

# Mikrotik y Suricata

Por José M. Román

FiberCli

Somos pura fibra

# JOSE MANUEL ROMAN

17 años de experiencia, Mikrotik Certified Consultant and Trainer.  
MTCNA, MTCRE, MTCTCE, MTCUME, MTCWE, MTCINE, CISA, CISSP, Master  
ITIL

- (2015 – Now) CEO @ WISP Cloud Networking Spain
- (2008 – Now) Security Consultant and Analyst
- ***(2000 – 2007) Profesor de redes, programación, sistemas y Base de datos.***



MADRID / PRAGUE



@MAFIASOLEH



+34 652 241431



Jose.roman@fibercli.com

José Manuel Román para FiberCli





# FAJAR NUGROHO

Network Engineer by Job and Troublemaker by Act, currently focusing on MikroTik, Juniper, Arista, UBNT, Vmware Virtualization, Linux/Unix (Debian & FreeBSD). CCNA, MTCNA, MTCRE, MTCTCE, JNCIA, JNCIS-ENT, JNCIS-SP, JNCIP-SP, MikroTik Certified Trainer.

- (2015 – 2016) Infrastructure (*System, Network & Security*) Engineer. @ [Technology and Information Department of Jakarta Capital City](#) and [Jakarta SmartCity](#)
- (2012 – Now) Freelancer @ SMB to Enterprise customers
- (2008 – 2012) Helpdesk, NOC (*Network Operator Center*). @ [Wireless Internet Service Provider](#) and [Triple Play \(CaTV, VoIP and Internet\) Service Provider](#)



TOLEDO / JAKARTA




@MAFIASOLEH  
José Manuel Román para FiberCli



+62 813 1777 1455



fajar@fibercli.com

A top-down view of a meeting table with people's hands, papers, a laptop, and a tablet. The text is overlaid on the image.

# Llave en mano fibra óptica Soporte 24 x 7 Formación en Mikrotik y Seguridad



## Problema

Sufrimos ataques continuos contra nuestros equipos de perimetro.



## Síntomas

Tenemos subidas de CPU y tráfico anómalo en la red.



Solución

Suricata(IDS o IPS) 8



# AGENDA

- Introduction
- IDS / IPS
- Suricata
- Arquitectura
- Reglas
- Salida
- Q and A



# *¿Que es?* **IDS / IPS**



# IPS (Intrusion Prevention System)

Es un dispositivo o aplicación que analiza paquetes completos, tanto cabeceras como payload en busca de eventos conocidos. Cuando se detecta un evento conocido se trata con una acción (drop, reject, alert, pass).



# IDS (Intrusion Detection System)

Es un dispositivo o aplicación que analiza paquetes completos, tanto cabeceras como and **payload**, en busca de eventos conocidos. Cuando se detecta un evento se genera un mensaje de log.



IPS



IDS



# SURICATA



# ¿Qué es Suricata?



“The Suricata Engine is an Open Source Next Generation Intrusion Detection and Prevention Engine. This engine is not intended to just replace or emulate the existing tools in the industry, but will bring new ideas and technologies to the field. The Suricata Engine and the HTP Library are available to use under the GPLv2 “

source :

[https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What\\_is\\_Suricata](https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What_is_Suricata)



# ¿Por qué Suricata?





Features	Bro	Snort	Suricata
Multi-Threaded Processing	No	No	Yes
Complete IPv6 Support	Yes	Some	Yes
IP Reputation	Somewhat	No	Yes
Automated Protocol Detection	Yes	No	Yes
GPU Acceleration	No	No	Yes
Global Variables/Flowbits	Yes	No	Yes
Inline Windows Support	No	No	Yes
GeoIP Lookups	Yes	No	Yes
Advanced HTTP Parsing	Yes	No	Yes
HTTP Access Logging	Yes	No	Yes
SMB Access Logging	Planned	No	Yes
HTTP Blocklist Lookups	Yes	No	Yes
Free	Yes	Some	Yes

