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, programaación, sistemas y Base de datos.***

MADRID / PRAGUE

+34 652 241431

@MAFIASOLEH

Jose.roman@fibercli.com

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) Infrastucture *(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

+62 813 1777 1455

@MAFIASOLEH

fajar@fibercli.com

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 :

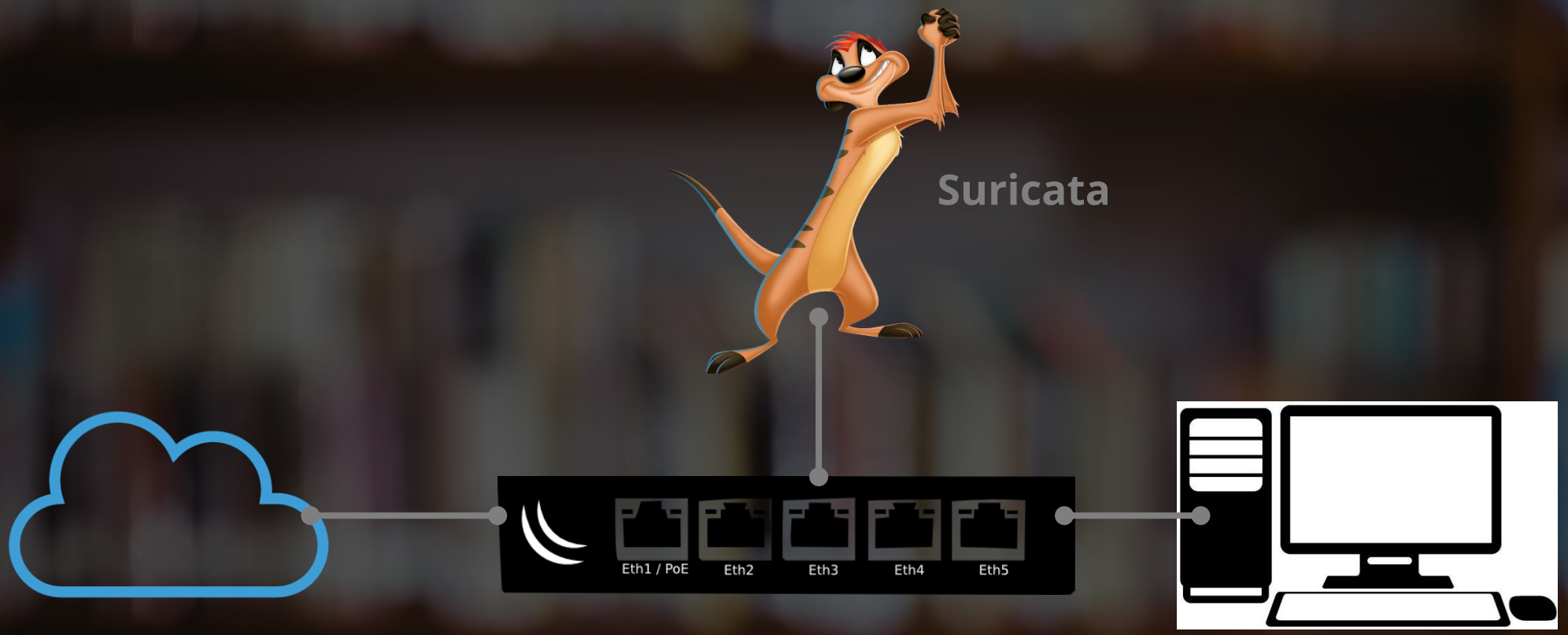
https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What_is_Suricata

