MUM MikroTik User Meeting

Utilizando RouterOS como IPS / IDS

Por: Maximiliano Dobladez
MKE Solutions

25 de Julio de 2017

Asunción - Paraguay

CC BY NC SA

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**
  - Entrenamientos Oficiales
  - Soporte IT

info@mkesolutions.net

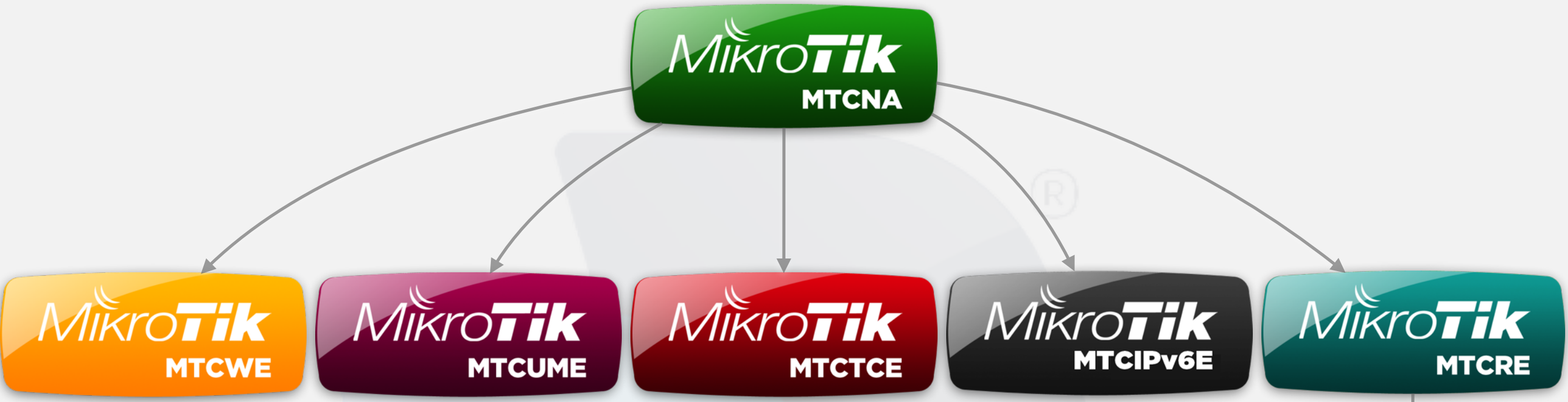
@mkesolutions

/mkesolutions

/mkesolutions

MUM

Entrenamientos Oficiales



- Entrenamientos Públicos y Privados.
- ~300 alumnos por año, con un 75% de certificados.

