**Identidade e segurança**

**AWS IAM**







Escuta as requisições de uma API especifica ou várias API e passa por uma sequência de condições como por exemplo:

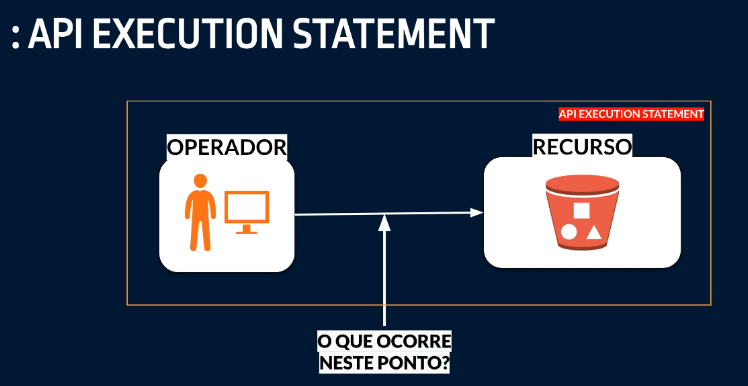
-tipo de recurso

-se está especificado em uma única rede ou mais

-a localização

-o caminho

Todos esses elementos formam este documento do formato JSON, que devemos associar a um usuário, a um grupo ou uma função para que tenha as permissões habilitadas.



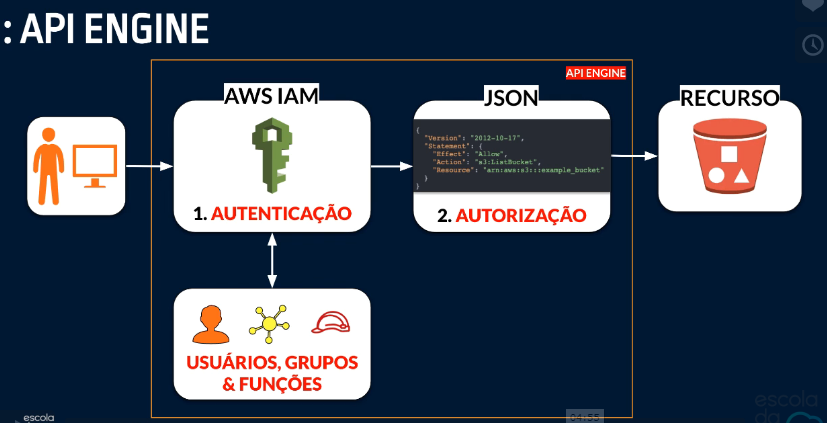
1. Executa uma API Engine (verifica se a autenticação é valida nas identidades do IAM, se o operador é permanente ou se é um operador temporário)

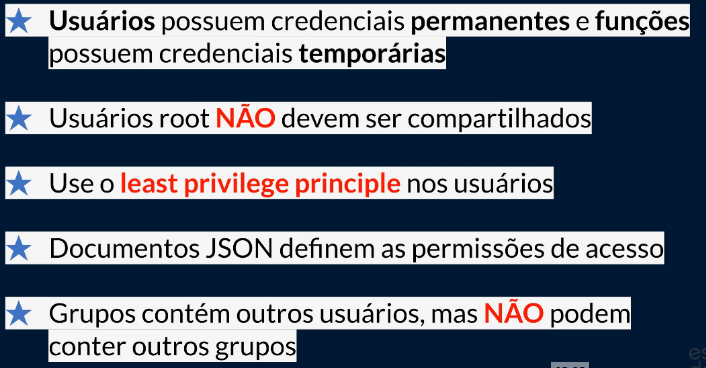
OBS: autenticação deu como válida

1. Validação do JSON e identifica o que deve ser autorizado para aquele operador

OBS: autorização concedida

3)O objeto é adicionado no bucket S3





**AWS WAF**

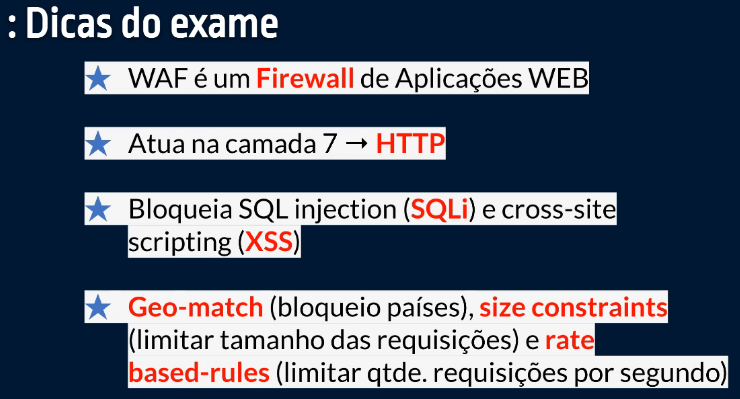
-É um firewall de aplicativos web que permite especificar qual tráfego tem o seu acesso permitido ou bloqueado, mediante a definição de regras personalizáveis



-Personalização de regras, pode conter filtros baseados pelo endereço IP, por cabeçalho HTTP, pelo corpo HTTP e algumas Springs Uri.

