



---

# SISTEMAS DE DETECCIÓN DE INTRUSIONES (SURICATA)

---

Actividad 3



CRISTÓBAL SUÁREZ ABAD  
SEGURIDAD Y ALTA DISPONIBILIDAD  
2º ASIR

## Contenido

|   |    |
|---|----|
| Introducción:.....  | 2  |
| Instalación de Suricata en Ubuntu. ....                     | 3  |
| Automatiza el inicio de Suricata. ....                      | 5  |
| Prueba la funcionalidad de Suricata. ....                   | 7  |
| Actualiza las normas de Suricata. ....                      | 9  |
| Detectar amenazas conocidas: usar reglas predefinidas. .... | 11 |

## Introducción:

Sigue el siguiente tutorial:

### [Tutorial Instalación configuración y prueba de suricata](#)

- Documenta los pasos realizados y los problemas que te puedas encontrar durante el proceso.
- Elige entre estos casos u otro que tu desees entre la funcionalidades de suricata. Configura esto y prueba que funciona:
  - Monitorizar red corporativa: detectar intrusiones, malware o tráfico sospechoso.
  - Identificar ataques simulados o escaneos de puertos.
  - Analizar tráfico de red: registrar protocolos, flujos y estadísticas de uso.
  - Detectar amenazas conocidas: usar reglas predefinidas

## Instalación de Suricata en Ubuntu.

**`sudo apt update`**

**`sudo apt install -y suricata`**

Para comprobar que está instalado usamos:

**`suricata -V`**

```
Tu Nombre viernes 7 noviembre 2025 08:47
[root@server2asir usuario]$suricata -V
This is Suricata version 6.0.4 RELEASE
```

También puedes usar el siguiente comando para filtrar los paquetes que “apt” tiene instalados en el equipo:

**`sudo apt list --installed | grep suricata`**

```
Tu Nombre viernes 7 noviembre 2025 08:47
[root@server2asir usuario]$sudo apt list --installed | grep suricata

WARNING: apt does not have a stable CLI interface. Use with caution in scripts.

suricata-update/jammy,now 1.2.3-1 amd64 [instalado, automático]
suricata/jammy,now 1:6.0.4-3 amd64 [instalado]
```

### ***Configuración de Suricata.***

“El paquete Suricata incluye un archivo de configuración **YAML** para ajustar la configuración y el comportamiento de la herramienta. Puedes editarlo con un [editor de texto como nano](#):”

**`sudo nano /etc/suricata/suricata.yaml`**

Vamos a modificar este archivo con las configuraciones que se detallaran a continuación:

- Habilitar interfaces de red:

Debemos indicar la interfaz de red que Suricata debe supervisar para proteger el sistema. Por defecto no rastrea ninguna actividad y debemos especificar la interfaz de red y el método de captura.

Para saber cual es nuestra interfaz de red podemos usar:

**`“ip a”` o `“ip -p -j route show”`.**

En nuestro caso es la **“ens18”**.

```
Tu Nombre viernes 7 noviembre 2025 08:51
[root@server2asir usuario]$ip -p -j route show
[ {
    "dst": "default",
    "gateway": "10.2.17.1",
    "dev": "ens18",
    "protocol": "dhcp",
    "prefsrc": "10.2.17.107",
    "metric": 100,
    "flags": [ ]
}, {
```

En nuestro caso vamos a configurar la interfaz para que se use en ella el método de captura de paquetes “af”.

```
# Linux high speed capture support
af-packet:
- interface: ens18|
  # Number of receive threads. "auto
  #threads: auto
  # Default clusterid. AF_PACKET wil
```

Iniciando Suricata.

Suricata no se activa una vez que se instala. Debemos hacer la configuración que necesitamos y luego encenderlo.

**sudo systemctl start suricata**

**sudo systemctl status suricata**

```
Tu Nombre viernes 7 noviembre 2025 09:03
[root@server2asir usuario]$sudo systemctl start suricata
Tu Nombre viernes 7 noviembre 2025 09:03
[root@server2asir usuario]$systemctl status suricata
● suricata.service - Suricata IDS/IDP daemon
   Loaded: loaded (/lib/systemd/system/suricata.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2025-11-07 09:03:31 UTC; 1s ago
     Docs: man:suricata(8)
           man:suricatasc(8)
           https://suricata-ids.org/docs/
   Process: 3247 ExecStart=/usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile=
 Main PID: 3248 (Suricata-Main)
    Tasks: 8 (limit: 3426)
   Memory: 45.1M
      CPU: 479ms
   CGroup: /system.slice/suricata.service
           └─3248 /usr/bin/suricata -D --af-packet -c /etc/suricata/suricata.yaml --pidfile /run/su

nov 07 09:03:31 server2asir systemd[1]: Starting Suricata IDS/IDP daemon...
nov 07 09:03:31 server2asir suricata[3247]: 7/11/2025 -- 09:03:31 - <Notice> - This is Suricata versi
nov 07 09:03:31 server2asir systemd[1]: Started Suricata IDS/IDP daemon.
lines 1-17/17 (END)
```

Si vamos a realizar más cambios en Suricata, recuerda que debes reiniciar el servicio.

**sudo systemctl restart suricata**

## Automatiza el inicio de Suricata.

Vamos a configurar el inicio automático de Suricata para no tener que iniciarlo manualmente cada vez que encendamos el servidor. Para ello debemos crear un archivo:

```
sudo nano /etc/systemd/system/suricata.service
```

Debemos introducir lo siguiente: Fíjate que debemos poner nuestra interfaz (en mi caso "ens18").

*# Define the Suricata systemd unit*

*[Unit]*

*Description=Suricata IDS/IPS*

*After=network.target*

*# Specify the Suricata binary path, the configuration files location, and the network interface*

*[Service]*

*ExecStart=/usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens18*

*[Install]*

*WantedBy=default.target*

```
GNU nano 6.2 /etc/systemd/system/suricata.service *
# Define the Suricata systemd unit
[Unit]
Description=Suricata IDS/IPS
After=network.target

# Specify the Suricata binary path, the configuration files location, and the network interface
[Service]
ExecStart=/usr/bin/suricata -c /etc/suricata/suricata.yaml -i ens18
[Install]

WantedBy=default.target
```

Guardamos y ejecutamos:

```
sudo systemctl enable suricata
```

```
[root@server2asir usuario]$sudo systemctl enable suricata
Synchronizing state of suricata.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable suricata
Created symlink /etc/systemd/system/default.target.wants/suricata.service → /etc/systemd/system/suricata.service.
Tu Nombre viernes 7 noviembre 2025 09:09
[root@server2asir usuario]$
```

Ahora debemos modificar el archivo “**suricata.yaml**”.

**default-rule-path: /var/lib/suricata/rules**

**rule-files:**

**- suricata.rules**

```
default-rule-path: /var/lib/suricata/rules
rule-files:
- suricata.rules
```

Guardamos y reiniciamos el servicio.

**systemctl restart suricata**

Si hacemos un “**systemctl status suricata**” o podemos usar el siguiente comando para comprobar que la configuración es correcta:

“**sudo suricata -T -c /etc/suricata/suricata.yaml -v**”. Nos puede salir el siguiente error.

**<Warning> - [ERRCODE: SC\_ERR\_NO\_RULES(42)] - No rule files match the pattern /var/lib/suricata/rules/suricata.rules**

```
7/11/2025 -- 09:12:52 -- <Info> -- Status output device (regular) initialized: stats.tlog
7/11/2025 -- 09:12:52 -- <Warning> -- [ERRCODE: SC_ERR_NO_RULES(42)] - No rule files match the pattern /var/lib/suricata/rules/suricata.rules
Tu Nombre viernes 7 noviembre 2025 09:12
```