powered by Mke Solutions

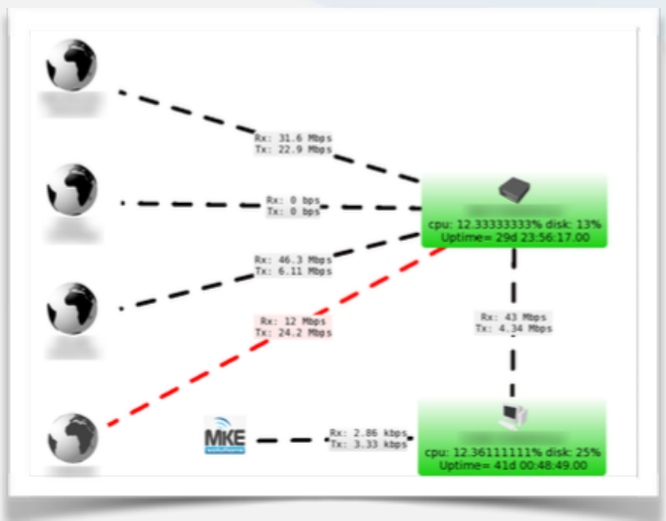
Academia DE ENTRENAMIENTOS

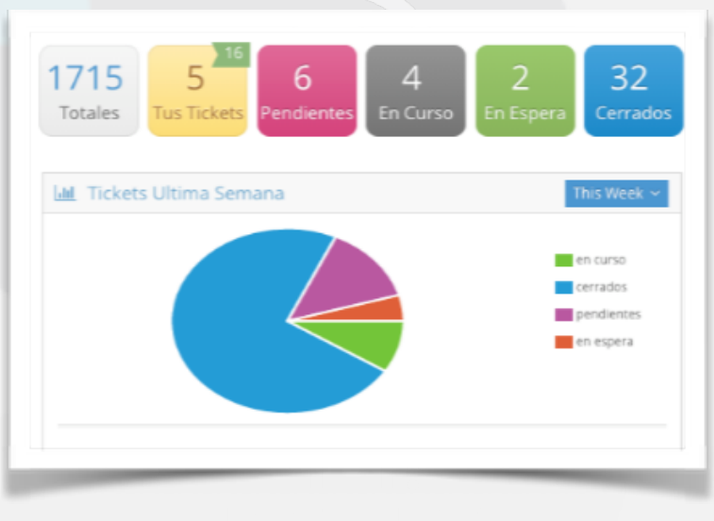
MUM

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





Agenda

Desarrollo de la presentación:

- **IDS / IPS**
- **Suricata**: qué es?, cómo funciona? cómo se instala?
- **Rules Manager**: 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 and payload, en busca de eventos conocidos.
- Cuando se detecta un evento se genera un mensaje de log.

IPS (Intrusion Prevention System)

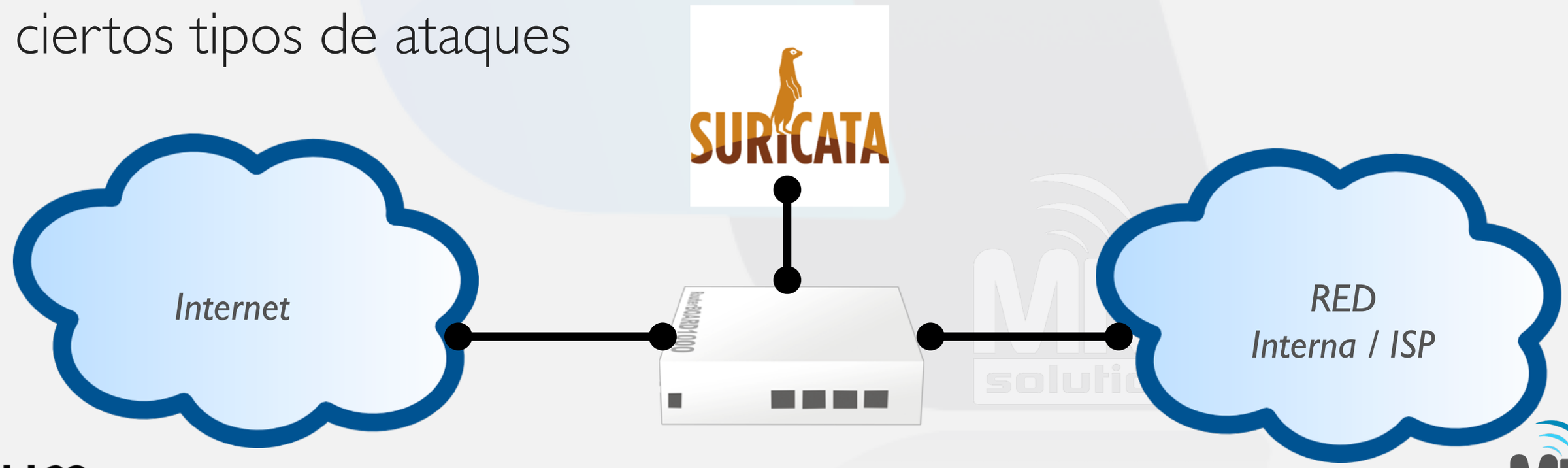
- Es un dispositivo o aplicación que analiza paquetes completos, tanto cabeceras como payload en busca de eventos conocidos.
- Utiliza *Firmas*, *Patrones de comportamientos*, *Políticas de seguridad*
- Cuando se detecta un evento conocido se trata con una acción (drop, reject, alert, pass)

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-3.2.tar.gz

tar -xvzf suricata-3.2.tar.gz ; cd suricata-3.2
./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]"

Para que se ejecute al inicio ***init.d:***

RUN=yes

Interface donde escuchará:

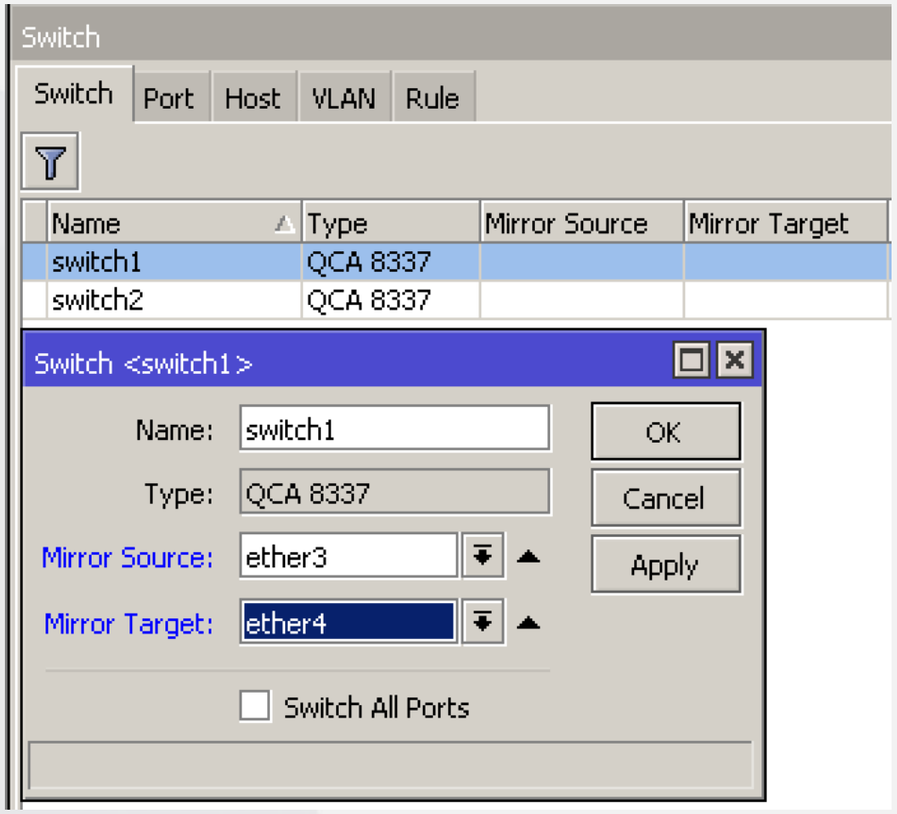
IFACE=eth0

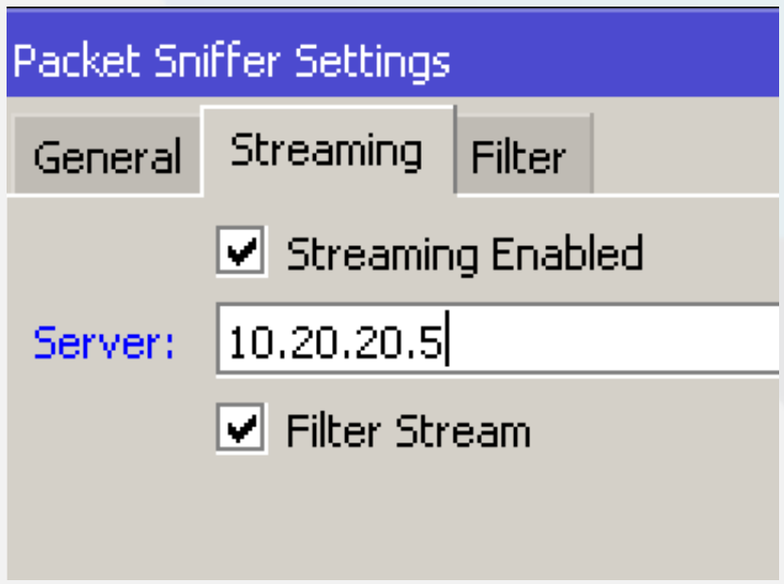
Suricata - Integración con rOS

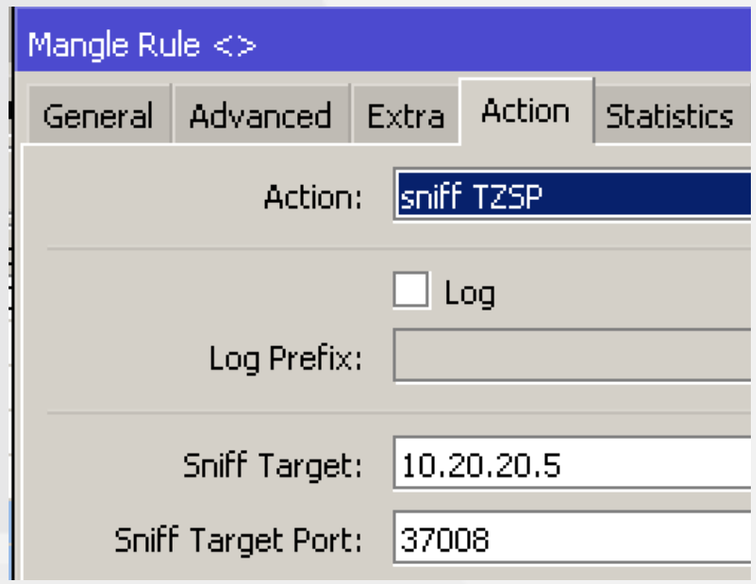
Para que empiece a trabajar hay que redireccionar el tráfico desde el *MikroTik RouterOS* hacia *Suricata*

Podemos realizarlo con:

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







Suricata - Reportes

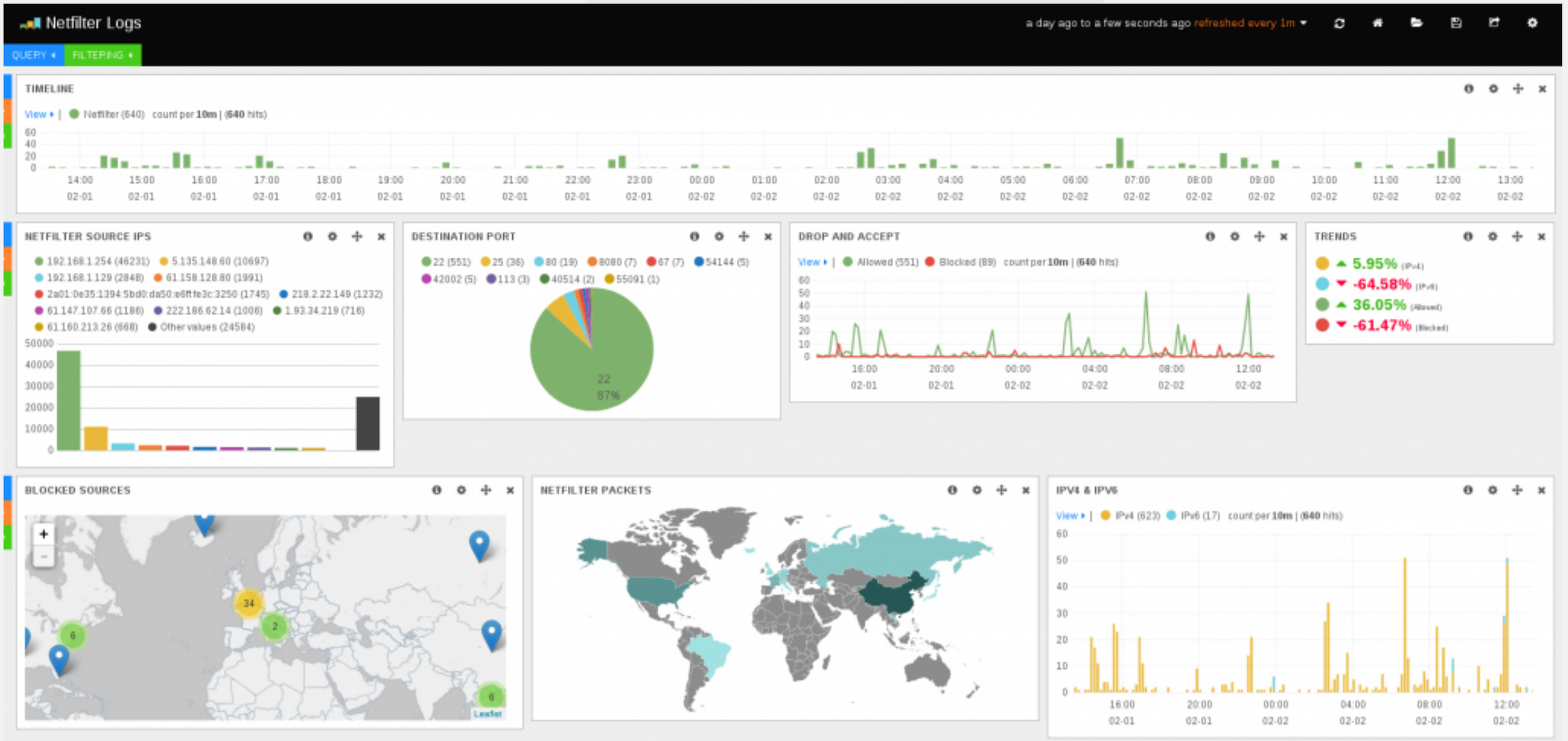
Los logs estarán en */var/log/suricata*

```
[**] [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 - Reportes

Es posible integrarlo con otras Aplicaciones para un reporte mas "amigable"

ELK (Elasticsearch, Logstash, Kibana)



Suricata - Herramientas

Existen distribuciones listas para utilizar:

- ***SmoothSec*** = *Ubuntu* + *Suricata* + *Snorby*

  Disponible en: http://bailey.st/blog/smooth-sec/

- ***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*

Home Sources Rulesets Suricata About

Scirius

Logged in as selks-user

System status

Suricata Elasticsearch Disk Memory

Sources

- SSLBL abuse.ch
- ETOpen Ruleset

Rulesets

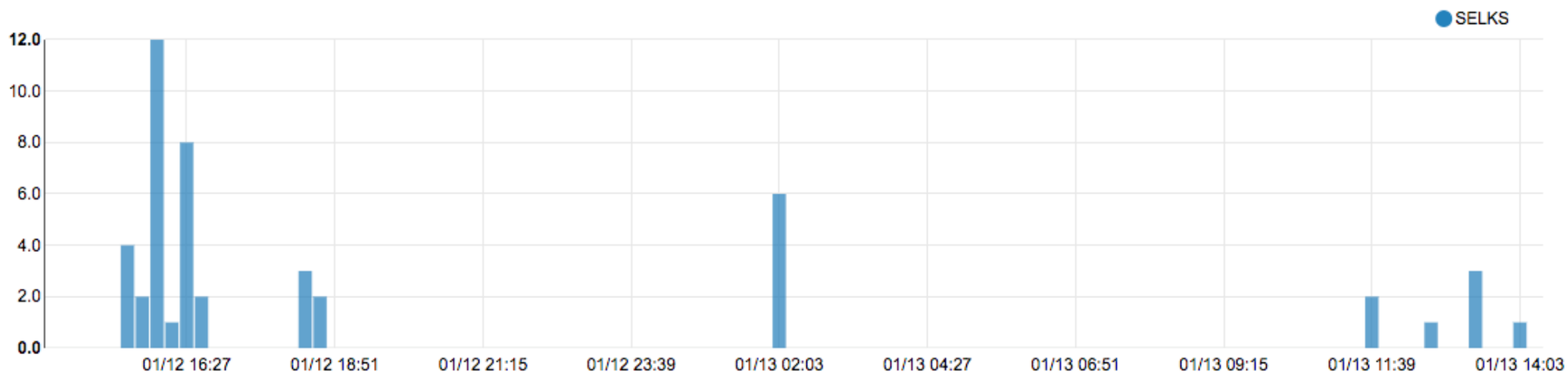
- Default SELKS ruleset

Rules activity (last 24h)

Sid	msg	category	Hits
2200037	SURICATA TCP duplicated option	decoder-events	38
2100498	GPL ATTACK_RESPONSE id check returned root	emerging-attack_response	9

2 items

Alerts activity (last 24h)



Scirius v1.1.10. Copyright (c) 2014-2016 Stamus Networks.

Proyecto

IPS MikroTik Suricata

MUM IPS-MikroTik-Suricata - Qué es?

IPS-MikroTik-Suricata:

- Módulo que se conecta a la DB del ***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*)
- Inspirado en el post de *Tom Fisk*: http://forum.mikrotik.com/viewtopic.php?t=111727

IPS-MikroTik-Suricata

Notificaciones:

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

Requerimientos:

- *Suricata* con *Barnyard2* (*MySQL*)
- *Snorby* (opcional)
- *Git*
- *IP Address y credenciales de login con acceso write (API)*

IPS-MikroTik-Suricata

Instalación:

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

  cd /opt
  git clone https://github.com/elmaxid/ips-mikrotik-suricata.git
  cd ips-mikrotik-suricata

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

  mysql -u user -p db_name < schema.sql

- *Comprobar conexión a DB y API:*

  php -f mikrotik-ips-install.php

IPS-MikroTik-Suricata

Instalación:

- Setear los permisos de ejecución para el archivo que inicia el servicio

  chmod 777 /opt/ips-mikrotik-suricata/ips_start.sh

- Ejecutar iniciador de servicio

  sh /opt/ips-mikrotik-suricata/ips_start.sh

Funcionamiento:

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

MUM IPS-MikroTik-Suricata

Firewall

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

	Name	Address	Timeout	Comment
D	Blocked	50.251.2.113	00:00:00	From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 32 => 1:2403331 => event timestamp: 2017-07-13 19:45:08
