27°

Lab - AWS re/Start

Malware de Firewall

SWIPE

Tarea 01

Protección contra Malware usando Netwrok AWS Firewall

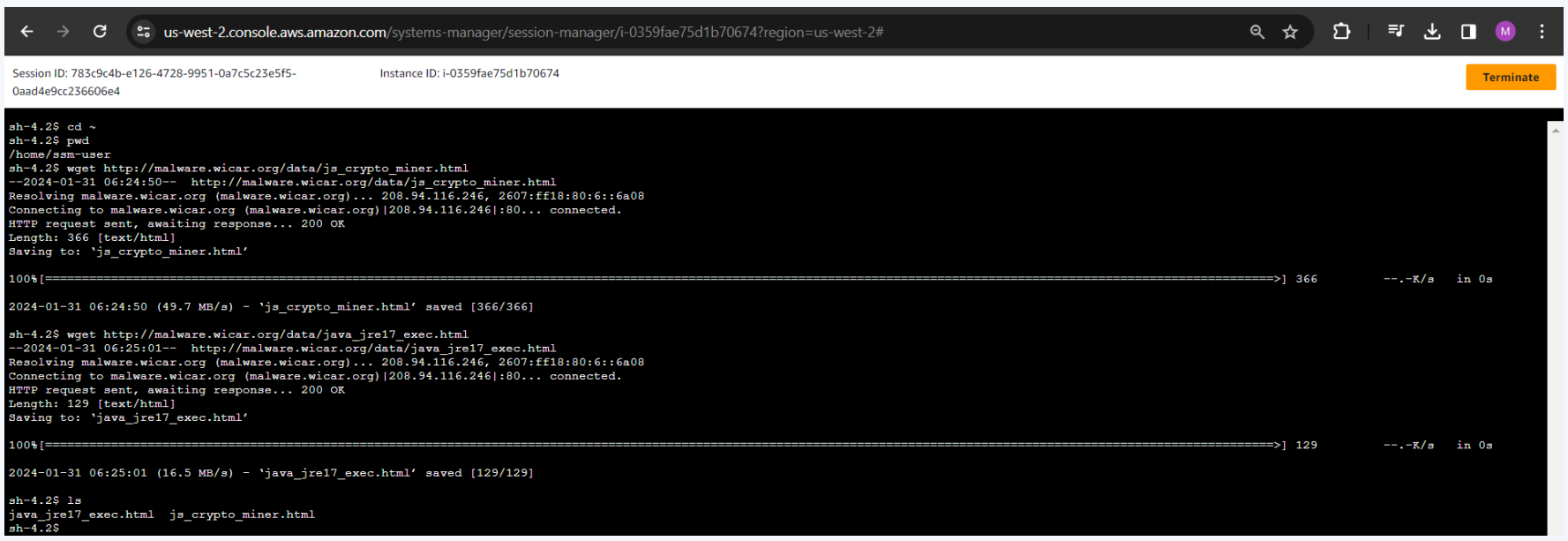
A continuación, se muestra los objetivos del laboratorio:

- Actualizar un firewall de red de AWS
- Crear un grupo de reglas de firewall
- Verificar y probar que el acceso a los sitios maliciosos esté bloqueado

