UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS
CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES

ACTIVIDAD PROYECTO II PARCIAL – INDIVIDUAL

EXPLICAR EDGE SECURITY FOR CLOUD FRONT WITH WAF

(Configurar el básico)

ESTUDIANTE:

SUAREZ ORRALA HELEN

CURSO:

ISI-S-NO-7-5

DOCENTE:

ING. CRESPO LEON CHRISTOPHER GABRIEL, MSC.

ASIGNATURA:

SISTEMAS OPERATIVOS DISTRIBUIDOS

FECHA:

25/02/2022

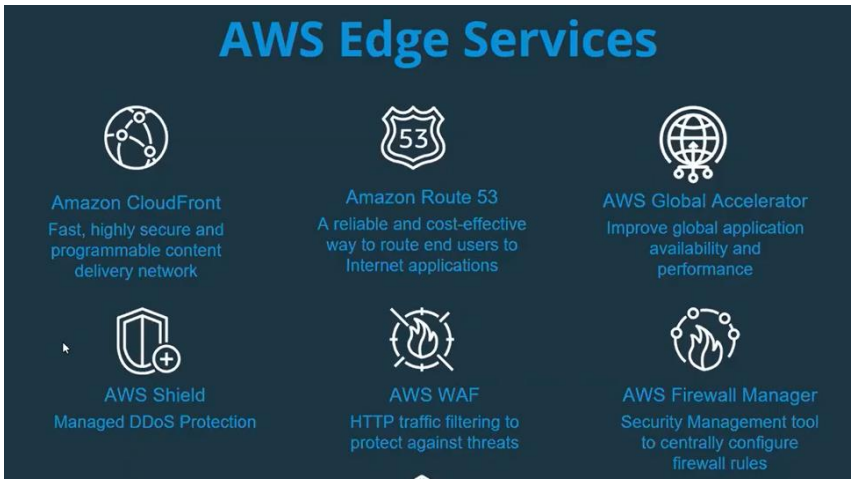
PERÍODO:

2021– CII

Tabla de contenido

TEMA DE EXPOSICIÓN

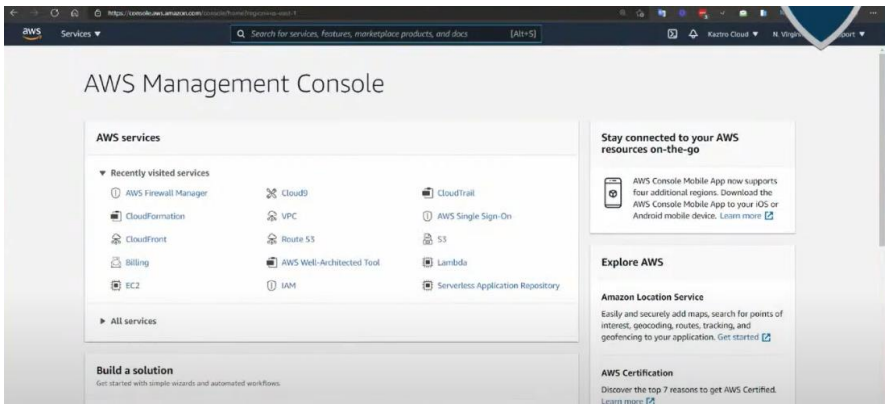
EDGE SECURITY FOR CLOUD FRONT WITH WAF (configurar el básico)



AWS WAF es un firewall para aplicaciones web que ayuda a proteger las aplicaciones web o API contra ataques web y bots comunes que pueden afectar la disponibilidad, poner en riesgo la seguridad o consumir demasiados recursos. AWS WAF brinda control sobre cómo el tráfico llega a sus aplicaciones, lo que le permite crear reglas de seguridad que controlan el tráfico de bots bloquean los patrones de ataque comunes, como la inyección de SQL o el scripting entre sitios.

PRÁCTICA PARA EL DÍA DE LA EXPOSICIÓN

Vamos a la consola:



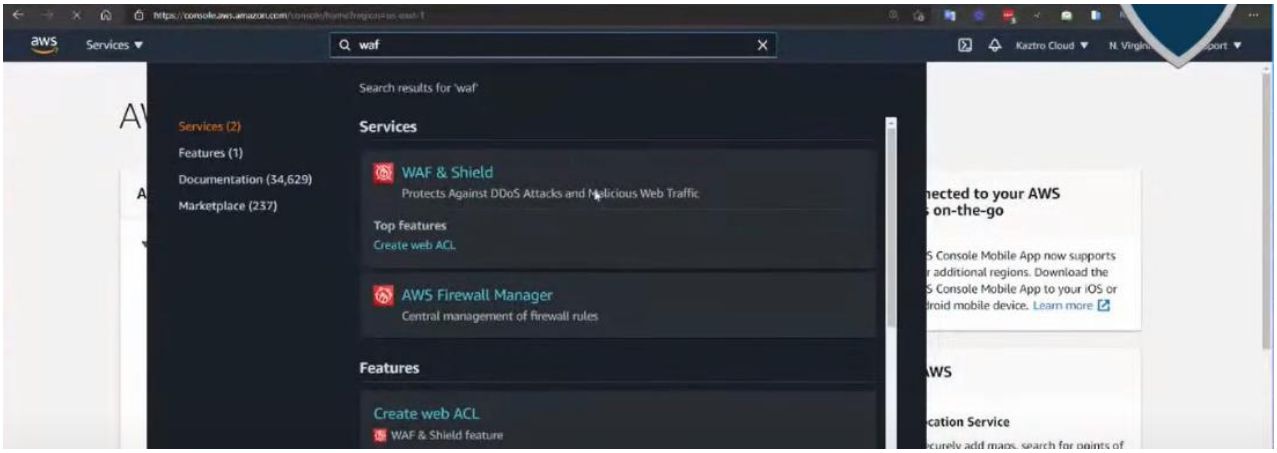
-Bueno estos son 2 Sitio que provienen de OWASP JUICE SHOP.

El owasp tiene un sitio demo que esta expuesto en internet. Al entrar en este sitio le va cargar con https. La finalidad de este sitio demo es que busca 2 cosas: 1. Entrar a un aprendizaje de seguridad ofensiva y 2.Empieces a buscar vulnerabilidades dentro de este sitio que crean, hay muchas vulnerabilidades que se pueden descubrir.

Pues a este owasp se le hace una réplica, Pues en la réplica se va colocar debajo del aws waf porque se va a relizat una web acl , por lo tanto la función es la siguiente: la replica va estar protegida por aws waf para enviarle algunos ataques y ver como aws waf protege ese tráfico , es decir te niega ese tráfico malicioso, y voy a utilizar el sitio original para enviar el mismo ataque que es muy sencillo.

Y dentro de cloud front tenemos una distribución web.