# Arquitecturas



# Modo IDS





# A favor

- Barato
- No hay un punto único de fallo
- Rápido para desplegar



# En contra

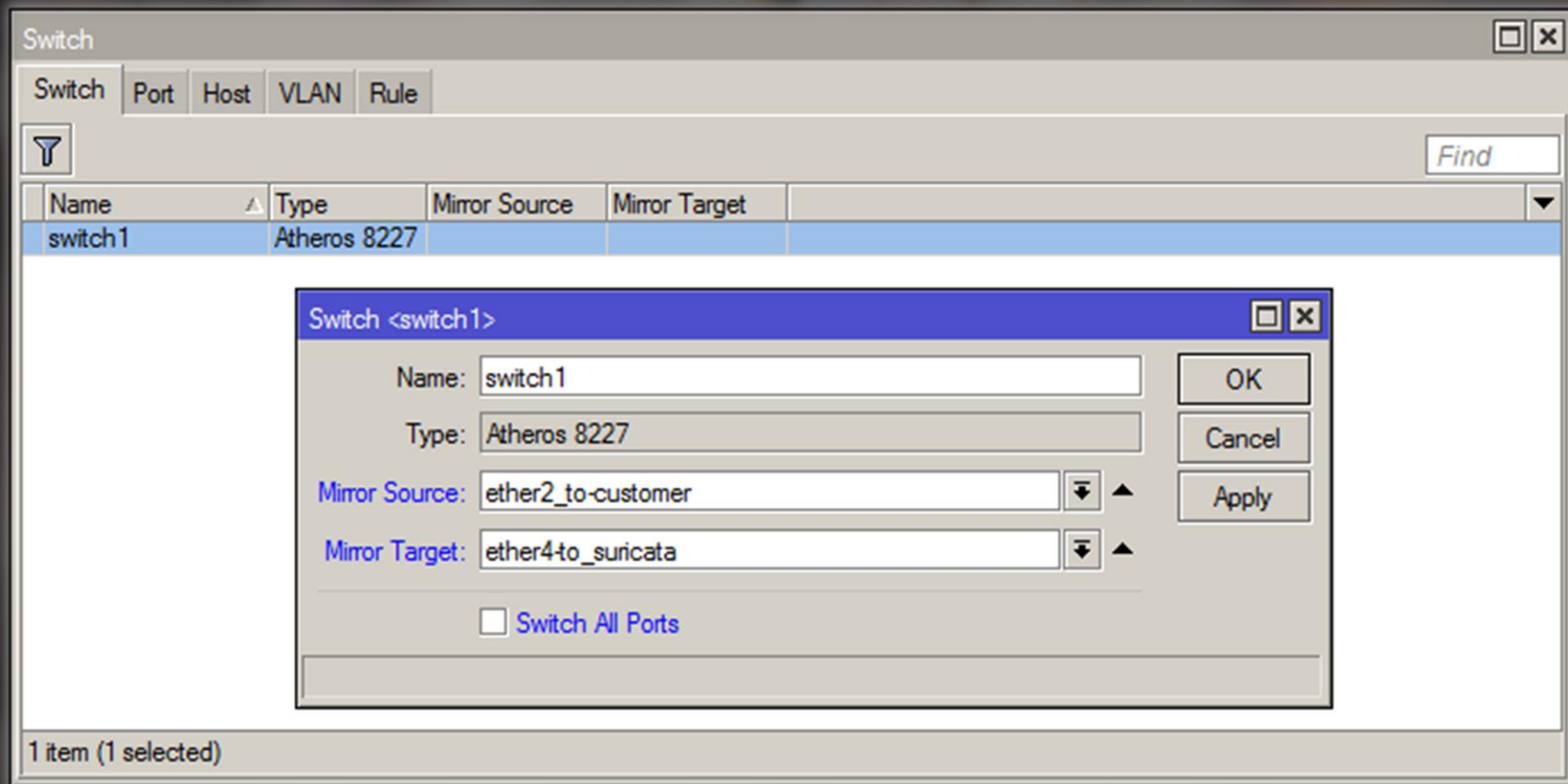
- Vista limitada del ataque
- Acciones limitadas ante un ataque.