-Proteção e bloqueio de requisições maliciosas.

-Bloqueio por países usando (geo-match)

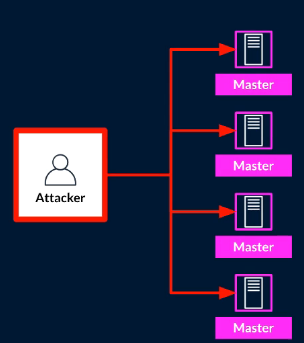


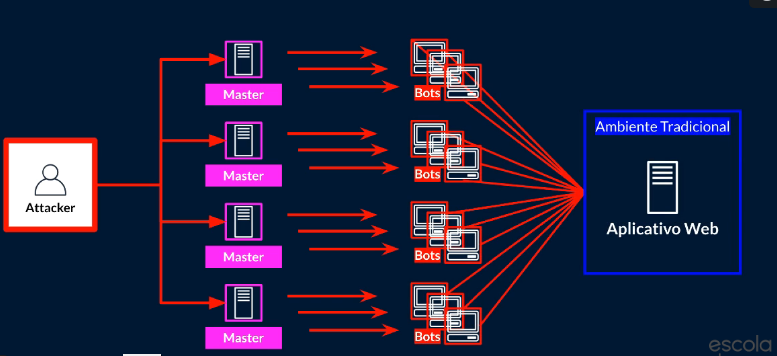
**AWS Shield**

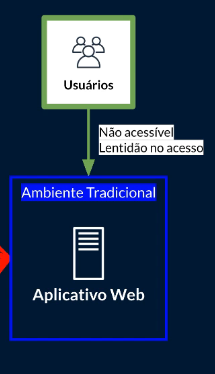
-DDoS: Distributed Denial of Service



indivíduo que deseja fazer o ataque na aplicação

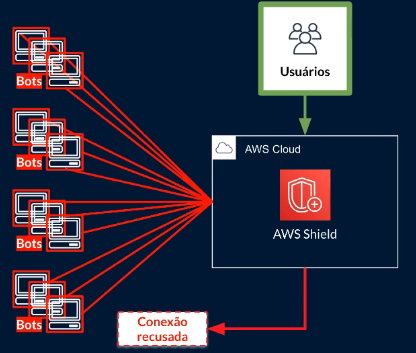


ele inicializa múltiplos servidores mestres esses servidores irão inicializar bost, fazendo com que a aplicação não consiga responder as múltiplas requisições, e nega o acesso de novas requisições.



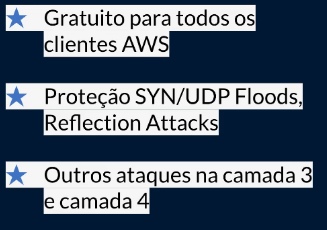
Quando o cliente acessar sua aplicação, eles vão identificar que o servidor não está mais disponível, ou estar lento, e quem já estava conectado fica com a navegação lenta, ai quando a aplicação não aguenta mais a sobre carga de requisições o servidor acaba caindo.

Como fazer para se proteger desses ataques?

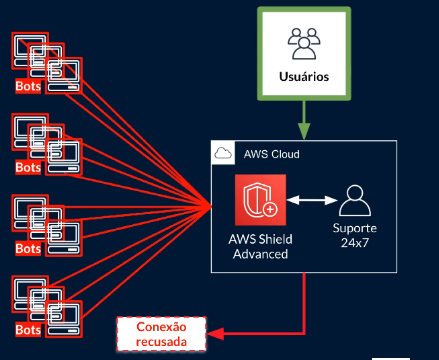


Deixar o serviço da AWS Shield Standard liberado, porque ele protege contra os ataques no site o aplicação que estão em uso (hospedado na nuvem publica AWS)

OBS:



**AWS Shield Advanced**



O Advanced tem equipe de suporte 24 por 7, eles podem intervir para mitigar contra esse tipo de ataque

OBS:

