MUM MikroTik User Meeting

Detectando DDoS e intrusiones con RouterOS

Por: Maximiliano Dobladez
MKE Solutions

20 de Enero de 2017

Ciudad de Guatemala

Guatemala

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

Entrenamientos Oficiales

- Certificaciones Disponibles

MTCNA

MTCUME

MTCTCE

MTCWE

MTCRE

MTCINE

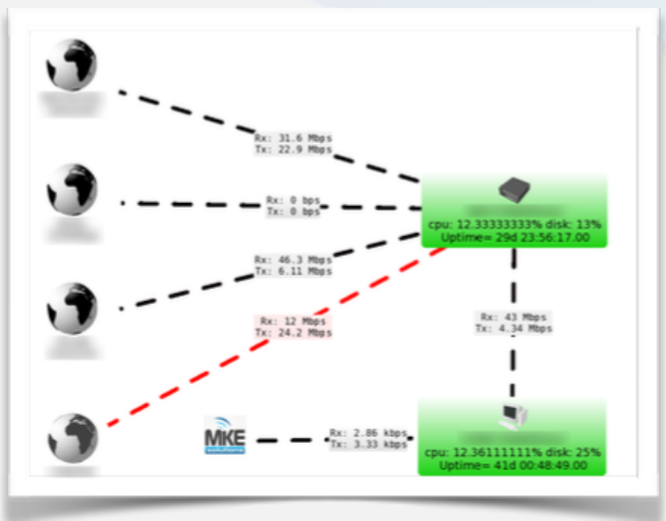
- Entrenamientos Públicos y Privados.
- ~300 alumnos por año, con un 75% de certificados.

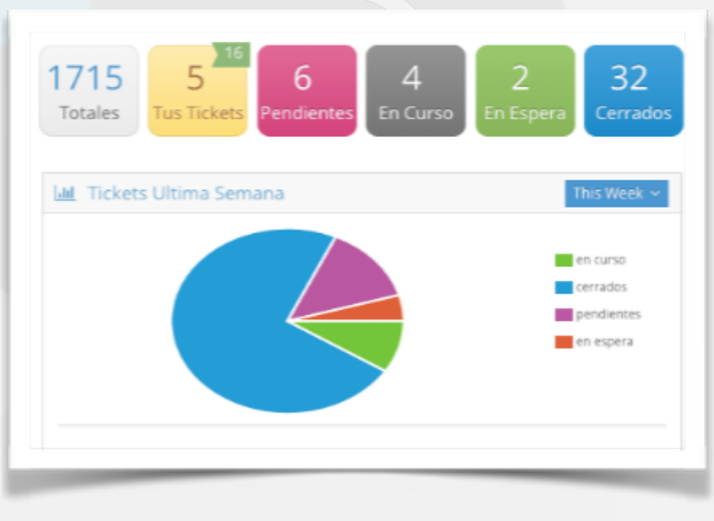
powered by Mke Solutions

Academia DE ENTRENAMIENTOS

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 / DDoS**
- **Suricata**: qué es?, cómo funciona? cómo se instala?
- **FastNetMon**: qué es?, cómo funciona? cómo se instala?
- Integración con **RouterOS**
- Recursos y bibliografía

IDS / IPS

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* (drop, reject, alert, pass)
- Cuando se detecta un evento conocido se trata con una acción

IDS (Intrusion Detection System)

