Public / Private API Guidance

Guiding Principles

Application Programming Interfaces (APIs) are a critical part of almost any application design. Guidance to date for the implementation of APIs in AWS, has been inconsistent and poorly aligned with AWS best practices. This guidance will address those issues as it relates to Public APIs as well as provide guidance on securing Public APIs to make them private.

Goals

Provide architecture guidance on approved patterns for implementing Public and Private APIs in AWS including:

- Guidance for using both AWS CloudFront and Akamai as the Content Delivery Network (CDN).
- Guidance for securing Public APIs to make them Private.
- Options for implementing authentication and the role authentication plays in simplifying API implementation.
- Architecture Controls that specify required implementation details

Out of Scope

- Configuration of Akamai services
- Configuration of Authentication services outside the specification to use Strong Authentication (e.g. MFA) as a means to secure public APIs.

Approved Patterns

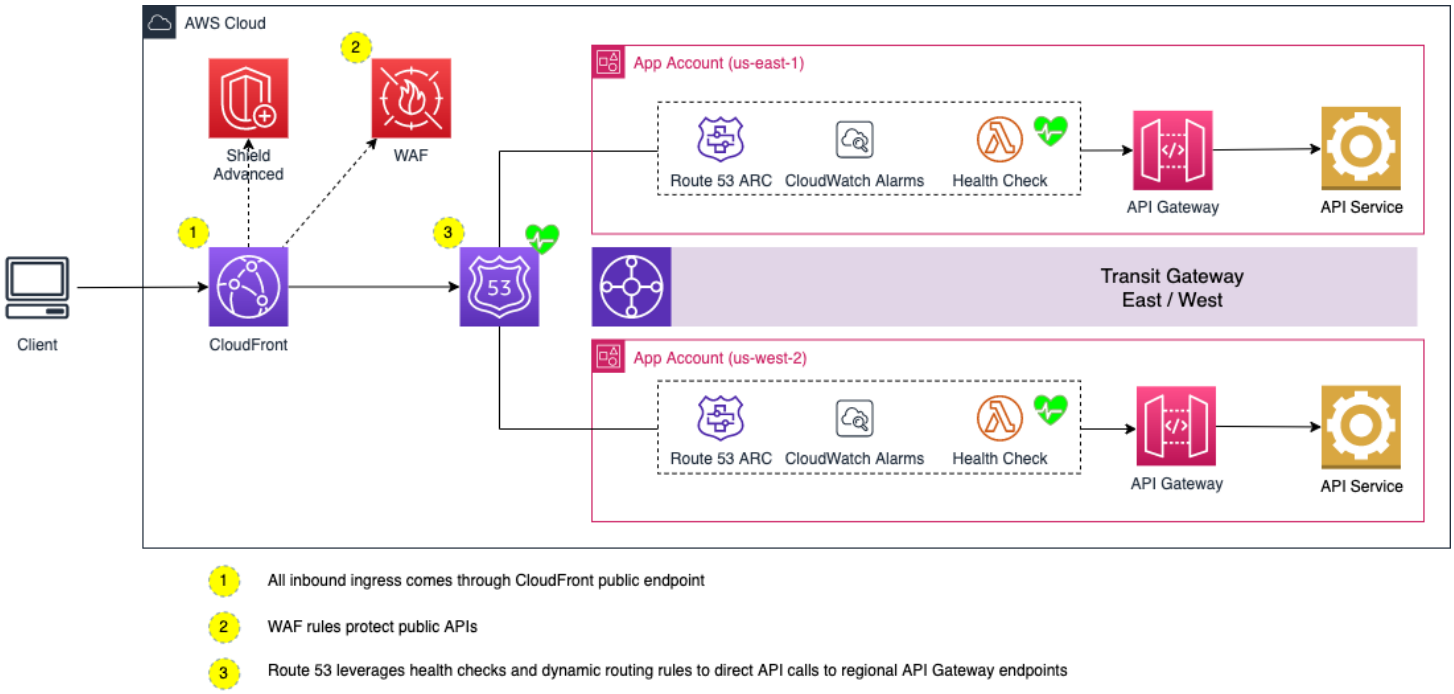
The following Architecture Patterns are approved for use for Public and Private APIs where the underlying API service runs in a SWA AWS environment.