¿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


Suricata
Eth1 / PoE
Eth2
Eth3
Eth4
Eth5
Internet
MikroTik
Customer

A favor

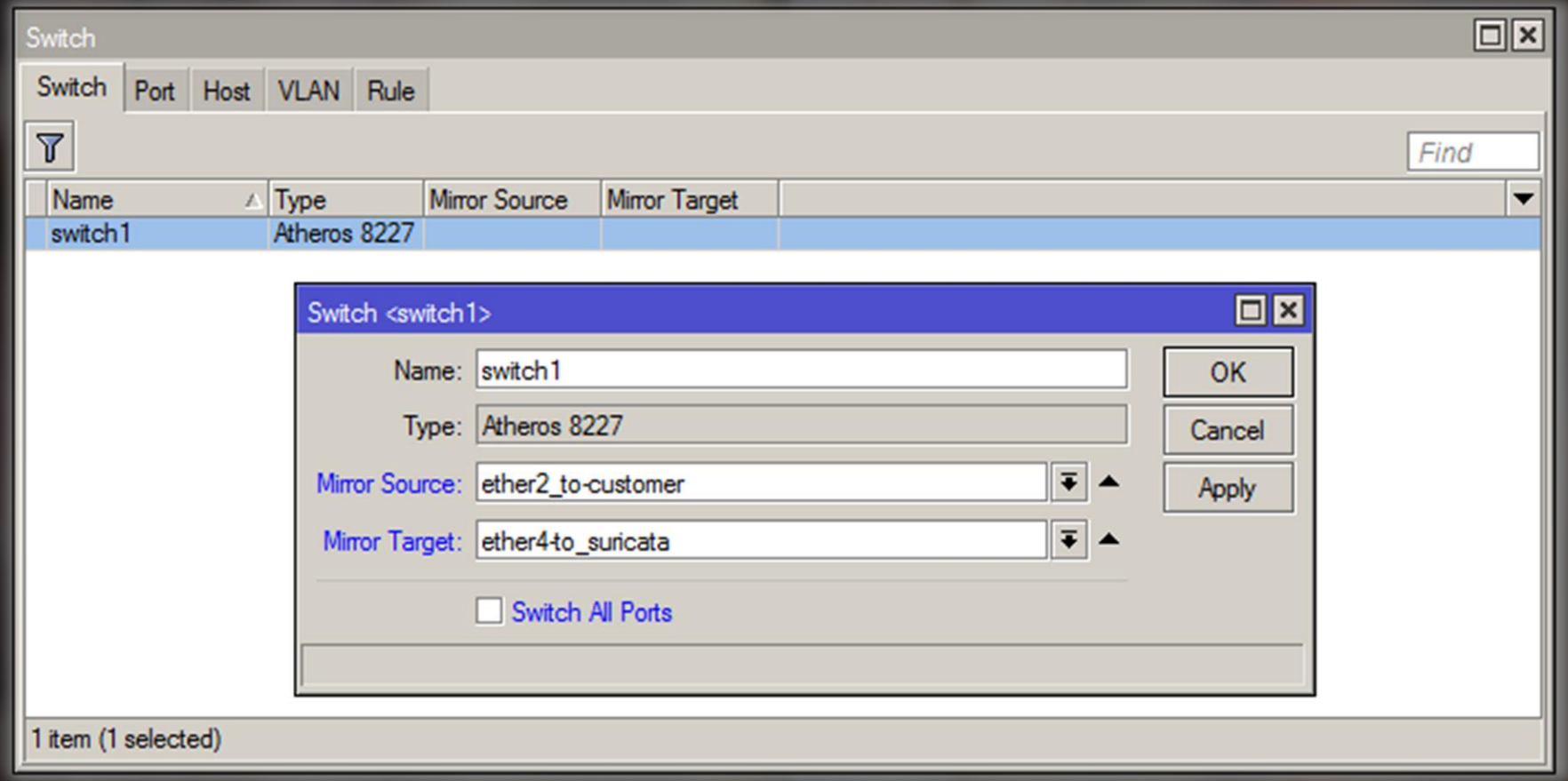
- Barato
- No hay un punto único de fallo
- Rápido para desplegar

