



280-[SF]-Lab - Malware de firewall

Datos Generales:

Nombre: Tomás Alfredo Villaseca Constantinescu

País: Chile

Fecha: 23/09/2023

Contacto: tomas.villaseca.c@gmail.com

Después de completar este laboratorio, podrá realizar lo siguiente:

- 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

Escenario:

AnyCompany te ha contratado como nuevo ingeniero de seguridad, y la empresa te ha encargado que refuerces el perímetro de seguridad de la empresa. Ha habido informes de usuarios que han descargado accidentalmente malware tras acceder a sitios web específicos. El equipo de TI de AnyCompany le ha proporcionado las URL de los sitios que alojan el malware. Su trabajo consiste en encontrar una solución para mitigar el acceso a estos archivos de actores maliciosos.

Entorno del laboratorio → Instancia EC2 pre-configurada TestInstance

- TestInstance → Utilizada para probar el acceso al sitio web que aloja archivos maliciosos (malware)
- TestInstance está contenida en una zona perimetral y separada del resto de los servidores importantes de AnyCompany.

Malware = Cualquier tipo de software malicioso diseñado para infiltrarse en un dispositivo informático sin el conocimiento del usuario y causar daños o interrupciones en el sistema o robar datos.

Firewall = Sistema de seguridad que protege una red informática de accesos no autorizados. Funciona como una barrera entre una red interna y una red externa (como internet).



Tarea 1: Confirmar accesibilidad

En esta tarea, iniciará sesión en la instancia EC2 TestInstance, en donde emitirá un comando wget a los archivos del actor malicioso que el equipo de TI le proporcionó para confirmar la accesibilidad.

- wget = utilidad de línea de comandos de Linux que se utiliza para descargar archivos desde Internet.

Paso 1: Conectarse a la instancia TestInstance vía Session Manager utilizando TestInstanceURL (link entregado por el laboratorio) en un navegador web.

Session ID: user2741130=Tom__sVillaseca-0deec82489e2d88c1

Instance ID: i-02d0775b885e65f44

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

En el paso 2 & 3 se reproduce como un usuario descargaría un archivo malicioso utilizando un navegador web.

Paso 2: Ingresar el comando **wget** para descargar el malware número 1:

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

Session ID: user2741130=Tom__sVillaseca-0deec82489e2d88c1

Instance ID: i-02d0775b885e65f44

```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2023-09-24 01:16:19-- 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%[=====]

2023-09-24 01:16:19 (47.7 MB/s) - 'js_crypto_miner.html' saved [366/366]

sh-4.2$
```

Paso 3: Ingresar el comando **wget** para descargar el malware número 2:

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

Session ID: user2741130=Tom__sVillaseca-0deec82489e2d88c1

Instance ID: i-02d0775b885e65f44

```
sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2023-09-24 01:16:43-- 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%[=====]

2023-09-24 01:16:43 (19.5 MB/s) - 'java_jre17_exec.html' saved [129/129]

sh-4.2$
```

Paso 4: Verificar que ambos archivos fueron descargados.

Session ID: user2741130=Tom__sVillaseca-0deec82489e2d88c1

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

En esta tarea se confirmó que la URL que aloja los archivos maliciosos es accesible a través de la red actual y Network Firewall que utiliza AnyCompany.


Se utilizó una instancia EC2 aislada TestInstance para ejecutar comandos y descargar los mismos archivos maliciosos que descargaron los usuarios.

Tarea 2: Inspeccionar el firewall de red

En esta tarea, inspeccionará el Firewall de red. La actualización de este firewall es la principal prioridad que AnyCompany le ha asignado como nuevo ingeniero de seguridad.