# Mikrotik

## Port Mirroring



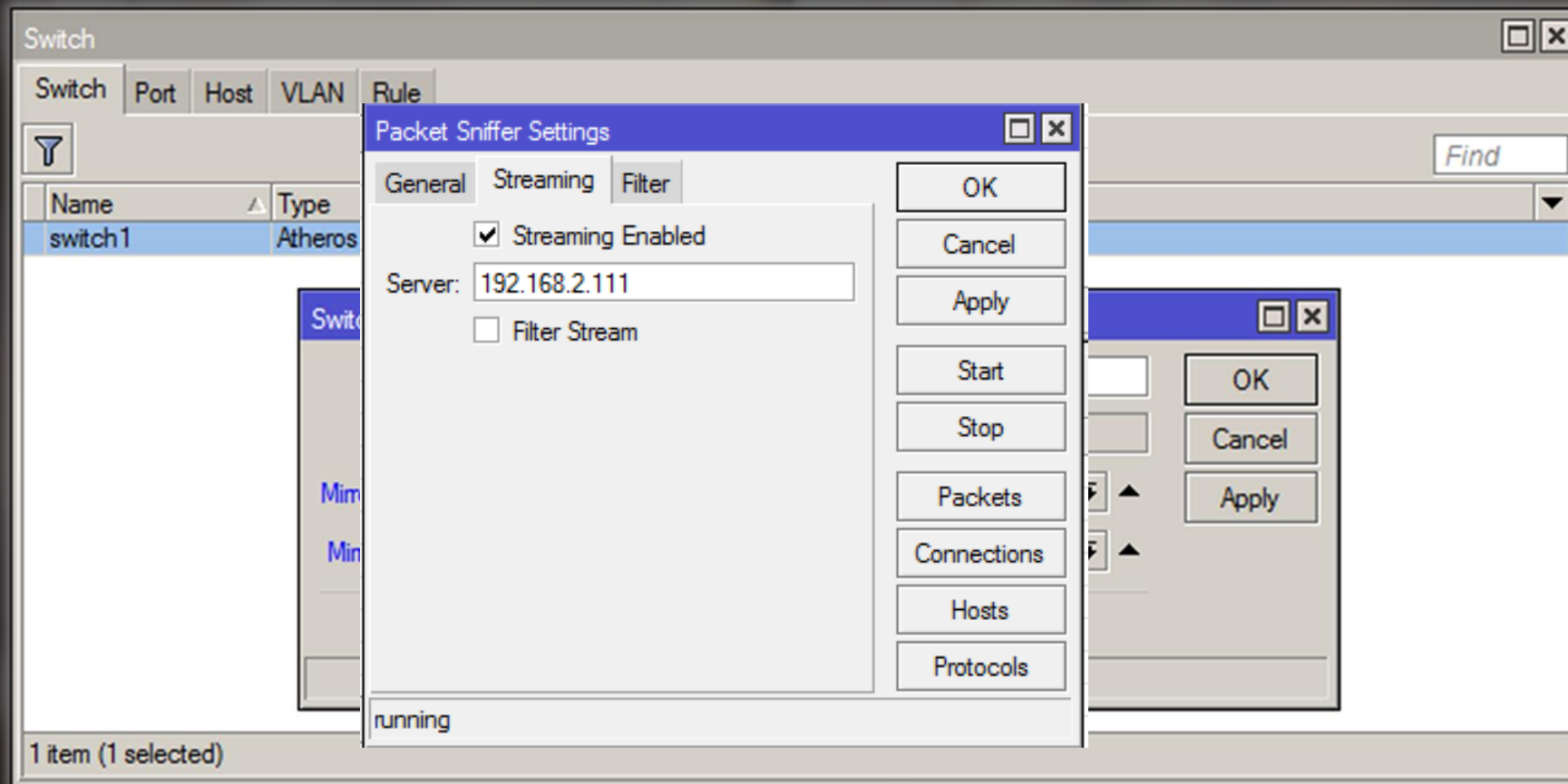


<http://www.mikrotik.com/download/trafr.tgz>

`interface ethernet switch set switch1 mirror-source=ether2_to-customer mirror-target=ether4-to_suricata name=switch1`