En contra

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

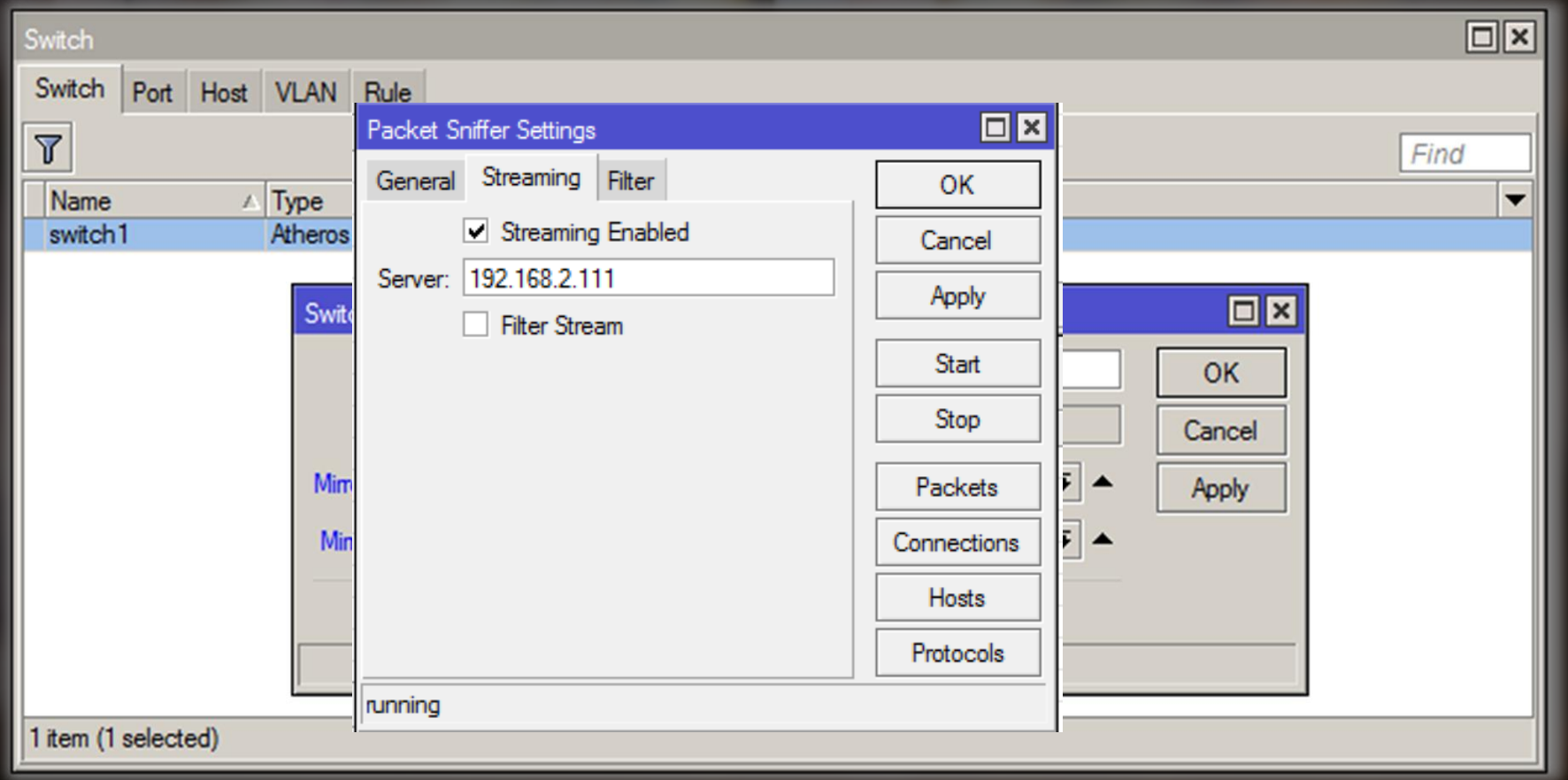
Mikrotik

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

Internet Suricata MikroTik Customer

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, suricatapara inmediatamente el emisor del paquete no recibe un mensaje con lo que ha pasado. Suricatagenera 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, icmpe 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 direccionesIPv4 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 -> $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

Puertos

Se pueden asignar puertos o wildcars 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