Public APIs

Public APIs should be those APIs that are read-only and only provide access to data deemed **Public** by the Data Classification guidelines.

Public API using CloudFront

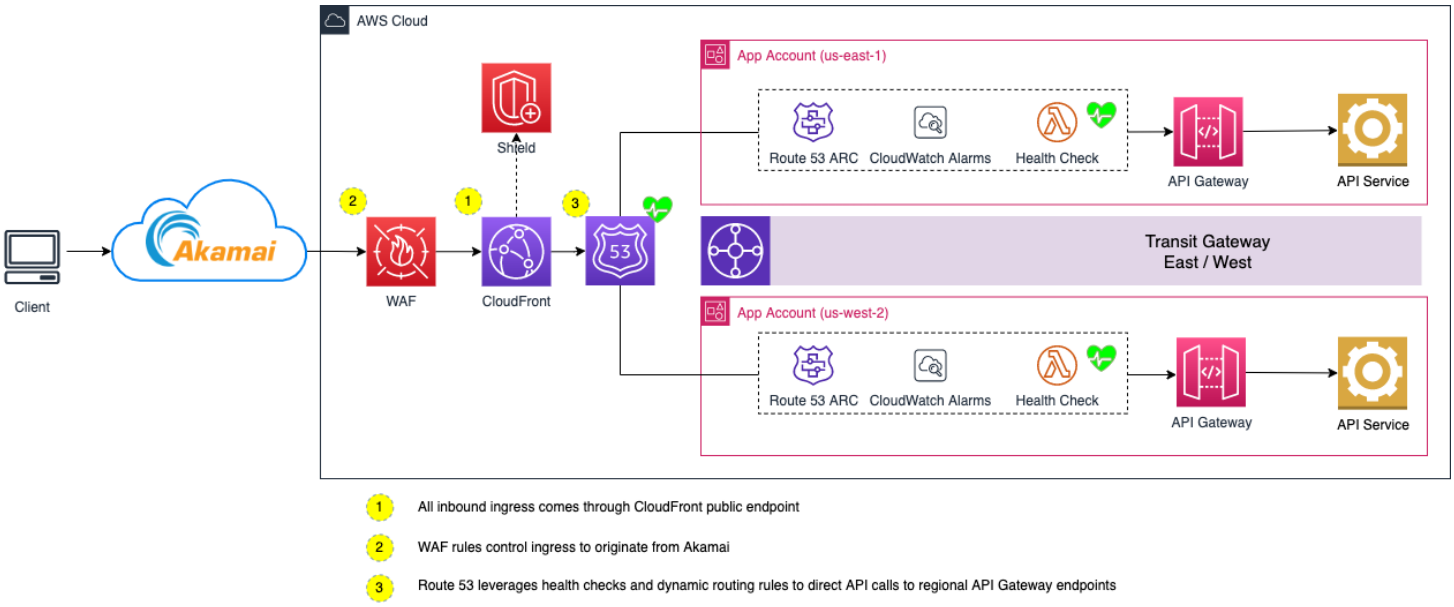
For Public API services running entirely in AWS, those services should use the following architecture design.



- CloudFront provides a Public API global endpoint.
- CloudFront is integrated with AWS Shield Advanced. Shield Advanced is configured to allow the AWS DDoS Response Team to detect Distributed Denial of Service attacks and notify SWA.
- CloudFront is also integrated with AWS Web Application Firewall (WAF) and the appropriate firewall rulesets have been loaded. Examples include but are not limited to: AWS Managed Baseline Rule Groups
- CloudFront uses Route 53 to lookup the most appropriate API Gateway endpoint to forward API requests to.
- Route 53 leverages health checks and Route 53 Application Recovery Controller to determine which API Gateway endpoint to direct API requests to.

Public API using Akamai

For Public API services using Akamai to provide the global API endpoint, the following architecture design should be used.



