

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'

100%[=====>] 366 --.-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'

100%[=====>] 129 --.-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$
```

Malware de Firewall:

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).

The screenshot displays the AWS Management Console interface. On the left, the navigation menu shows 'Network Firewall' expanded, with 'Firewall policies' highlighted. A red arrow points to this option. The main content area shows a notification: 'You've successfully updated firewall policy LabFirewallPolicy.' Below this, the 'Stateless default actions' dialog is open. The dialog has two sections: 'Fragmented packets' and 'Rule action'. In the 'Fragmented packets' section, the option 'Use the same actions for all packets' is selected. In the 'Rule action' section, the option 'Forward to stateful rule groups' is selected. At the bottom of the dialog, there is a 'Publish metrics - optional' section with an 'Enable' checkbox. The 'Save' button is highlighted in orange. The footer of the console shows 'CloudShell', 'Feedback', and copyright information for Amazon Web Services, Inc. or its affiliates.

aws Services Search [Alt+S] Oregon voclabs/user2846438=Guillermina_Antonaccio_Scaffo @ 5355-5269...

▼ DNS firewall
Rule groups
Domain lists

▼ Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Network Firewall resource groups

▼ Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN connections

You've successfully updated firewall policy LabFirewallPolicy.

VPC > Network Firewall > LabFirewallPolicy

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

Stateless rule groups (0)

CloudShell Feedback © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Malware de Firewall:

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.

The screenshot shows the AWS IAM console interface for creating a new Network Firewall rule group. The left sidebar lists the steps: Step 1: Choose rule group type, Step 2: Describe rule group, Step 3: Configure rules, Step 4 - optional: Configure advanced settings, Step 5 - optional: Add tags, and Step 6: Review and create. The main content area is titled 'Review and create' and shows the configuration for Step 1: Rule group type.

Step 1: Rule group type [Edit step 1](#)

| Rule group type | | |
|-----------------|---------------------------------|------------|
| Rule group type | Stateful rule group option | Rule order |
| Stateful | Suricata compatible rule string | strict |

Step 2: Rule group [Edit step 2](#)

| Rule group details | | |
|--------------------|-------------|----------|
| Name | Description | Capacity |
| StatefulRuleGroup | - | 100 |

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.

The screenshot shows the AWS Management Console interface for configuring a Network Firewall. At the top, a green banner indicates a successful update of the 'LabFirewall'. The breadcrumb trail shows the path: VPC > Network Firewall: Firewalls > LabFirewall > Add my own stateful rule groups. The main heading is 'Add unmanaged stateful rule groups' with an 'Info' link. Below this, a message explains that a firewall policy can be associated with multiple firewalls and provides a link to 'AWS Partner Network (APN) integrations'. A section titled 'Stateful rule group (1/1)' contains a search bar and a table of resources. The table has a checkbox column and a 'Name' column. One resource, 'StatefulRuleGroup', is listed and is selected with a checked checkbox. A red arrow points to this checkbox. At the bottom right, there are 'Cancel' and 'Add stateful rule group' buttons.

aws Services Search [Alt+S] Oregon voclabs/user2846438=Guillermina_Antonaccio_Scaffo @ 5355-5269...

You've successfully updated the firewall LabFirewall

VPC > Network Firewall: Firewalls > LabFirewall > Add my own stateful rule groups

→ Add unmanaged stateful rule groups [Info](#)

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

Stateful rule group (1/1) [Create rule group](#)

Find resources by name or value

| <input checked="" type="checkbox"/> | Name |
|-------------------------------------|-------------------|
| <input checked="" type="checkbox"/> | StatefulRuleGroup |

Cancel Add stateful rule group

Malware de Firewall:

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

aws Services Search [Alt+S] Oregon voclabs/user2846438=Guillermina_Antonaccio_Scaffo @ 5355-5269...

▼ Network Firewall

- Firewalls
- Firewall policies
- Network Firewall rule groups
- TLS inspection configurations
- Network Firewall resource groups

▼ Virtual private network (VPN)

- Customer gateways
- Virtual private gateways
- Site-to-Site VPN connections
- Client VPN endpoints

▼ AWS Verified Access

- Verified Access instances

✓ You've successfully updated firewall policy LabFirewallPolicy.

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

Stateful rule evaluation order and default actions Edit

The way that your stateful rules are ordered for evaluation.

| Rule order | Default actions |
|--------------|-----------------|
| Action order | - |

Stateful rule groups (1) Actions ▲

| <input type="checkbox"/> | Name | Capacity | Is managed? | Run in alert mode? |
|--------------------------|-----------------------------------|----------|-------------|--------------------|
| <input type="checkbox"/> | StatefulRuleGroup | 100 | No | Not available |

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