D	Blocked	146.0.78.20	00:00:46	From suricata, ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection (Inbound) => 1:2001972 => event timestamp: 2017-...
D	Blocked	176.126.252.11	00:01:03	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 19 => 1:2522036 => event timestamp: 2017-07-13 19:46:20
D	Blocked	77.72.82.16	00:01:07	From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 63 => 1:2403362 => event timestamp: 2017-07-13 19:46:23
D	Blocked	118.193.31.179	00:01:40	From suricata, ET POLICY Suspicious inbound to mySQL port 3306 => 1:2010937 => event timestamp: 2017-07-13 19:46:56
D	Blocked	169.54.233.125	00:02:10	From suricata, GPL DNS named version attempt => 1:2101616 => event timestamp: 2017-07-13 19:47:26
D	Blocked	197.231.221.211	00:02:16	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 34 => 1:2522066 => event timestamp: 2017-07-13 19:47:32
D	Blocked	27.115.160.222	00:02:21	From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 14 => 1:2403313 => event timestamp: 2017-07-13 19:47:37
D	Blocked	83.233.166.43	00:02:23	From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 81 => 1:2403380 => event timestamp: 2017-07-13 19:47:40
D	Blocked	199.87.154.255	00:02:25	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 40 => 1:2522078 => event timestamp: 2017-07-13 19:47:43
D	Blocked	114.255.78.180	00:02:58	From suricata, ET COMPROMISED Known Compromised or Hostile Host Traffic group 6 => 1:2500010 => event timestamp: 2017-07-13 19:48:15
D	Blocked	199.249.223.76	00:03:00	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 38 => 1:2522074 => event timestamp: 2017-07-13 19:48:18
D	Blocked	61.164.46.188	00:03:02	From suricata, ET COMPROMISED Known Compromised or Hostile Host Traffic group 38 => 1:2500074 => event timestamp: 2017-07-13 19:48:19
D	Blocked	77.247.181.165	00:03:10	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 67 => 1:2522132 => event timestamp: 2017-07-13 19:48:26
D	Blocked	162.247.72.27	00:03:11	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 13 => 1:2522024 => event timestamp: 2017-07-13 19:48:28
D	Blocked	163.172.217.50	00:03:19	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 14 => 1:2522026 => event timestamp: 2017-07-13 19:48:37
D	Blocked	109.163.234.8	00:03:21	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 3 => 1:2522004 => event timestamp: 2017-07-13 19:48:37
D	Blocked	212.47.242.127	00:03:26	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 43 => 1:2522084 => event timestamp: 2017-07-13 19:48:44
D	Blocked	198.20.69.74	00:03:30	From suricata, GPL DNS named version attempt => 1:2101616 => event timestamp: 2017-07-13 19:48:48