Como crear una web acl. Primero buscamos waf & shield

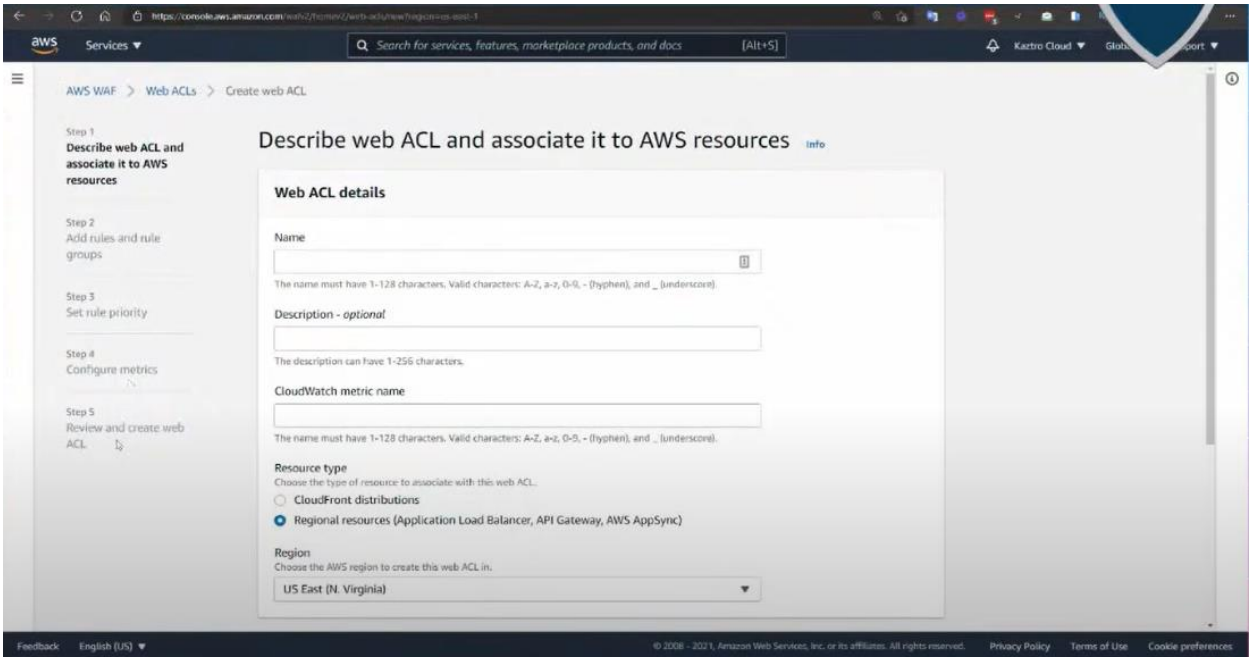


Paso 1: Creación de una ACL web

Para crear una ACL web

Desde la AWS WAF Elija de inicio **Creación de ACL web**.

Aquí podemos ver 5 pasos.



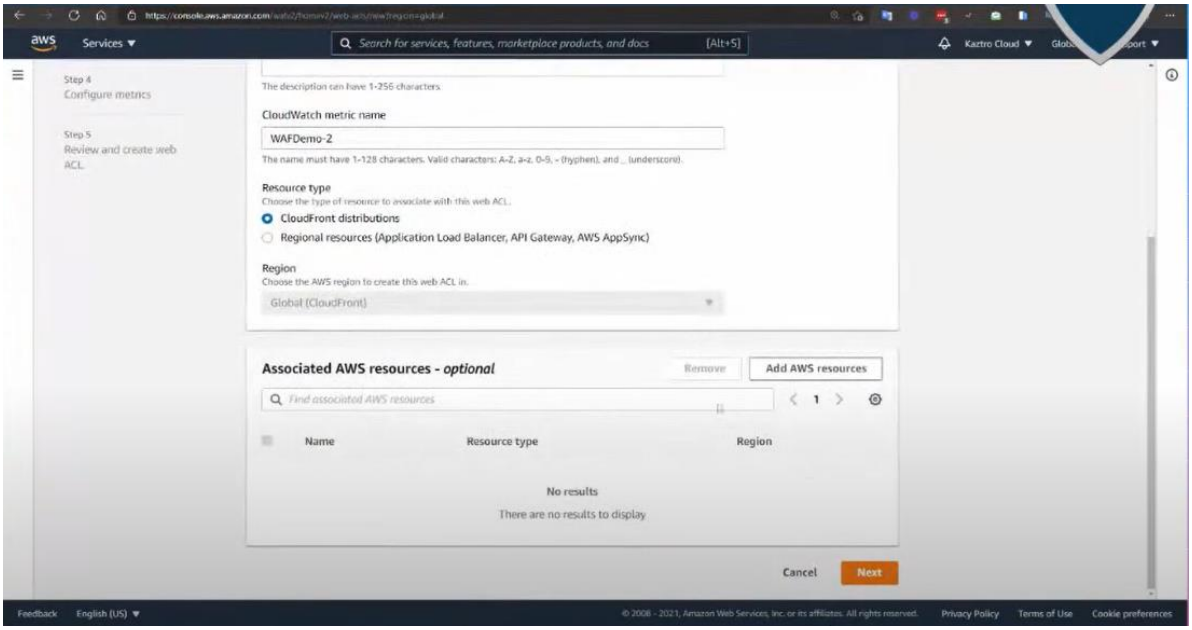
1. En **Name (Nombre)**, se escribe el nombre que desea utilizar para identificar la ACL web.

Nota: No se puede cambiar el nombre después de crear la ACL web.

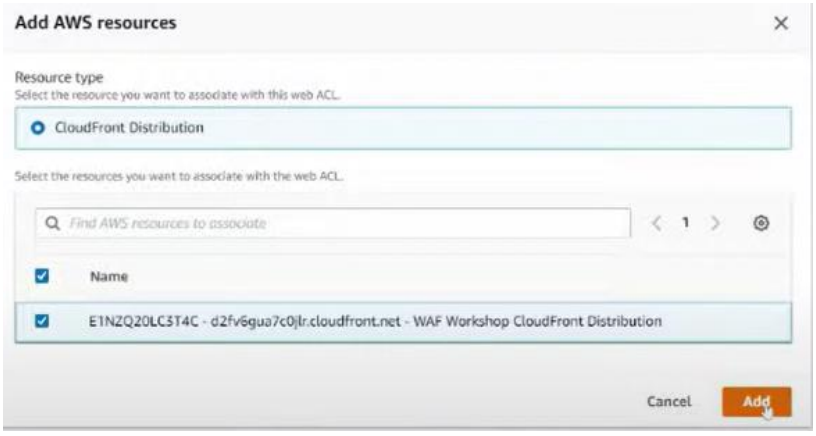
2. (Opcional) En **Description - optional (Descripción: opcional)**, se introduce una descripción más larga para la ACL web si lo desea.
3. Para **Nombre de la mé CloudWatch** Cambie el nombre predeterminado de, si procede. El nombre no puede contener caracteres especiales, espacios en blanco ni se pueden utilizar nombres de métricas reservados para AWS WAF.

Nota: No se puede cambiar el nombre de las métricas de CloudWatch después de crear la ACL web.