O bien

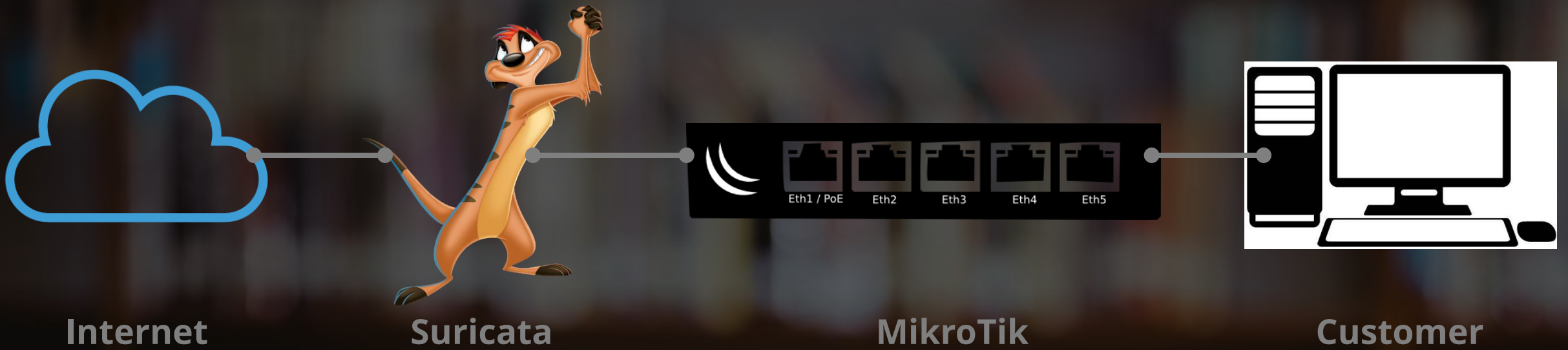
`/ip firewall calea add chain=forward action=sniff sniff-target=192.168.30.1`



# IDS / IPS

## In-line mode





# A favor

- Capaz de tomar acciones contra el tráfico malicioso
- Puede identificar origen y destino con mayor precisión
- No necesita mucha configuración en otros equipos de la red(i.e. router or switch)



# En contra

- Punto único de fallo.
- Mayores requisitos hardware.
- Configuración más compleja.



# Instalación y Configuración

```
apt-get -y install libpcre3 libpcre3-dbg libpcre3-dev build-essential autoconf automake libtool libpcap-dev libnet1-dev libyaml-0-2 libyaml-dev zlib1g zlib1g-dev libmagic-dev libcap-ng-dev libjansson-dev pkg-config
```



# Instalación y Configuración

```
wget http://www.openinfosecfoundation.org/download/suricata-3.0.tar.gz  
tar -xvzf suricata-3.0.tar.gz cd suricata-3.022
```



# Instalación y Configuración

```
./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var
```

```
make
```

```
make install
```

O bien

```
make install-rules
```





# Formato de las Reglas



# Formato de las reglas

1. Action = (drop, reject, alert, pass)
2. Header = (protocol address port direction address port)
  - Protocol = IP (all/any), TCP, UDP, ICMP
  - Address = IPv4, IPv6, \$HOME\_NET, \$EXTERNAL\_NET
  - Direction = -> (*from to*), <> (*bidirectional*)
3. Rule option



# Formato de las reglas

```
alert dns any any -> any any (msg:"SURICATA DNS Z flag set";  
app-layer-event:dns.z_flag_set; sid:2240006; rev:1;)
```



Acción



Header



Opciones



# Acción

Pass: Si una firma coincide y contiene pass, Suricata detiene el escaneo del paquete y salta al final de todas las reglas (solamente para el paquete actual)



# Acción

Drop: Esta acción es solo para el modo IPS. Si el programa encuentra una firma que coincide, suricata para inmediatamente el emisor del paquete no recibe un mensaje con lo que ha pasado. Suricata genera una alerta.



# Acción

Reject: Esta acción es un rechazo activo del paquete, tanto el emisor como el receptor reciben un paquete rechazado. Si es TCP será a Rest-packet, si es otro protocolo recibirán un icmp-error packet. Suricata también genera una alerta.



# Acción

Alert: Si una firma coincide y contiene alert, el paquete será tratado como cualquier otro paquete que no es una amenaza, pero se generará un alerta.