- Akamai provides the Global API endpoint and provides multiple API services (e.g. Bot Management, DDoS mitigation services, etc).
- Akamai connects directly to AWS CloudFront, and AWS WAF limits connections to the CloudFront Public API endpoint to sources originating from Akamai. The AWS WAF does not need to be configured to leverage any other managed rulesets.
- Shield Advanced is still configured to perform DDoS mitigation, similar to the Public API pattern above.
- CloudFront uses Route 53 to lookup the most appropriate API Gateway endpoint to forward API requests to.
- Route 53 leverages health checks and Route 53 Application Recovery Controller to determine which API Gateway endpoint to direct API requests to.

Private APIs

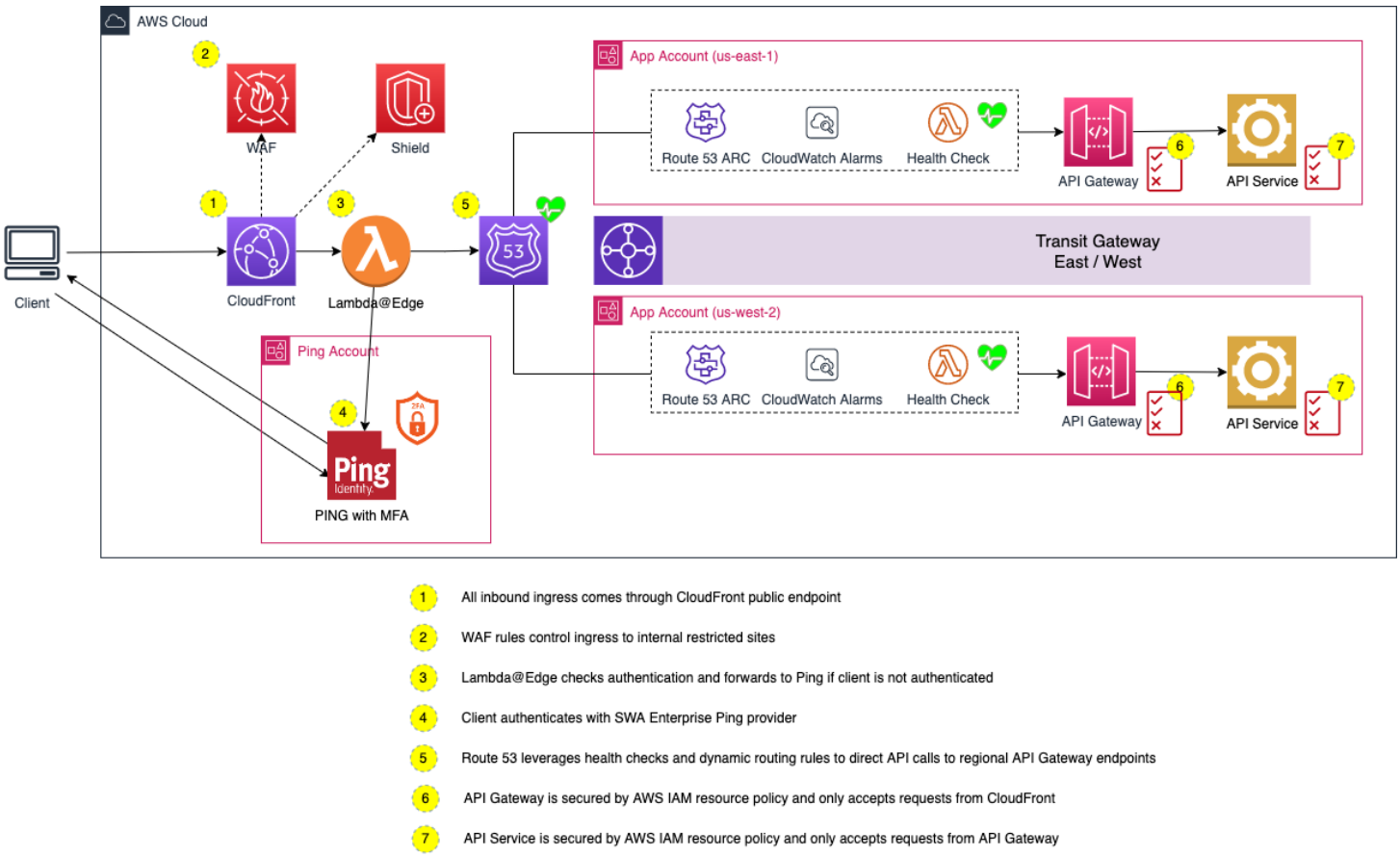
Private APIs are those APIs that either provide access to non-public SWA data or are operational in nature. If the API facilitates a change in state to a SWA system, then the API is considered **Private** and one of the following patterns must be used.