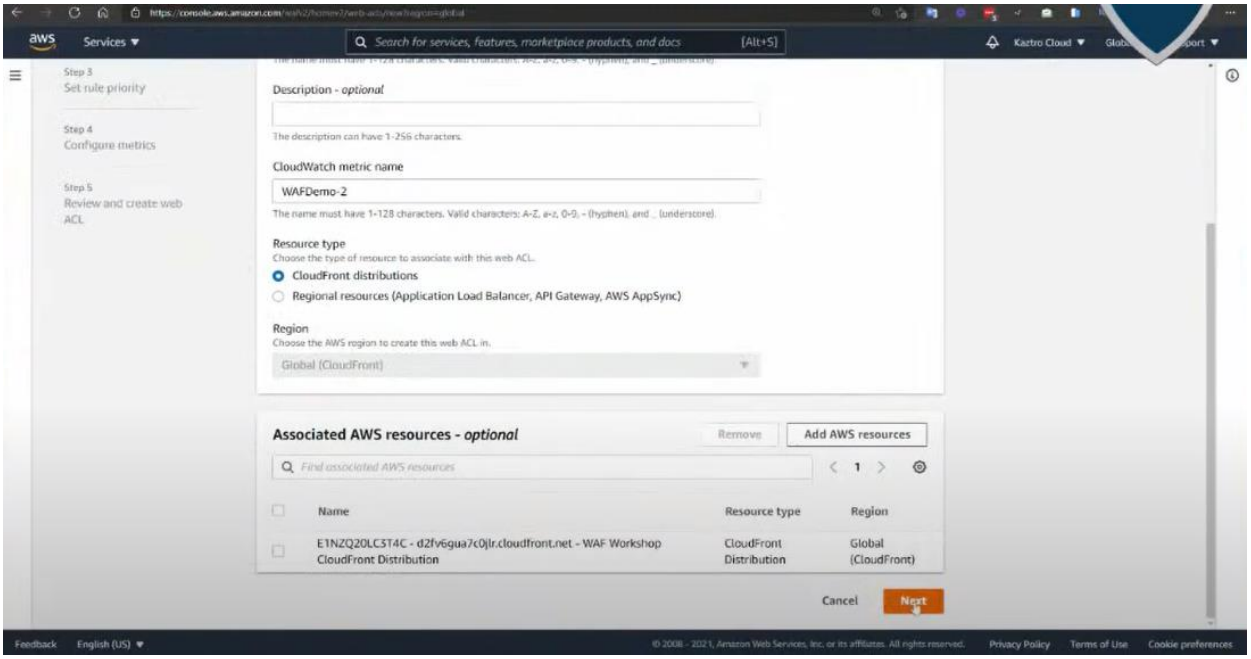
4. En **Resource type (Tipo de recurso)**, elija **CloudFront distributions (Distribuciones de CloudFront)**. se rellena automáticamente como **Global (CloudFront)** para distribuciones de CloudFront distributions.
5. (Opcional) Para **Asociated AWS recursos - opcional**, elija **AddAWSrecursos**. Debemos definir a que tipo de recurso que vamos asociar al aws waf, CloudFront distributions es un servicio global. Aquí en este ejemplo es que web ACL será de cloudFront. Y damos click en Add AWS resources, enla cual aquí agregamos recursos.



Luego aquí podemos ver las distribuciones cloudFront que tengamos. En este caso seleccionamos el que tenemos y le damos clic en agregar.



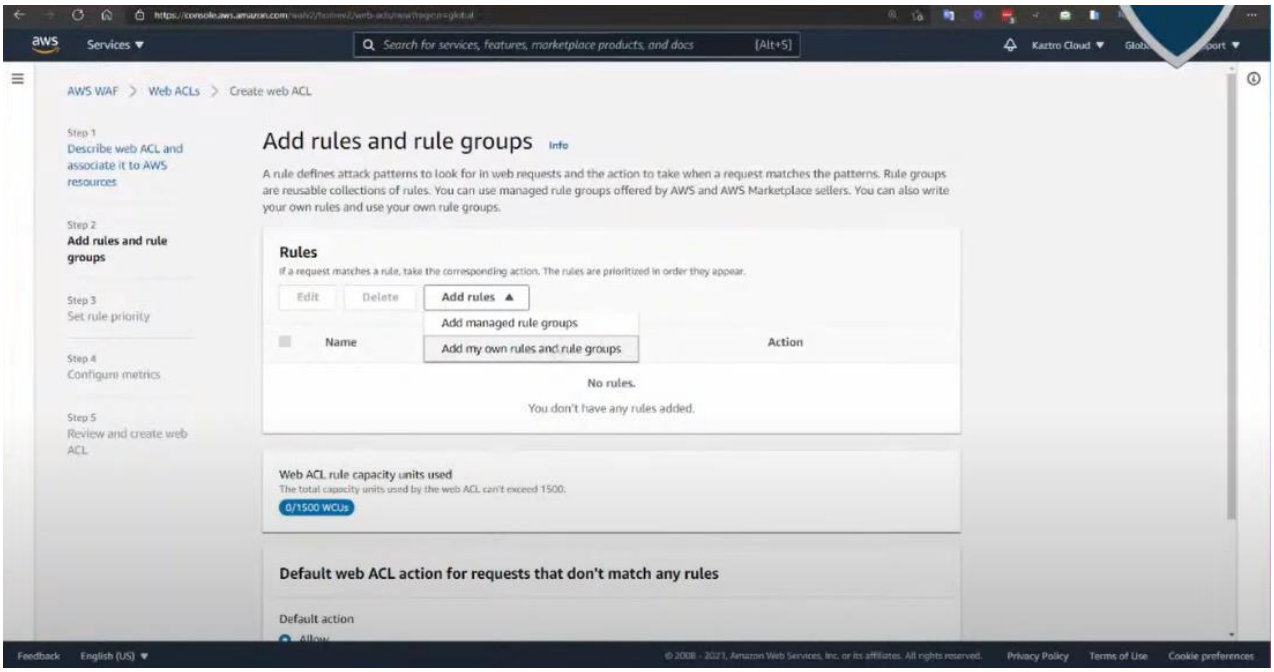
6. Le damos clic en siguiente.

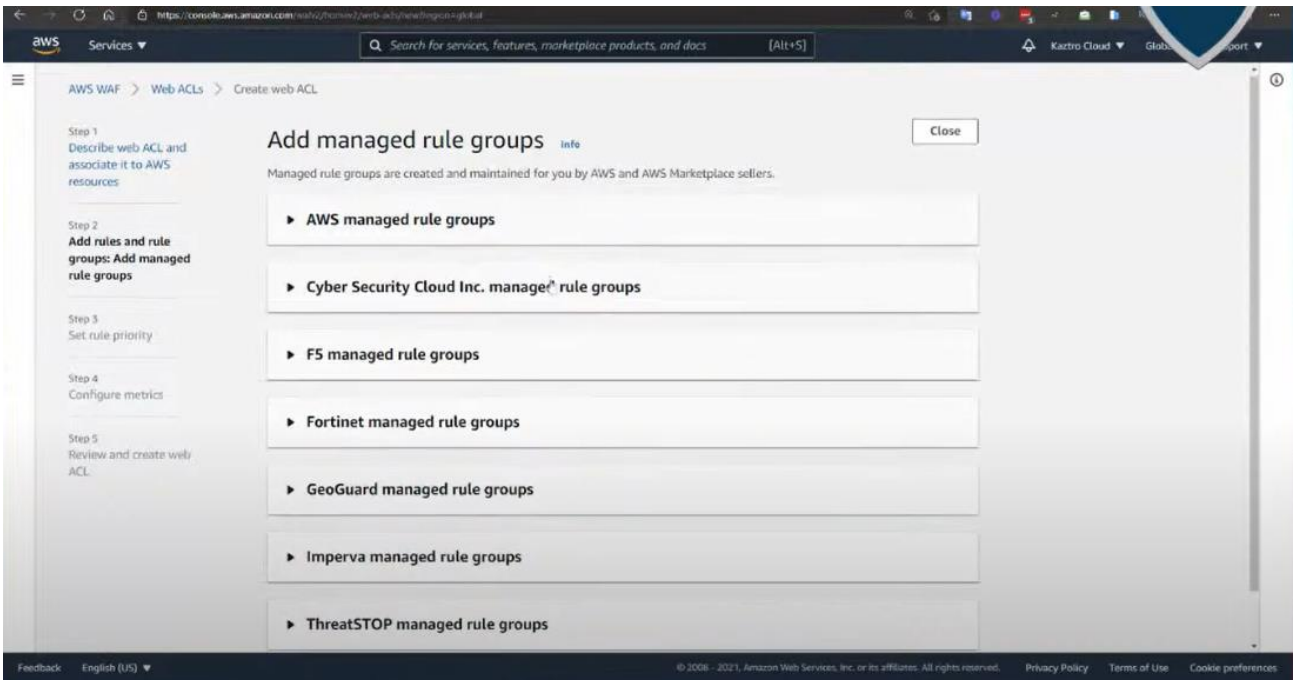


Paso 2: Agregar reglas y grupos de reglas

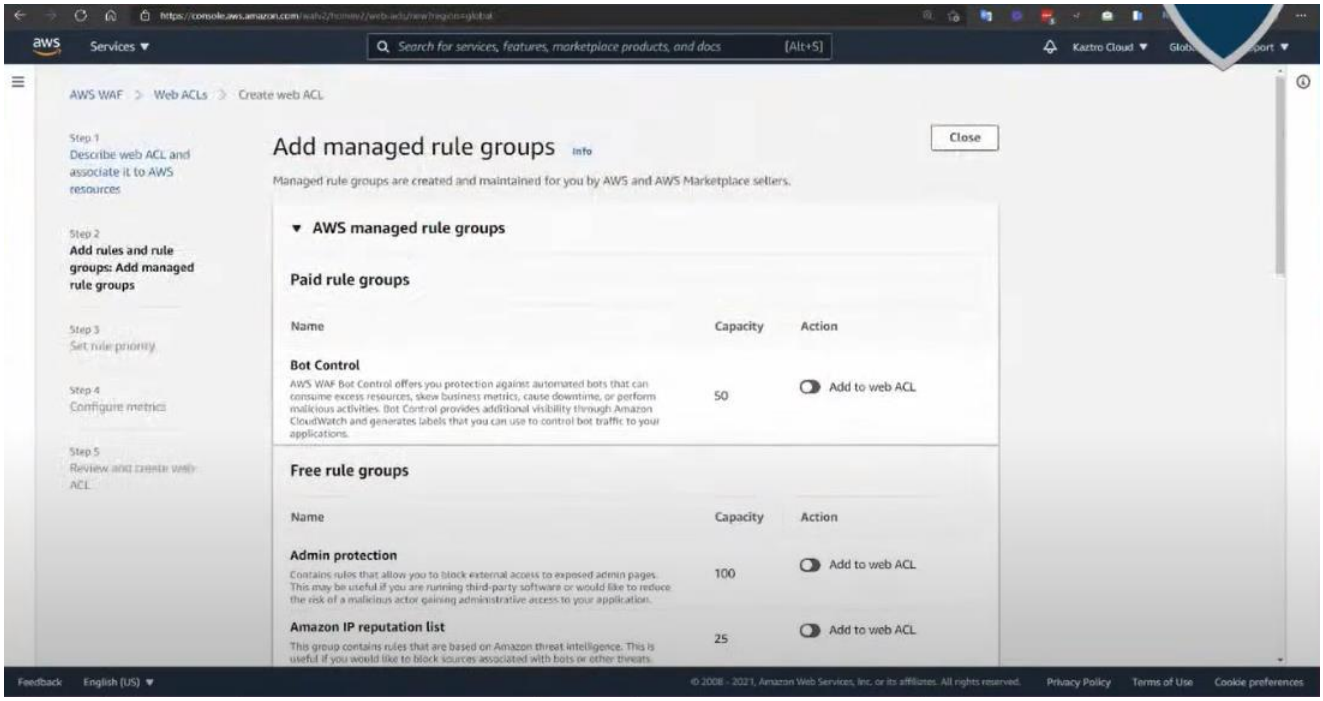
Podemos agregar reglas que yo pueda crear o que yo haya creado anteriormente y reglas administradas por aws. Si yo quiero crear reglas para agg en la web acl pues me voy a la opción 2; y si son reglas administradas por aws vamos a la opción 1.

AWS Las reglas administradas ofrecen un conjunto de grupos de reglas administrados, la mayoría de los cuales son gratuitos para AWS WAF Clientes. Añadiremos un AWS Grupo de reglas administradas a esta ACL web.





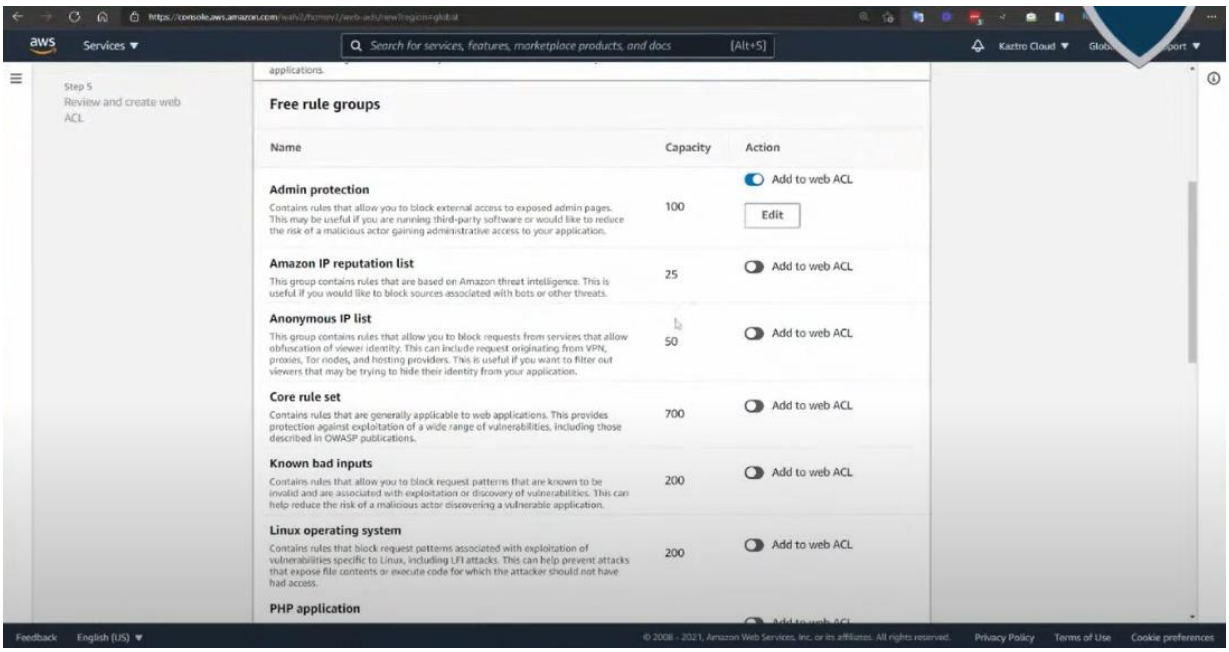
En la página **Agregar grupos de reglas administrados**, damos clic y tenemos un listado de la página**AWS Grupos de reglas administrados.**



