# PRÁCTICAS DE LABORATORIO

**Guillermina Antonaccio** 

Vigésimo sexto laboratorio (280):

Malware de Firewall







## Malware de Firewall:



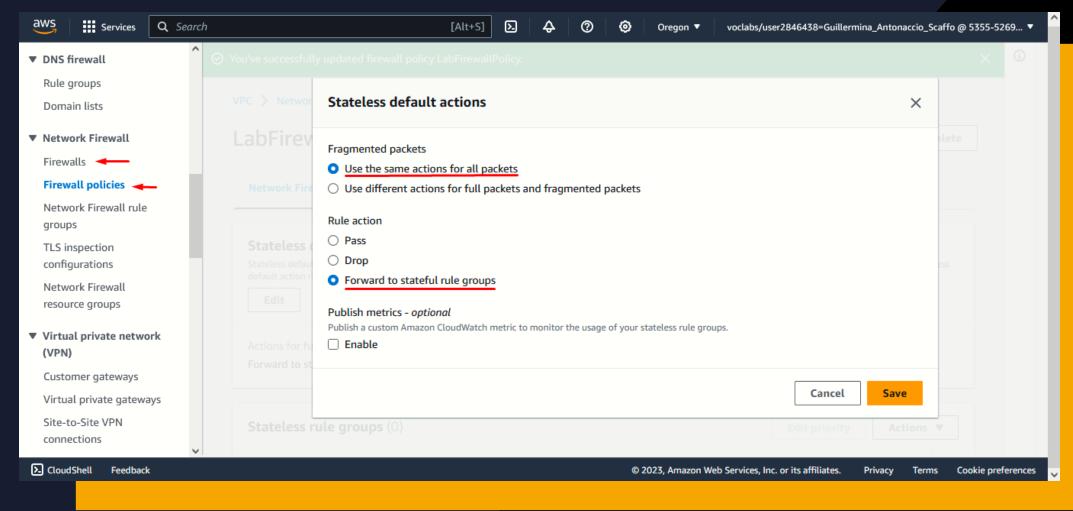
1-En esta tarea debíamos acceder a la instancia EC2 y utilizar el comando wget para descargar los archivos maliciosos y confirmar que se podía acceder a los mismos mediante la instancia de prueba que era igual a la de nuestra compañía (la cual tenía unas reglas de firewall que debíamos cambiar para que esto no suceda).

```
Session ID:
                                    Instance ID: i-0b2e3d782b53db48c
                                                                                                                                               Terminate
user2846438=Guillermina_Antonaccio_Scaffo-
010c7bd5692d1537b
sh-4.2$ cd
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ wget http://malware.wicar.org/data/js crypto miner.html
--2023-11-13 18:27:02-- http://malware.wicar.org/data/js crypto miner.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org) | 208.94.116.21 |: 80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 366 [text/html]
Saving to: 'js crypto miner.html'
                                                                                                                                  --.-K/s in 0s
2023-11-13 18:27:02 (44.3 MB/s) - 'js crypto miner.html' saved [366/366]
sh-4.2$ wget http://malware.wicar.org/data/java jre17 exec.html
--2023-11-13 18:27:27-- http://malware.wicar.org/data/java jre17 exec.html
Resolving malware.wicar.org (malware.wicar.org)... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org) | 208.94.116.21 |: 80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 129 [text/html]
Saving to: 'java jre17 exec.html'
                                                                                                                                  --.-K/s in 0s
2023-11-13 18:27:27 (15.5 MB/s) - 'java jre17 exec.html' saved [129/129]
sh-4.2$ ls
java jre17 exec.html js crypto miner.html
sh-4.2$
```