D	Blocked	164.132.51.91	00:03:34	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 15 => 1:2522028 => event timestamp: 2017-07-13 19:48:52
D	Blocked	94.242.246.23	00:03:47	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 84 => 1:2522166 => event timestamp: 2017-07-13 19:49:05
D	Blocked	62.102.148.67	00:03:58	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 60 => 1:2522118 => event timestamp: 2017-07-13 19:49:14
D	Blocked	193.107.85.62	00:04:00	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 32 => 1:2522062 => event timestamp: 2017-07-13 19:49:17
D	Blocked	171.25.193.77	00:04:05	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 16 => 1:2522030 => event timestamp: 2017-07-13 19:49:22
D	Blocked	82.209.173.176	00:04:32	From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 79 => 1:2403378 => event timestamp: 2017-07-13 19:49:49
D	Blocked	169.54.244.78	00:04:40	From suricata, GPL DNS named version attempt => 1:2101616 => event timestamp: 2017-07-13 19:49:58
D	Blocked	139.162.108.129	00:04:43	From suricata, ET POLICY Suspicious inbound to mySQL port 3306 => 1:2010937 => event timestamp: 2017-07-13 19:50:00
D	Blocked	59.127.90.251	00:04:48	From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 45 => 1:2403344 => event timestamp: 2017-07-13 19:50:04
D	Blocked	176.10.104.243	00:04:50	From suricata, ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 18 => 1:2522034 => event timestamp: 2017-07-13 19:50:08
D	Blocked	221.229.166.78	00:05:05	From suricata, ET POLICY Suspicious inbound to mySQL port 3306 => 1:2010937 => event timestamp: 2017-07-13 19:50:21
D	Blocked	59.3.211.107	00:05:13	From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 36 => 1:2403335 => event timestamp: 2017-07-13 19:50:31
D	Blocked	59.14.242.86	00:07:25	From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 37 => 1:2403336 => event timestamp: 2017-07-13 19:52:43
D	Blocked	68.114.95.226	00:07:27	From suricata, ET CINS Active Threat Intelligence Poor Reputation IP group 58 => 1:2403357 => event timestamp: 2017-07-13 19:52:45
D	Blocked	12.237.226.234	00:09:05	From suricata, ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection (Inbound) => 1:2001972 => event timestamp: 2017-...

MUM IPS-MikroTik-Suricata

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

Proyecto

Rules Manager

Rules Manager - Qué es?

WebPanel-IPS-MikroTik-Suricata ó Rules Manager:

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

✓ Gratuito, Open Source, Colaborativo (Alojado en *Github*)

Active Top Ten IP Attack

Count	IP Block	Country
2	46.17.47.89	Russian Federation
2	80.82.70.26	Netherlands
2	163.172.110.117	United Kingdom
