MUM MikroTik User Meeting

# Utilizando RouterOS como IPS / IDS (II)

Por: Maximiliano Dobladez
MKE Solutions

15, 16 November

Buenos Aires, Argentina



MKE solutions

# Presentación Personal

- Nombre: Maximiliano Dobladez
- ***CEO MKE Solutions***
- Consultor y Entrenador ***MikroTik RouterOS***
- Experiencia con *MikroTik RouterOS* desde 1999
- Entrenador desde 2006


- info@mkesolutions.net


- mdobladez


- @mdobladez

# MKE Solutions

- Consultora en Telecomunicaciones
- Establecida en 2008
- Certificada en **ISO 9001:2015**
  - Soporte IT
  - Entrenamientos Oficiales


info@mkesolutions.net

@mkesolutions

/mkesolutions

/mkesolutions

*www.MKESolutions.net*

+54 9 358 4210029

MUM

# Academia de Entrenamientos

MikroTik MTCNA

MikroTik MTCWE

MikroTik MTCTCE

MikroTik MTCUME

MikroTik MTCIPv6E

MikroTik MTCRE

MikroTik MTCINE

- Entrenamientos Públicos y Privados.
- MikroTik Academy

Academia DE ENTRENAMIENTOS

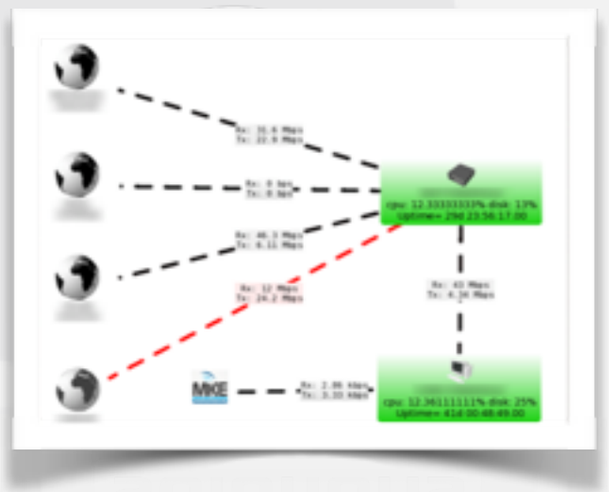
MikroTik

powered by MKE Solutions

MKE solutions

# Soporte IT

- Diseño, desarrollo e implementación de soluciones.
- Incidencias puntuales.
- Soporte mensual (OutSourcing).
  - Revisión y Optimización
  - Actualización
  - Mantenimiento preventivo
  - Monitoreo
  - Asesoramiento
  - Soporte Prioritario
  - Guardia 24x7
  - Implementaciones Adicionales

MUM

# Oráculo

oraculo monitoreo de redes

Status | Dashboard | Devices (226) | Maps | Syslog | Settings | Backups | Events (2) | ConfigHistory (1450) | Timeouts (4) | Account

**NETWORK ONLINE** 98.23% — Online 222 | Offline 4

**TOTAL DEVICES** 226 — Warning 3 | Timeout 4 | No Login 0

**TOTAL PORTS &** 76419 — Sensors 73147 | Ports 3230 | Add Options 42

**EVENTS UNREAD** 2 — With Warning Status 2

**CONFIG HISTORY** 1450 — Monitoring Devices 1

**DISK USAGE** 54% — Files Backups 21537 | Disk Backups 27G

## Oraculo Server Status

| Date | Uptime | License | Status | Bot Telegram | WebService |
|---|---|---|---|---|---|
| 2018-04-11 14:30:28 | 14:30:28 | OUTSOURCING | VALID_LICENSE | OK | OK |
| **# CPU info** | **CPU avr** | **Memory** | **Mem Used** | **Disk System** | **Disk Used** |
| 3 Cores - Virtual a7769a6388d5 | *2.61 1.92 1.91* | 3.9 GiB | 95% | 59 GiB | 56% |

## Overview (1 Hour)

| Device | AV 1h | RTT | PL | Downs | Alarms | Reboot | PF | Important |
|---|---|---|---|---|---|---|---|---|
| [redacted] | 0% | 0 ms | 100% | 0 | 0 | 0 | 0 | 4 |
| [redacted] | 0% | 0 ms | 99.97% | 0 | 0 | 0 | 0 | 4 |
| [redacted] | 0% | 0 ms | 99.97% | 0 | 0 | 0 | 0 | 4 |
| [redacted] | 0% | 0 ms | 98.21% | 0 | 0 | 0 | 0 | 2 |
| [redacted] | 95.729% | 331.52 ms | 20.7% | 15 | 0 | 0 | 0 | 2 |

## GeoMAPs Category

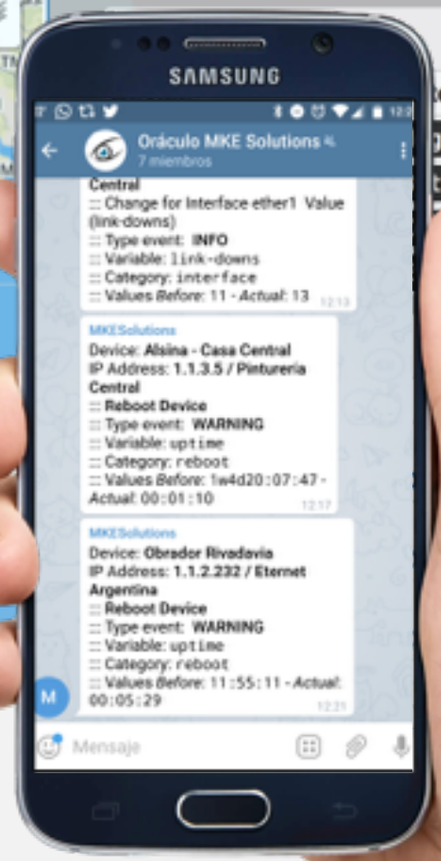
ZoomOut


## Last Devices Timeout

| Category | Last Seen | Last Probe | Status |
|---|---|---|---|
| gaImagen | 40 minutes ago | 44 minutes ago | Timeout |
| te Solution S.A. | 20 hours ago | 20 hours ago | Timeout |
| IP | March 28 | March 28 | Timeout |
| Argentina | March 27 | March 27 | Timeout |

## Last Events

| Event | Variable | Before | Actual |
|---|---|---|---|
| bgp | Change value for **peer** **Cache de Facebook BGP** | connect | active |
| bgp | Change value for **peer** **Cache de Facebook BGP** | active | connect |
| bgp | Change value for **peer** **Cache de Facebook BGP** | connect | active |
| bgp | Change value for **peer** | active | connect |




oraculo.mkesolutions.net

MikroTik

MKE solutions

# Agenda

*Desarrollo de la presentación:*

- **IDS / IPS**
- **Suricata**: qué es?, cómo funciona? cómo se instala?
- **Suricata-Update**: qué es?, cómo funciona? cómo se instala?
- **Suricata2MikroTik**: qué es?, cómo funciona? cómo se instala?
- Integración con **RouterOS**
- Recursos y bibliografía