# Cabecera

Protocolo: Esta palabra reservada significa el protocolo que va a analizar la firma. Se puede elegir entre cuatro configuraciones: tcp, udp, icmp e ip.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET  
TROJAN Likely Bot  
Nick in IRC (USA +..)"; flow:established,to_server;  
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK  
.USA.[0-9]{3,}/i"; classtype:trojan-activity;  
reference:url,doc.emergingthreats.net/2008124;  
reference:url,www.emergingthreats.net/cgi-  
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;  
sid:2008124; rev:2;)
```





# Cabecera

## Source y destination

Se pueden asignar direcciones IPv4 y IPv6 tanto combinadas como separadas. Se pueden utilizar también variables. Estas variables se pueden asignar en el fichero Yaml

```
drop tcp $HOME_NET any -> SEXTERNAL_NET any (msg:"ET  
TROJAN Likely Bot  
Nick in IRC (USA +..)"; flow:established,to_server;  
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK  
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;  
reference:url,doc.emergingthreats.net/2008124;  
reference:url,www.emergingthreats.net/cgi-  
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;  
sid:2008124; rev:2;)
```



# Cabecera

## Puertos

Se pueden asignar puertos o wildcards como any.

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET  
TROJAN Likely Bot  
Nick in IRC (USA +..)"; flow:established,to_server;  
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK  
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;  
reference:url,doc.emergingthreats.net/2008124;  
reference:url,www.emergingthreats.net/cgi-  
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;  
sid:2008124; rev:2;)
```



# Cabecera

## Dirección

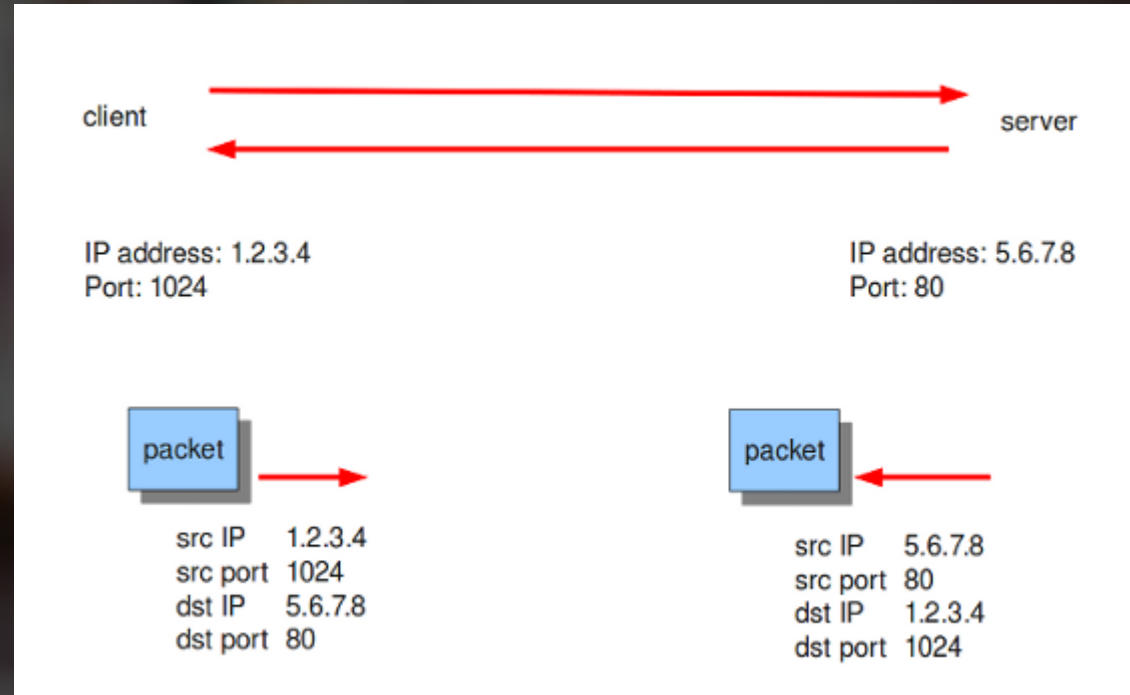
Nos indica en que dirección debe coincidir la firma.

source -> destination

source <> destination ambas direcciones



# Cabecera



# Cabecera

```
drop tcp $HOME_NET any -> $EXTERNAL_NET any (msg:"ET  
TROJAN Likely Bot  
Nick in IRC (USA +..)"; flow:established,to_server;  
flowbits:isset,is_proto_irc; content:"NICK "; pcre:"/NICK  
.*USA.*[0-9]{3,}/i"; classtype:trojan-activity;  
reference:url,doc.emergingthreats.net/2008124;  
reference:url,www.emergingthreats.net/cgi-  
bin/cvsweb.cgi/sigs/VIRUS/TROJAN_IRC_Bots;  
sid:2008124; rev:2;)
```