Restricting access with Authentication

The preferred pattern to secure Private APIs, is to enable strong authentication. The authentication used must be considered to be strong authentication.

- Examples of strong authentication:
  - Multi-Factor Authentication
  - OAuth-based Authentication
- Examples that do NOT qualify as strong authentication:

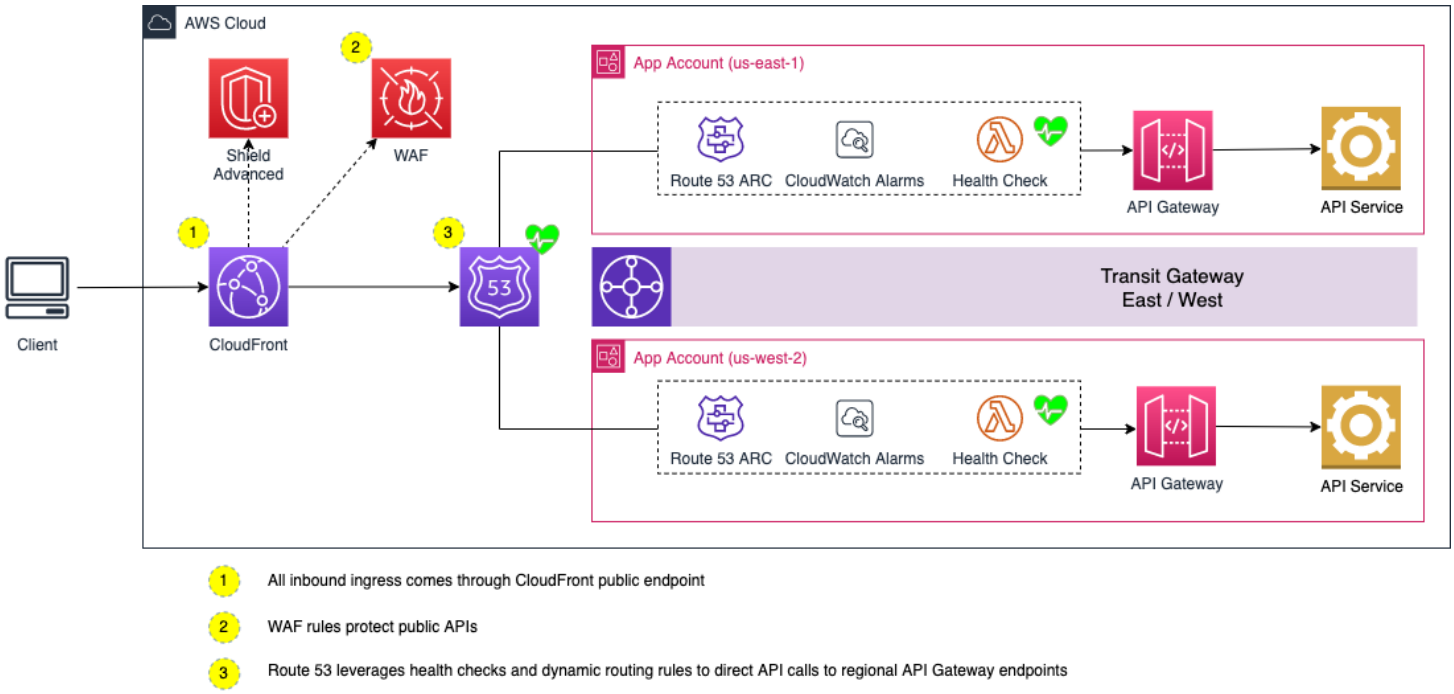
- Username and password
- Certificate based mutual authentication



