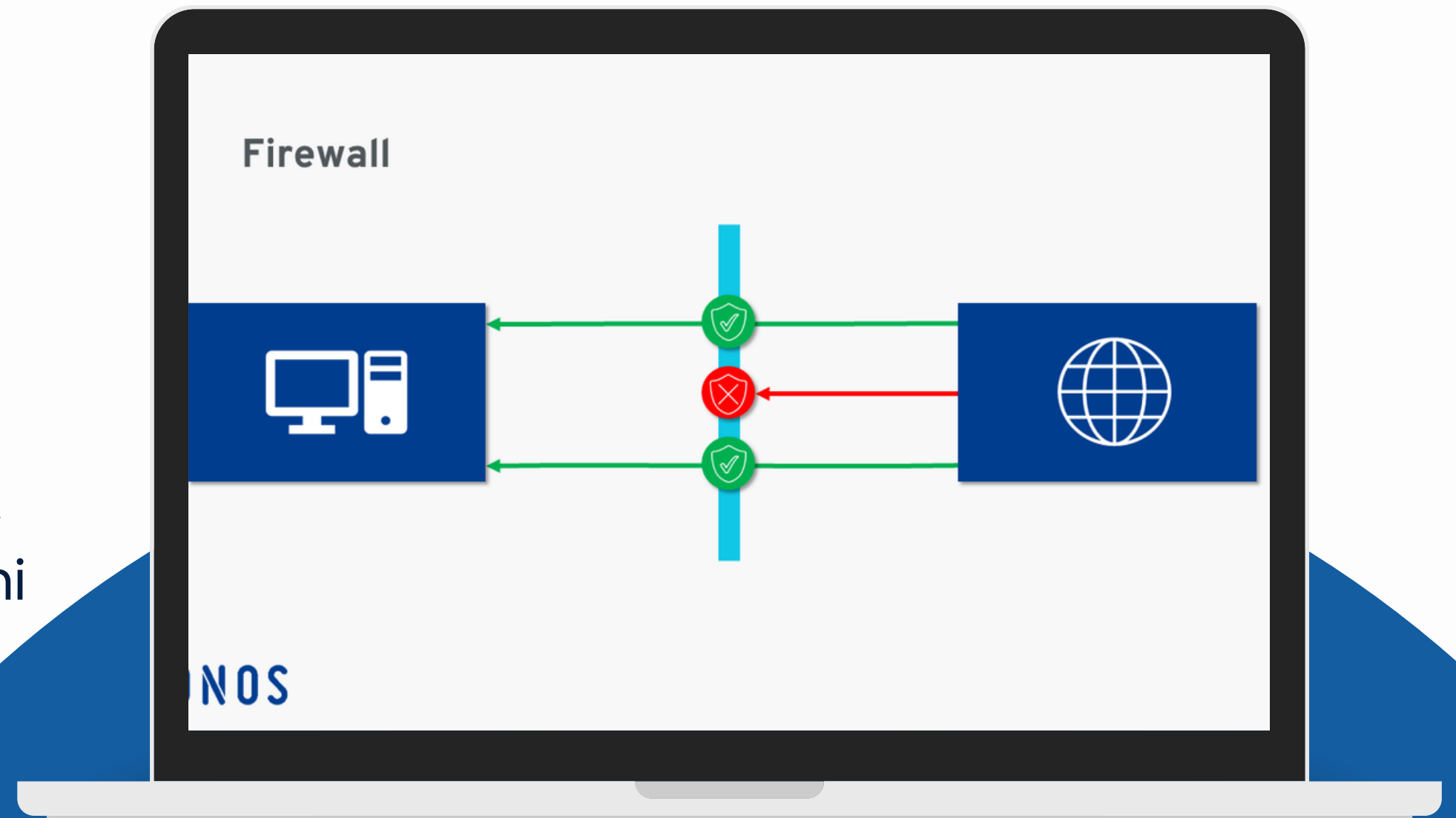




# Lab - Malware de firewall

Presentación realizada por Brendon Buriol, Paulo Sena, Ignivé Amaro y Valeria Cantoni



# Objetivos

Después de completar esta práctica de laboratorio, debería poder:

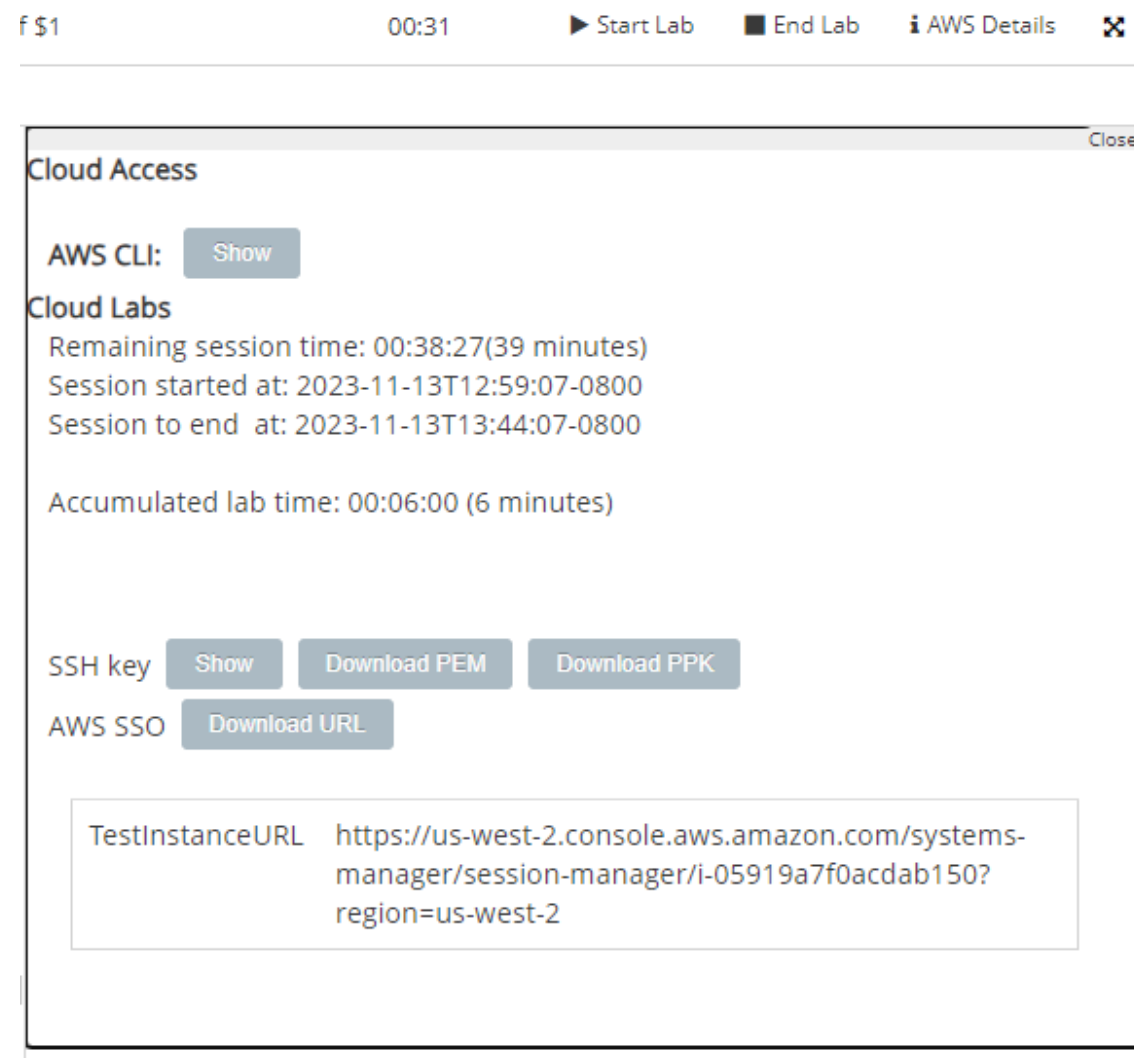
- Actualizar un firewall de red
- Crear un grupo de reglas de firewall
- Verifique y pruebe que el acceso a sitios maliciosos esté bloqueado

## Guión

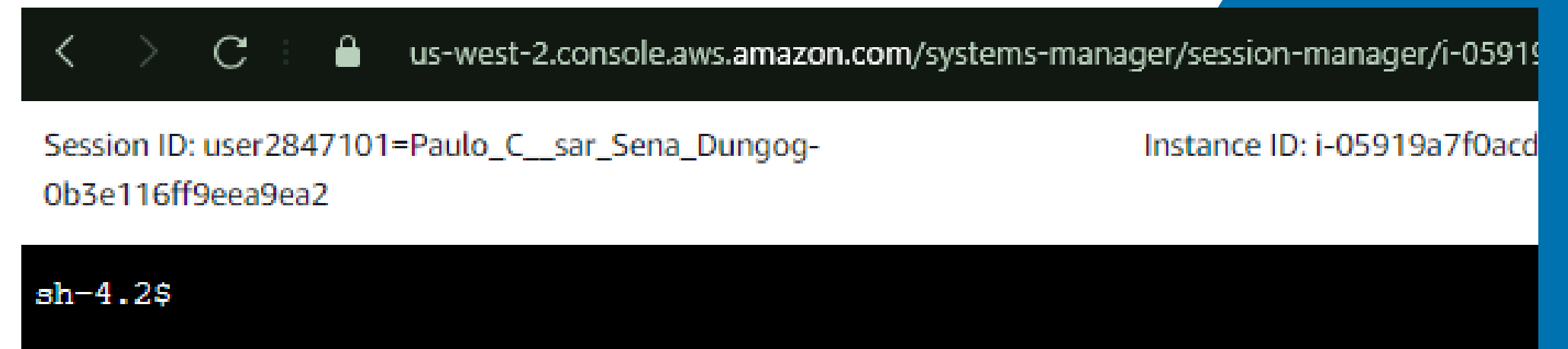
AnyCompany lo contrató como nuevo ingeniero de seguridad y le asignó la tarea de reforzar el perímetro de seguridad de la empresa. Ha habido informes de usuarios que descargaron accidentalmente malware después de acceder a sitios web específicos. El equipo de TI de AnyCompany le ha proporcionado las URL de los sitios que alojan el malware. Es su trabajo encontrar una solución para mitigar el acceso a estos archivos de actores maliciosos.

# Tarea 1: Confirmar la accesibilidad

Para iniciar la tarea hay que ir al botón AWS Details y pegar en el buscador TestInstanceURL



Debería verse así:



Para cambiar el directorio y ver el trabajo actual ejecutamos el siguiente comando:

```
cd ~  
pwd
```

```
sh-4.2$ cd ~  
sh-4.2$ pwd  
/home/ssm-user  
sh-4.2$
```

El siguiente paso replica cómo un usuario final descargaría un archivo malicioso usando un navegador web. La acción se simula usando el comando `wget` en los archivos maliciosos en la línea de comandos.

En este entorno de laboratorio protegido, ingrese el siguiente código y presione Intro para descargar parte del malware:

```
wget http://malware.wicar.org/data/js_crypto_miner.html
```

```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html  
--2023-11-13 21:16:33-- 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'  
  
100%[=====]  
  
2023-11-13 21:16:34 (46.3 MB/s) - 'js_crypto_miner.html' saved [366/366]  
  
sh-4.2$
```

Luego ingresamos el siguiente código para descargar el resto del malware:

```
wget http://malware.wicar.org/data/java_jre17_exec.html
```

```
sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2023-11-13 21:17:27-- 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'

100%[=====]

2023-11-13 21:17:27 (6.32 MB/s) - 'java_jre17_exec.html' saved [129/129]

sh-4.2$
```

Por último se ejecuta el siguiente comando:

```
ls
```

```
sh-4.2$ ls
java_jre17_exec.html  js_crypto_miner.html
sh-4.2$
```

## Tarea 2: inspeccionar el firewall de la red

- En la consola buscar y entrar en VPC y NETWORK FIREWALL
- Despues hay seleccionar el LabFirewall

### ▼ Network Firewall

#### Firewalls

Firewall policies

Network Firewall rule groups

TLS inspection configurations

Network Firewall resource groups

VPC > Network Firewall: Firewalls

### Firewalls Info

This page lists your firewalls in AWS Network Firewall.

#### Firewalls (1)

🔍 Find by keyword

Name

☐ LabFirewall

VPC > Network Firewall: Firewalls > LabFirewall

### LabFirewall Info

#### Overview Info

Firewall status

🟢 Ready

Firewall details

**Firewall policy settings**

Monitoring

#### Stateless default actions

Stateless default actions determine how Network Firewall should handle packets that don't

Actions for full packets

Pass

Para Stateless default actions hay que configurar lo siguiente:

- En **Fragmented packets** selecciona Use the same actions for all packets
- Luego en **Rule action** selecciona Forward to stateful rule groups

Stateless default actions

Fragmented packets

☒ Use the same actions for all packets

☐ Use different actions for full packets and fragmented packets

Rule action

☐ Pass

☐ Drop

☒ Forward to stateful rule groups

Publish metrics - optional

Publish a custom Amazon CloudWatch metric to monitor the usage of your stateless rule groups.

☐ Enable

Cancel

Save



# Tarea 3: crear un grupo de reglas de firewall

En el panel izquierdo seleccionamos Firewall Rule Groups y clicar el botón de Create Network Firewall rule group

Ahora configuramos se la siguiente forma:

- Para Rule group type seleccionar seleccione Stateful rule group

▼ Network Firewall

Firewalls

Firewall policies

Network Firewall rule groups

TLS inspection configurations

Network Firewall resource groups

VPC > Network Firewall: Rule groups

Rule groups [Info](#)

A rule group is a reusable set of firewall rules for inspecting and filtering network traffic. You can use stateless or stateful rule groups to configure the traffic inspection criteria for your firewall policies. You can create your own rule groups or you can use rule groups that are managed by AWS Marketplace Sellers.

Your rule groups

AWS managed rule groups

The following table lists all of your rule groups.