Debemos hacer un “**suricata-update**” para que se descargue las reglas en el directorio que hemos configurado. Tarda un poco. Después haz un “**systemctl restart suricata**”.

```
Tu Nombre viernes 7 noviembre 2025 09:12
[root@server2asir usuario]$sudo suricata-update
7/11/2025 -- 09:18:52 -- <Info> -- Using data-directory /var/lib/suricata.
7/11/2025 -- 09:18:52 -- <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
7/11/2025 -- 09:18:52 -- <Info> -- Using /etc/suricata/rules for Suricata provided rules.
7/11/2025 -- 09:18:52 -- <Info> -- Found Suricata version 6.0.4 at /usr/bin/suricata.
7/11/2025 -- 09:18:52 -- <Info> -- Loading /etc/suricata/suricata.yaml
7/11/2025 -- 09:18:52 -- <Info> -- Disabling rules for protocol http2
7/11/2025 -- 09:18:52 -- <Info> -- Disabling rules for protocol modbus
7/11/2025 -- 09:18:52 -- <Info> -- Disabling rules for protocol dnp3
7/11/2025 -- 09:18:52 -- <Info> -- Disabling rules for protocol enip
7/11/2025 -- 09:18:52 -- <Info> -- No sources configured, will use Emerging Threats Open
7/11/2025 -- 09:18:52 -- <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-6.0.4/emerging.rules.tar.gz.
100% - 5182374/5182374
7/11/2025 -- 09:18:53 -- <Info> -- Done.
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
7/11/2025 -- 09:18:54 -- <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
```

## Prueba la funcionalidad de Suricata.

Volvemos a usar “**sudo suricata -T -c /etc/suricata/suricata.yaml -v**” y comprobamos que la configuración es correcta.

```
Tu Nombre viernes 7 noviembre 2025 09:40
[root@server2asir usuario]$sudo suricata -T -c /etc/suricata/suricata.yaml -v
7/11/2025 -- 09:20:49 - <Info> - Running suricata under test mode
7/11/2025 -- 09:20:49 - <Notice> - This is Suricata version 6.0.4 RELEASE running in SYSTEM mode
7/11/2025 -- 09:20:49 - <Info> - CPUs/cores online: 2
7/11/2025 -- 09:20:49 - <Info> - fast output device (regular) initialized: fast.log
7/11/2025 -- 09:20:49 - <Info> - eve-log output device (regular) initialized: eve.json
7/11/2025 -- 09:20:49 - <Info> - stats output device (regular) initialized: stats.log
7/11/2025 -- 09:21:05 - <Info> - 1 rule files processed. 46210 rules successfully loaded, 0 rules failed
7/11/2025 -- 09:21:05 - <Info> - Threshold config parsed: 0 rule(s) found
7/11/2025 -- 09:21:06 - <Info> - 46213 signatures processed. 962 are IP-only rules, 5158 are inspecting packet payload, 39876 inspect application layer, 108 are decoder event only
7/11/2025 -- 09:22:22 - <Notice> - Configuration provided was successfully loaded. Exiting.
7/11/2025 -- 09:22:22 - <Info> - cleaning up signature grouping structure... complete
Tu Nombre viernes 7 noviembre 2025 09:22
[root@server2asir usuario]$
```

Ahora vamos a comprobar las reglas de Suricata para ver que detectan correctamente el tráfico malicioso. Para ello usaremos el siguiente comando:

**curl http://testmynids.org/uid/index.html**

*“La guía de inicio rápido de Suricata recomienda utilizar la regla ET Open número 2100498 y conectarse a una URL de prueba mediante el comando **curl**:”*

```
Tu Nombre viernes 7 noviembre 2025 09:44
[root@server2asir usuario]$curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
```

*“El comando enviará una petición HTTP para activar la regla de alerta. A continuación, Suricata generará eventos de registro en el archivo **eve.json** y **fast.log** sobre el tráfico detectado.”*

Ahora vamos a comprobar que Suricata etiqueta esta petición a un enlace HTTP como tráfico potencialmente malicioso. Para ello debemos buscar en el archivo “fast.log”:

**grep 2100498 /var/log/suricata/fast.log**

```
Tu Nombre viernes 7 noviembre 2025 09:44
[root@server2asir usuario]$curl http://testmynids.org/uid/index.html
uid=0(root) gid=0(root) groups=0(root)
Tu Nombre viernes 7 noviembre 2025 09:44
[root@server2asir usuario]$grep 2100498 /var/log/suricata/fast.log
11/07/2025-09:39:31.579354  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 52.222.132.64:80 -> 10.2.17.107:35192
11/07/2025-09:39:45.051440  [**] [1:2100498:7] GPL ATTACK_RESPONSE id check returned root [**] [Classification: Potentially Bad Traffic] [Priority: 2] {TCP} 52.222.132.64:80 -> 10.2.17.107:51640
Tu Nombre viernes 7 noviembre 2025 09:44
[root@server2asir usuario]$
```

Ahora vamos a mirar el registro “**eve.json**”. Para poder ver su contenido debemos instalar paquetería para poder entender las entradas JSON.