# IDS / IPS

## IDS (Intrusion Detection System)

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

## IPS (Intrusion Prevention System)

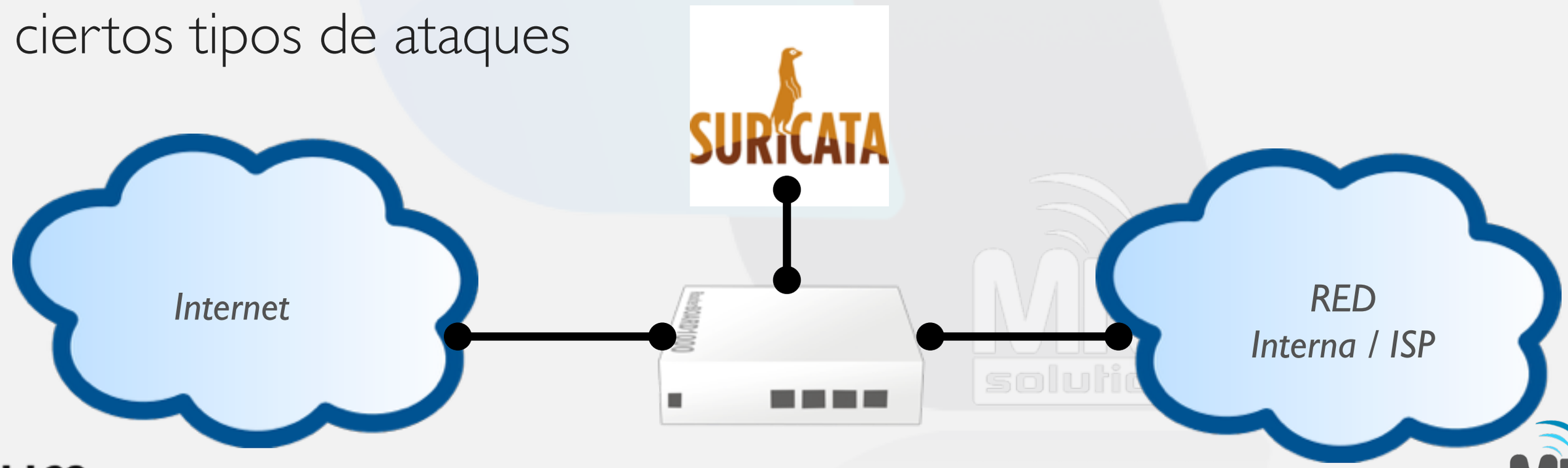
- Es un dispositivo o aplicación que analiza paquetes completos, tanto cabeceras como payload en busca de eventos conocidos.
- Utiliza *Firmas*, *Patrones de comportamientos*, *Políticas de seguridad*
- Cuando se detecta un evento conocido se trata con una acción (drop, reject, alert, pass)

# Suricata

# Suricata - Qué es?

**Suricata**:

- Es un IDS / IPS
- Gratuito, Open Source, rápido y robusto.
- Se puede descargar desde: ***https://suricata-ids.org/***
- Puede trabajar en conjunto con ***RouterOS*** para detectar intrusos o ciertos tipos de ataques



# Suricata - Instalación

La instalación de ***Suricata*** puede ser a través de su código fuente o con los pre empaquetados del SO

- Debian: ***apt-get install suricata***.
- Fuente:

*wget https://www.openinfosecfoundation.org/download/suricata-4.0.5.tar.gz*

*tar -xvzf suricata-4.0.5.tar.gz ; cd suricata-4.0.5*
*./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var*

*make*

*make install*

*make install-rules*

# Suricata - Configuración

La configuración de ***Suricata*** se realiza en ***/etc/suricata/suricata.yaml***

Hay que definir:

- Las redes internas:

  *HOME_NET:"[192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]"*

- Activar el formato ***EVE*** con:

  *- eve-log:*

    *enabled: yes*

    *filetype: regular*

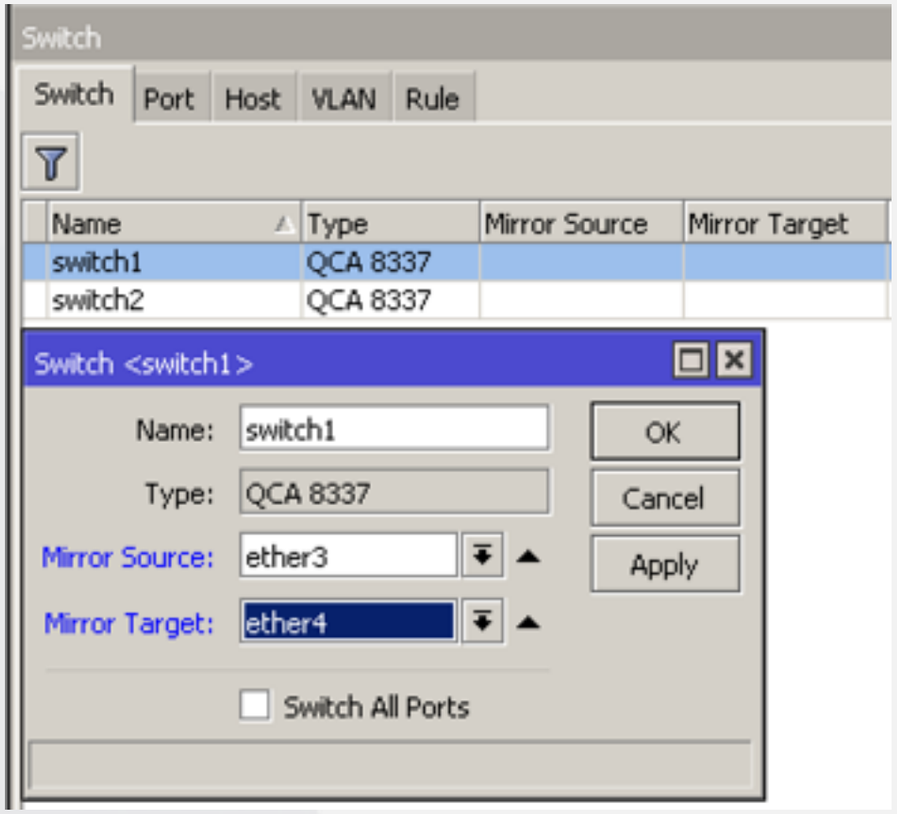
    *filename: eve.json*

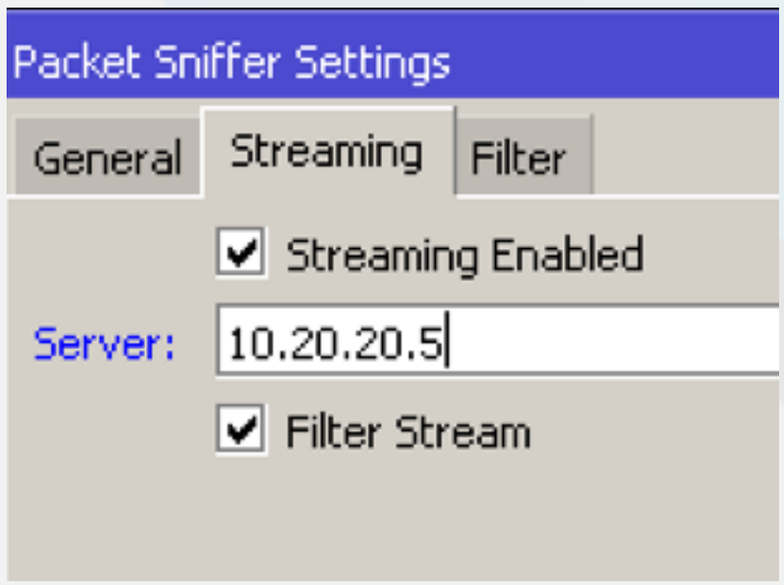
# Suricata - Integración con rOS

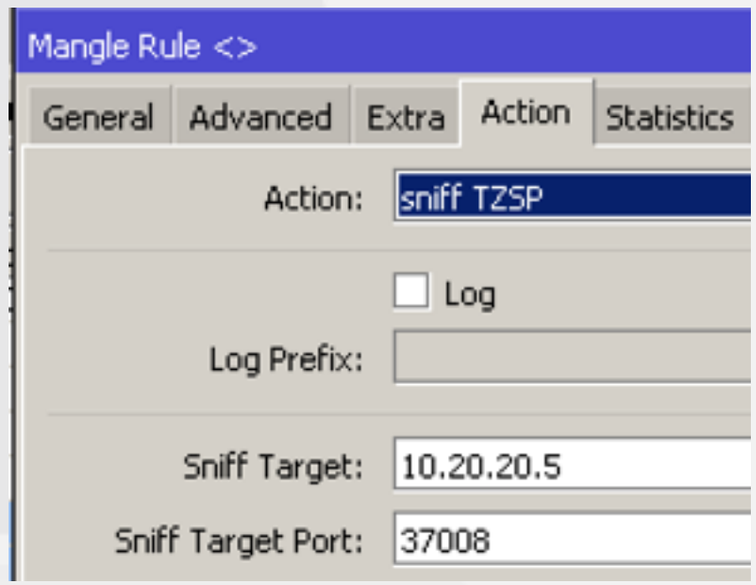
Para que empiece a trabajar hay que redireccionar el tráfico desde el *MikroTik RouterOS* hacia *Suricata*

Podemos realizarlo con:

- ***Port Mirror*** (Switch)
- ***Packet Sniffer*** (Tool Packet Sniffer)
- ***Mangle*** (Sniff TZSP)



# Suricata - Reportes

Los logs estarán en */var/log/suricata*

```
[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority:
[**] [1:2010937:2] ET POLICY Suspicious inbound to mySQL port 3306 [**] [Classification: Potentially Bad Traffic] [Priority:
[**] [1:2010936:2] ET POLICY Suspicious inbound to Oracle SQL port 1521 [**] [Classification: Potentially Bad Traffic] [Prior
[**] [1:2010936:2] ET POLICY Suspicious inbound to Oracle SQL port 1521 [**] [Classification: Potentially Bad Traffic] [Prior
[**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority:
[**] [1:2010935:2] ET POLICY Suspicious inbound to MSSQL port 1433 [**] [Classification: Potentially Bad Traffic] [Priority:
[**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 1
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 19
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 192.168.1.
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 19
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 192.168.1.
[**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 1
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 19
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 192.168.1.
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 19
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 192.168.1.
[**] [1:2002910:4] ET SCAN Potential VNC Scan 5800-5820 [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 1
[**] [1:2010939:2] ET POLICY Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Prior
[**] [1:2010939:2] ET POLICY Suspicious inbound to PostgreSQL port 5432 [**] [Classification: Potentially Bad Traffic] [Prior
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 19
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 192.168.1.
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 19
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 192.168.1.
[**] [1:2002910:4] ET SCAN Potential VNC Scan 5800-5820 [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 1
[**] [1:2003068:6] ET SCAN Potential SSH Scan OUTBOUND [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 19
[**] [1:2001219:18] ET SCAN Potential SSH Scan [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 192.168.1.
[**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 1
[**] [1:2002911:4] ET SCAN Potential VNC Scan 5900-5920 [**] [Classification: Attempted Information Leak] [Priority: 3] {6} 1
[**] [1:2002993:5] ET SCAN Rapid POP3S Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priori
[**] [1:2002992:5] ET SCAN Rapid POP3 Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priorit
[**] [1:2002994:5] ET SCAN Rapid IMAP Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priorit
[**] [1:2002995:8] ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priori
[**] [1:2002995:8] ET SCAN Rapid IMAPS Connections - Possible Brute Force Attack [**] [Classification: Misc activity] [Priori
```

# Suricata - Rules Update

Es necesario mantener la base de datos de reglas actualizadas, para ello utilizaremos ***suricata-update***

***Suricata-update*** permite actualizar las reglas desde varias listas:

```
Name: oisf/trafficid
  Vendor: OISF
  Summary: Suricata Traffic ID ruleset
  License: MIT
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
Name: sslbl/ssl-fp-blacklist
  Vendor: Abuse.ch
  Summary: Abuse.ch SSL Blacklist
  License: Non-Commercial
Name: ptresearch/attackdetection
  Vendor: Positive Technologies
  Summary: Positive Technologies Attack Detection Team ruleset
  License: Custom
```

# Suricata - Rules Update

| | | | | | |
|---|---|---|---|---|---|
| 2026027 | ET TROJAN [PT MALWARE] Hacked Mikrotik C2 Request | Created: 2018-08-23 | Updated: 2018-08-23 | Category: emerging-trojan | Alerts 0 |
| 2025972 | ET EXPLOIT Mikrotik Winbox RCE Attempt (CVE-2018-14847) | Created: 2018-08-06 | Updated: 2018-09-11 | Category: emerging-exploit | Alerts 0 |
| 2025426 | ET EXPLOIT MikroTik RouterOS Chimay Red Remote Code Execution Probe | Created: 2018-03-13 | Updated: 2018-03-13 | Category: emerging-exploit | Alerts 0 |
| 10002456 | ATTACK [PTsecurity] Mikrotik Router OS 6.38.4 Stack Clash RCE | Created: | Updated: | Category: pt-rules | Alerts 0 |
| 10002457 | ATTACK [PTsecurity] Mikrotik Router OS 6.38.4 Stack Clash RCE | Created: | Updated: | Category: pt-rules | Alerts 0 |
| 10002680 | ATTACK [PTsecurity] Mikrotik <6.41.3 <6.42rc27 RCE Attempt (CVE-2018-7445) | Created: | Updated: | Category: pt-rules | Alerts 0 |
| 10002681 | ATTACK [PTsecurity] ShellCode Upload Mikrotik <6.41.3 <6.42rc27 RCE (CVE-2018-7445) | Created: | Updated: | Category: pt-rules | Alerts 0 |
| 10002682 | ATTACK [PTsecurity] Successful Mikrotik <6.41.3 <6.42rc27 RCE (CVE-2018-7445) | Created: | Updated: | Category: pt-rules | Alerts 0 |
| 10003917 | ATTACK [PTsecurity] Mikrotik <6.42 Password disclosure path traversal (CVE-2018-14847) | Created: | Updated: | Category: pt-rules | Alerts 0 |

```
alert tcp any any -> $HOME_NET any (msg:"ET EXPLOIT Mikrotik Winbox RCE Attempt (CVE-2018-14847)"; flow:established,to_server; content:"|680100664d320500ff010600ff09050700
ff090701000021352f2f2f2f2f2e2f2e2e2e2f2f2f2f2f2f2e2f2e2e2e2f2f2f2f2f2f2e2f2e2e2f666c6173682f72772f73746f72652f757365722e6461740200ff8802000000000000800000000100ff8802000200000002
000000|"; offset:0; metadata: former_category EXPLOIT; reference:url,github.com/mrmtwoj/0day-mikrotik; reference:url,www.helpnetsecurity.com/2018/08/03/mikrotik-cryptojack
ing-campaign; reference:cve,2018-14847; classtype:attempted-admin; sid:2025972; rev:3; metadata:affected_product Linux, attack_target Networking_Equipment, deployment Peri
meter, signature_severity Major, created_at 2018_08_06, updated_at 2018_09_11;)
```

# Suricata - Rules Update

Para instalar ***suricata-update***:

Requiere de ***python*** y ***pip***

*pip install --pre --upgrade suricata-update*

Agregamos al ***suricata.yaml***:

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

*rule-files:*

*- suricata.rules*

Actualizamos con:

*suricata-update*

```
6/11/2018 -- 00:13:43 - <Info> -- Done.
6/11/2018 -- 00:13:43 - <Info> -- Checking https://raw.githubusercontent.com/ptresearch/AttackDetection/master/pt.rules.t
6/11/2018 -- 00:13:44 - <Info> -- Remote checksum has not changed. Not fetching.
6/11/2018 -- 00:13:44 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
6/11/2018 -- 00:13:44 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
6/11/2018 -- 00:13:44 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
6/11/2018 -- 00:13:44 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
6/11/2018 -- 00:13:44 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
6/11/2018 -- 00:13:44 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
6/11/2018 -- 00:13:44 - <Info> -- Loading distribution rule file /etc/suricata/rules/smtp-events.rules
6/11/2018 -- 00:13:44 - <Info> -- Loading distribution rule file /etc/suricata/rules/stream-events.rules
6/11/2018 -- 00:13:44 - <Info> -- Loading distribution rule file /etc/suricata/rules/tls-events.rules
6/11/2018 -- 00:13:44 - <Info> -- Ignoring file rules/emerging-deleted.rules
6/11/2018 -- 00:13:46 - <Info> -- Loaded 24253 rules.
6/11/2018 -- 00:13:47 - <Info> -- Disabled 18 rules.
6/11/2018 -- 00:13:47 - <Info> -- Enabled 0 rules.
6/11/2018 -- 00:13:47 - <Info> -- Modified 0 rules.
6/11/2018 -- 00:13:47 - <Info> -- Dropped 0 rules.
6/11/2018 -- 00:13:47 - <Info> -- Enabled 36 rules for flowbit dependencies.
6/11/2018 -- 00:13:47 - <Info> -- Backing up current rules.
6/11/2018 -- 00:13:50 - <Info> -- Writing rules to /var/lib/suricata/rules/suricata.rules: total: 24253; enabled: 19309;
6/11/2018 -- 00:13:50 - <Info> -- Testing with suricata -T.
6/11/2018 -- 00:13:59 - <Info> -- Done.
```

# Suricata - Reportes

Es posible integrarlo con otras Aplicaciones para un reporte mas "amigable", podemos integrar ***ELK*** (Elasticsearch, Logstash, Kibana)

# Suricata - Live CD

Existen distribuciones listas para utilizar:

- ***SELKS*** (Live CD - Open Source *IDS/IPS* basado en *Debian*) bajo GPLv3 por ***Stamus Networks***