Add rule groups to policy

Your rule groups (0)

Delete

Create rule group

Find resources by name or value

< 1 > ⚙

Name	Type
No rule groups	
You don't have any rule groups.	
<div>Create rule group</div>	

# Tarea 3: crear un grupo de reglas de firewall

Es importante que sigas esta configuración:

- Stateful rule group
- Suricata compatible rule string
- Action order

## Choose rule group type [Info](#)

Network Firewall rule groups are either stateless or stateful. Stateless rule groups evaluate packets in isolation, while stateful rule groups evaluate them in the context of their traffic flow.

### Rule group type

Rule group type

- ☒ Stateful rule group  
Use stateful rule groups to inspect packets within the context of the traffic flow.
- ☐ Stateless rule group  
Use stateless rule groups to inspect individual packets on their own, without the context of the traffic flow.

Rule group format

Suricata compatible rule string ▼

Rule evaluation order [Info](#)

The way that your stateful rules are ordered for evaluation.

- ☐ Strict order - *recommended*  
Rules are processed in the order that you define, starting with the first rule.
- ☒ Action order  
Rules with a pass action are processed first, followed by drop, reject, and alert actions. This option was previously named **Default order**.

Cancel

Next

En la sección Stateful rule group seleccionar de la siguiente manera:

- Name: StatefulRuleGroup
- Capacity: ingresar 100
- tateful rule group options: seleccionar Suricata compatible IPS rules
- En Suricata compatible IPS rules: el siguiente código:

```
drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution"; flow:
to_server,established; classtype:trojan-activity; sid:2002001;
content:"/data/js_crypto_miner.html";http_uri; rev:1;)
```

```
drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom solution"; flow:
to_server,established; classtype:trojan-activity; sid:2002002;
content:"/data/java_jre17_exec.html";http_uri; rev:1;)
```

# Edita la parte de Rule gruop details

## Describe rule group [Info](#)

Name and describe your rule group so you can easily identify it and distinguish it from other resources.

### Rule group details

#### Name

Enter a name for the rule group that's unique within your stateful rule groups.

StatefulRuleGroup

The name must have 1-128 characters. Valid characters: a-z, A-Z, 0-9 and - (hyphen). The name can't start or end with a hyphen, and it can't contain two consecutive hyphens.

#### Description - optional

This description appears when you view this rule group's details. It can help you quickly identify what your rule group is used for.

Enter rule group description

The description can have 0-256 characters.

#### Capacity [Info](#)

The number of rules you expect to have in this rule group during its lifetime. You can't change capacity after rule group creation, so leave room to grow.

100

The capacity must be greater than or equal to 1 and less than 30,000.

Cancel

Previous

Next

## Configure rules [Info](#)

An AWS Network Firewall rule group is a reusable set of criteria for inspecting and handling network traffic.

### ► Rule variables - optional [Info](#)

Define IP sets and ports as variables. These variables can be used within this rule group for standard stateful rules and Suricata compatible rule strings.

### ► IP set references - optional [Info](#)

An IP set reference is a variable used in your rules that refers to a resource associated with a list of IPs or CIDRs.

### Suricata compatible rule string [Info](#)

Suricata is an open source network IPS that includes a standard rule-based language for traffic inspection.

#### Suricata compatible rule string

```
drop http $HOME_NET any -> $EXTERNAL_NET 80 (msg:"MALWARE custom  
solution"; flow: to_server,established; classtype:trojan-activity; sid:2002002;  
content:"/data/java_jre17_exec.html";http_uri; rev:1;)
```

 Copy rules

Cancel

Previous

Next

En Add tags escribir sala 3 y value 1

Add tags - optional

Info

A tag is a label that you assign to an AWS resource. You can use tags to search and filter your resources or track your AWS costs.

Add tags - optional

Key

sala 3

Value - optional

1

Remove tag

Add tag

You can add up to 49 more tags.

Cancel

Previous

Next

Suricata compatible rule string

drop http \$HOME\_NET any -> \$EXTERNAL\_NET 80 (msg:"MALWARE custom solution"; flow: to\_server,established; classtype:trojan-activity; sid:2002002; content:"/data/java\_jre17\_exec.html";http\_uri; rev:1;)

Step 4: Advanced settings

Edit step 4

Customer managed key

Key type

AWS owned key

Step 5: Tags

Edit step 5

Rule group tags (1)

< 1 > ⚙

Key

Value

-

Cancel

Previous

Create rule group

Finalmente seleccionar Create stateful rule group

Si no te deja crearlo hay que ir a Rule evaluation orden y seleccionar Action orden

# Choose rule group type [Info](#)

Network Firewall rule groups are either stateless or stateful. Stateless rule groups evaluate packets in isolation, while stateful rule groups evaluate them in the context of their traffic flow.

## Rule group type

Rule group type

- ☒ Stateful rule group  
Use stateful rule groups to inspect packets within the context of the traffic flow.
- ☐ Stateless rule group  
Use stateless rule groups to inspect individual packets on their own, without the context of the traffic flow.