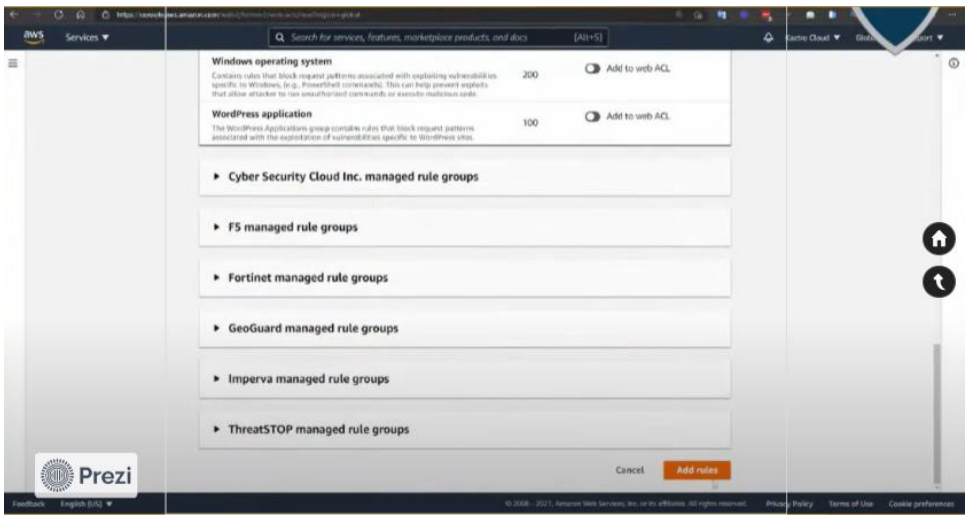
Para el grupo de reglas que desee agregar, haga lo siguiente:

a. En el navegador**Acción**, active la casilla**Agregar a ACL web**Alternar.

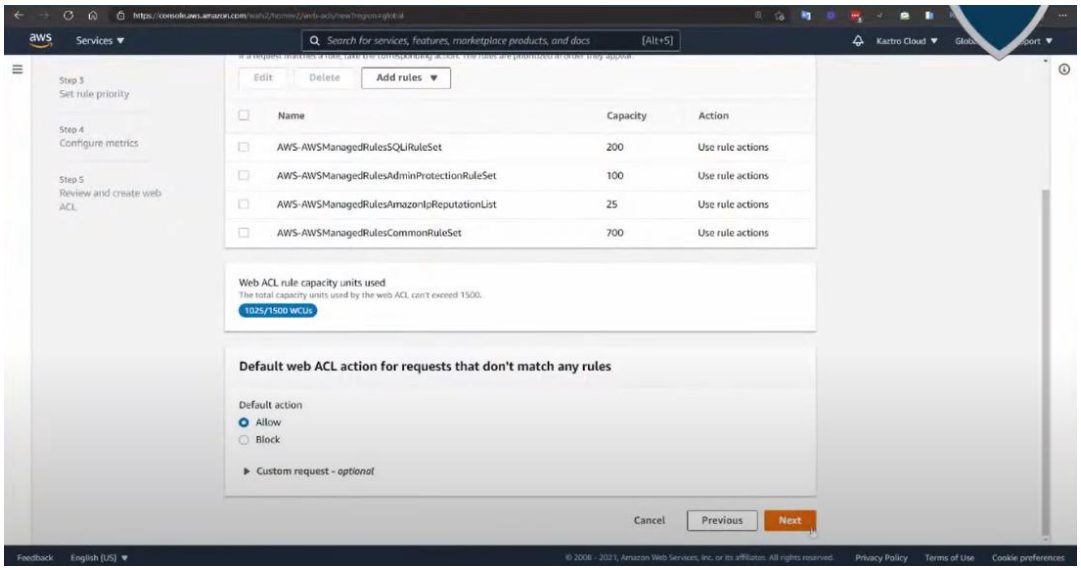
Admin protection: Contiene reglas que le permiten bloquear el acceso externo a las páginas de administración expuestas. Esto puede ser útil si está ejecutando software de terceros o desea reducir el riesgo de que un actor malicioso obtenga acceso administrativo a su aplicación.



En el navegador**Agregar grupos de reglas administrados**, elija **Agregar reglas**. Esto le devuelve al **Agregar reglas y grupos de reglas** (Se ha creado el certificado).

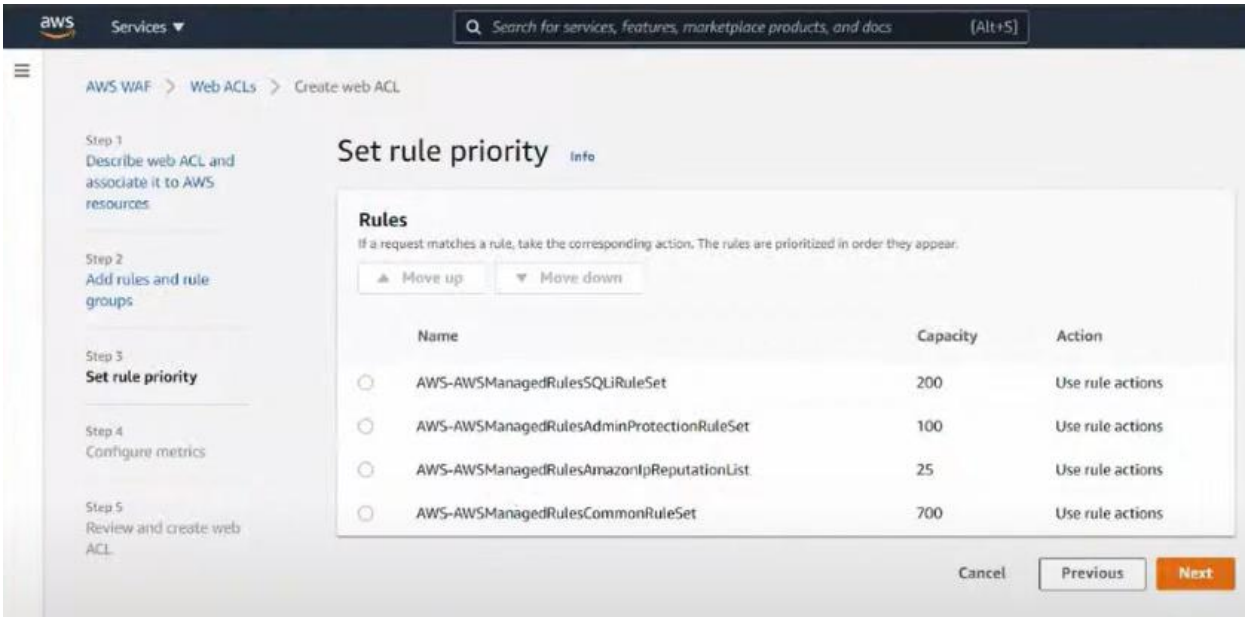


Damos clic en siguiente:



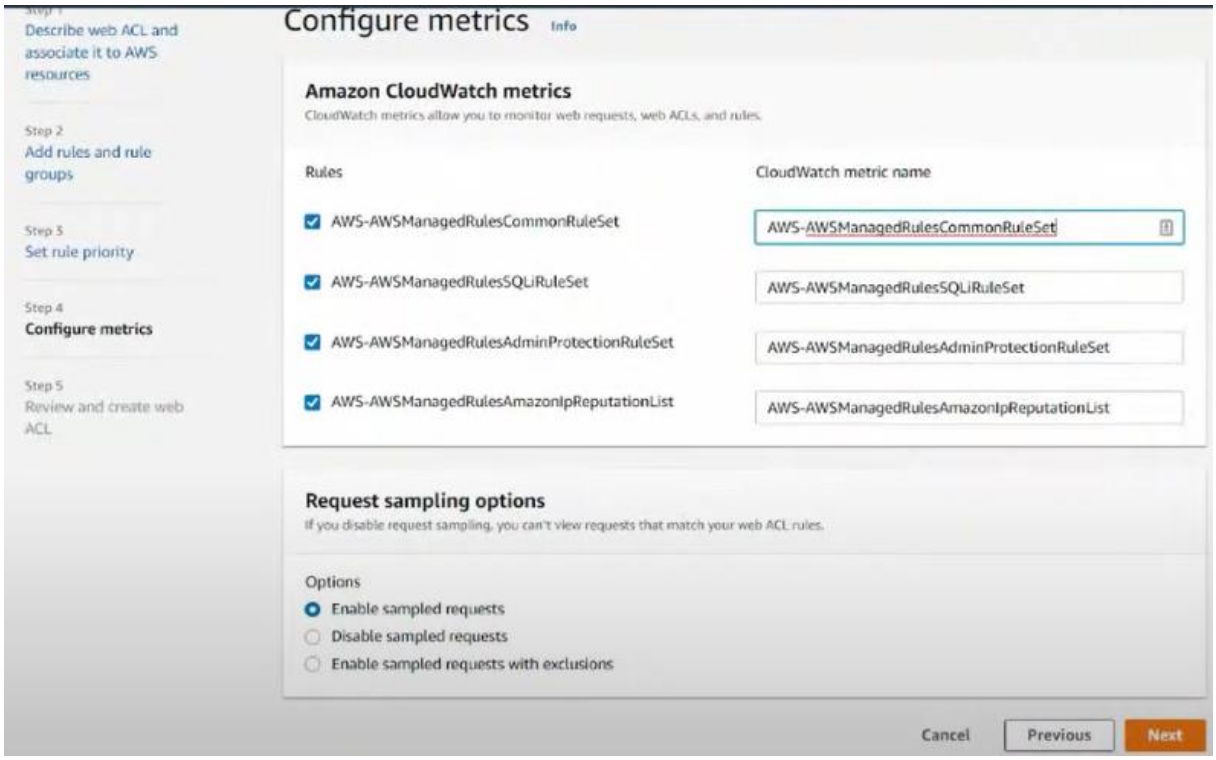
Paso 3: Set rule Priority

En la página Set rule priority (Establecer prioridad de regla) puede ver el orden de procesamiento de las reglas y grupos de reglas en la ACL web. AWS WAF los procesa desde arriba. Para cambiar el orden de procesamiento, muévalos hacia arriba y hacia abajo. Para ello. Elija **Next (Siguiente)**.



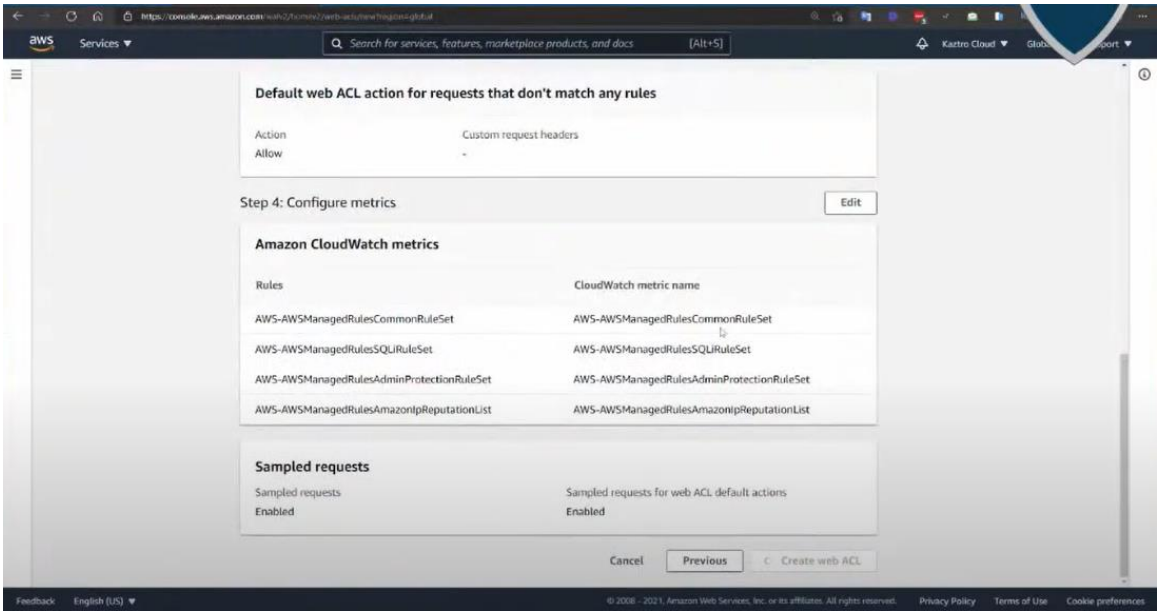
Paso 4: Configure metrics

En la página **Configurar métricas**, para **Métricas de Amazon CloudWatch**, puede ver las métricas planificadas para las reglas y grupos de reglas y puede ver las opciones de muestreo de solicitudes web. Elija **Next (Siguiente)**.