**sudo apt install jq**

“A continuación, introduce el siguiente comando para filtrar las entradas del archivo de registro en función del ID de firma y del tipo de alerta:”

```
jq 'select(.alert .signature_id==2100498)' /var/log/suricata/eve.json
```

“Deberías ver el ID de la regla (2100498) y la misma categoría **“Tráfico potencialmente malo”**. Significa que Suricata ha emparejado el tráfico de tu red con la regla de detección correcta.”

```
[root@server2asir usuario]$jq 'select(.alert .signature_id==2100498)' /var/log/suricata/eve.json
{
  "timestamp": "2025-11-07T09:39:31.579354+0000",
  "flow_id": 2074717210238040,
  "in_iface": "ens18",
  "event_type": "alert",
  "src_ip": "52.222.132.64",
  "src_port": 80,
  "dest_ip": "10.2.17.107",
  "dest_port": 35192,
  "proto": "TCP",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2100498,
    "rev": 7,
    "signature": "GPL ATTACK_RESPONSE id check returned root",
    "category": "Potentially Bad Traffic",
    "severity": 2,
    "metadata": {
      "confidence": [
        "Medium"
      ],
      "created_at": [
        "2010_09_23"
      ],
      "signature_severity": [
        "Informational"
      ],
      "updated_at": [
        "2019_07_26"
      ]
    }
  },
  "http": {
    "hostname": "testmynids.org",
    "url": "/uid/index.html",
    "http_user_agent": "curl/7.81.0",
    "http_content_type": "text/html",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 39
  },
  "files": [
    {
      "filename": "/uid/index.html",
      "sid": [],
      "gaps": false,
      "state": "CLOSED",
      "stored": false,
    }
  ]
}
```

## Actualiza las normas de Suricata.

Vamos a añadir nuevas normas a Suricata, porque, aunque viene con algunas por defecto, pueden ser no suficientes para un servidor que recibe tráfico de muchas fuentes.

Vamos a listar reglas adicionales de proveedores externos (algunos gratis y otros no). Usamos:

**sudo suricata-update list-sources**

```
Tu Nombre viernes 7 noviembre 2025 09:49
[root@server2asir usuario]$sudo suricata-update list-sources
7/11/2025 -- 09:54:42 - <Info> -- Using data-directory /var/lib/suricata.
7/11/2025 -- 09:54:42 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
7/11/2025 -- 09:54:42 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
7/11/2025 -- 09:54:42 - <Info> -- Found Suricata version 6.0.4 at /usr/bin/suricata.
7/11/2025 -- 09:54:42 - <Info> -- No source index found, running update-sources
7/11/2025 -- 09:54:42 - <Info> -- Downloading https://www.openinfosecfoundation.org/rules/index.yaml
7/11/2025 -- 09:54:42 - <Info> -- Adding all sources
7/11/2025 -- 09:54:42 - <Info> -- Saved /var/lib/suricata/update/cache/index.yaml
Name: et/open
  Vendor: Proofpoint
  Summary: Emerging Threats Open Ruleset
  License: MIT
Name: et/pro
  Vendor: Proofpoint
  Summary: Emerging Threats Pro Ruleset
  License: Commercial
  Replaces: et/open
  Parameters: secret-code
  Subscription: https://www.proofpoint.com/us/threat-insight/et-pro-ruleset
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT
Name: scwx/enhanced
  Vendor: Secureworks
  Summary: Secureworks suricata-enhanced ruleset
  License: Commercial
  Parameters: secret-code
  Subscription: https://www.secureworks.com/contact/ (Please reference CTU Countermeasures)
```

Para incorporar un conjunto de reglas usamos el siguiente comando:

**sudo suricata-update enable-source nombre-del-proveedor**

Ejemplo:

**sudo suricata-update enable-source sslbl/ja3-fingerprints**

```
Tu Nombre viernes 7 noviembre 2025 09:54
[root@server2asir usuario]$sudo suricata-update enable-source sslbl/ja3-fingerprints
7/11/2025 -- 09:57:39 - <Info> -- Using data-directory /var/lib/suricata.
7/11/2025 -- 09:57:39 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
7/11/2025 -- 09:57:39 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
7/11/2025 -- 09:57:39 - <Info> -- Found Suricata version 6.0.4 at /usr/bin/suricata.
7/11/2025 -- 09:57:39 - <Info> -- Creating directory /var/lib/suricata/update/sources
7/11/2025 -- 09:57:39 - <Info> -- Enabling default source et/open
7/11/2025 -- 09:57:39 - <Info> -- Source sslbl/ja3-fingerprints enabled
Tu Nombre viernes 7 noviembre 2025 09:57
[root@server2asir usuario]$
```