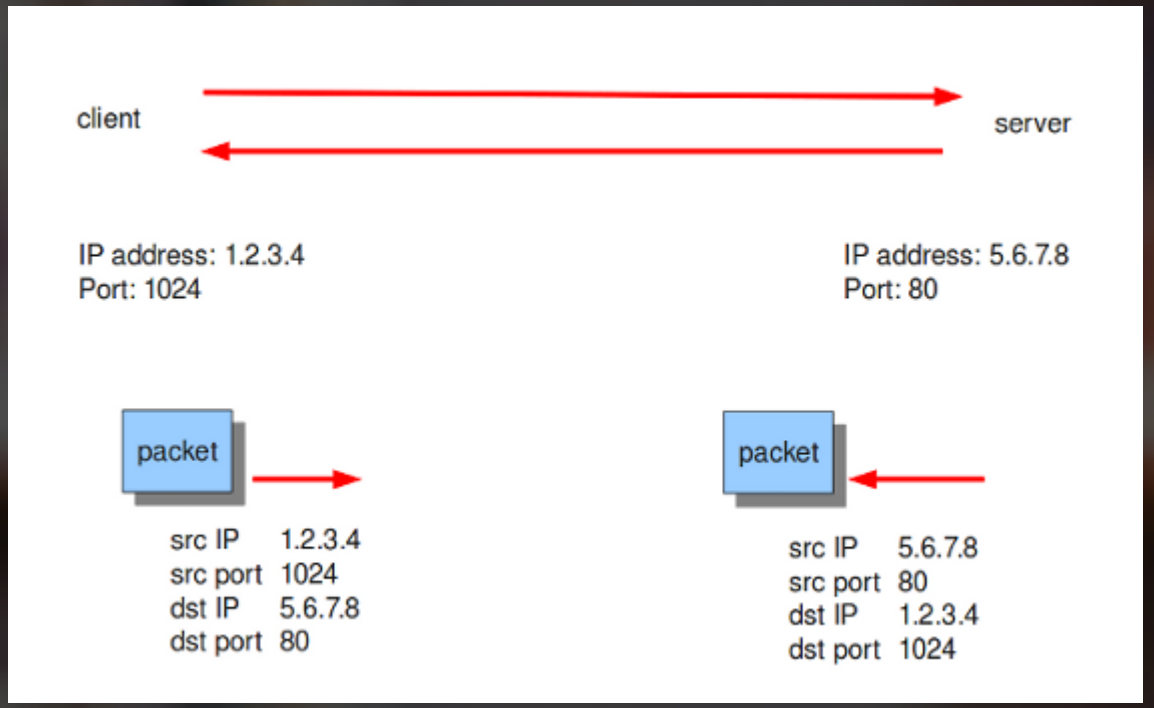
Dirección

Nos indica en que dirección debe coincidir la firma.

source -> destination

source <> destination ambas direcciones

Cabecera


client
server
IP address: 1.2.3.4
Port: 1024
IP address: 5.6.7.8
Port: 80
packet
src IP 1.2.3.4
src port 1024
dst IP 5.6.7.8
dst port 80
packet
src IP 5.6.7.8
src port 80
dst IP 1.2.3.4
dst port 1024

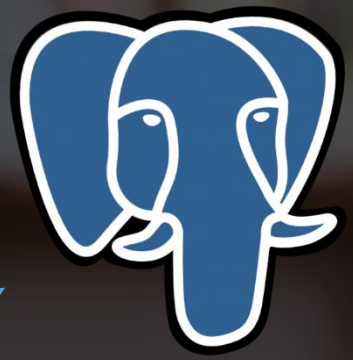
Cabecera

```
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;)
```