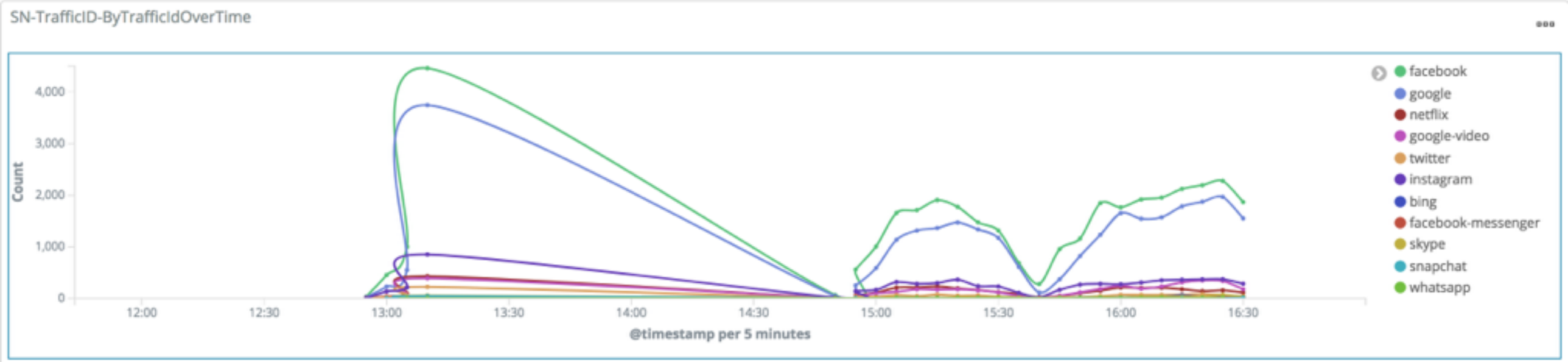
***SELKS*** tiene los siguientes componentes:

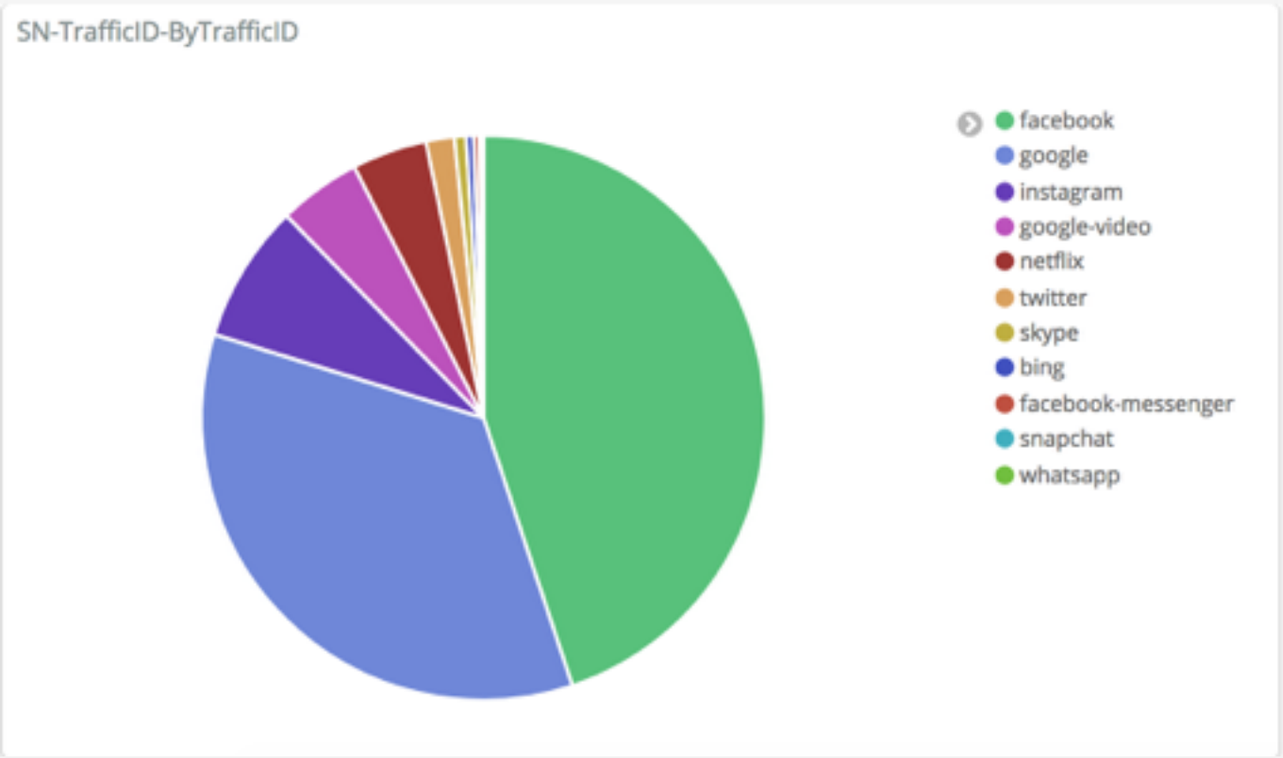
- S - ***Suricata*** - http://suricata-ids.org/
- E - ***Elasticsearch*** - http://www.elasticsearch.org/overview/
- L - ***Logstash*** - http://www.elasticsearch.org/overview/
- K - ***Kibana*** - http://www.elasticsearch.org/overview/
- S - ***Scirius*** - https://github.com/StamusNetworks/scirius
- ***EveBox*** - https://codemonkey.net/evebox/

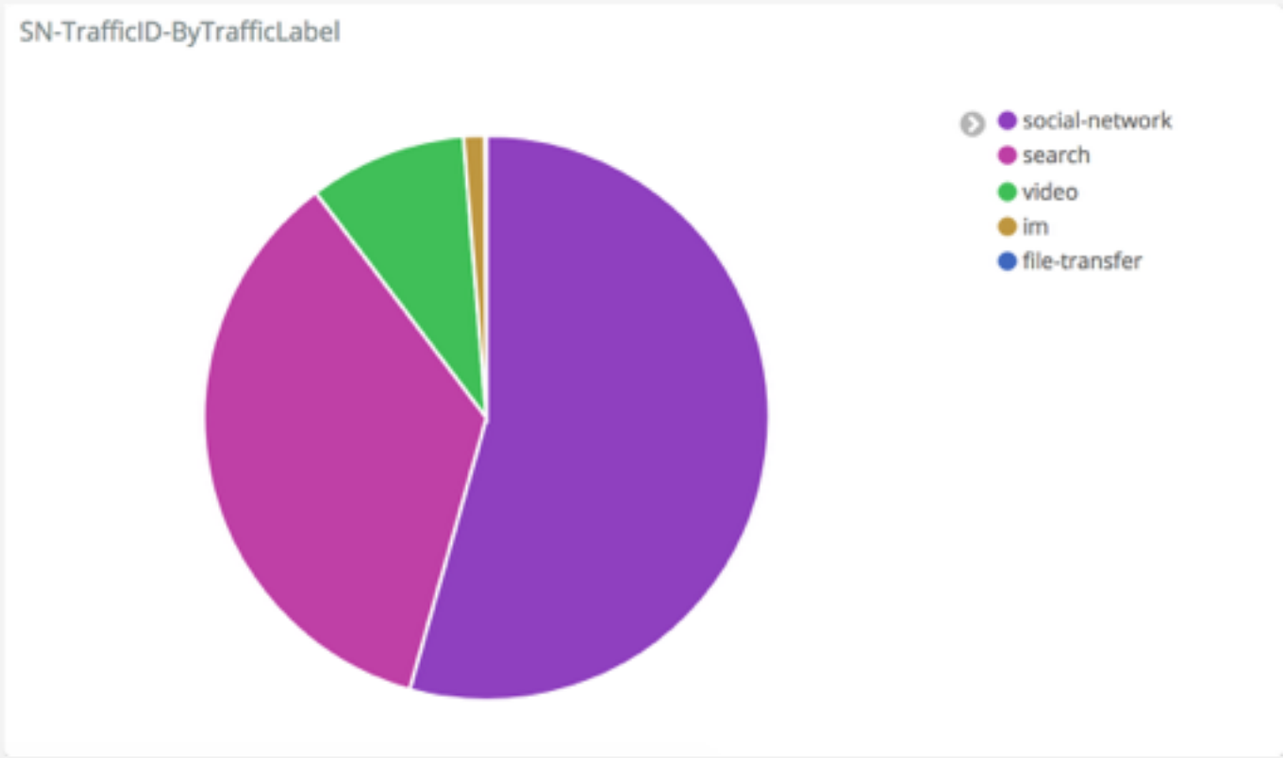
- Disponible en https://github.com/StamusNetworks/SELKS