Ahora debes ejecutar “**suricata-update**” para que el archivo “**/etc/suricata/rules**” actualice y valide las reglas.

```
Tu Nombre  viernes  7 noviembre 2025 09:57
[root@server2asir usuario]$suricata-update
7/11/2025 -- 09:59:42 - <Info> -- Using data-directory /var/lib/suricata.
7/11/2025 -- 09:59:42 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
7/11/2025 -- 09:59:42 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
7/11/2025 -- 09:59:42 - <Info> -- Found Suricata version 6.0.4 at /usr/bin/suricata.
7/11/2025 -- 09:59:42 - <Info> -- Loading /etc/suricata/suricata.yaml
7/11/2025 -- 09:59:42 - <Info> -- Disabling rules for protocol http2
7/11/2025 -- 09:59:42 - <Info> -- Disabling rules for protocol modbus
7/11/2025 -- 09:59:42 - <Info> -- Disabling rules for protocol dnp3
7/11/2025 -- 09:59:42 - <Info> -- Disabling rules for protocol enip
7/11/2025 -- 09:59:42 - <Warning> -- Source has been deprecated: sslbl/ja3-fingerprints: Renamed to abuse.ch/sslbl-ja3
('https://rules.emergingthreats.net/open/suricata-6.0.4/emerging.rules.tar.gz', None, True)
7/11/2025 -- 09:59:42 - <Info> -- Checking https://rules.emergingthreats.net/open/suricata-6.0.4/emerging.rules.tar.gz.md5.
7/11/2025 -- 09:59:42 - <Info> -- Remote checksum has not changed. Not fetching.
7/11/2025 -- 09:59:43 - <Info> -- Fetching https://sslbl.abuse.ch/blacklist/ja3_fingerprints.tar.gz.
100% - 3508/3508
7/11/2025 -- 09:59:43 - <Info> -- Done.
7/11/2025 -- 09:59:43 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
7/11/2025 -- 09:59:43 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
7/11/2025 -- 09:59:43 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
7/11/2025 -- 09:59:43 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
7/11/2025 -- 09:59:43 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
7/11/2025 -- 09:59:43 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
7/11/2025 -- 09:59:43 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
7/11/2025 -- 09:59:43 - <Info> -- Loading distribution rule file /etc/suricata/rules/insec-events.rules
7/11/2025 -- 09:59:43 - <Info> -- Enabled 150 rules for Ptoorbit dependencies.
7/11/2025 -- 09:59:49 - <Info> -- Backing up current rules.
7/11/2025 -- 09:59:54 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 62118; enabled: 46307; added: 97; removed 0; modified: 0
7/11/2025 -- 09:59:55 - <Info> -- Writing /var/lib/suricata/rules/classification.config
7/11/2025 -- 09:59:55 - <Info> -- Testing with suricata -T.
7/11/2025 -- 10:01:10 - <Info> -- Done.
Tu Nombre  viernes  7 noviembre 2025 10:01
```

También puedes usar herramientas de gestión de reglas de Suricata como [Pulledpork](#) y [Oinkmaster](#) que te ayudará a mejorar el método de detección. Puedes usar nano para modificar el archivo

## Detectar amenazas conocidas: usar reglas predefinidas.

Creamos un archivo de reglas propio:

`nano /etc/suricata/rules/mi_pc_mis_reglas.rules`

```
Tu Nombre  viernes  7 noviembre 2025 10:24
[root@server2asir usuario]$ nano /etc/suricata/rules/mi_pc_mis_reglas.rules
```

Introducimos la siguiente línea:

**action protocol source-ip/port -> destination-ip/port (options; options; ... )**

“Definición:

- **action:** la acción a realizar cuando se cumpla la condición de la regla. Entre los valores posibles se incluyen **drop**, **alert** y **log**
- **Protocol:** el protocolo de red supervisado, incluyendo **TCP**, **UDP**, **ICMP** o **IP**.
- **source-ip/port:** la **IP** y el **puerto** desde los que se origina el tráfico.
- **destination-ip/port:** la **IP** y el **puerto** en los que se aplica la regla.
- **(options; options; ...):** palabras clave que determinan ajustes o condiciones adicionales.”