Paso 1: AWS Management Console → Services → VPC

Services

 **VPC** ☆
Isolated Cloud Resources

Firewalls (1)

Q Find by keyword

Name	Status
LabFirewall	Ready

Paso 2: Panel de navegación → Firewalls → LabFirewall → Overview

LabFirewall [Info](#)

Overview [Info](#)

Firewall status
Ready

Associated firewall policy
[LabFirewallPolicy](#)

Paso 3: LabFirewall → Overview → Step 2: Configure the firewall policy

- Seleccionar el link de LabFirewallPolicy para abrir la política asociada.
- Política de Firewall = Define el comportamiento del firewall.

LabFirewallPolicy [Info](#)

[Network Firewall rule groups](#) | [TLS inspection configuration](#) | [Details](#)

Stateless default actions
Stateless default actions determine how Network Firewall should handle packets that don't match any stateless rule group contained in the policy.

Actions for full packets
Pass

Stateless rule groups (0)

☐

Priority

▼

Name

Paso 4: LabFirewallPolicy → Stateless default actions → Edit

- Choose how to treat fragmented packets = Use the same actions for all packets.
- Action = 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

Estos ajustes ahora reenvían todos los paquetes a un **stateful rule group** para su inspección posterior.

- Un **stateful rules engine** inspecciona los paquetes en el contexto de su flujo de tráfico, le ofrece la posibilidad de utilizar reglas más complejas y le permite registrar el tráfico de red y las alertas del firewall de AWS Network Firewall sobre el tráfico.
- Las **stateful rules** tienen en cuenta la dirección del tráfico.
- El **stateful rules engine** puede retrasar la entrega de paquetes para agruparlos para su inspección.

Un **stateless rules engine** inspecciona cada paquete de forma aislada sin tener en cuenta factores como la dirección del tráfico o si el paquete forma parte de una conexión existente y aprobada.

- El **stateless rules engine** prioriza la velocidad de evaluación.

En esta tarea, inspeccionó el firewall de red y actualizó la política del firewall. Se actualizó la política del firewall para reenviar todos los paquetes a un **stateful rule group** para la inspección de los paquetes.

Tarea 3: Crear un grupo de reglas de firewall

En esta tarea, creará un Network Firewall rule group que bloquean el acceso a las URL maliciosas. Posteriormente, adjuntará este grupo de reglas a su política de firewall.

Network Firewall rule group = Es un conjunto reutilizable de criterios para inspeccionar y gestionar el tráfico de red.

- Puede añadir uno o más grupos de reglas a una política de cortafuegos como parte de la configuración de políticas.

Paso 1: VPC → Panel de navegación → 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 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.

Your rule groups (0)	
<input type="text" value="Find resources by name or value"/>	
Name	Type
No rule groups	
You don't have any rule groups.	
Create rule group	

Paso 2: Create Network Firewall rule group → Configurar

- Rule group type → Stateful rule group
- Name = StatefulRuleGroup
- Capacity = 100
- Stateful rule group option = Suricata compatible IPS rules

Choose rule group type [Info](#)

Network Firewall rule groups are either stateless or stateful. Stateless rule groups evaluate packets on their own, without the context of their traffic flow. 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**.

Describe rule group [Info](#)

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

Rule group details

Name

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

StatefulGroupRule

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 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 does.

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 you create the rule group.

100

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

Paso 3: Ingresar el código entregado por el laboratorio en la sección “Suricata compatible rule string”.

```
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;)
```

- Las dos reglas de Suricata agregadas bloquean el tráfico que coincide con los URLs **http_uri contents /data/js_crypto_miner.html** y **http_uri contents /data/js_crypto_miner.html** cuando el tráfico es iniciado desde la red pública de LabVPC.