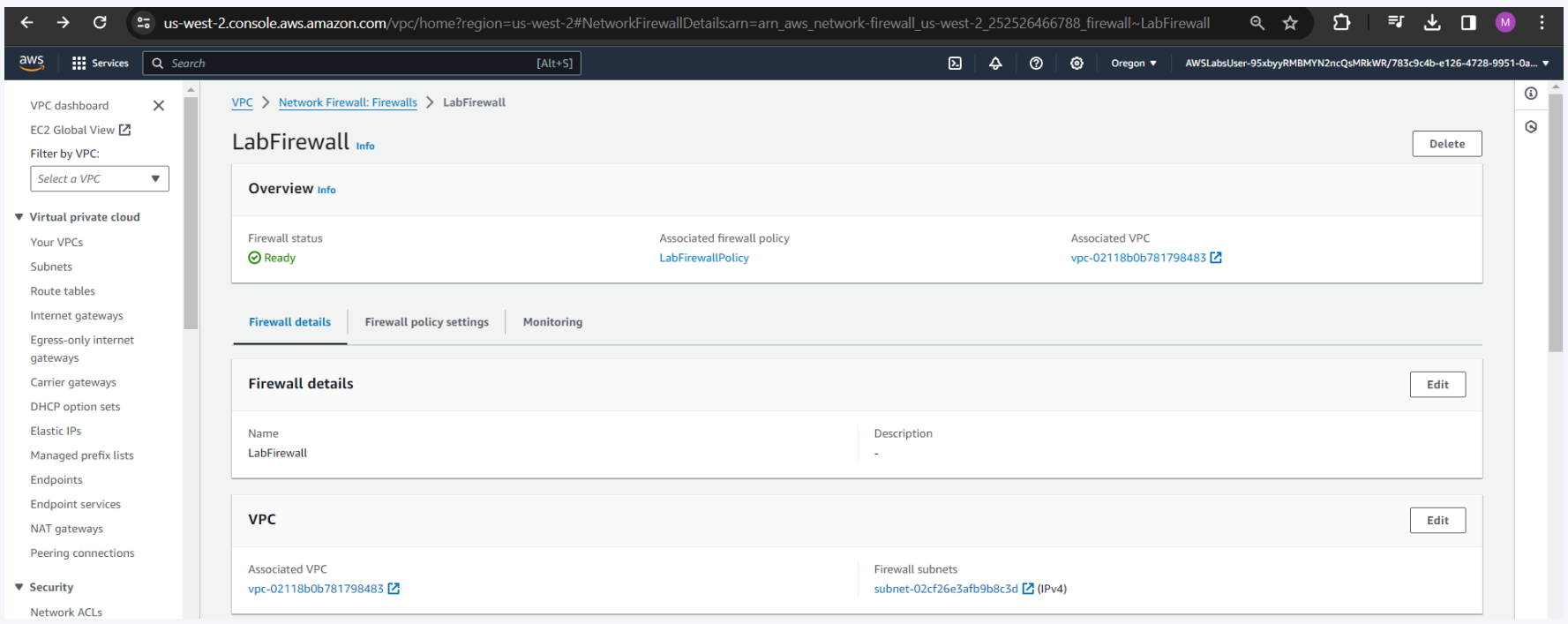
Nota. Un Malware es un software malicioso desarrollado por hacker, eg: virus, troyanos, spywares, adwares y ransomware. Mientras que los firewalls son como muros de seguridad físicos que se encuentran entre la red interna de la organización y cualquier red pública externa.

Tarea 01

Empezaremos confirmando la accesibilidad a la instancia de EC2 llamada **TestInstance**. Esto mediante *Session Manager*. Una vez conectados, procedemos a descargar un Malware:



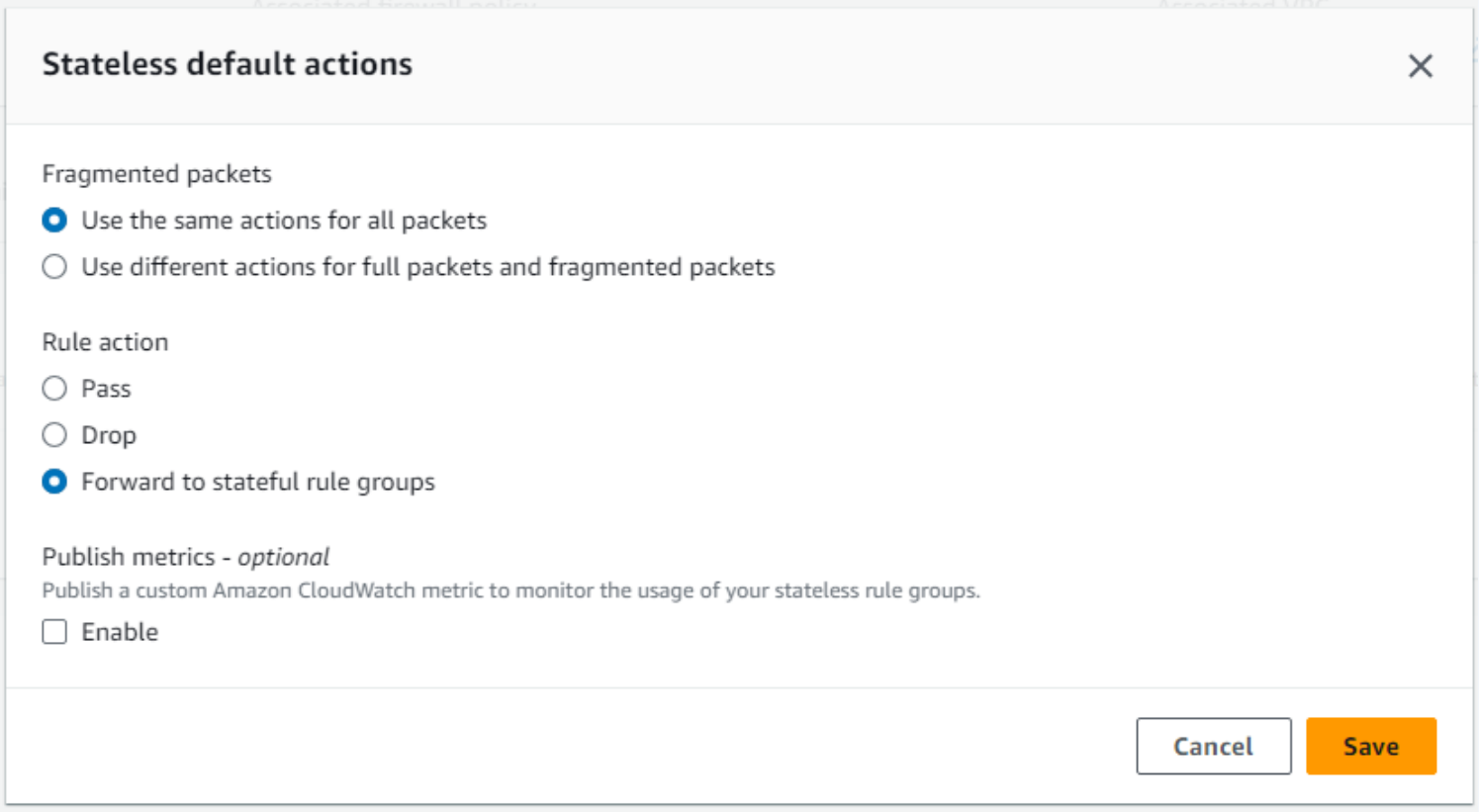
Esto solo con fines académicos, después de ello, procederemos a inspeccionar el firewall de la red



SWIPE

Tarea 01

Podemos ver que ya existe una política del firewall, la cual es la encargada de definir el comportamiento en una colección de grupos de reglas con estado (stateful) y sin estado (stateless), y otros ajustes. Asimismo, editamos las acciones sin estado predeterminadas:

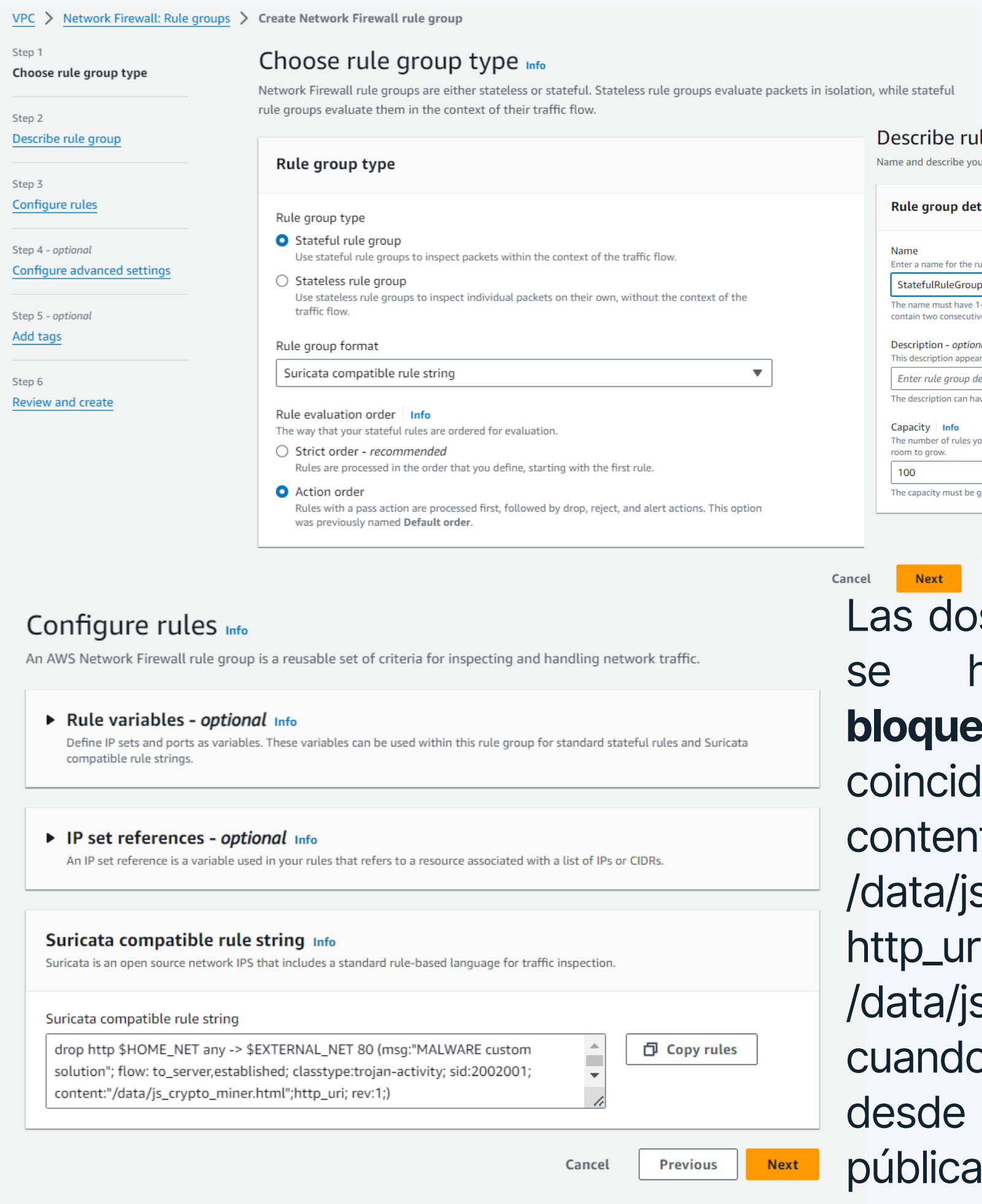


Ahora, procedemos a crear un grupo de reglas para el firewall, el cual te ayudará a bloquear el acceso a URLs maliciosos