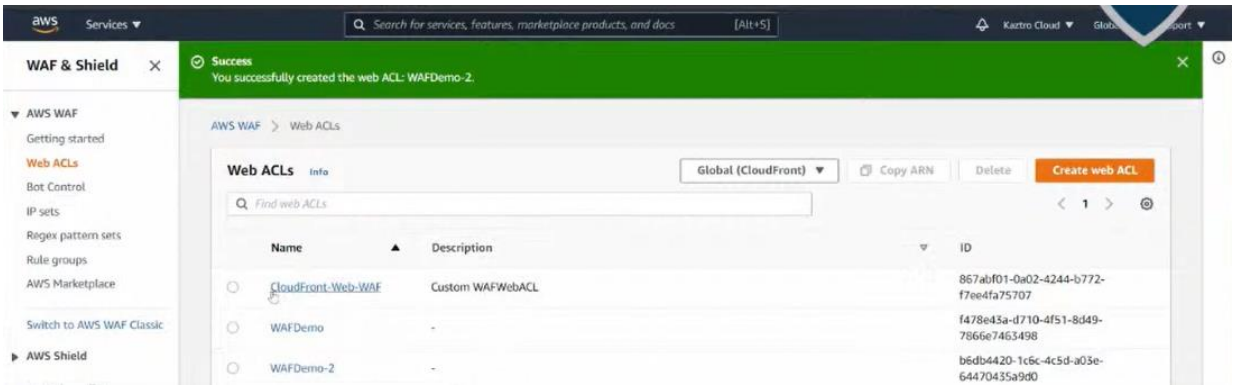


Paso 5: Configure metrics

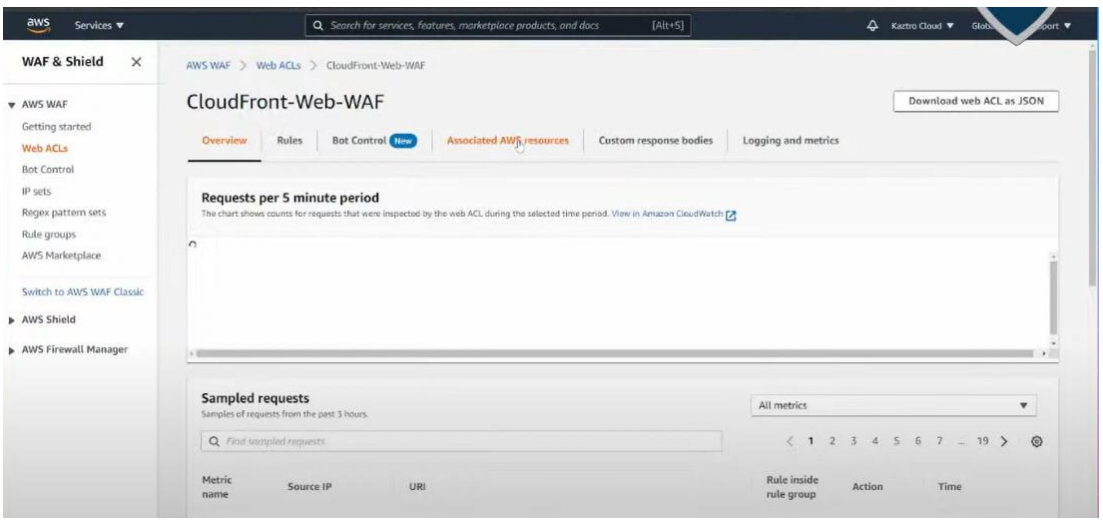
En la página **Review and create web ACL (Revisar y crear ACL web)**, revise la configuración y, a continuación, elija **Create web ACL (Crear ACL web)**.



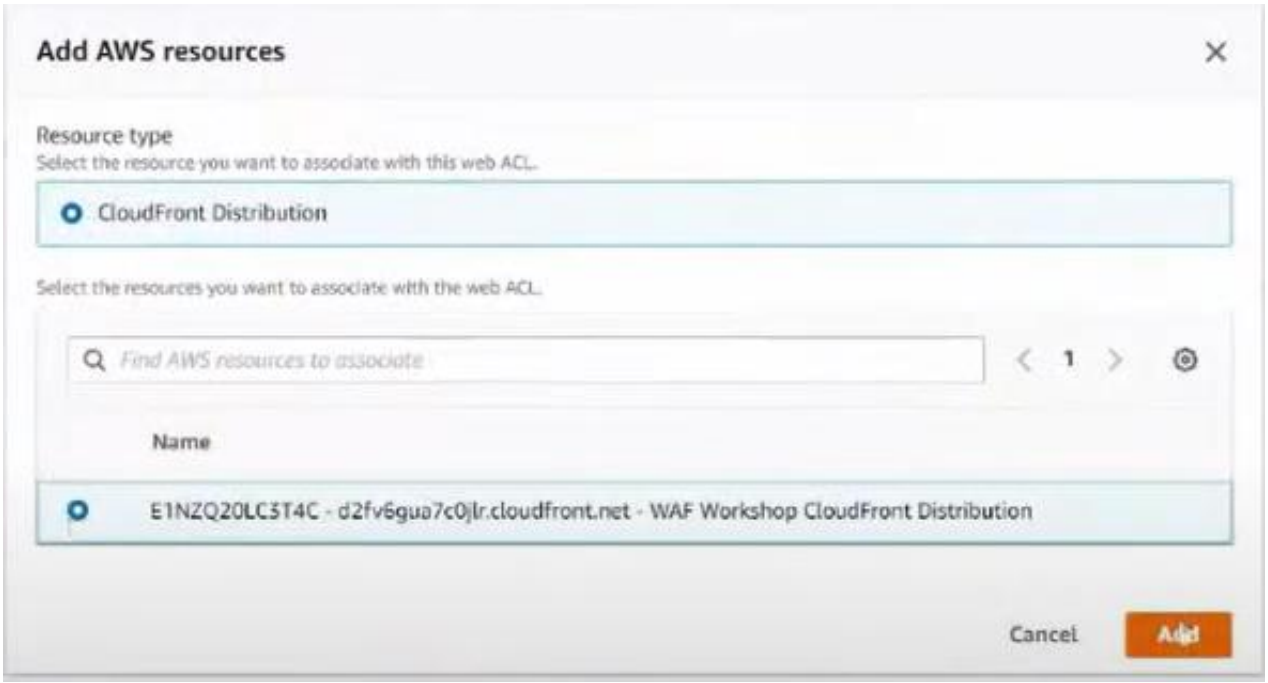
El asistente le devuelve a la página de **Web ACL (ACL web)**, donde aparece la nueva ACL Web. Desde el momento que yo creo mi web ACL y asocie el recurso que en este caso es la distribución de cloudFront, desde ese momento a un tiempo máximo de 1 minuto, ya la protección se ha activado.

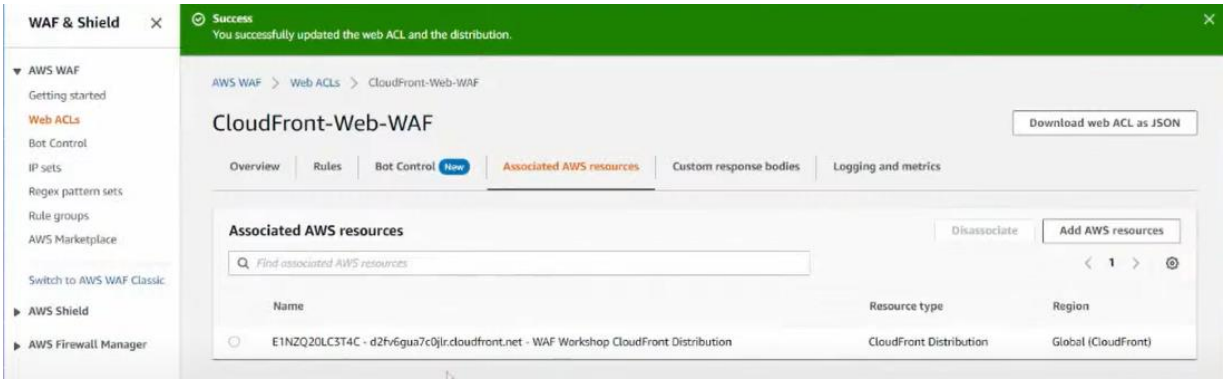


En el nuevo ACL se asocia los recursos.