# Suricata - Herramientas

- *SELKS > Kibana > SN-TrafficID*

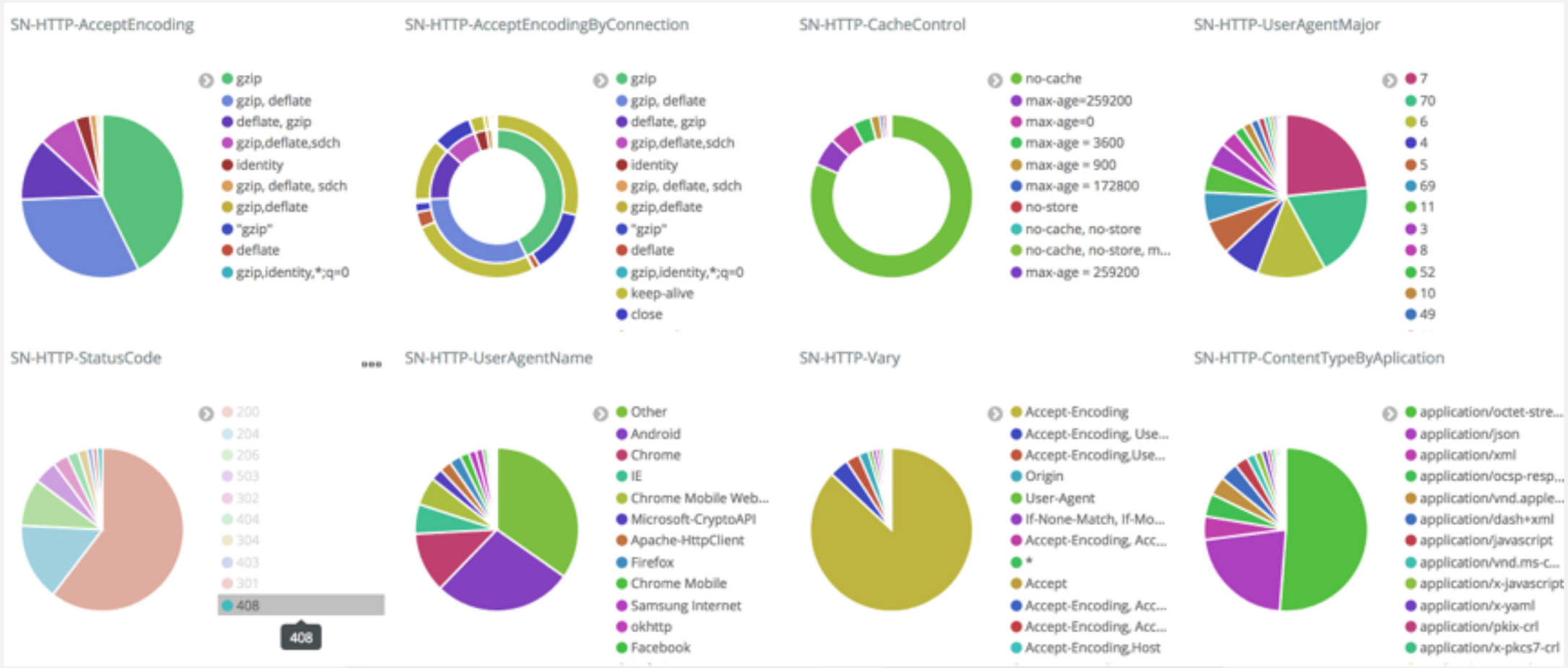


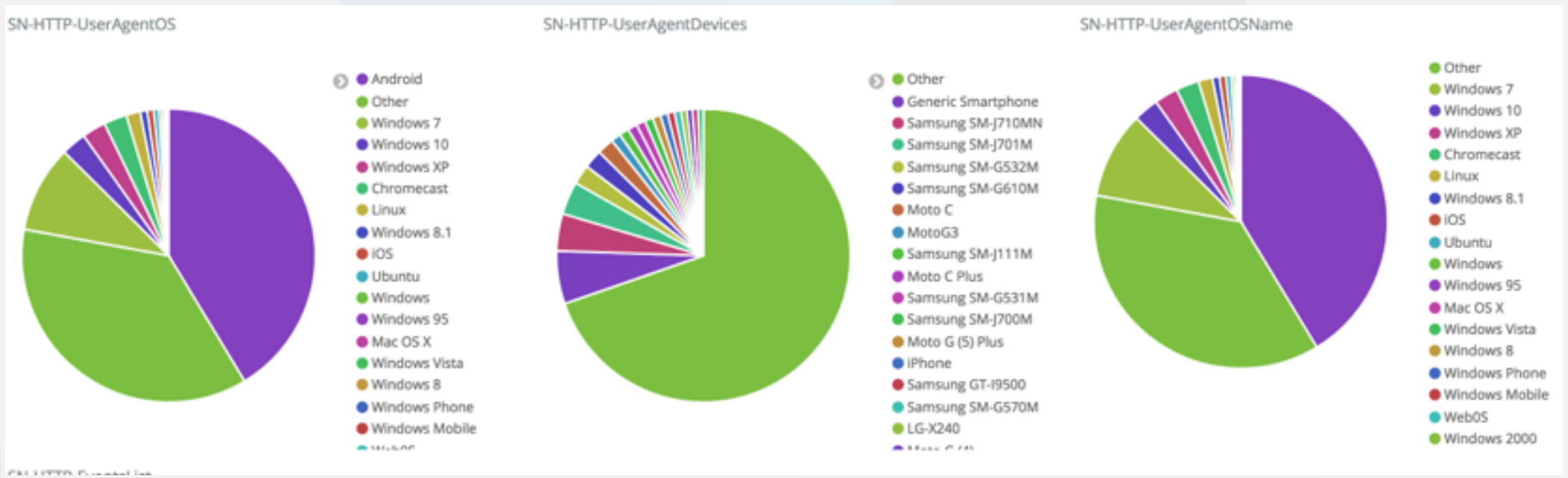



# Suricata - Herramientas

- *SELKS > Kibana > SN-HTTP*



# Suricata - Herramientas

- *SELKS > Scirius CE*

**5 Sources**

| | | | | |
|---|---|---|---|---|
| ETOpen Ruleset | Last update: Oct. 30, 2018, 9:19 p.m.. | 45 Categories | 25138 Rules | View |

**Type** sigs
**URI** https://rules.emergingthreats.net/open/suricata-git/emerging.rules.tar.gz
**Creation date** Oct. 24, 2018, 1:25 p.m.

| | | | | |
|---|---|---|---|---|
| Etnetera aggressi... | Last update: Oct. 30, 2018, 9:17 p.m.. | 1 Category | 79 Rules | View |
| Positive Technolo... | Last update: Oct. 30, 2018, 9:17 p.m.. | 1 Category | 128 Rules | View |

**Type** sigs
**URI** https://raw.githubusercontent.com/ptresearch/AttackDetection/master/pt.rules.tar.gz
**Creation date** Oct. 30, 2018, 9:16 p.m.

| | | | | |
|---|---|---|---|---|
| SSLBL abuse.ch | Last update: Oct. 30, 2018, 9:20 p.m.. | 1 Category | 2830 Rules | View |
| Suricata Traffic I... | Last update: Oct. 30, 2018, 9:20 p.m.. | 1 Category | 34 Rules | View |

# Proyecto

# Suricata2MikroTik IPS

## *-Community Edition-*

# Suricata2MikroTik— Qué es?

**Suricata2MikroTik -Community Edition- IPS**

- Módulo que lee el logging *EVE* de *Suricata* para buscar alertas particulares
- Al encontrarlas toma una acción (*IPS*) y se conecta al ***RouterOS*** vía ***API*** para bloquear el ***IP Address*** atacante.
- Se pueden personalizar la acción a realizar (por defecto agrega un IP a un Address list)
- Gratuito, Open Source, Colaborativo (Alojado en *Github*)
- Actualización del proyecto ***MikroTik Suricata IPS***

# Suricata2MikroTik

*Notificaciones*:

- Permite enviar notificaciones vía ***Email*** / ***Telegram***

*Administración:*

- Panel Web de monitoreo y actualizaciones

*Requerimientos:*

- *Suricata* con logging *Eve.Json*
- *Git*
- *IP Address y credenciales de login con acceso write (API)*