Rule group format

Suricata compatible rule string ▼

Rule evaluation order [Info](#)

The way that your stateful rules are ordered for evaluation.

- ☐ Strict order - *recommended*  
Rules are processed in the order that you define, starting with the first rule.
- ☒ Action order  
Rules with a pass action are processed first, followed by drop, reject, and alert actions. This option was previously named **Default order**.

Cancel

Next

✔ Ha creado correctamente grupo de reglas IngresarStatefulRuleGroup.

VPC > Grupos de reglas de Network Firewall

## Tarea 4: Adjuntar un grupo de reglas al firewall de la red

- En el panel de navegación izquierdo en NETWORK FIREWALL seleccionar Firewalls
- Despues seleccionar LabFirewall
- Luego en la lista del desplegabñe de Add rule groups seleccionar Agregar desde grupos de reglas con estado existentes

### ▼ Network Firewall

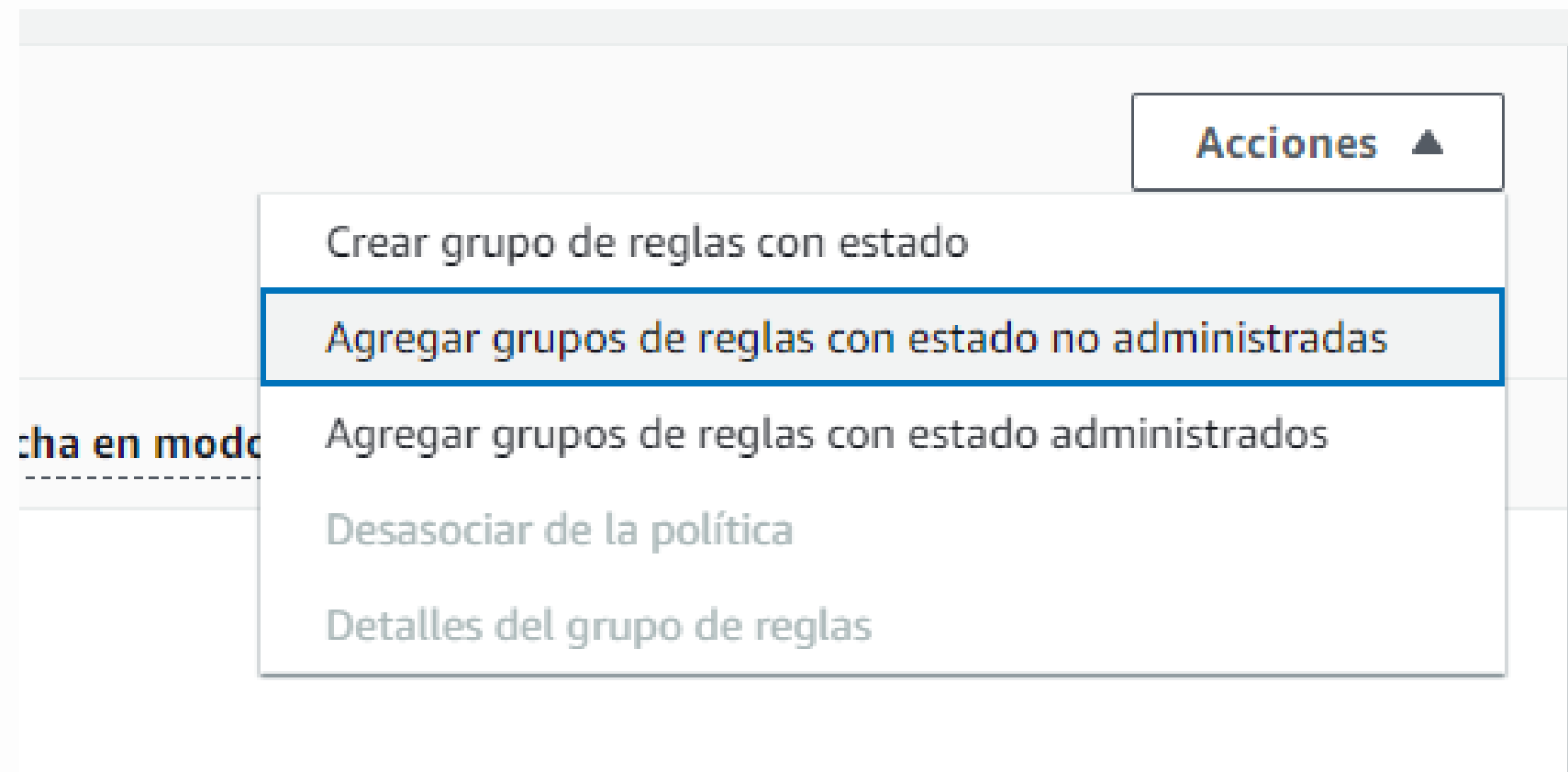