SWIPE

Tarea 01

Esta es la configuración

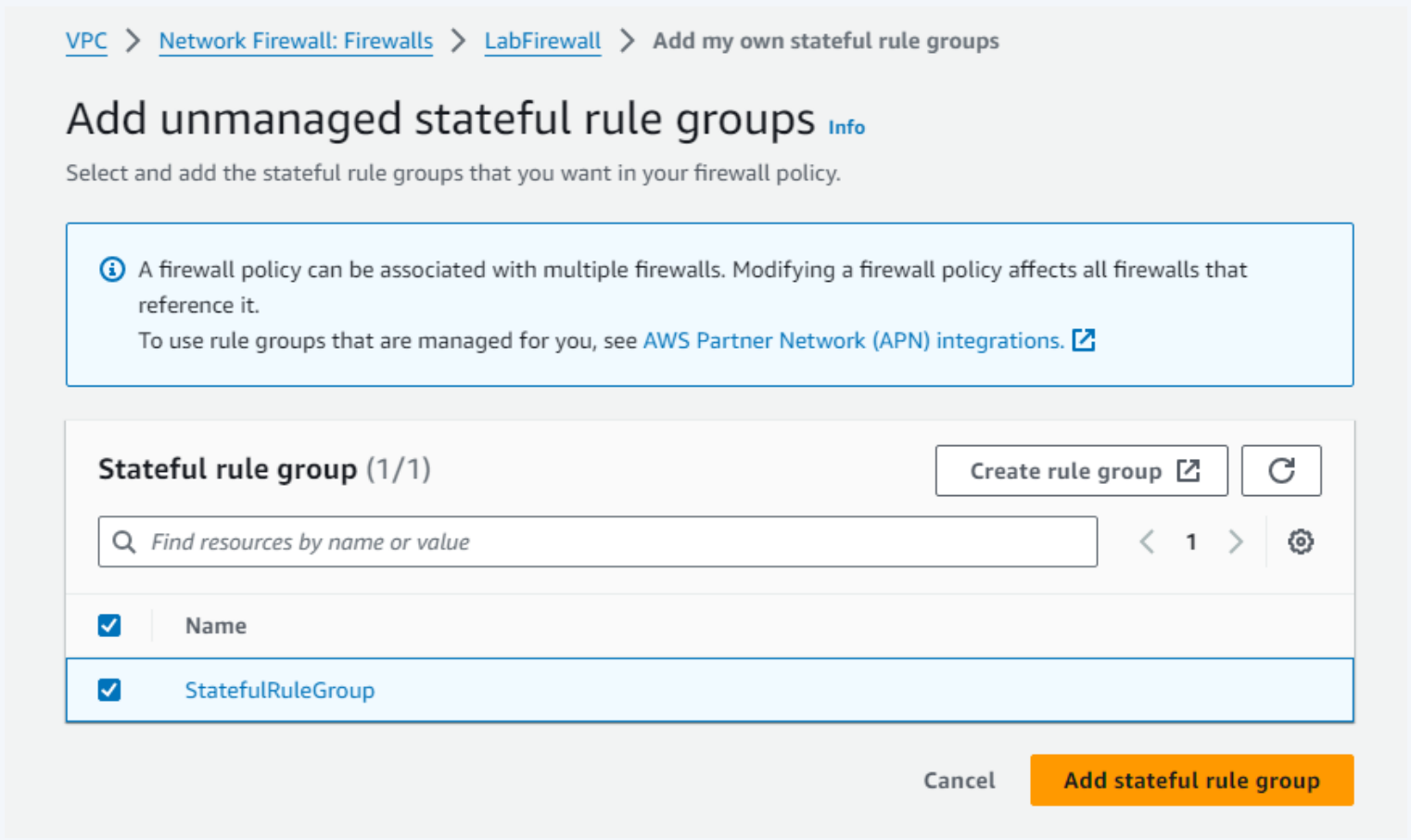


Las dos reglas de Suricata que se han añadido ahora **bloquean el tráfico** que coincide con las **URLs** http_uri contents /data/js_crypto_miner.html y http_uri contents /data/js_crypto_miner.html cuando el tráfico se inicia desde el LabVPC a la red pública.

SWIPE

Tarea 01

Ahora, asignamos el grupo de reglas a un firewall de red



Finalmente, validamos la solución. Y vemos que al momento de intentar descargar una parte del malware, ha sido bloqueado por el firewall de la red

Y removemos estos archivos de prueba

SWIPE