# Suricata2MikroTik

## **Suricata2MikroTik Panel Web**:

- Monitorear las "alertas bloqueadas" activas
- Crear y actualizar las Reglas (Alertas a bloquear)
- Permite Geolocalizar el IP Atacante

Active Top Ten IP Attack

| Count | IP Block | Country |
|---|---|---|
| 11 | 109.248.9.16 | Russian Federation |
| 5 | 176.119.4.12 | Ukraine |
| 4 | 176.119.4.29 | Ukraine |
| 4 | 194.55.142.41 | Germany |
| 4 | 176.119.4.56 | Ukraine |
| 3 | 185.255.31.78 | |
| 3 | 45.227.253.6 | |
| 3 | 77.72.85.8 | Russian Federation |
| 2 | 176.119.4.50 | Ukraine |
| 2 | 176.119.4.53 | Ukraine |

Active Top Ten Alert Rules

| Count | Alert | Sid |
|---|---|---|
| 27 | ET DROP Dshield Block Listed Source group 1 | 2402000 |
| 14 | ETN AGGRESSIVE IPs Group 2 | 5000002 |
| 13 | ETN AGGRESSIVE IPs Group 3 | 5000003 |
| 4 | ETN AGGRESSIVE IPs Group 10 | 5000010 |
| 3 | ETN AGGRESSIVE IPs Group 4 | 5000004 |
| 2 | ETN AGGRESSIVE IPs Group 8 | 5000008 |
| 2 | ETN AGGRESSIVE IPs Group 19 | 5000019 |
| 2 | ETN AGGRESSIVE IPs Group 13 | 5000013 |
| 2 | ET DROP Spamhaus DROP Listed Traffic Inbound group 6 | 2400005 |
| 1 | ET CINS Active Threat Intelligence Poor Reputation IP group 81 | 2403380 |

# Suricata2MikroTik

## *Instalación*:

- Clonar el repositorio de ***GitHub***

  *cd /var/www/html/*
  *git clone https://github.com/elmaxid/suricata2mikrotik.git*
  *cd suricata2mikrotik*

- Editar archivo *config.php (Datos DB, Router Login, notificaciones, etc)*

- *Crear esquema DB:*

  *mysql -u user -p < schema.sql*

# Suricata2MikroTik

***Instalación:***

- Setear los permisos de ejecución para los archivos que inician los servicios

  *chmod +x /var/www/html/suricata2mikrotik/bin/start**

- Ejecutar iniciador de servicios

  *cd /var/www/html/suricata2mikrotik/bin/*

  *./start_ips*

  *./start_suricata*

***Funcionamiento:***

- Reenviar el tráfico desde el ***Router MikroTik*** que se desea analizar con alguno de las opciones ya vistas.

# Suricata2MikroTik

Suricata2Mikrotik

Suricata2MikroTik IPS

Uptime 8 days  Load Avr: 2.22 2.75 3.09 2/1444  MEM Free: 49.57%

Suricata IDS: OK  IPS Daemon: OK  API: OK

Active Alert Blocked (89) - Time: 14:09:39

| Time | IP Block | Rule | SID | Action |
|---|---|---|---|---|
| a minute ago | 125.64.94.201 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| a minute ago | 176.119.4.7 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 3 minutes ago | 185.255.31.69 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 4 minutes ago | 85.233.153.69 | ET CINS Active Threat Intelligence Poor Reputation IP group 84 | 2403383 | |
| 4 minutes ago | 1.1.2.119 | ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted | 2006380 | |
| 5 minutes ago | 89.35.39.78 | ET CINS Active Threat Intelligence Poor Reputation IP group 92 | 2403391 | |
| 8 minutes ago | 77.72.85.8 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 8 minutes ago | 185.153.197.6 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 9 minutes ago | 176.119.4.9 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 12 minutes ago | 176.119.4.49 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 28 minutes ago | 62.173.154.248 | ETN AGGRESSIVE IPs Group 4 | 5000004 | |
| 38 minutes ago | 83.252.127.164 | ET CINS Active Threat Intelligence Poor Reputation IP group 81 | 2403380 | |
| 57 minutes ago | 198.108.66.28 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 57 minutes ago | 198.108.66.29 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 1 hour ago | 115.238.245.14 | ETN AGGRESSIVE IPs Group 13 | 5000013 | |
| 1 hour ago | 176.119.4.53 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 1 hour ago | 176.119.4.56 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 1 hour ago | 194.55.142.41 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 1 hour ago | 196.52.43.125 | ETN AGGRESSIVE IPs Group 20 | 5000020 | |
| 1 hour ago | 176.119.4.50 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |
| 1 hour ago | 5.101.40.252 | ET CINS Active Threat Intelligence Poor Reputation IP group 4 | 2403303 | |
| 1 hour ago | 196.52.43.62 | ETN AGGRESSIVE IPs Group 19 | 5000019 | |
| 1 hour ago | 61.164.97.74 | ET CINS Active Threat Intelligence Poor Reputation IP group 56 | 2403355 | |
| 1 hour ago | 196.52.43.56 | ETN AGGRESSIVE IPs Group 16 | 5000016 | |
| 1 hour ago | 176.119.4.51 | ET DROP Dshield Block Listed Source group 1 | 2402000 | |

Active Top Ten IP Attack

| Count | IP Block | Country |
|---|---|---|
| 11 | 109.248.9.16 | Russian Federation |
| 5 | 176.119.4.12 | Ukraine |
| 4 | 176.119.4.29 | Ukraine |
| 4 | 194.55.142.41 | Germany |
| 4 | 176.119.4.56 | Ukraine |
| 3 | 185.255.31.78 | |
| 3 | 45.227.253.6 | |
| 3 | 77.72.85.8 | Russian Federation |
| 2 | 176.119.4.50 | Ukraine |
| 2 | 176.119.4.53 | Ukraine |

Active Top Ten Alert Rules

| Count | Alert | Sid |
|---|---|---|
| 27 | ET DROP Dshield Block Listed Source group 1 | 2402000 |
| 14 | ETN AGGRESSIVE IPs Group 2 | 5000002 |
| 13 | ETN AGGRESSIVE IPs Group 3 | 5000003 |
| 4 | ETN AGGRESSIVE IPs Group 10 | 5000010 |
| 3 | ETN AGGRESSIVE IPs Group 4 | 5000004 |
| 2 | ETN AGGRESSIVE IPs Group 8 | 5000008 |
| 2 | ETN AGGRESSIVE IPs Group 19 | 5000019 |
| 2 | ETN AGGRESSIVE IPs Group 13 | 5000013 |
| 2 | ET DROP Spamhaus DROP Listed Traffic Inbound group 6 | 2400005 |
| 1 | ET CINS Active Threat Intelligence Poor Reputation IP group 81 | 2403380 |

MKE Solutions

**Suricata2Mikrotik CE** -Community Edition-

# Suricata2MikroTik

Active Alerts Rules (23)

| | Rule | IP Block | Timeout | |
|---|---|---|---|---|
| ✓ | ET CINS Active Threat Intelligence Poor Reputation IP | src | 01:00:00 | |
| ✓ | ET CNC Ransomware Tracker Reported CnC Server | dst | 01:59:59 | |
| ✓ | ET COMPROMISED Known Compromised or Hostile Host Traffic | src | 01:00:00 | |
| ✓ | ET DOS DNS Amplification Attack Inbound | src | 02:00:00 | |
| ✓ | ET DOS Possible NTP DDoS Inbound Frequent | src | 00:10:00 | |
| ✓ | ET DROP Dshield Block Listed Source | src | 01:00:00 | |
| ✓ | ET DROP Spamhaus DROP Listed Traffic Inbound | src | 01:00:00 | |
| ✓ | ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted | dst | 23:59:59 | |
| ✓ | ET POLICY Suspicious inbound to | src | 01:00:00 | |
| ✓ | ET POLICY Suspicious inbound to mySQL port 3306 | src | 00:10:00 | |
| ✓ | ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection (Inbound) | src | 00:10:00 | |
| ✓ | ET SCAN SipCLI VOIP Scan | src | 01:00:00 | |
| ✓ | ET SCAN Sipvicious Scan | src | 01:00:00 | |
| ✓ | ET SCAN Sipvicious User-Agent Detected (friendly-scanner) | src | 01:00:00 | |
| ✓ | ET TOR Known Tor Relay/Router (Not Exit) Node Traffic | src | 01:00:00 | |
| ✓ | ET TROJAN MS Terminal Server | src | 01:00:00 | |
| ✓ | ET VOIP Modified Sipvicious Asterisk PBX User-Agent | src | 01:00:00 | |
| ✓ | ET VOIP Multiple Unauthorized SIP Responses UDP | dst | 00:59:59 | |
| ✓ | GPL ATTACK_RESPONSE id check returned root | src | 00:01:10 | |
| ✓ | GPL DNS named version attempt | src | 01:00:00 | |
| ✓ | GPL RPC portmap listing UDP 111 | src | 01:00:00 | |
| ✓ | GPL RPC xdmcp info query | src | 01:00:00 | |
| ✓ | GPL SNMP public access udp | src | 01:00:00 | |