Configure rules [Info](#)

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

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:2002001; content:"/data/js_crypto_miner.html";http_uri; rev:1;)
```

Your rule groups (1)

Find resources by name or value

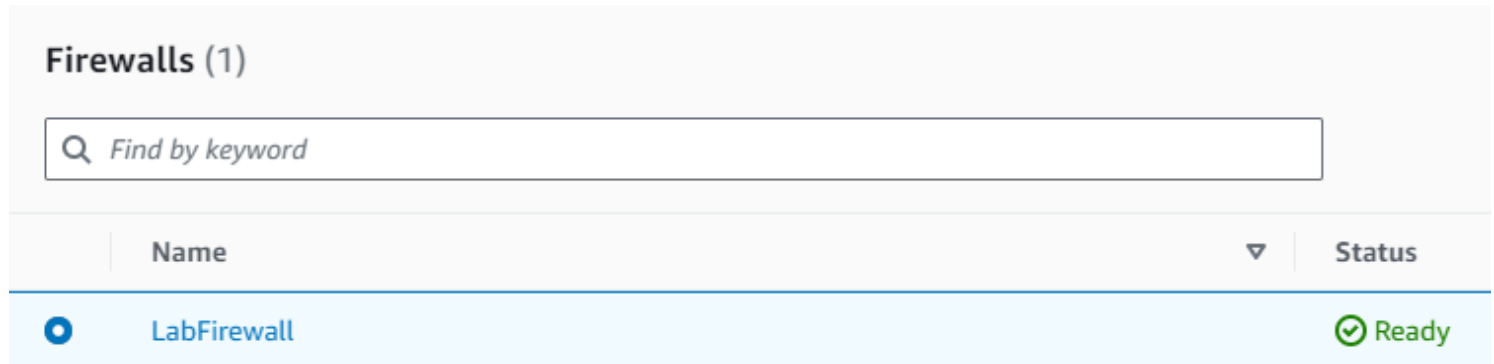
<input checked="" type="checkbox"/>	Name	Type
<input checked="" type="checkbox"/>	StatefulGroupRule	Stateful

En esta tarea se creó un Stateful Network Firewall rule group que utiliza reglas de Suricata. Una vez que sea adjuntado a LabFirewall, bloqueará los sitios web maliciosos a los que accedieron los usuarios de AnyCompany.

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

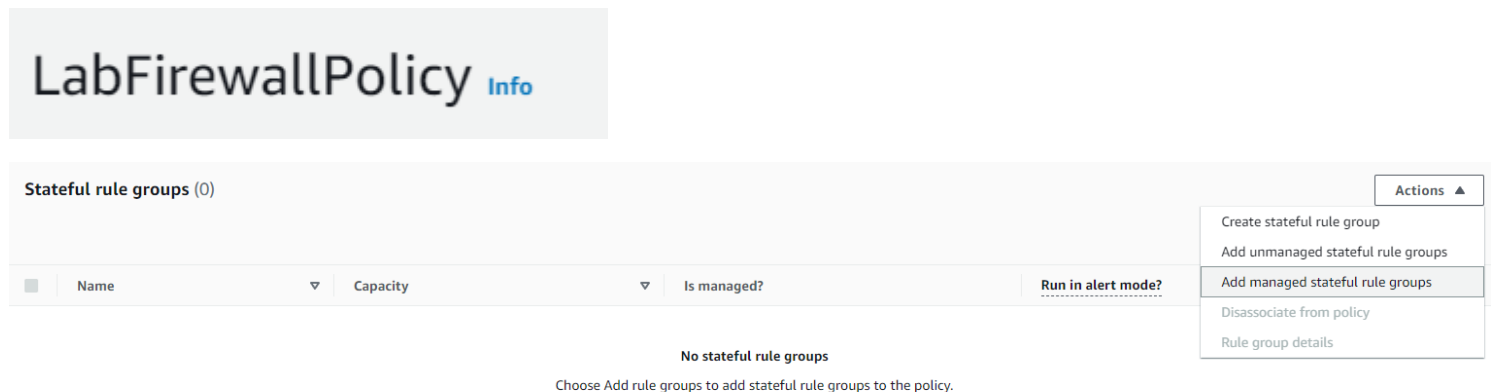
En esta tarea, se adjunta el Network Firewall rule group creado al LabFirewall.

Paso 1: VPC → Panel de navegación → Firewalls → LabFirewall



Name	Status
LabFirewall	Ready

Paso 2: LabFirewall → Overview → Step 2: Configure the firewall policy → Add rule group



Stateful rule groups (0)

Actions

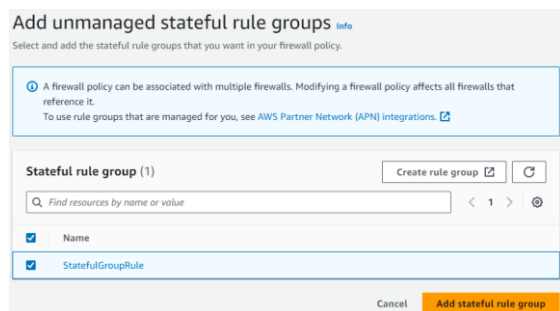
- Create stateful rule group
- Add unmanaged stateful rule groups
- Add managed stateful rule groups
- Disassociate from policy
- Rule group details

No stateful rule groups

Choose Add rule groups to add stateful rule groups to the policy.

Paso 3: Add rule group → Add from existing stateful rule groups

- Seleccionar la casilla para “StatefulRuleGroup”
- Seleccionar “Add stateful rule group”



Add unmanaged stateful rule groups

Select and add the stateful rule groups that you want in your firewall policy.

A firewall policy can be associated with multiple firewalls. Modifying a firewall policy affects all firewalls that reference it. To use rule groups that are managed for you, see [AWS Partner Network \(APN\) integrations](#).

Stateful rule group (1)

Create rule group

Find resources by name or value

StatefulRuleGroup

Cancel Add stateful rule group

Paso 4: Verificar que el rule group fue adjuntado a la Firewall.

Stateful rule groups (1)			
<input type="checkbox"/>	Name	Capacity	Is managed?
<input type="checkbox"/>	StatefulGroupRule	100	No

Se adjuntó el Network Firewall rule group a LabFirewall, que bloquea los intentos de acceso a los archivos del actor malicioso alojados en el sitio web.

Tarea 5: Validar la solución

En esta tarea, se vuelve a iniciar sesión en la TestInstance para comprobar que el Network Firewall bloquea correctamente los intentos de acceso a los archivos del sitio web malicioso.

Paso 1: AWS Management Console → Services → EC2 → Instances → TestInstance → Connect

- Session Manager → Connect

Session ID: user2741130=Tom__sVillaseca-0deec82489e2d88c1

Instance ID: i-02d0775b885e65f44

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

Paso 2: Ingresar el comando **wget** para descargar el malware número 1:

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

Session ID: user2741130=Tom__sVillaseca-00a98fc2df1d57ea8

Instance ID: i-02d0775b885e65f44