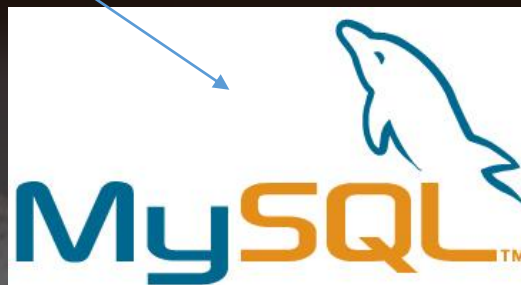
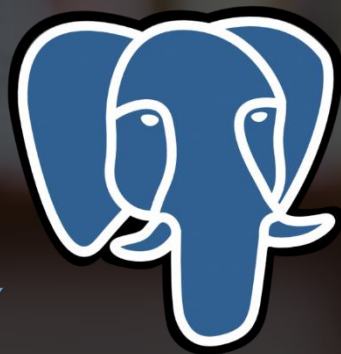
# Cabecera

- Hay configuraciones especiales para
- meta-information.
- headers
- payloads
- flows



# Salidas de Suricata







## Eve JsonOutput

Desde la versión 2.0, Suricata puede producir la salida de alerts, http events, dnsevents, tlsevents a través de json.



La forma más común de utilizar esta salida es a través de EVE, donde todos los logs van a un solo fichero.



Esta salida puede ser tratada por una variedad importante de herramientas.  
ELK (elasticsearch, logstash, kibana)



Options

5m 15m 1h 6h 12h 24h 2d 7d 30d

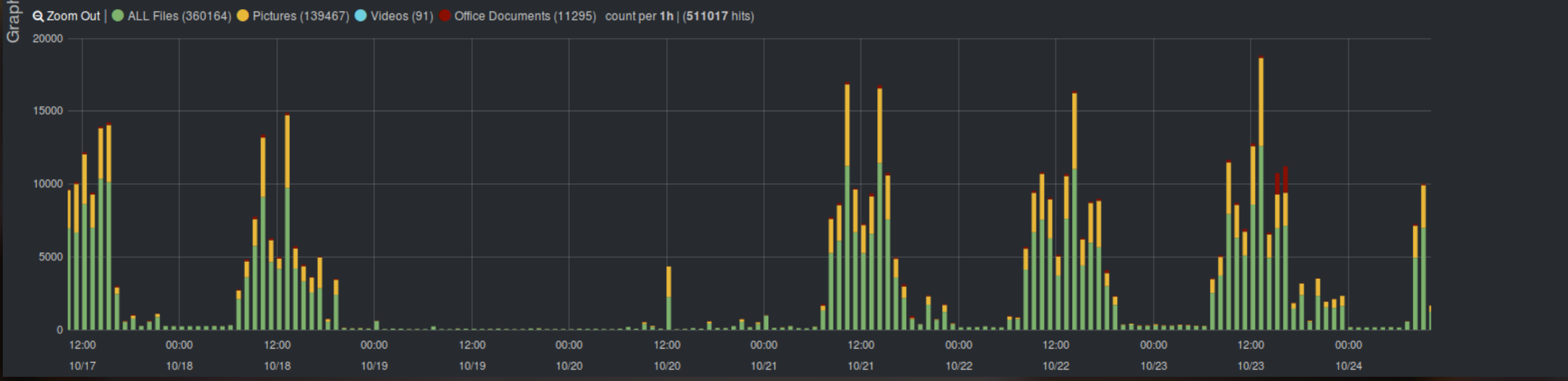
Relative | Absolute | Since |  Auto-refresh

Term	Count	Action
logs	360164	<a href="#">Q</a> <a href="#">🔍</a>

Query Filters

### Events over time

Zoom Out | ALL Files (360164) | Pictures (139467) | Videos (91) | Office Documents (11295) | count per 1h | (511017 hits)