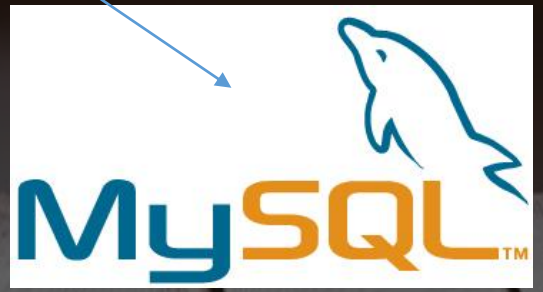
Cabecera

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

Salidas de Suricata




mongoDB


MySQL

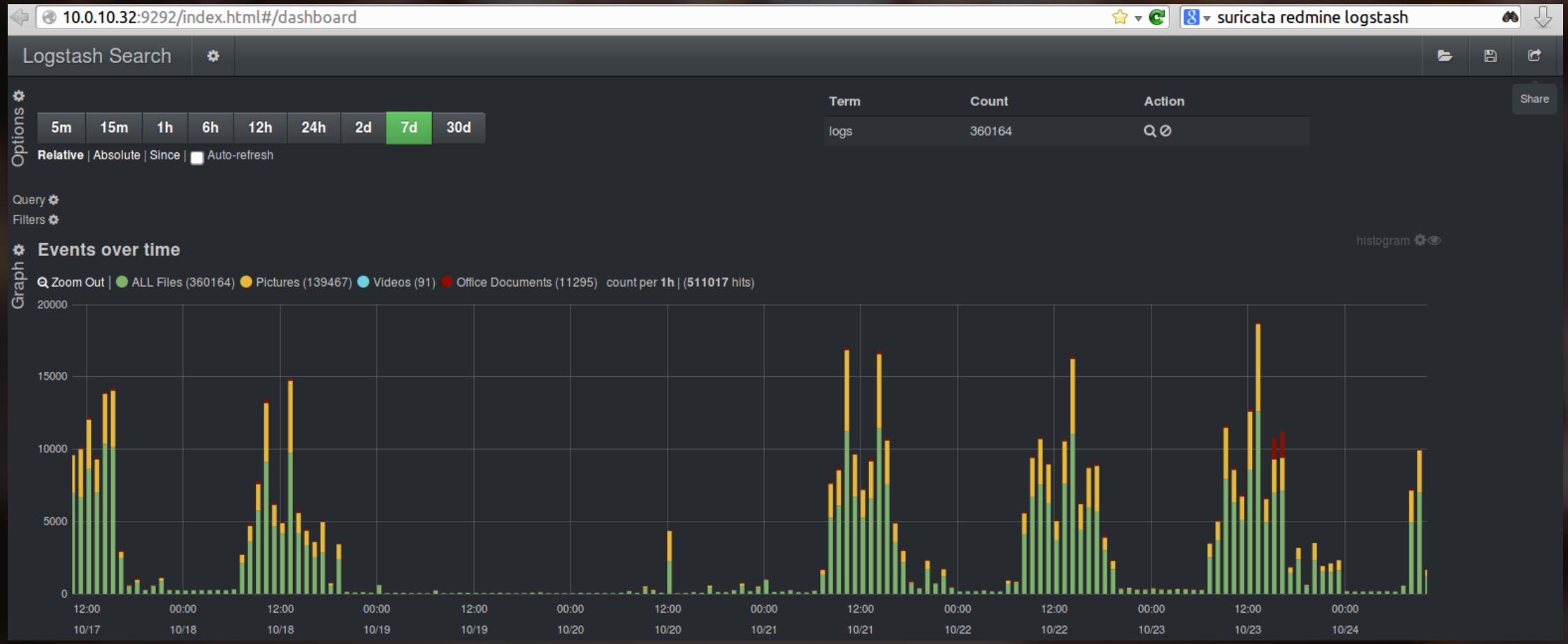
Eve JsonOutpus

Desde la versión2.0, 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)


10.0.10.32:9292/index.html#/dashboard
suricata redmine logstash
Logstash Search
Share
Options
5m 15m 1h 6h 12h 24h 2d 7d 30d
Relative | Absolute | Since | Auto-refresh
Term Count Action
logs 360164
Query
Filters
Graph
Events over time
histogram
Zoom Out | ALL Files (360164) Pictures (139467) Videos (91) Office Documents (11295) count per 1h | (511017 hits)
20000
15000
10000
5000
0
12:00 10/17
00:00 10/18
12:00 10/18
00:00 10/19
12:00 10/19
00:00 10/20
12:00 10/20
00:00 10/21
12:00 10/21
00:00 10/22
12:00 10/22
00:00 10/23
12:00 10/23
00:00 10/24

Downloaded files from www hosts

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

Netfilter Logs

a day ago to a few seconds ago refreshed every 1m

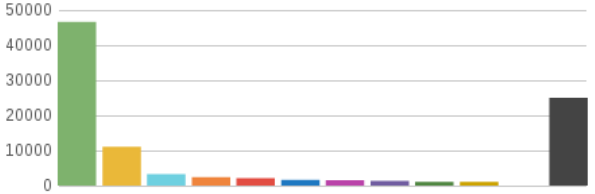
QUERY FILTERING

TIMELINE

View | Netfilter (640) count per **10m** | (**640** hits)