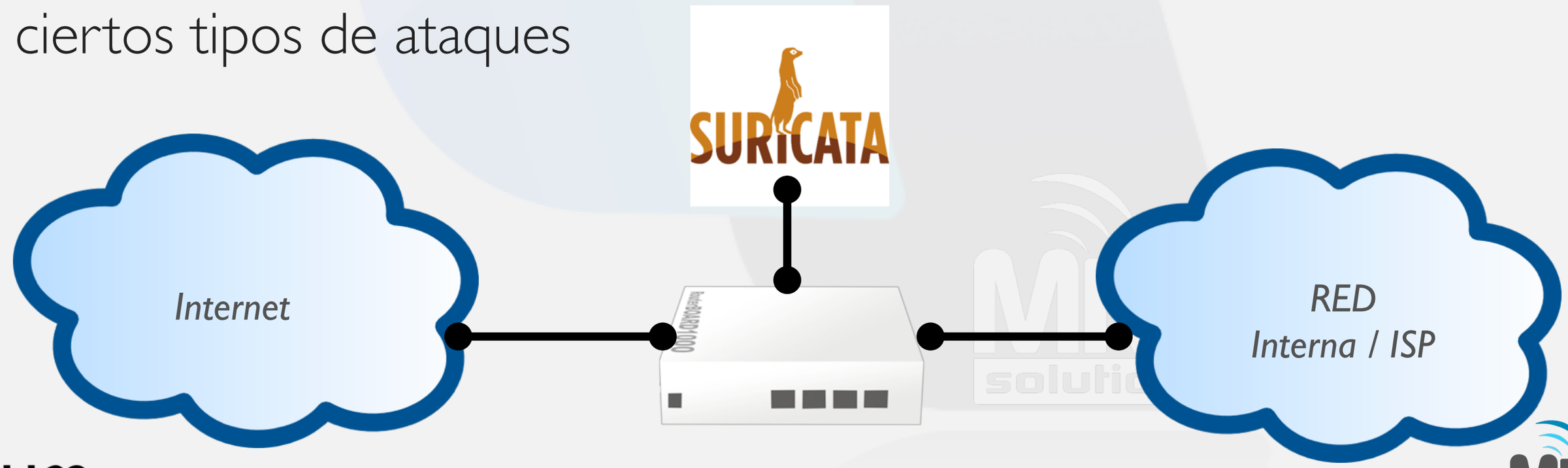
- Es un dispositivo o aplicación que analiza paquetes completos, tanto cabeceras como and payload, en busca de eventos conocidos.
- Cuando se detecta un evento se genera un mensaje de log.

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:

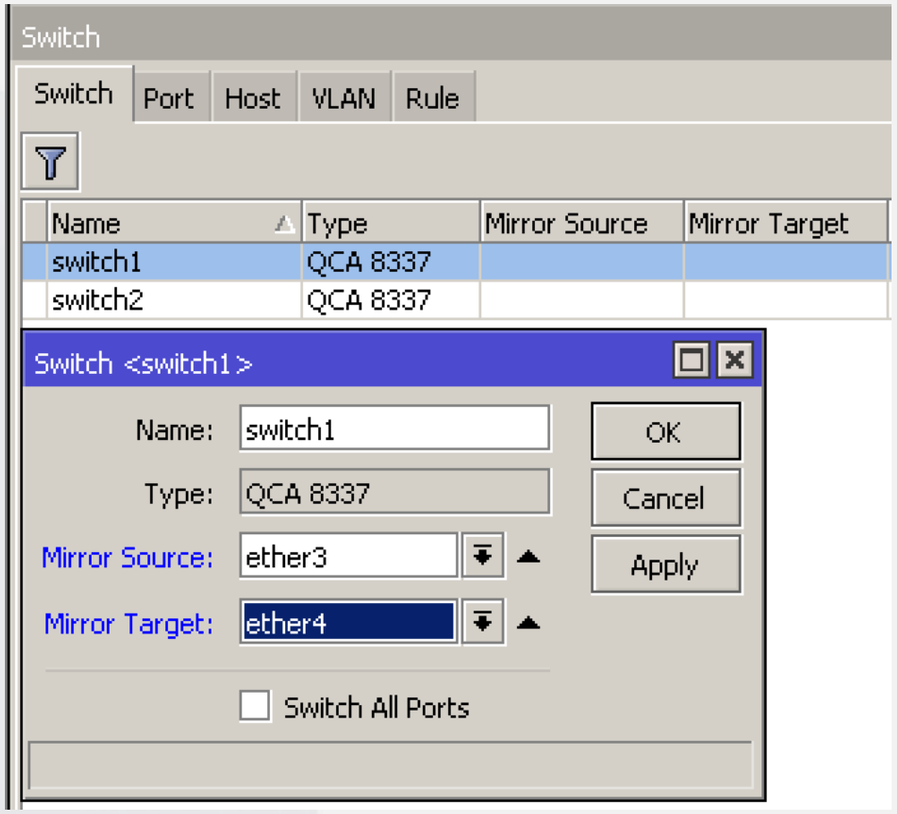
IFACE=eth0

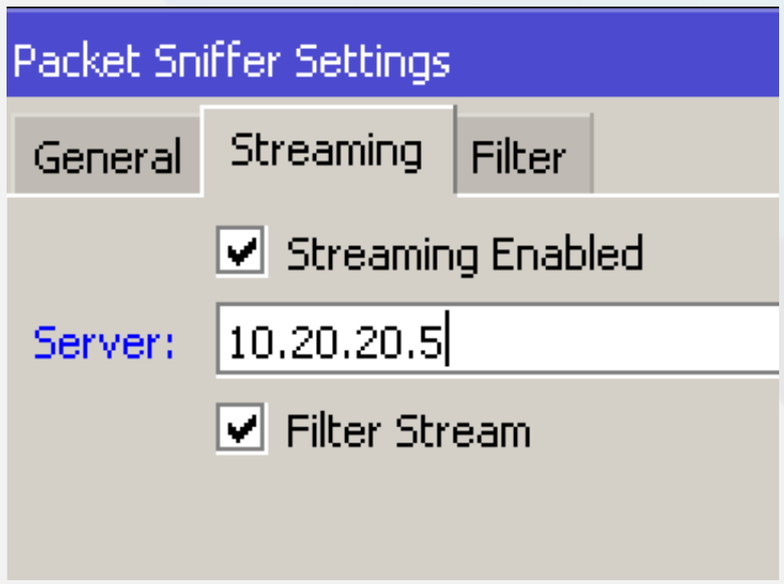
Suricata - Integración con rOS

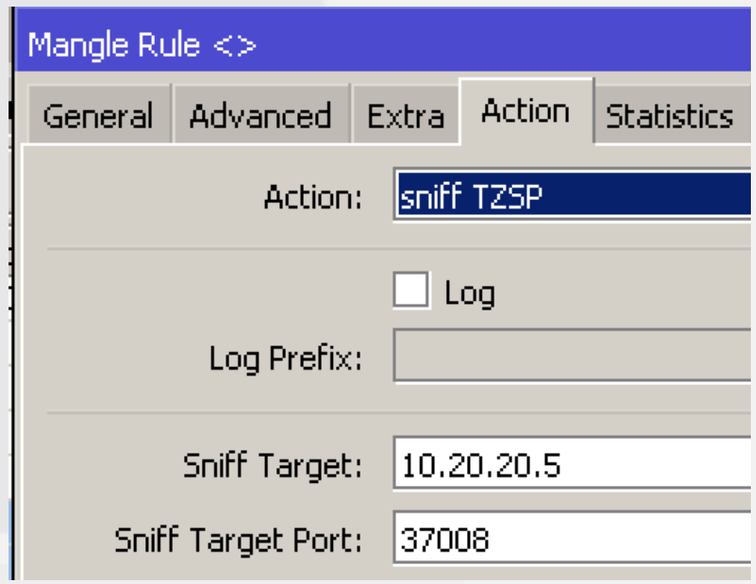
Para que empiece a trabajar hay que redireccionar el tráfico desde el *MikroTik RouterOS* hacia *Suricata*

Podemos realizarlo con:

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







Suricata - Reportes

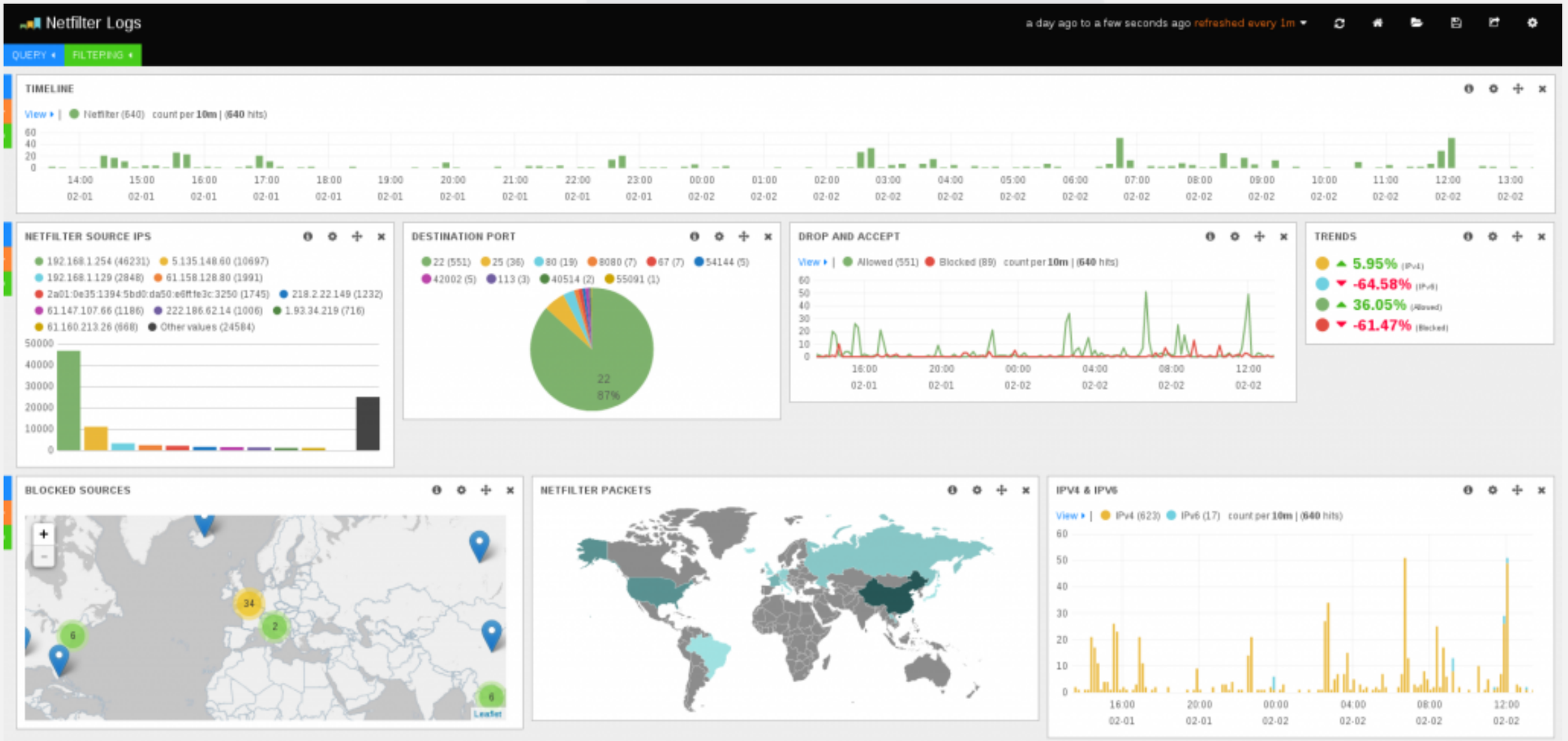
Los logs estarán en */var/log/suricata*

```
[**] [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.
[**] [1:2002910:4] 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

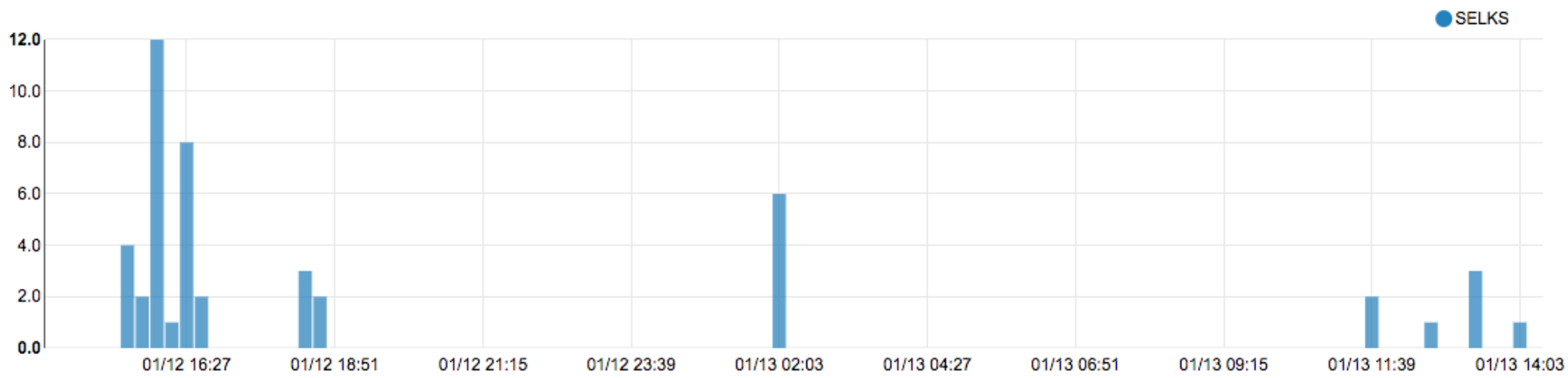
- Default SELKS ruleset

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)

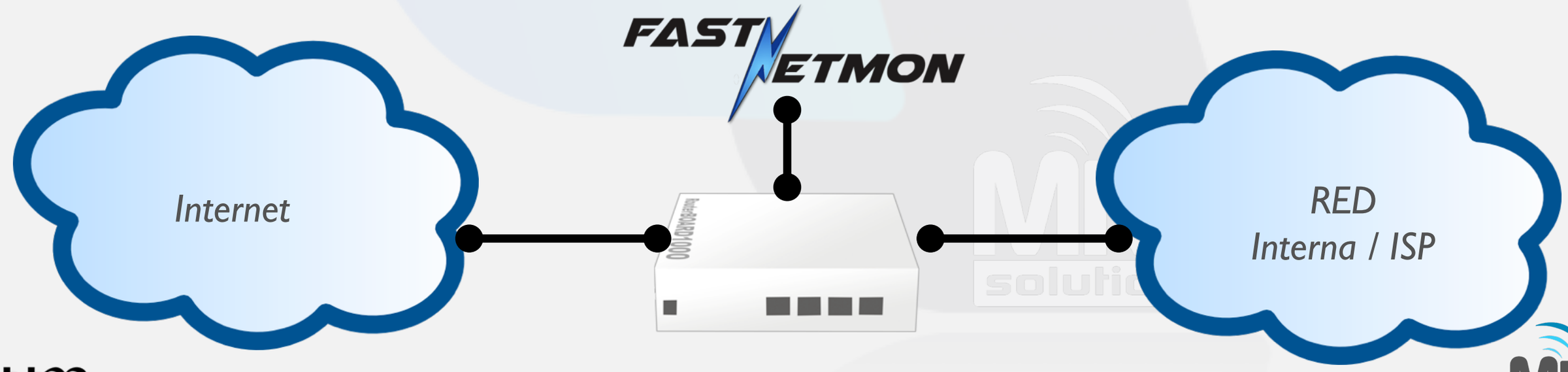


FastNetMon

FastNetMon - Qué es?

FastNetMon:

- Herramienta para detectar ***DDoS*** en 2 segundos
- Gratuito, Open Source, Colaborativo
- Soporte para ***BGP4*** y ***BGP flow spec*** (RFC 5575)
- Soporta ***NetFlow*** v5, v9, ***IPFIX***, ***sFlow*** v4, v5, ***Port Mirror/SPAN***
- Al detectar un ataque, permite mandar el IP atacado a ***BlackHole***



FastNetMon - Qué es?

Ataques que puede detectar:

- ***syn_flood:*** TCP packets with enabled SYN flag
- ***udp_flood:*** flood with UDP packets
- ***icmp flood:*** flood with ICMP packets
- ***ip_fragmentation_flood:*** IP packets with MF flag set or with non zero fragment offset
- *DNS, NTP, SSDP, SNMP amplification*

Dispone de agregados adicionales:

- *MikroTik RouterOS, A10 Networks*
- *Slack, Python, Bash*