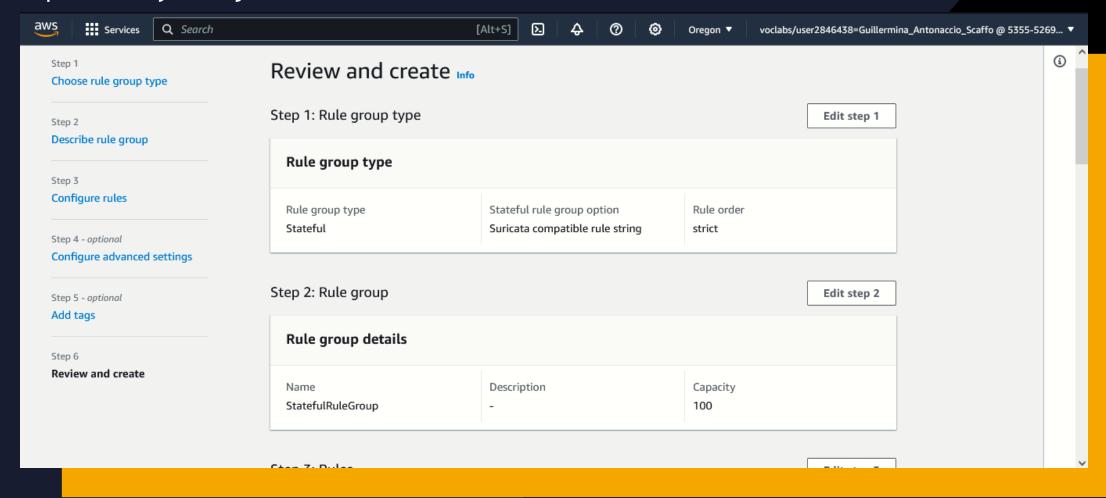
2-En la segunda tarea debíamos inspeccionar el Firewall de la red y actualizar la política para reenviar todos los paquetes a la inspección de reglas con estado. Estas configuraciones ahora reenvían todos los paquetes a un grupo de reglas con estado para su posterior inspección (stateful significa con estado).







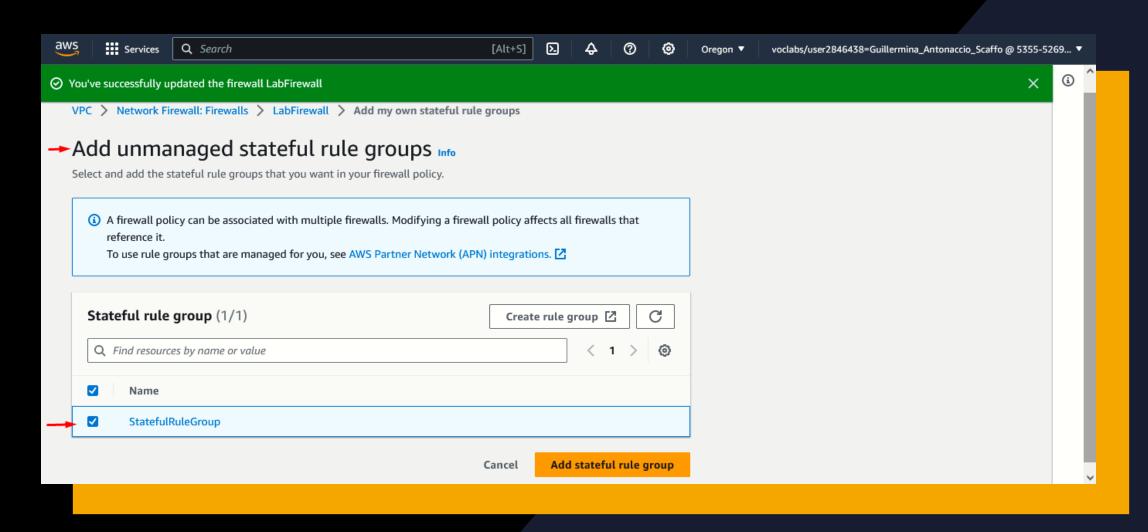
3-En esta tarea debíamos crear un grupo con reglas de firewall de red con estado, que bloquearan el acceso a las URL maliciosas que descargamos en la tarea 1.Es un conjunto reutilizable de criterios para inspeccionar y manejar el tráfico de red.