#### Firewalls

Políticas de firewall

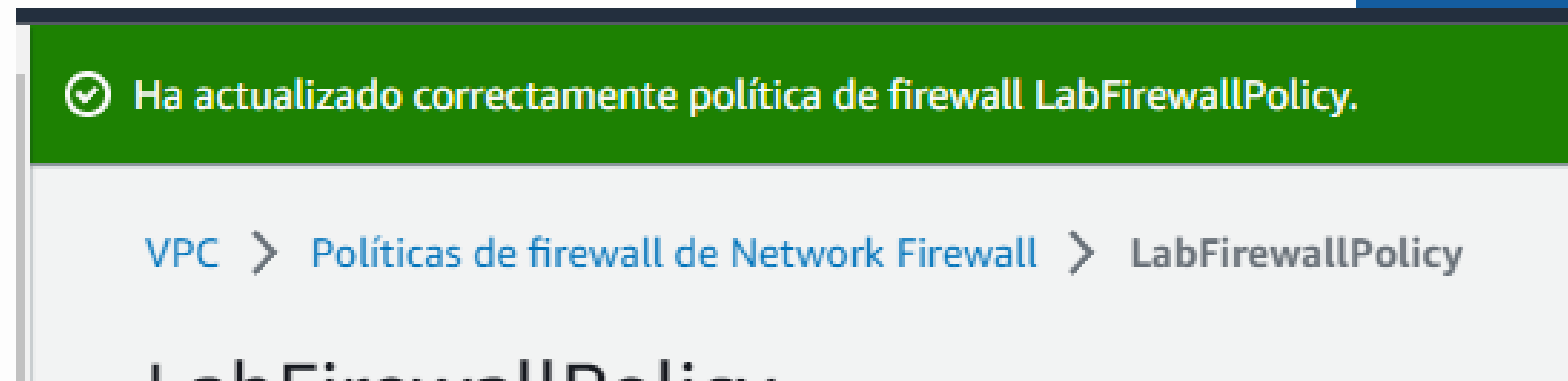
Grupos de reglas de  
Network Firewall

Configuraciones de  
inspección de TLS

Grupos de recursos de  
firewall de red




En la parte superior debería salir un cartel el verde de **You successfully updated FirewallPolicy** y al desplazarnos hacia la seccion Stateful rule groups para ver que el grupo de reglas se agrego correctamente



## Agregar grupos de reglas con estado no administradas [Información](#)

Seleccione y agregue los grupos de reglas con estado que desee en la política de firewall.

 Una política de firewall se puede asociar a varios firewalls. La modificación de una política de firewall afecta a todos los firewalls que hacen referencia a ella.  
Para utilizar grupos de reglas administrados por usted, consulte las [integraciones de la red de socios de AWS \(APN\)](#).  
[🔗](#)

### Grupo de reglas con estado (1/1)

[Crear grupo de reglas](#) 



