Cognito Notes

Authentication for HTTP API

Amazon API Gateway HTTP API supports JSON Web Tokens (JWTs) as part of OpenID Connect (OIDC) and OAuth 2.0 frameworks to restrict client access to your APIs. Those are open standards which means that API Gateway HTTP API can integrate with many third-party tools. A great resource to learn more about these two can be found at:
https://openid.net/connect/faq/.

It is recommended to make use of Access Token Scopes when using JWTs so that you can limit the authorization to your API only to those who have the scope you specified while defining your HTTP API. You can find more information about scopes in HTTP API at:
https://docs.aws.amazon.com/apigateway/latest/developerguide/http-api-jwt-authorizer.html.

API Gateway resource policy

Combining API Gateway resource policies with other authorizers affects how they can be used and what you can add to your resource policy. For example, combining a resource policy with IAM as an authorizer means that authentication with IAM will be done first. You can then use the information supplied by IAM in the resource policy. You can find diagrams explaining the authorization flow with any combination of these here:
https://docs.aws.amazon.com/apigateway/latest/developerguide/apigateway-authorization-flow.html

Signing AWS requests

Every request to the APIs of AWS needs to be signed so AWS can identify who sent them. It also allows to protect the data in transit because a signature was created from the request. This means that even if a bad actor was to modify the request in transit from let's say a "create" to a "delete", it wouldn't be accepted by the APIs of AWS as the signature wouldn't match. It also protects against replay attacks as the requests are only valid for a set period of time. To sign the request, you must use an Access Key and a Secret Key. If you use the AWS Management Console, the CLI or the SDK, this signature is done automatically for you. However, if you prefer to make your own calls to the APIs, which is not recommended, you would need to understand Signature Version 4 process. You can find more information about it here:
https://docs.aws.amazon.com/general/latest/gr/sigv4_signing.html