2	83.143.246.30	Europe
2	158.85.81.124	Canada
2	54.80.47.150	United States
2	51.15.67.72	United Kingdom
1	76.122.101.255	United States
1	107.189.238.243	Canada
1	50.26.129.20	United States

Active Top Ten Alert Rules

Count	Alert	Sid
111	ET DOS DNS Amplification Attack Inbound	2016016
6	GPL DNS named version attempt	2101616
3	ET SCAN Sipvicious Scan	2008578
3	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	2011716
2	ET CINS Active Threat Intelligence Poor Reputation IP group 94	2403393
1	ET CINS Active Threat Intelligence Poor Reputation IP group 83	2403382
1	ET DROP Dshield Block Listed Source group 1	2402000
1	ET CINS Active Threat Intelligence Poor Reputation IP group 51	2403350

Rules Manager

Rules Manager ≡

Uptime 21 Minutes | Load Avr: 1.25 1.06 1.32 2/411 | MEM Free: 100%

Suricata IDS: OK | DB Daemon: OK | IPS Daemon: OK | Snorby: OK | API: OK

Active Alert Blocked (447) - Time: 20:47:37

Time	IP Block	Rule	SID	Action
3 seconds	61.222.213.190	ET CINS Active Threat Intelligence Poor Reputation IP group 54	2403353	
a minute ago	80.88.102.253	ET CINS Active Threat Intelligence Poor Reputation IP group 73	2403372	
a minute ago	196.52.43.57	ET POLICY Suspicious inbound to mySQL port 3306	2010937	
2 minutes ago	196.52.43.63	GPL DNS named version attempt	2101616	
3 minutes ago	66.240.219.146	GPL DNS named version attempt	2101616	
4 minutes ago	88.12.14.132	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection (Inbound)	2001972	
4 minutes ago	59.7.253.139	ET CINS Active Threat Intelligence Poor Reputation IP group 36	2403335	
4 minutes ago	14.44.3.240	ET CINS Active Threat Intelligence Poor Reputation IP group 8	2403307	
4 minutes ago	73.100.29.216	ET CINS Active Threat Intelligence Poor Reputation IP group 61	2403360	
4 minutes ago	61.236.231.37	ET CINS Active Threat Intelligence Poor Reputation IP group 54	2403353	
6 minutes ago	36.37.213.219	ET CINS Active Threat Intelligence Poor Reputation IP group 17	2403316	
6 minutes ago	78.189.229.238	ET CINS Active Threat Intelligence Poor Reputation IP group 70	2403369	
6 minutes ago	91.211.3.108	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection (Inbound)	2001972	
7 minutes ago	188.16.84.145	ET CNC Ransomware Tracker Reported CnC Server group 56	2404455	
7 minutes ago	92.63.91.9	ET SCAN Behavioral Unusually fast Terminal Server Traffic, Potential Scan or Infection (Inbound)	2001972	
9 minutes ago	158.85.81.119	GPL SNMP public access udp	2101411	
10 minutes ago	42.53.229.230	ET DROP Spamhaus DROP Listed Traffic Inbound group 2	2400001	
10 minutes ago	81.215.201.162	ET CINS Active Threat Intelligence Poor Reputation IP group 75	2403374	