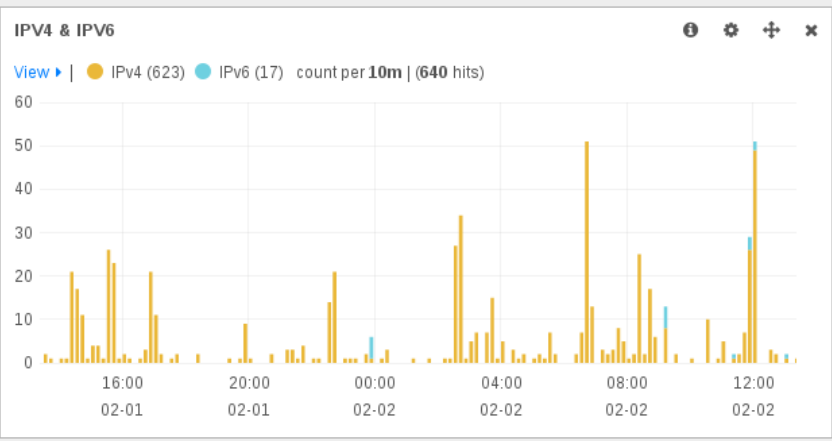
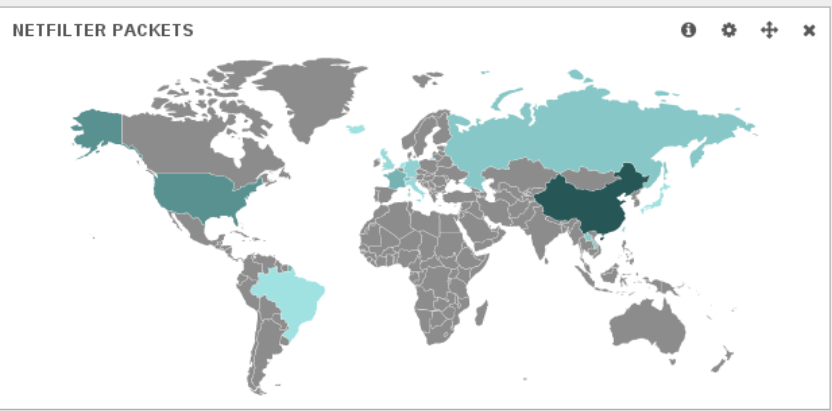
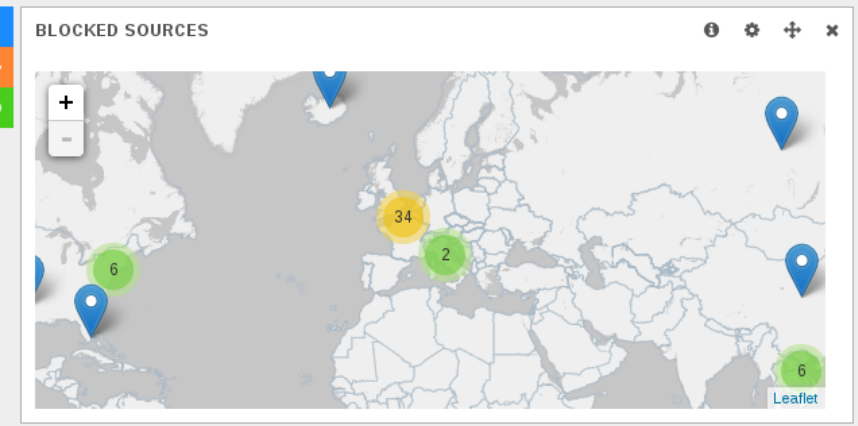
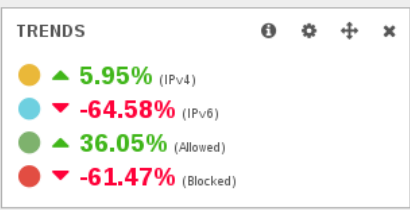
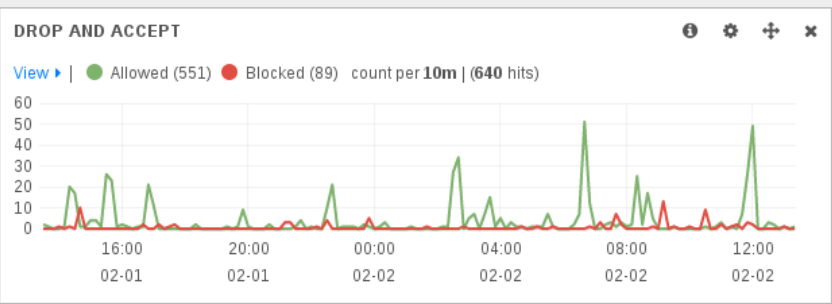
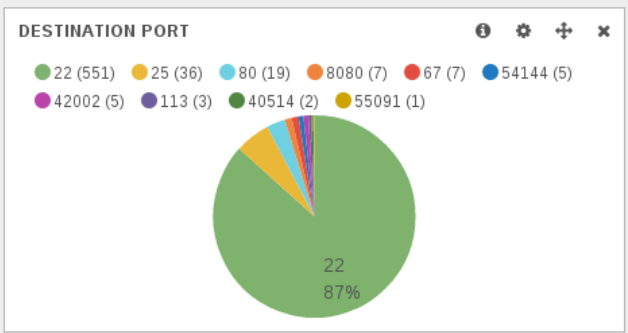
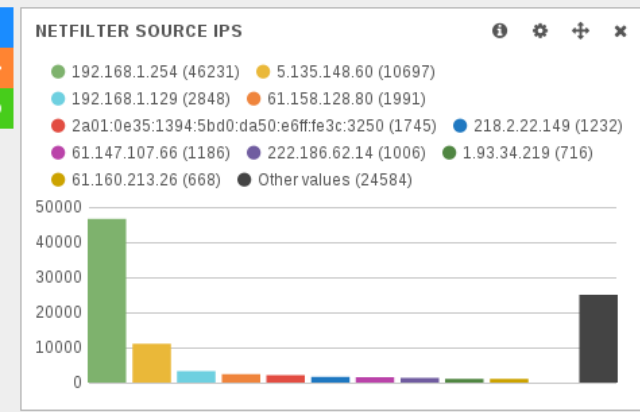
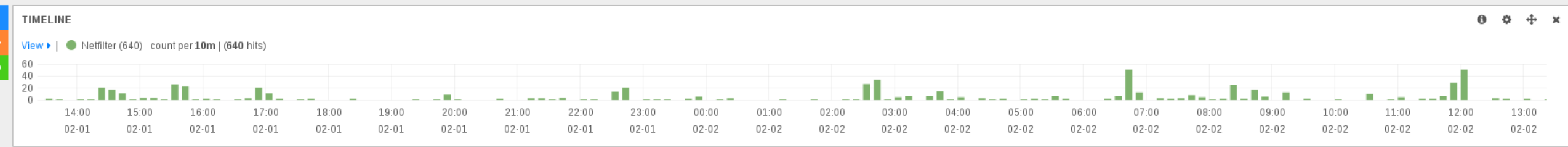