 *Buscar recursos por nombre o valor*

 1 



☒ Nombre

☒ IngresarStatefulRuleGroup

Cancelar

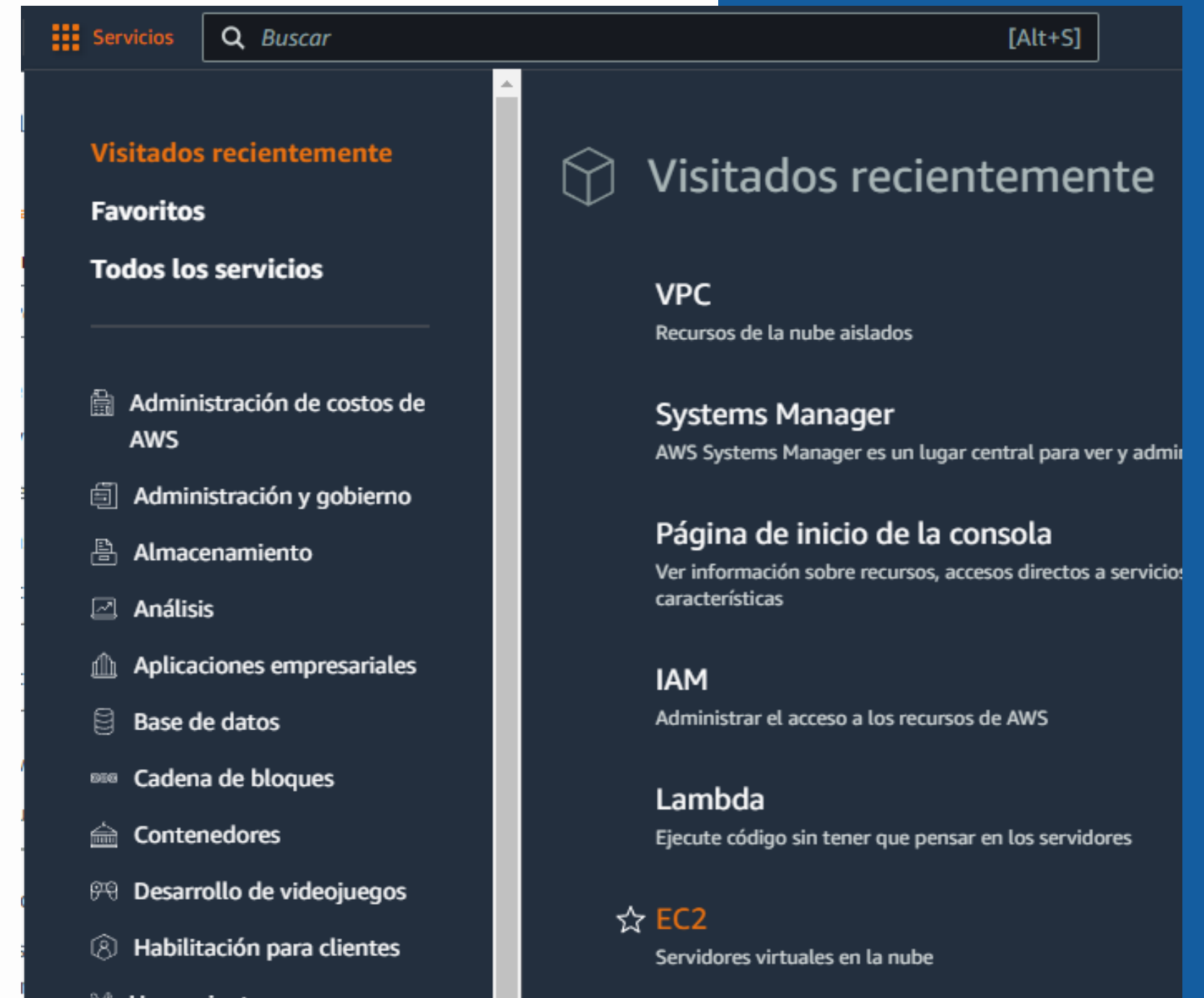
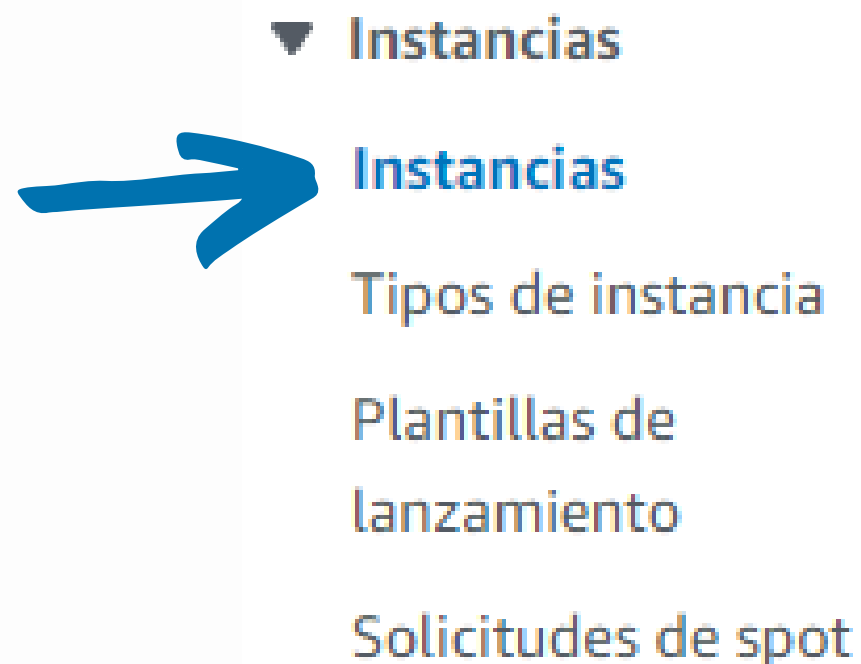
**Agregar un grupo de reglas con estado**



## Tarea 5: Validar la solución

En esta tarea, volverá a iniciar sesión en TestInstance para probar que el firewall de red bloquee correctamente los intentos de acceder a los archivos del sitio web malicioso.