# MUM Suricata2MikroTik

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

Find: Blocked

| | Name | Address | Timeout | Creation Time | Comment |
|---|---|---|---|---|---|
| D | Blocked | 176.119.4.53 | 00:59:56 | Nov/09/2018 13:14:31 | From SuricataIPS, ETN AGGRESSIVE IPs Group 3 => 1:5000003 => event timestamp: 2018-11-09 14:13:32 |
| D | Blocked | 188.246.226.71 | 00:59:54 | Nov/09/2018 13:14:29 | From SuricataIPS, ETN AGGRESSIVE IPs Group 8 => 1:5000008 => event timestamp: 2018-11-09 14:13:29 |
| D | Blocked | 185.101.33.2 | 00:59:50 | Nov/09/2018 13:14:25 | From SuricataIPS, ETN AGGRESSIVE IPs Group 25 => 1:5000025 => event timestamp: 2018-11-09 14:13:28 |
| D | Blocked | 196.52.43.98 | 00:59:48 | Nov/09/2018 13:14:23 | From SuricataIPS, ETN AGGRESSIVE IPs Group 17 => 1:5000017 => event timestamp: 2018-11-09 14:13:28 |
| D | Blocked | 198.108.66.245 | 00:59:44 | Nov/09/2018 13:14:19 | From SuricataIPS, ET DROP Dshield Block Listed Source group 1 => 1:2402000 => event timestamp: 2018-11-09 14:13:27 |
| D | Blocked | 198.108.66.244 | 00:59:42 | Nov/09/2018 13:14:17 | From SuricataIPS, ET DROP Dshield Block Listed Source group 1 => 1:2402000 => event timestamp: 2018-11-09 14:13:27 |
| D | Blocked | 62.173.154.248 | 00:59:38 | Nov/09/2018 13:14:13 | From SuricataIPS, ETN AGGRESSIVE IPs Group 4 => 1:5000004 => event timestamp: 2018-11-09 14:13:26 |
| D | Blocked | 196.52.43.105 | 00:59:36 | Nov/09/2018 13:14:11 | From SuricataIPS, ETN AGGRESSIVE IPs Group 22 => 1:5000022 => event timestamp: 2018-11-09 14:13:25 |
| D | Blocked | 196.52.43.100 | 00:59:33 | Nov/09/2018 13:14:08 | From SuricataIPS, ETN AGGRESSIVE IPs Group 16 => 1:5000016 => event timestamp: 2018-11-09 14:13:24 |
| D | Blocked | 31.192.108.68 | 00:59:31 | Nov/09/2018 13:14:06 | From SuricataIPS, ETN AGGRESSIVE IPs Group 1 => 1:5000001 => event timestamp: 2018-11-09 14:13:24 |
| D | Blocked | 58.246.12.122 | 00:59:27 | Nov/09/2018 13:14:02 | From SuricataIPS, ETN AGGRESSIVE IPs Group 38 => 1:5000038 => event timestamp: 2018-11-09 14:13:22 |
| D | Blocked | 198.108.66.254 | 00:59:25 | Nov/09/2018 13:14:00 | From SuricataIPS, ET DROP Dshield Block Listed Source group 1 => 1:2402000 => event timestamp: 2018-11-09 14:13:20 |
| D | Blocked | 198.108.67.42 | 00:59:22 | Nov/09/2018 13:13:57 | From SuricataIPS, ETN AGGRESSIVE IPs Group 12 => 1:5000012 => event timestamp: 2018-11-09 14:13:20 |
| D | Blocked | 196.52.43.104 | 00:59:20 | Nov/09/2018 13:13:55 | From SuricataIPS, GPL SNMP public access udp => 1:2101411 => event timestamp: 2018-11-09 14:13:17 |
| D | Blocked | 196.52.43.111 | 00:59:16 | Nov/09/2018 13:13:51 | From SuricataIPS, ETN AGGRESSIVE IPs Group 17 => 1:5000017 => event timestamp: 2018-11-09 14:13:16 |
| D | Blocked | 185.255.31.18 | 00:59:14 | Nov/09/2018 13:13:49 | From SuricataIPS, ETN AGGRESSIVE IPs Group 1 => 1:5000001 => event timestamp: 2018-11-09 14:13:15 |
| D | Blocked | 85.93.20.244 | 00:59:10 | Nov/09/2018 13:13:45 | From SuricataIPS, ETN AGGRESSIVE IPs Group 10 => 1:5000010 => event timestamp: 2018-11-09 14:13:13 |
| D | Blocked | 185.208.209.6 | 00:59:09 | Nov/09/2018 13:13:44 | From SuricataIPS, ETN AGGRESSIVE IPs Group 4 => 1:5000004 => event timestamp: 2018-11-09 14:13:12 |
| D | Blocked | 5.188.206.22 | 00:59:05 | Nov/09/2018 13:13:40 | From SuricataIPS, ETN AGGRESSIVE IPs Group 2 => 1:5000002 => event timestamp: 2018-11-09 14:13:11 |
| D | Blocked | 27.223.90.210 | 00:59:03 | Nov/09/2018 13:13:38 | From SuricataIPS, ET CINS Active Threat Intelligence Poor Reputation IP group 16 => 1:2403315 => event timestamp: 2018-11-09 14:13:10 |
| D | Blocked | 77.72.85.8 | 00:58:59 | Nov/09/2018 13:13:34 | From SuricataIPS, ETN AGGRESSIVE IPs Group 3 => 1:5000003 => event timestamp: 2018-11-09 14:13:09 |
| D | Blocked | 78.128.112.98 | 00:58:57 | Nov/09/2018 13:13:32 | From SuricataIPS, ETN AGGRESSIVE IPs Group 1 => 1:5000001 => event timestamp: 2018-11-09 14:13:09 |
| D | Blocked | 80.82.77.33 | 00:58:54 | Nov/09/2018 13:13:29 | From SuricataIPS, ETN AGGRESSIVE IPs Group 10 => 1:5000010 => event timestamp: 2018-11-09 14:13:09 |
| D | Blocked | 36.226.6.56 | 00:58:52 | Nov/09/2018 13:13:27 | From SuricataIPS, ET CINS Active Threat Intelligence Poor Reputation IP group 24 => 1:2403323 => event timestamp: 2018-11-09 14:13:09 |
| D | Blocked | 193.29.13.25 | 00:58:48 | Nov/09/2018 13:13:23 | From SuricataIPS, ETN AGGRESSIVE IPs Group 9 => 1:5000009 => event timestamp: 2018-11-09 14:13:07 |
| D | Blocked | 196.52.43.57 | 00:58:47 | Nov/09/2018 13:13:22 | From SuricataIPS, ETN AGGRESSIVE IPs Group 12 => 1:5000012 => event timestamp: 2018-11-09 14:13:06 |
| D | Blocked | 198.108.67.44 | 00:58:43 | Nov/09/2018 13:13:18 | From SuricataIPS, ETN AGGRESSIVE IPs Group 17 => 1:5000017 => event timestamp: 2018-11-09 14:13:04 |
| D | Blocked | 176.119.4.26 | 00:58:41 | Nov/09/2018 13:13:16 | From SuricataIPS, ETN AGGRESSIVE IPs Group 3 => 1:5000003 => event timestamp: 2018-11-09 14:13:04 |
| D | Blocked | 186.5.214.195 | 00:58:37 | Nov/09/2018 13:13:11 | From SuricataIPS, GPL SNMP public access udp => 1:2101411 => event timestamp: 2018-11-09 14:13:04 |
| D | Blocked | 196.52.43.102 | 00:58:35 | Nov/09/2018 13:13:10 | From SuricataIPS, ET DROP Dshield Block Listed Source group 1 => 1:2402000 => event timestamp: 2018-11-09 14:13:02 |
| D | Blocked | 185.208.208.144 | 00:58:32 | Nov/09/2018 13:13:07 | From SuricataIPS, ETN AGGRESSIVE IPs Group 4 => 1:5000004 => event timestamp: 2018-11-09 14:13:01 |
| D | Blocked | 109.248.9.16 | 00:58:30 | Nov/09/2018 13:13:05 | From SuricataIPS, ETN AGGRESSIVE IPs Group 3 => 1:5000003 => event timestamp: 2018-11-09 14:13:00 |
| D | Blocked | 186.5.214.34 | 00:58:26 | Nov/09/2018 13:13:01 | From SuricataIPS, GPL SNMP public access udp => 1:2101411 => event timestamp: 2018-11-09 14:13:00 |
| D | Blocked | 196.52.43.97 | 00:58:20 | Nov/09/2018 13:12:55 | From SuricataIPS, ETN AGGRESSIVE IPs Group 16 => 1:5000016 => event timestamp: 2018-11-09 14:12:59 |
| D | Blocked | 196.52.43.131 | 00:58:18 | Nov/09/2018 13:12:53 | From SuricataIPS, ETN AGGRESSIVE IPs Group 19 => 1:5000019 => event timestamp: 2018-11-09 14:12:59 |
| D | Blocked | 193.106.29.82 | 00:58:14 | Nov/09/2018 13:12:49 | From SuricataIPS, ETN AGGRESSIVE IPs Group 5 => 1:5000005 => event timestamp: 2018-11-09 14:12:59 |
| D | Blocked | 186.5.214.12 | 00:58:13 | Nov/09/2018 13:12:48 | From SuricataIPS, GPL SNMP public access udp => 1:2101411 => event timestamp: 2018-11-09 14:12:57 |
| D | Blocked | 186.5.215.167 | 00:58:09 | Nov/09/2018 13:12:44 | From SuricataIPS, GPL SNMP public access udp => 1:2101411 => event timestamp: 2018-11-09 14:12:56 |
| D | Blocked | 198.108.67.36 | 00:58:07 | Nov/09/2018 13:12:42 | From SuricataIPS, ETN AGGRESSIVE IPs Group 14 => 1:5000014 => event timestamp: 2018-11-09 14:12:56 |
| D | Blocked | 185.208.208.198 | 00:58:03 | Nov/09/2018 13:12:38 | From SuricataIPS, ETN AGGRESSIVE IPs Group 3 => 1:5000003 => event timestamp: 2018-11-09 14:12:56 |