10 minutes ago	87.251.245.80	ET CINS Active Threat Intelligence Poor Reputation IP group 91	2403390	
10 minutes ago	50.21.199.100	ET CINS Active Threat Intelligence Poor Reputation IP group 32	2403331	
11 minutes ago	168.1.128.34	GPL DNS named version attempt	2101616	
11 minutes ago	71.6.167.142	ET POLICY Suspicious inbound to mySQL port 3306	2010937	
11 minutes ago	91.200.12.44	ET DROP Spamhaus DROP Listed Traffic Inbound group 5	2400004	
12 minutes ago	82.246.107.85	ET CINS Active Threat Intelligence Poor Reputation IP group 79	2403378	
12 minutes ago	59.29.123.97	ET CINS Active Threat Intelligence Poor Reputation IP group 38	2403337	

Active Top Ten IP Attack

Count	IP Block	Country
52	118.193.31.179	China
41	139.162.108.129	United States
20	103.10.197.106	Hong Kong
19	83.143.246.30	Europe
15	71.6.202.243	United States
14	103.10.197.18	Hong Kong
14	116.193.159.66	Hong Kong
13	37.49.224.185	Netherlands
12	163.172.211.135	United Kingdom
11	139.162.110.42	United States

Active Top Ten Alert Rules

Count	Alert	Sid
135	GPL DNS named version attempt	2101616
125	ET POLICY Suspicious inbound to mySQL port 3306	2010937
24	GPL SNMP public access udp	2101411
15	ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	2011716
13	ET COMPROMISED Known Compromised or Hostile Host Traffic group 31	2500060
11	ET COMPROMISED Known Compromised or Hostile Host Traffic group 13	2500024
9	ET COMPROMISED Known Compromised or Hostile Host Traffic group 6	2500010
9	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 33	2522064
8	ET COMPROMISED Known Compromised or Hostile Host Traffic group 28	2500054
5	ET TOR Known Tor Relay/Router (Not Exit) Node Traffic group 81	2522160

MKE Solutions

Designed by Maximiliano Dobladez

Rules Manager

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	

Rules Manager

Instalación:

- Instalar dependencias ***php5-geoip*** y ***php5-mysql***
- Clonar el repositorio de ***GitHub***

cd /www/html/snorby/public/
git clone https://github.com/elmaxid/webpanel_ips_mikrotik_suricata.git
mv webpanel_ips_mikrotik_suricata rules

- *Modificar el esquema DB:*

mysql -u user -p db_name < schema.sql

- *Ingresar via web:* http://IP_SURICATA/rules

Referencias

Sitios y bibliografia utilizada:

- ***Suricata:***
  https://suricata-ids.org/
- ***IPS-Mikrotik-Suricata:***
  https://github.com/elmaxid/ips-mikrotik-suricata
- ***Rule Manager / WebPanel***
  https://github.com/elmaxid/webpanel_ips_mikrotik_suricata

Presentaciones MUMs:

- ***Mikrotik y Suricata -***
  José M. Román - MUM España 16

  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

CC BY NC SA