Se asocia la distribución CloudFront



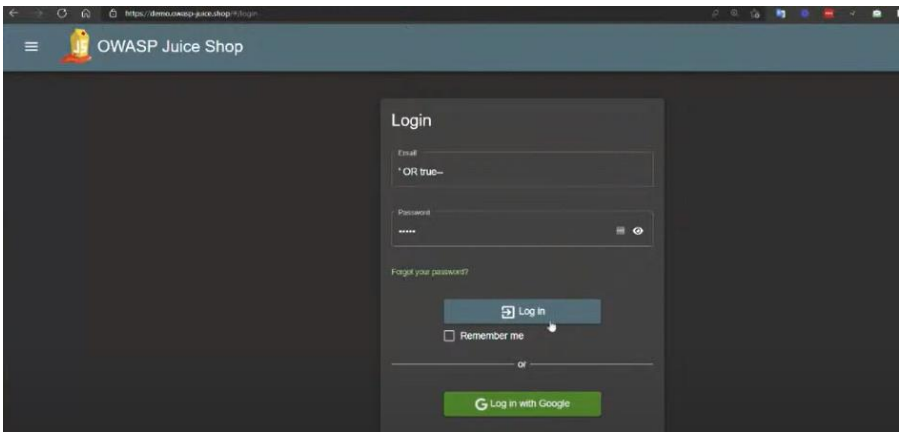


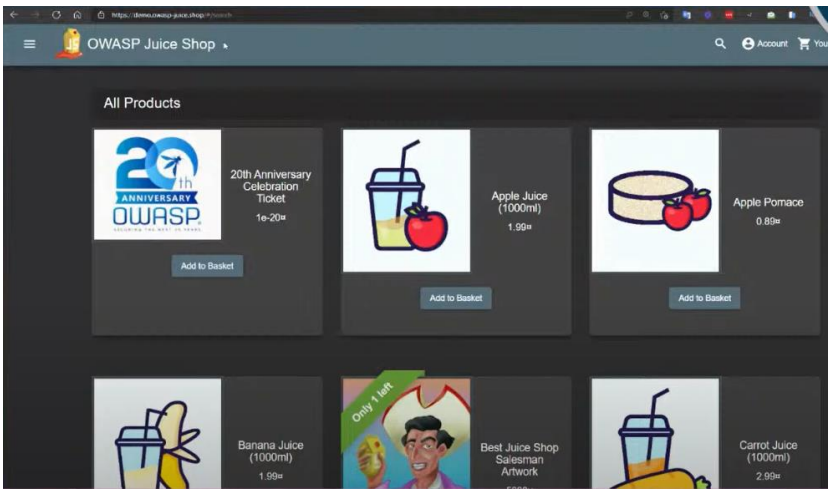
Aquí se describe una sql inyección básico. Y se escribe contraseña.

Y lo que se está haciendo aquí es enviar una inyección sql a este sitio original de owasp para poder verificar si es que puedo ingresar con un perfil de administrador sin haber tenido las credenciales correctas.

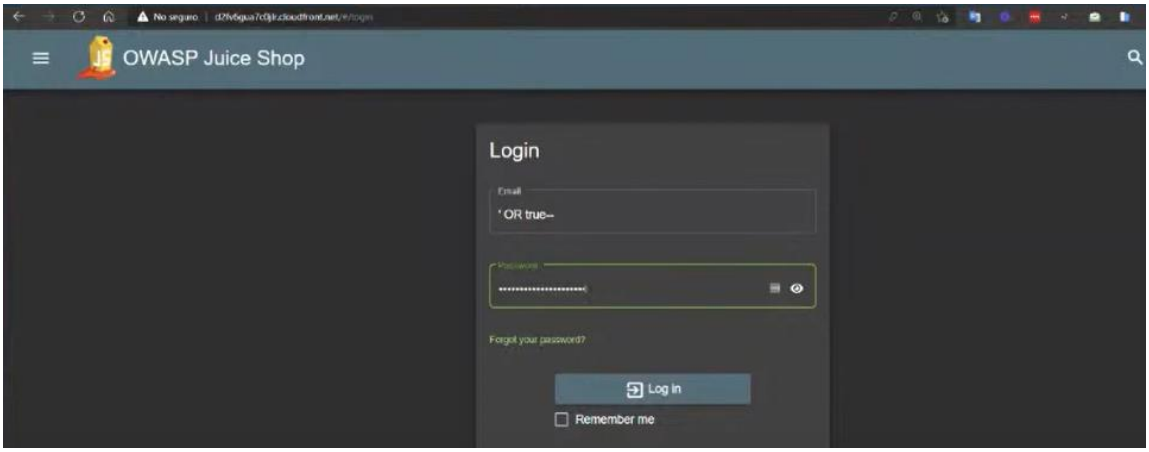
Le da click en login y evidentemente tiene acceso.

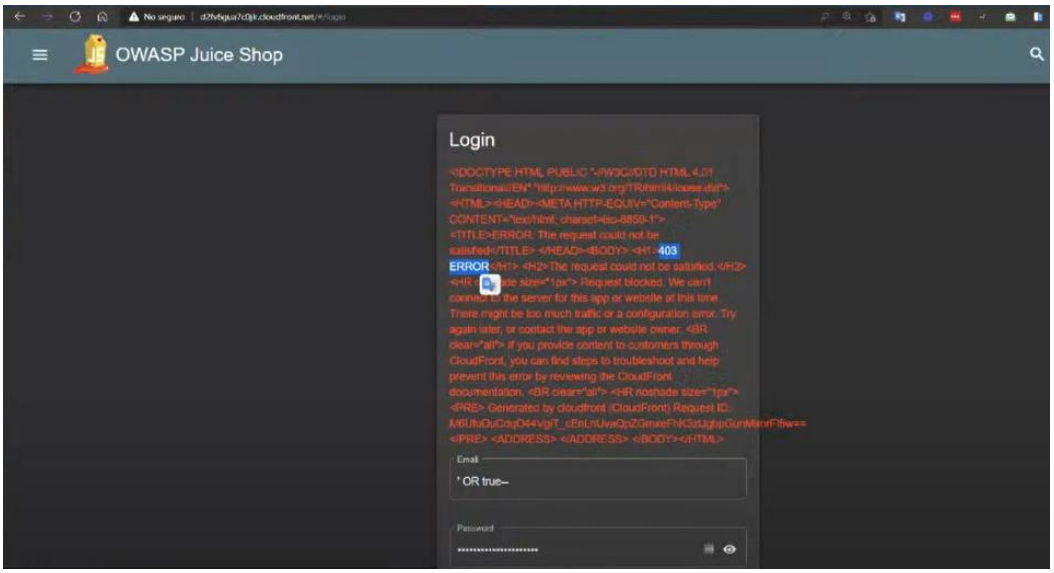
Aquí se tiene acceso hacia las aplicaciones a través de un ataque sql inyección.





Ahora nos vamos a la réplica que esta protegida con aws waf. Es decir que si hacemos ataque inyección y cualquier contraseña. Aquí genera error. Da un 403 que es un código http que indica que el request a sido bloqueada por una solución waf, que esta protegiendo y analizando el trafico que llega a esa aplicación.





URL o Urls en la que se basó para realizar la práctica.

- https://www.youtube.com/watch?v=dXlVtncc2vk
- https://www.youtube.com/watch?v=Ma3RZy1Ah68