹 애플리케이션으로 리디렉션
1
www.example.com
users
5
Edge location
rules
managed rules
https://ip-ranges.amazonaws.com/ip-ranges.json
AWS Lambda
9
Corporate data center
on-premises firewall
On-premises web application
4
AWS SSM Agent
Web application resources
Secret management layer
6
Amazon CloudWatch scheduled event
AWS Step Functions
AWS Systems Manager
8
Parameter Store
generate secret header and store
Add-Header-Runbook
append secret to config
Execute-AWS-API
deploy secret header
Remove-Header-Runbook
remove previous secret
7

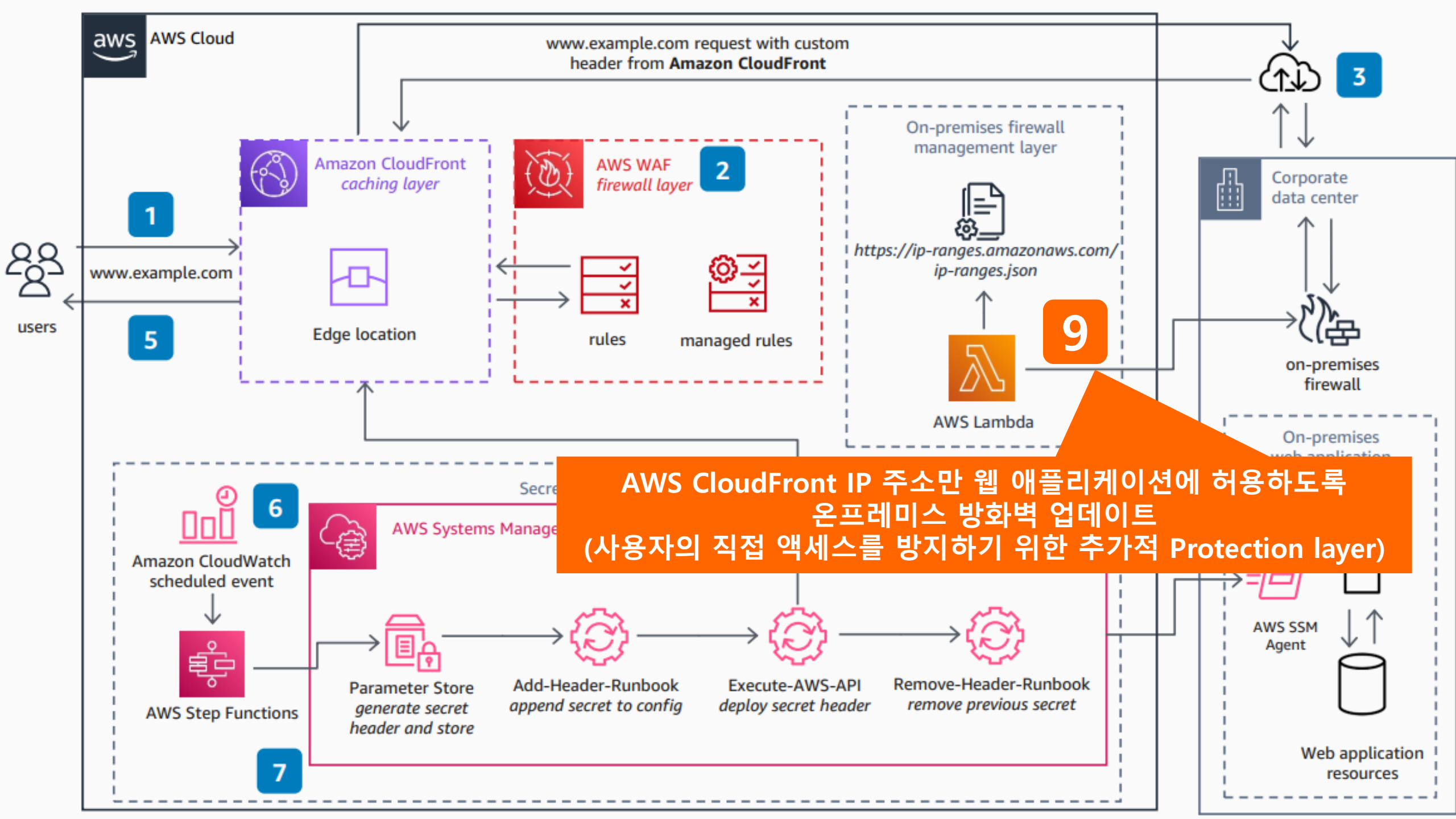

AWS Cloud
www.example.com request with custom header from Amazon CloudFront
3
Amazon CloudFront
caching layer
AWS WAF
firewall layer
2
On-premises firewall management layer
Corporate data center
1
www.example.com
users
5
Edge location
rules
managed rules
https://ip-ranges.amazonaws.com/ip-ranges.json
9
AWS Lambda
on-premises firewall
웹 애플리케이션은 Amazon CloudFront에서 추가한 보안
Secret custom header 없이 도착하는 모든 요청을 삭제/차단
모든 트래픽은 AWS WAF에서 검사되어, 직접 액세스로부터 App을 보호함
On-premises web application
4
AWS Step Functions
Parameter Store
generate secret header and store
Add-Header-Runbook
append secret to config
Execute-AWS-API
deploy secret header
Remove-Header-Runbook
remove previous secret
AWS SSM Agent
7
Web application resources