- CloudFront provides a Public API global endpoint.
- CloudFront is integrated with AWS Shield Advanced. Shield Advanced is configured to allow the AWS DDoS Response Team to detect Distributed Denial of Service attacks and notify SWA.
- CloudFront is also integrated with AWS Web Application Firewall (WAF) and the appropriate firewall rulesets have been loaded. Examples include but are not limited to: AWS Managed Baseline Rule Groups
- CloudFront is leveraging Lambda@Edge to inspect the headers for a previously successful authentication session. If the appropriate header is not found and validated, then the client is redirected to the SWA Enterprise Ping instance to be authenticated.
- Once authentication is complete, CloudFront uses Route 53 to lookup the most appropriate API Gateway endpoint to forward API requests to.
- Route 53 leverages health checks and Route 53 Application Recovery Controller to determine which API Gateway endpoint to direct API requests to.
- API Gateway has an AWS IAM resource policy attached to it to only allow connections from the specific CloudFront origin.
- API Service has an AWS IAM resource policy attached to it to only allow connections from the specific API Gateway configured for the service.

Restricting access with AWS WAF

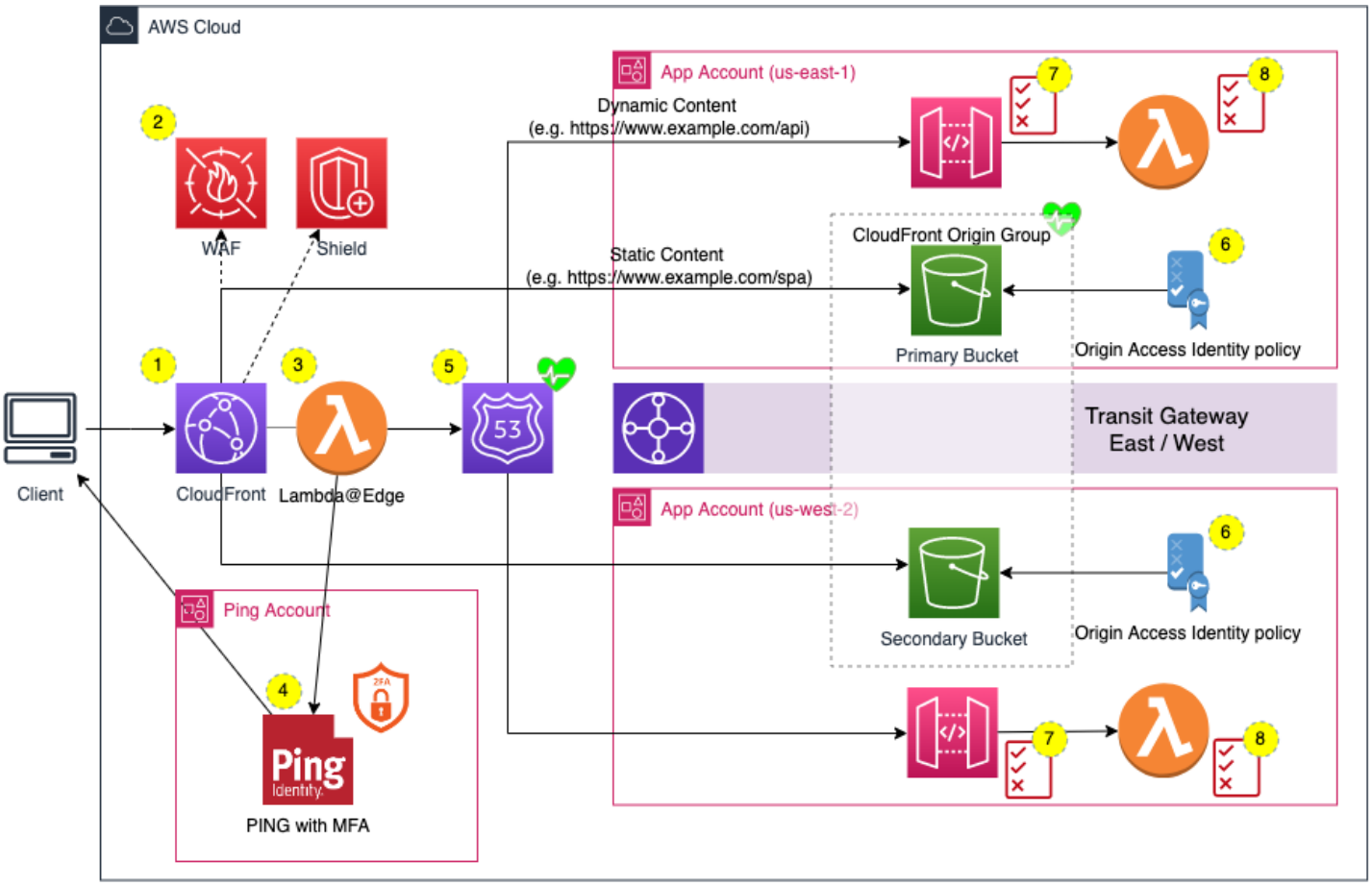
If strong authentication cannot be used, then a pattern similar to the Public API with CloudFront can be used, provided the WAF rules are configured to restrict access to SWA internal networks and SWA public IP addresses.