# Suricata2MikroTik

Firewall

Filter Rules | NAT | Mangle | Raw | Service Ports | Connections | Address Lists | Layer7 Protocols

| | Name | Address | Timeout | Creation Time | Comment |
|---|---|---|---|---|---|
| D | Blocked | 93.14.178.11 | 00:10:16 | Jul/13/2017 14:5... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 14:57:02 |
| D | Blocked | 66.70.149.166 | 00:10:40 | Jul/13/2017 14:5... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 14:57:25 |
| D | Blocked | 5.254.66.135 | 00:11:16 | Jul/13/2017 14:5... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 14:58:02 |
| D | Blocked | 189.27.23.209 | 00:11:41 | Jul/13/2017 14:5... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 14:58:27 |
| D | Blocked | 174.108.49.9 | 00:12:17 | Jul/13/2017 14:5... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 14:59:02 |
| D | Blocked | 77.108.198.31 | 00:12:41 | Jul/13/2017 14:5... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 14:59:27 |
| D | Blocked | 216.106.55.39 | 00:13:19 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:00:03 |
| D | Blocked | 178.63.60.2 | 00:13:43 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:00:28 |
| D | Blocked | 151.33.35.185 | 00:14:18 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:01:03 |
| D | Blocked | 98.158.66.106 | 00:14:44 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:01:29 |
| D | Blocked | 104.57.138.146 | 00:15:18 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:02:03 |
| D | Blocked | 174.17.80.108 | 00:15:46 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:02:32 |
| D | Blocked | 104.153.108.135 | 00:16:18 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:03:03 |
| D | Blocked | 99.64.50.126 | 00:16:46 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:03:32 |
| D | Blocked | 172.56.20.35 | 00:17:18 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:04:04 |
| D | Blocked | 77.77.164.102 | 00:17:49 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:04:35 |
| D | Blocked | 96.50.192.51 | 00:18:19 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:05:05 |
| D | Blocked | 184.154.68.149 | 00:18:49 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:05:35 |
| D | Blocked | 68.196.168.219 | 00:19:19 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:06:05 |
| D | Blocked | 98.214.19.73 | 00:19:49 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:06:35 |
| D | Blocked | 212.129.1.15 | 00:20:09 | Jul/13/2017 15:0... | From suricata, ET SCAN Sipvicious Scan => 1:2008578 => event timestamp: 2017-07-13 15:06:55 |
| D | Blocked | 108.61.232.52 | 00:20:19 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:07:05 |
| D | Blocked | 82.53.27.142 | 00:20:49 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:07:35 |
| D | Blocked | 73.8.131.155 | 00:21:20 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:08:05 |
| D | Blocked | 201.0.37.156 | 00:21:50 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:08:35 |
| D | Blocked | 82.66.230.133 | 00:22:20 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:09:05 |
| D | Blocked | 172.90.214.88 | 00:22:50 | Jul/13/2017 15:0... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:09:35 |
| D | Blocked | 177.40.212.166 | 00:23:24 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:10:09 |
| D | Blocked | 82.161.161.246 | 00:23:50 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:10:35 |
| D | Blocked | 69.248.1.182 | 00:24:22 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:11:09 |
| D | Blocked | 73.52.44.161 | 00:24:50 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:11:36 |
| D | Blocked | 77.72.82.16 | 00:25:06 | Jul/13/2017 15:1... | From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 88 => 1:2403387 => event timestamp: 2017-07-13 15:11... |
| D | Blocked | 203.100.223.38 | 00:25:24 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:12:11 |
| D | Blocked | 144.76.182.86 | 00:25:55 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:12:40 |
| D | Blocked | 50.25.68.88 | 00:26:29 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:13:14 |
| D | Blocked | 98.110.43.176 | 00:27:01 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:13:46 |
| D | Blocked | 24.10.131.238 | 00:27:29 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:14:15 |
| D | Blocked | 37.217.166.246 | 00:28:01 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:14:46 |
| D | Blocked | 91.252.219.139 | 00:28:31 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:15:16 |
| D | Blocked | 174.78.193.206 | 00:29:01 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:15:47 |
| D | Blocked | 75.86.71.95 | 00:29:31 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:16:16 |
| D | Blocked | 64.121.102.124 | 00:30:01 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:16:47 |
| D | Blocked | 179.108.251.249 | 00:30:31 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:17:16 |
| D | Blocked | 109.159.19.60 | 00:31:00 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:17:47 |
| D | Blocked | 169.46.190.131 | 00:31:32 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:18:18 |
| D | Blocked | 191.181.175.60 | 00:32:02 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:18:47 |
| D | Blocked | 189.78.216.132 | 00:32:32 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:19:18 |
| D | Blocked | 108.176.244.190 | 00:33:02 | Jul/13/2017 15:1... | From suricata, ET DOS DNS Amplification Attack Inbound => 1:2016016 => event timestamp: 2017-07-13 15:19:47 |

# Referencias

## Sitios y bibliografia utilizada:

- ***Suricata:***
  https://suricata-ids.org/
- ***Suricata2MikroTik:***
  https://github.com/elmaxid/Suricata2MikroTik

## Presentaciones MUMs:

- ***Utilizando RouterOS como IPS / IDS (I)***
  Maximiliano Dobladez - MUM Paraguay 2017
  https://mum.mikrotik.com/presentations/PY17/presentation_4589_1502349113.pdf
- ***Mikrotik y Suricata -***
  José M. Román - MUM España 2016
  http://mum.mikrotik.com/presentations/ES16/presentation_3746_1476679132.pdf
- ***Securing your Mikrotik Network***
  Andrew Thrift - MUM Australia 2012
  http://mum.mikrotik.com/presentations/AU12/2_andrew.pdf

# ¿Preguntas?

# MUCHAS GRACIAS!

Maximiliano Dobladez

MKE Solutions

info@mkesolutions.net - http://www.mkesolutions.net

http://maxid.com.ar

http://twitter.com/mdobladez