```
sh-4.2$ wget http://malware.wicar.org/data/js_crypto_miner.html
--2023-09-24 01:42:44-- 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...
```

Paso 3: Ingresar el comando **wget** para descargar el malware número 2:

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

Session ID: user2741130=Tom__sVillaseca-00a98fc2df1d57ea8

Instance ID: i-02d0775b885e65f44

```
sh-4.2$ wget http://malware.wicar.org/data/java_jre17_exec.html
--2023-09-24 01:43:45-- 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...
```

- HTTP request sent, awaiting response → Indica que el sitio web malicioso fue bloqueado correctamente por el Firewall

Paso 4: Remover los archivos maliciosos descargados como prueba utilizando el siguiente comando:

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

Session ID: user2741130=Tom__sVillaseca-00a98fc2df1d57ea8

Instance ID: i-02d0775b885e65f44

```
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$
```

Se verificó que el Network Firewall se ha actualizado y configurado correctamente para bloquear los sitios web maliciosos. Se confirmó que el acceso está bloqueado iniciando sesión en la instancia EC2 de TestInstance y ejecutando comandos wget en estos archivos. Los usuarios ya no pueden acceder a estos archivos maliciosos desde este sitio web.

A horizontal banner with a dark blue background featuring a network of glowing blue nodes and lines. The text "Laboratorio Completado" is centered in a white, sans-serif font.

Laboratorio Completado