- CloudFront provides a Public API global endpoint.
- CloudFront is integrated with AWS Shield Advanced. Shield Advanced is configured to allow the AWS DDoS Response Team to detect Distributed Denial of Service attacks and notify SWA.
- CloudFront is integrated with AWS Web Application Firewall (WAF):
  - Specific WAF rules have been loaded to **restrict the Public API to SWA internal and public IP addresses**
  - Additional appropriate firewall rulesets have been loaded. Examples include but are not limited to: AWS Managed Baseline Rule Groups
- CloudFront uses Route 53 to lookup the most appropriate API Gateway endpoint to forward API requests to.
- Route 53 leverages health checks and Route 53 Application Recovery Controller to determine which API Gateway endpoint to direct API requests to.

Example Single Page App

Below is an example architecture for a Single Page Web Application. In this architecture, the Private API with MFA pattern has been extended to include static content hosting from S3.



1. All inbound ingress comes through CloudFront public endpoint
2. WAF rules control ingress to internal restricted sites
3. Lambda@Edge checks authentication and forwards to Ping if client is not authenticated
4. Client authenticates with SWA Enterprise Ping provider
5. Route 53 leverages health checks and dynamic routing rules to direct API calls to regional API Gateway endpoints
6. Origin Access Identity (OAI) policy secures access to S3 to only come from CloudFront
7. API Gateway is secured by AWS IAM resource policy and only accepts requests from CloudFront
8. API Service is secured by AWS IAM resource policy and only accepts requests from API Gateway

Summary

In summary, this architecture guidance for Public and Private APIs attempts to simplify the number of patterns around common use of AWS service aligned to AWS best practices. Value is placed on reusability, simplicity, and security. This guidance should be revisited regularly to ensure these principals continue to be met.

Architecture Controls

Control ID	Control Description
CLOUDAPI-01	Public APIs must only expose SWA data classified as "PUBLIC"
CLOUDAPI-02	CloudFront must be used as the API endpoint that users and services will interact with
CLOUDAPI-03	CloudFront must require authentication for Private APIs
CLOUDAPI-04	Where strong authentication using multi-factor cannot be used, WAF rules must be used to restrict access to SWA internal networks and SWA public IP addresses
CLOUDAPI-05	API Gateway must restrict access to source from CloudFront
CLOUDAPI-06	API services must restrict access to source from API Gateway
CLOUDAPI-07	CloudFront must be configured to be integrated with Shield Advanced
CLOUDAPI-08	Shield Advanced must minimally be configured to allow AWS DDoS Response Team (DRT) access to logs and must be configured with SWA contact info for DDoS event notification
CLOUDAPI-09	Where Akamai acts as the Content Delivery Network (CDN), CloudFront must be configured to only allow connections from Akamai