Y esta otra:

**alert http any any -> any any (msg:"PRUEBA - REGLA LOCAL FUNCIONA";  
content:"TEST-SURICATA-RULE"; sid:9999999; rev:1;)**

La primera la dejamos comentada (le ponemos delante una almohadilla #), porque si no nos dará problemas.

```
GNU nano 6.2 /etc/suricata/rules/mi_pc_mis_reglas.rules
#action protocol source-ip/port -> destination-ip/port (options; options; ... )
alert http any any -> any any (msg:"PRUEBA - REGLA LOCAL FUNCIONA"; content:"TEST-SURICATA-RULE"; sid:9999999; rev:1;)
```

Ahora modificamos el archivo “**/etc/suricata/suricata.yaml**” para que sepa donde está el archivo de reglas nuevo. En este caso hay que poner la ruta completa.

```
rule-files:
- suricata.rules
- /etc/suricata/rules/mi_pc_mis_reglas.rules|
##
## Auxiliary configuration files.
```

Hacemos un “**systemctl restart suricata**” y un “**suricata-update**”.

Una vez que hemos actualizado, usamos los dos siguientes comandos. El primero es para generar tráfico que Suricata pueda detectar con la regla que hemos configurado antes y ver que funciona. El segundo es para comprobar que efectivamente, lo detecta.

**curl http://example.com/TEST-SURICATA-RULE-CHECK**

**sudo cat /var/log/suricata/eve.json | grep 9999999**

```
Tu Nombre viernes 7 noviembre 2025 11:23
[root@server2asir usuario]$ curl http://example.com/TEST-SURICATA-RULE-CHECK
<!doctype html><html lang="en"><head><title>Example Domain</title><meta name="viewport" content="width
=device-width, initial-scale=1"><style>body{background:#eee;width:60vw;margin:15vh auto;font-family:sy
stem-ui,sans-serif}h1{font-size:1.5em}div{opacity:0.8}a:link,a:visited{color:#348}</style><body><div><
h1>Example Domain</h1><p>This domain is for use in documentation examples without needing permission.
Avoid use in operations.<p><a href="https://iana.org/domains/example">Learn more</a></div></body></htm
l>
Tu Nombre viernes 7 noviembre 2025 11:25
[root@server2asir usuario]$ sudo cat /var/log/suricata/eve.json | grep 9999999
{"timestamp":"2025-11-07T11:25:43.088844+0000","flow_id":49318425164636,"in_iface":"ens18","event_type
":"alert","src_ip":"10.2.17.107","src_port":39518,"dest_ip":"23.220.75.232","dest_port":80,"proto":"TC
P","alert":{"action":"allowed","gid":1,"signature_id":9999999,"rev":1,"signature":"PRUEBA - REGLA LOCA
L FUNCIONA","category":"","severity":3},"http":{"hostname":"example.com","url":"/TEST-SURICATA-RULE-CH
ECK","http_user_agent":"curl/7.81.0","http_content_type":"text/html","http_method":"GET","protocol":"H
TTP/1.1","status":404,"length":513},"app_proto":"http","flow":{"pkts_toserver":4,"pkts_toclient":3,"by
tes_toserver":371,"bytes_toclient":1110,"start":"2025-11-07T11:25:42.621404+0000"}}
Tu Nombre viernes 7 noviembre 2025 11:26
```

Una vez que hemos visto que las reglas predefinidas funcionan, vamos a volver a modificar el fichero “/etc/suricata/rules/mi\_pc\_mis\_reglas.rules” y comentar la activa y descomentar la otra.

```
GNU nano 6.2 /etc/suricata/rules/mi_pc_mis_reglas.rules *
action protocol source-ip/port -> destination-ip/port (options; options; ... )
#alert http any any -> any any (msg:"PRUEBA - REGLA LOCAL FUNCIONA"; content:"TEST-SURICATA-RULE"; sid:9999999; rev:1;)
```

Volvemos a actualizar y reiniciar el servicio.