- En la consola de administración de AWS, ingrese EC2 en la barra de búsqueda y luego seleccione EC2.
- En el panel de navegación izquierdo seleccionamos Instances



- Seleccionamos el check de la instancia nombrada TestInstance
- Luego presionamos sobre Conectar

Instancias (1/1) [Información](#)

🔍

Buscar Instance por atributo o etiqueta (case-sensitive)

<input checked="" type="checkbox"/>	Name <a href="#">✎</a> ▼	ID de la instancia	Estado de la i... ▼	Tipo de inst... ▼	Comprobación ...	Estado de la ...	Zona de dispo
<input checked="" type="checkbox"/>	TestInstance	i-0e53a6b05640b6271	✔ En ejecución <a href="#">🔍</a> <a href="#">🔍</a>	t2.micro	✔ 2/2 comprobaci...	Sin alarmas <a href="#">+</a>	us-west-2a

- Vamos a la pestaña que dice Session Manager
- Presionamos sobre Connect

Connect to instance [Info](#)

Connect to your instance i-05919a7f0acdab150 (TestInstance) using any of these options

EC2 Instance Connect

**Session Manager**

SSH client

EC2 serial console

Session Manager usage:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) [🔗](#) page.

Cancel

Connect

- Para intentar acceder al primer archivo malicioso, ejecutamos el siguiente comando wget

```
wget http://malware.wicar.org/data/js_crypto_miner.html
```

- Para probar el acceso a la otra URL maliciosa, ejecutamos el siguiente comando:

```
wget http://malware.wicar.org/data/java_jre17_exec.html
```

- Para probar el acceso a la otra URL maliciosa, ejecutamos el siguiente comando:

```
rm java_jre17_exec.html js_crypto_miner.html
```

```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2023-11-13 22:01:08--  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...
```

```
sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2023-11-13 22:02:09--  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
```

```
rm java_jre17_exec.html js_crypto_miner.html
ls
```

- Para confirmar que los archivos fueron eliminados, ejecutamos el comando ls

ls

```
chgrp      flock      kbdinfo    nf-log      ps
chmem      fmt        kbdrate    nf-monitor  psed
chmod      fold       kernel-install  nf-queue    psfaddtable
chown      free       keyctl     nfsiostat-sysstat  psfgettable
chronyc    funzip     kill       ngettext    psfstriptime
chrt       gappliation  killall    nice         psfxtable
chvt       gawk       kmod       nisdomainname  pstree
cifsiostat gdbm_dump  last       nl           pstree.x11
cksum      gdbm_load  lastb      nl-addr-add  pstruct
clear      gdbmtool   lastcomm   nl-addr-delete  ptx
cloud-id   gdbus      lastlog    nl-addr-list  pwd
cloud-init gencat     lchfn      nl-class-add  pwdx
cloud-init-per  genl-ctrl-list  lchsh      nl-class-delete  pwmame
cmp        geoiplookup  ld         nl-class-list  pwscore
cmsutil    geoiplookup6  ld.bfd     nl-classid-lookup  pydoc
col        geoipupdate  ldd        nl-cls-add     pydoc3
colcrt     geqn       less       nl-cls-delete  pydoc3.7
colrm      getconf    lessecho   nl-cls-list    pyrsa-decrypt-2
column     getent     lesskey    nl-fib-lookup  pyrsa-decrypt-bigfile-2
comm       getfacl    lesspipe.sh  nl-link-enslave  pyrsa-encrypt-2
command    getkeycodes  lexgrog    nl-link-ifindex2name  pyrsa-encrypt-bigfile-2
coredumpctl  getopt     link       nl-link-list    pyrsa-keygen-2
cp         getopt     linux-boot-prober  nl-link-name2ifindex  pyrsa-priv2pub-2
cpio       getopts    linux32    nl-link-release  pyrsa-sign-2
cpupower   gettext    linux64    nl-link-set     pyrsa-verify-2
crlutil    gettext.sh  ln         nl-link-stats   pystache
crontab    gio        loadkeys   nl-list-caches  pystache-3
csh        gio-querymodules-64  loadunimap  nl-list-sockets  pystache-test
csplit     glib-compile-schemas  locale      nl-monitor      pystache-test-3
csslint-0.6  gmake      locate     nl-neigh-add    python
curl       gneqn      localectl  nl-neigh-delete  python-config
cut        gnroff     locate     nl-neigh-list   python2
cvtsudoers  gpasswd    logger     nl-neighb1-list  python2-config
date       gpg        login      nl-pktloc-lookup  python2.7
db_archive  gpg-agent  loginctl   nl-qdisc-add     python2.7-config
db_checkpoint  gpg-connect-agent  logname     nl-qdisc-delete  python3
db_deadlock  gpg-error  look       nl-qdisc-list    python3.7
db_dump     gpg2       ls         nl-route-add     python3.7m
db_dump185  gpgconf    lsattr     nl-route-delete  pyvenv
db_hotbackup  gpgparsemail  lsblk     nl-route-get     pyvenv-3.7
sh-4.2$
```

## **Resumen de la tarea 5**

En esta tarea, verifiqué que el firewall de la red se haya actualizado y configurado correctamente para bloquear los sitios web maliciosos. Confirmó que el acceso está bloqueado iniciando sesión en la instancia TestInstance EC2 y ejecutando comandos wget en estos archivos. Los usuarios ahora no pueden acceder a estos archivos maliciosos desde este sitio web.