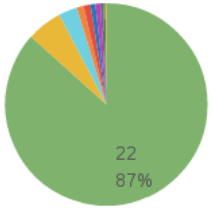
NETFILTER SOURCE IPS

192.168.1.254 (46231) 5.135.148.60 (10697)
192.168.1.129 (2848) 61.158.128.80 (1991)
2a01:0e35:1394:5bd0:da50:e6ff:fe3c:3250 (1745) 218.2.22.149 (1232)
61.147.107.66 (1186) 222.186.62.14 (1006) 1.93.34.219 (716)
61.160.213.26 (668) Other values (24584)



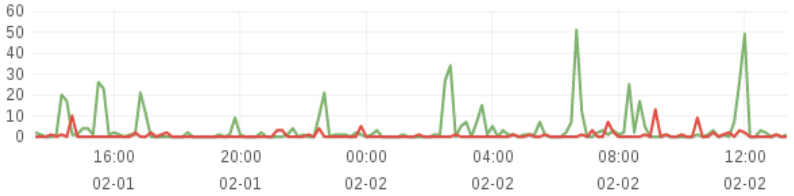
DESTINATION PORT

22 (551) 25 (36) 80 (19) 8080 (7) 67 (7) 54144 (5)
42002 (5) 113 (3) 40514 (2) 55091 (1)



DROP AND ACCEPT

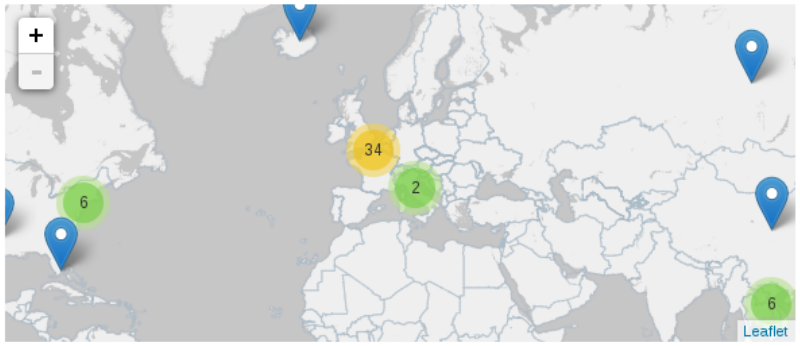
View | Allowed (551) Blocked (89) count per **10m** | (**640** hits)



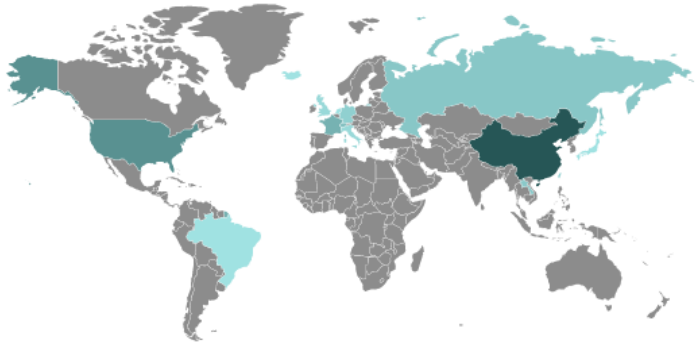
TRENDS

▲ 5.95% (IPv4)
▼ -64.58% (IPv6)
▲ 36.05% (Allowed)
▼ -61.47% (Blocked)

BLOCKED SOURCES

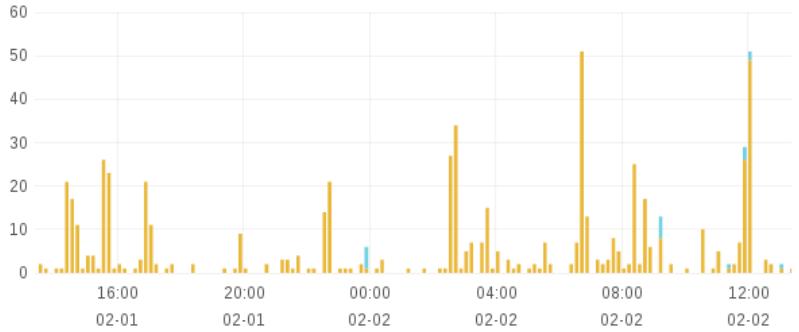


NETFILTER PACKETS



IPV4 & IPV6

View | IPv4 (623) IPv6 (17) count per **10m** | (**640** hits)




SELK


MUCHAS GRACIAS!


¿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

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

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/MySQL

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

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