# Malware de Firewall:

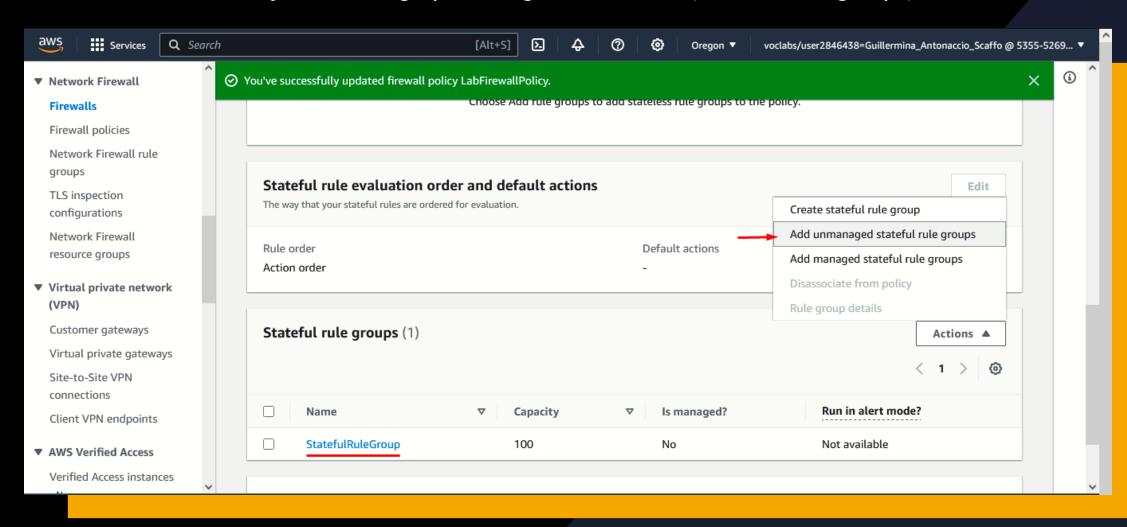
4-Aquí se nos pide adjuntar el grupo con reglas de firewall, al firewall de red. Este grupo bloquea los intentos de acceder a los archivos de actores maliciosos alojados en el sitio web.







4-Así se ve una vez adjuntado, el grupo de reglas con estado(stateful rule groups) al firewall.



## Malware de Firewall:



5-En la última tarea debíamos volver a entrar a la instancia para comprobar que el firewall de red bloqueara correctamente los intentos de acceder a los archivos maliciosos, logramos que lo hiciera ya que nos decía que estaba esperando la respuesta (el firewall los estaba bloqueando).

```
Session ID:
                                    Instance ID: i-0b2e3d782b53db48c
user2846438=Guillermina_Antonaccio_Scaffo-
0930276d29c409474
sh-4.2$ pwd
/home/ssm-user
sh-4.2$ wget http://malware.wicar.org/data/js crypto miner.html
--2023-11-13 19:08:08-- http://malware.wicar.org/data/js crypto miner.html
Resolving malware.wicar.org (malware.wicar.org) ... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org) | 208.94.116.21 |: 80... connected.
HTTP request sent, awaiting response... ^C
sh-4.2$ wget http://malware.wicar.org/data/java jre17 exec.html
--2023-11-13 19:08:36-- http://malware.wicar.org/data/java jre17 exec.html
Resolving malware.wicar.org (malware.wicar.org) ... 208.94.116.21, 2607:ff18:80::615
Connecting to malware.wicar.org (malware.wicar.org) | 208.94.116.21 |: 80... connected.
HTTP request sent, awaiting response... ^C
sh-4.2$ ls
java jre17 exec.html js crypto miner.html
sh-4.2$ rm java jre17 exec.html js crypto miner.html
sh-4.2$ ls
sh-4.2$ El malware fue bloqueado y eliminado correctamente!
```



# Aquí termina el laboratorio, muchas gracias