AWS Cloud
www.example.com request with custom header from Amazon CloudFront
3
Amazon CloudFront
caching layer
AWS WAF
firewall layer
2
On-premises firewall management layer
Corporate data center
1
www.example.com
users
Edge location
rules
managed rules
https://ip-ranges.amazonaws.com/ip-ranges.json
AWS Lambda
9
on-premises firewall
5
사용자는 Amazon CloudFront에서 요청에 대한 응답을 받음
데이터는 다음 요청을 위해 에지 위치에 캐시
On-premises web application
4
Secret management layer
6
Amazon CloudWatch scheduled event
AWS Systems Manager
8
AWS SSM Agent
AWS Step Functions
Parameter Store
generate secret header and store
Add-Header-Runbook
append secret to config
Execute-AWS-API
deploy secret header
Remove-Header-Runbook
remove previous secret
7
Web application resources


AWS Cloud
www.example.com request with custom header from Amazon CloudFront
3
Amazon CloudFront
caching layer
AWS WAF
firewall layer
2
On-premises firewall management layer
Corporate data center
1
www.example.com
users
https://ip-ranges.amazonaws.com/ip-ranges.json
ed rules
9
AWS Lambda
on-premises firewall
Secret header rotation 및 배포 프로세스는
configurable schedule에 따라
AWS Step Functions 워크플로에 의해 조정됨
On-premises web application
4
Secret management layer
6
AWS Systems Manager
8
Amazon CloudWatch scheduled event
AWS SSM Agent
AWS Step Functions
Parameter Store
generate secret header and store
Add-Header-Runbook
append secret to config
Execute-AWS-API
deploy secret header
Remove-Header-Runbook
remove previous secret
7
Web application resources


AWS Cloud
www.example.com request with custom header from Amazon CloudFront
3
Amazon CloudFront
caching layer
AWS WAF
firewall layer
2
On-premises firewall management layer
Corporate data center
1
www.example.com
users
5
Edge location
rules
managed rules
https://ip-ranges.amazonaws.com/ip-ranges.json
AWS Lambda
9
on-premises firewall
On-premises web application
4
Secret management layer
AWS Step Functions 워크플로는 custom header value에 대한 새 secret를 생성하고 AWS Parameter Store에 저장
8
AWS SSM Agent
Parameter Store
generate secret header and store
Add-Header-Runbook
append secret to config
Execute-AWS-API
deploy secret header
Remove-Header-Runbook
remove previous secret
AWS Step Functions
7
Web application resources


AWS Cloud
www.example.com request with custom header from Amazon CloudFront
3
Amazon CloudFront
caching layer
AWS WAF
firewall layer
2
On-premises firewall management layer
1
www.example.com
users
https://ip-ranges.amazonaws.com/ip-ranges.json
Corporate data center
on-premises firewall
새 헤더 값은 오류 제어가 포함된 롤링 업데이트와 같은 배포 전략을 사용하여
AWS SSM Agent 및 Automation Runbook을 통해 하나 이상의 웹 앱 서버에 추가
On-premises web application
4
Secret management layer
6
AWS Systems Manager
8
Amazon CloudWatch scheduled event
AWS SSM Agent
AWS Step Functions
Parameter Store
generate secret header and store
Add-Header-Runbook
append secret to config
Execute-AWS-API
deploy secret header
Remove-Header-Runbook
remove previous secret
7
Web application resources


AWS Cloud
www.example.com request with custom header from Amazon CloudFront
3
Amazon CloudFront
caching layer
AWS WAF
firewall layer
2
On-premises firewall management layer
Corporate data center
1
www.example.com
users
5
Edge location
rules
managed rules
https://ip-ranges.amazonaws.com/ip-ranges.json
on-premises firewall
AWS Lambda
9
AWS CloudFront IP 주소만 웹 애플리케이션에 허용하도록
온프레미스 방화벽 업데이트
(사용자의 직접 액세스를 방지하기 위한 추가적 Protection layer)
On-premises
6
Amazon CloudWatch scheduled event
AWS Systems Manage
AWS SSM Agent
AWS Step Functions
Parameter Store
generate secret header and store
Add-Header-Runbook
append secret to config
Execute-AWS-API
deploy secret header
Remove-Header-Runbook
remove previous secret
7
Web application resources

Thank you