```
27,7% - Cisco
26,4% - Juniper
6,8% - Extreme
6,1% - Brocade
6,1% - Mikrotik
3,38% - Dell
2,7% - HP
2% - Force6
1,35% - D-Link
1,35% - Fortigate
1,35% - Palo Alto
1,35% - VyOS
0,68% - Alcatel
0,68% - Allied
```

FastNetMon - Instalación

- Para instalarlo bajo Debian / CentOS:

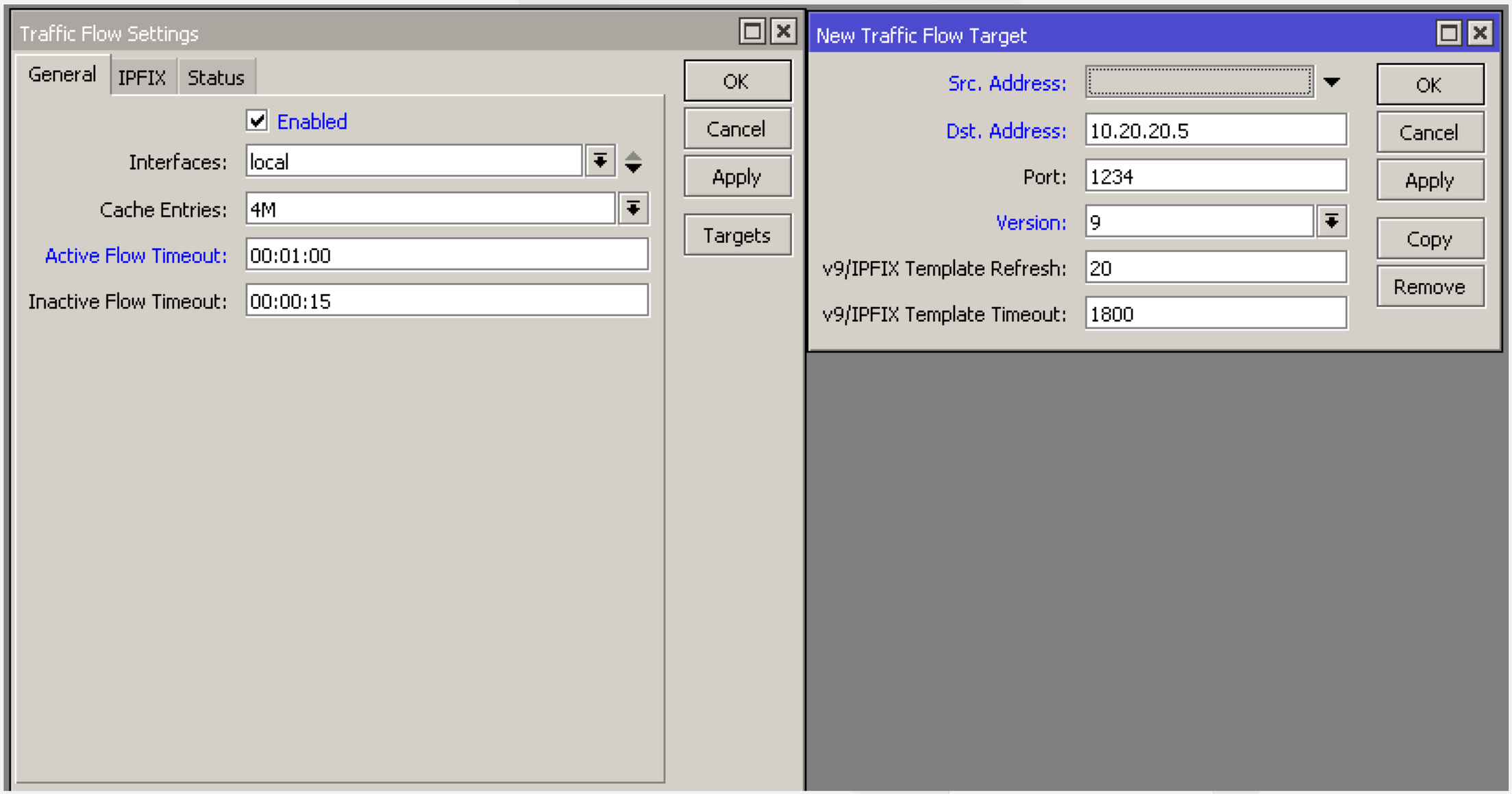
  wget https://raw.githubusercontent.com/pavel-odintsov/fastnetmon/master/src/fastnetmon_install.pl -Ofastnetmon_install.pl

  sudo perl fastnetmon_install.pl

- Configurar las redes locales en */etc/networks_list*
- Configurar lista de IP whitelist en */etc/networks_whitelist*
- Se ejecuta iniciando */opt/fastnetmon/fastnetmon*
- Logs son guardados en */var/log/fastnetmon.log*

MUM FastNetMon - Integración con rOS

- Para integrarlo con ***MikroTik RouterOS*** es necesario configurar ***NetFlow, IPFIX*** o ***Port Mirror***



FastNetMon - Cliente

- Ejecutando el cliente podemos ver como trabaja

/opt/fastnetmon/fastnetmon_client