### Downloaded files from www hosts

Term	Count	Action
dropbox.com	39001	Q Ø
notify2	8811	Q Ø
time.c[REDACTED].com	7949	Q Ø
track.adform.net	7714	Q Ø
notify9	6153	Q Ø
notify1	6011	Q Ø
analytics.com	5847	Q Ø
www.google	5843	Q Ø
engine.widespace.com	5143	Q Ø
emediate.eu	4602	Q Ø
ads.c[REDACTED]	4511	Q Ø
gymguide.com	4251	Q Ø
tracker.brokenstones.me	3648	Q Ø
42532	3648	Q Ø
img.tradera.com	3364	Q Ø



QUERY FILTERING






# SELK



MUCHAS GRACIAS!



A close-up photograph of a dog's face, focusing on its eyes and nose. The dog has light brown and white fur. The background is a clear blue sky with some blurred greenery on the left. A semi-transparent grey horizontal bar is overlaid across the middle of the image, containing the text '¿Preguntas?'.

¿Preguntas?

# Referencias

<http://security.stackexchange.com/questions/44931/difference-between-ids-and-ips-and-firewall>

[https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What\\_is\\_Suricata](https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What_is_Suricata)

<http://suricata-ids.org/features/all-features/>

[https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata\\_Rules](https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_Rules)

[https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Script\\_FollowJSON](https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Script_FollowJSON)

<https://redmine.openinfosecfoundation.org/projects/suricata/wiki/MySQL>

<https://redmine.openinfosecfoundation.org/projects/suricata/wiki/PostgreSQL>

<https://redmine.openinfosecfoundation.org/projects/suricata/wiki/MongoDB>