```
Incoming traffic        171015 pps    384 mbps  11973 flows
159.11.22.33              3309 pps   33.3 mbps     77 flows
159.11.22.33              3116 pps   34.8 mbps      2 flows
159.11.22.33              2567 pps   29.5 mbps      2 flows
159.11.22.33              2439 pps    1.8 mbps     76 flows
159.11.22.33              2364 pps    1.4 mbps     55 flows
159.11.22.33              2104 pps    1.5 mbps     19 flows
159.11.22.33              1938 pps    1.3 mbps     36 flows

Outgoing traffic        225121 pps   1905 mbps  17893 flows
159.11.22.33              3699 pps   39.9 mbps     83 flows
159.11.22.33              3557 pps   37.3 mbps    124 flows
159.11.22.33              2965 pps   32.8 mbps     98 flows
159.11.22.33              2645 pps   29.7 mbps     38 flows
159.11.22.33              2522 pps   26.1 mbps     65 flows
159.11.22.33              2474 pps   26.8 mbps     61 flows
159.11.22.33              2285 pps   18.9 mbps    194 flows

Internal traffic             0 pps      0 mbps
```

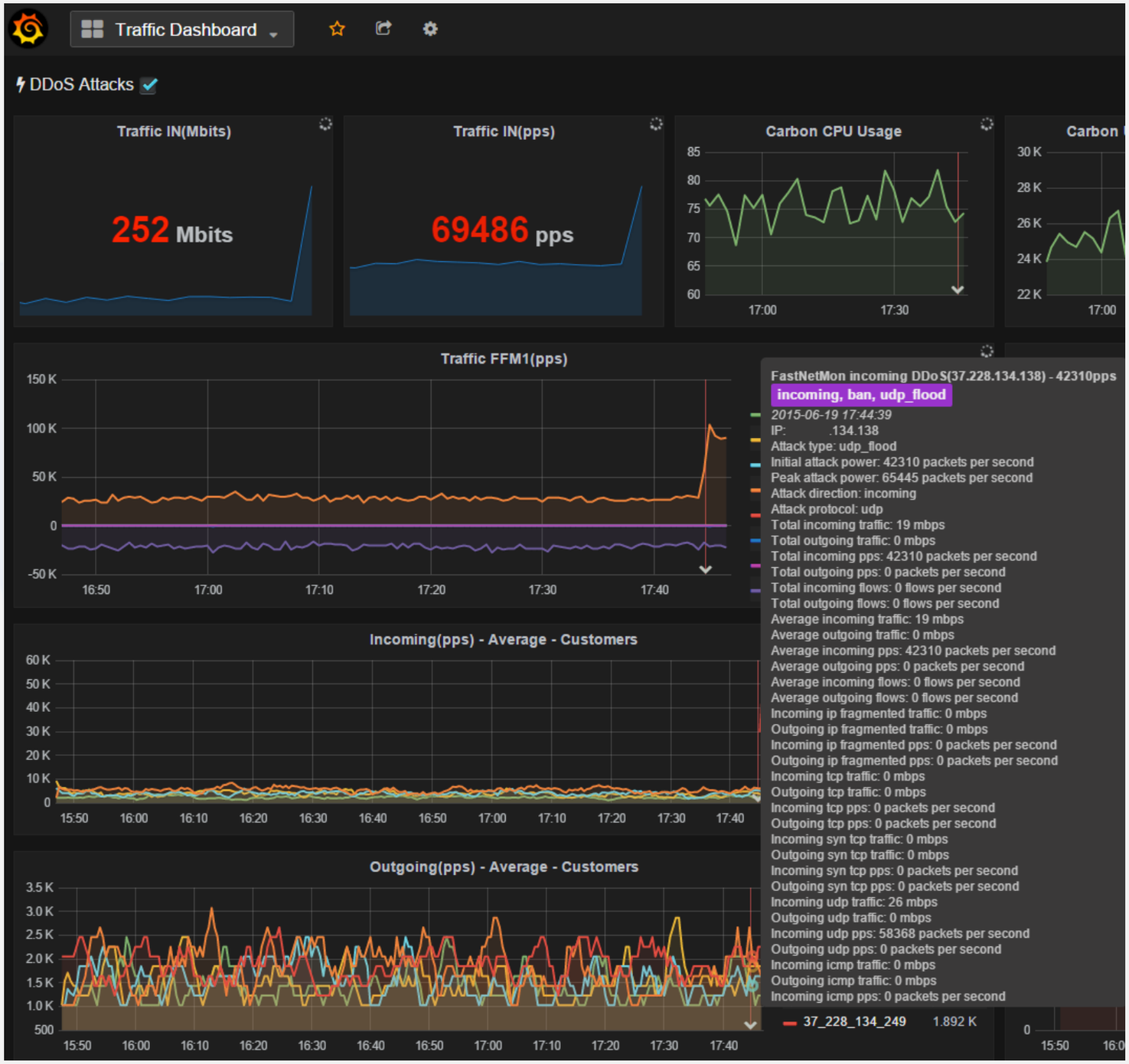
FastNetMon - Acción

Una vez detectado un ataque es posible:

- ***Ejecutar un script*** personalizado (enviar correo, aplicar reglas de ACL, etc)
- ***Blackhole*** en tabla de ruteo (script MikroTik)
- ***Anuncio BGP*** (comunidad, blackhole, cloud mitigation)
- ***BGP Flow spec*** (bloquear un tipo de tráfico selectivo)
- Guardar un ***muestreo del ataque*** para luego investigarlo (tcpdump durante el ataque)

FastNetMon - Reportes

Es posible utilizar herramientas adicionales para un reporte mas "amigable"



Grafana - http://github.com/grafana/grafana

Referencias

Sitios y bibliografia utilizada:

- ***Suricata:*** https://suricata-ids.org/
- ***FastNetMon:*** https://fastnetmon.com/

Presentaciones MUMs:

- ***Distributed Denial of Service Attacks Detection and Mitigation*** - Wardner Maia - MUM Slovenia 16

  http://mum.mikrotik.com/presentations/EU16/presentation_2960_1456752556.pdf

- ***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