



Реализуем проактивную систему IPS/IDS защиты на Mikrotik + Suricata

MUM Moscow 2018
mikrotik-training.ru





ОБО МНЕ

- Козлов Роман Сергеевич
- Сертифицированный тренер по MikroTik
- Технический директор IntegaSky
- Провожу бесплатные обучающие вебинары по MikroTik
- Более 200 выполненных проектов MikroTik
- Проводим мини-тренинги – mikrotik.team
- Являюсь соведущим linkmeup_sysadmins



Канал на youtube

<https://goo.gl/DSL6VG>



Запись на вебинары

<http://mikrotik-training.ru/webinar/>



Канал в телеграм

<https://t.me/miktrain>



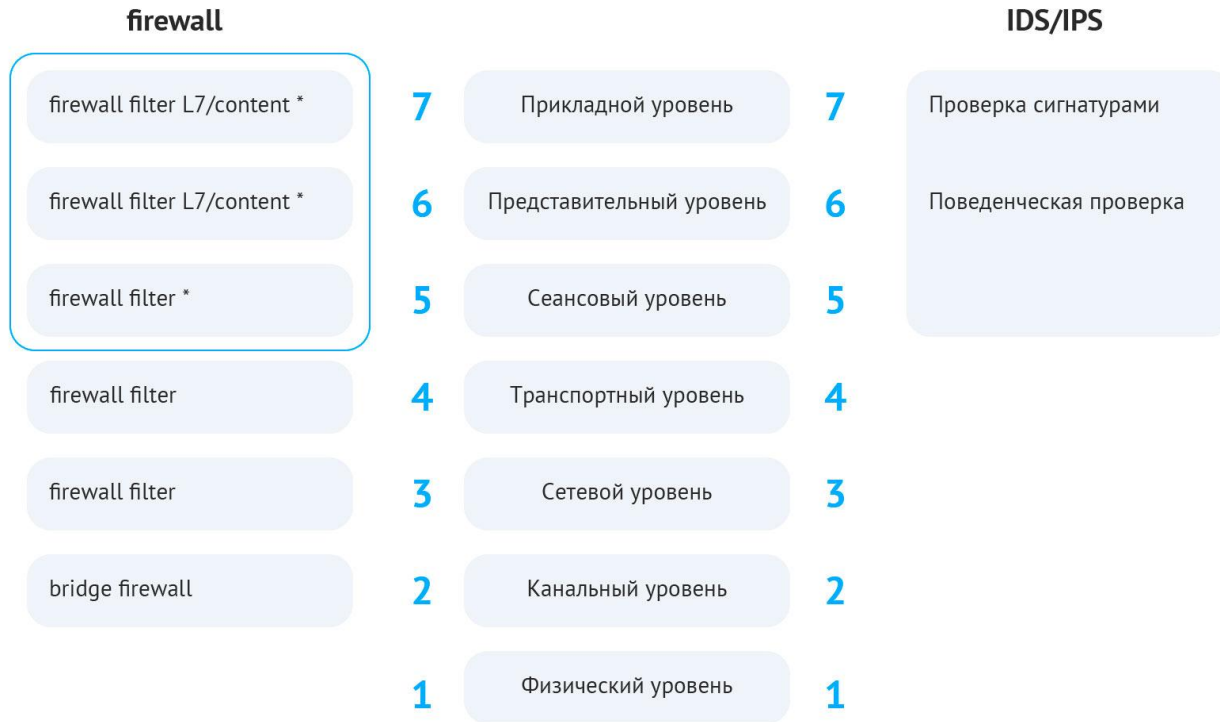
Содержание

- Общие сведения о IPS/IDS
- Проблема отсутствия встроенного функционала в RouterOS и варианты решений
- Обзор бесплатного решения Suricata
 - Принцип работы
 - Работа со списками правил
 - Интеграция с firewall RouterOS
- Отправка трафика routerOS
 - Port mirroring
 - TZSP – pcap
- SELKS – готовое решение



OSI

firewall vs IDS/IPS

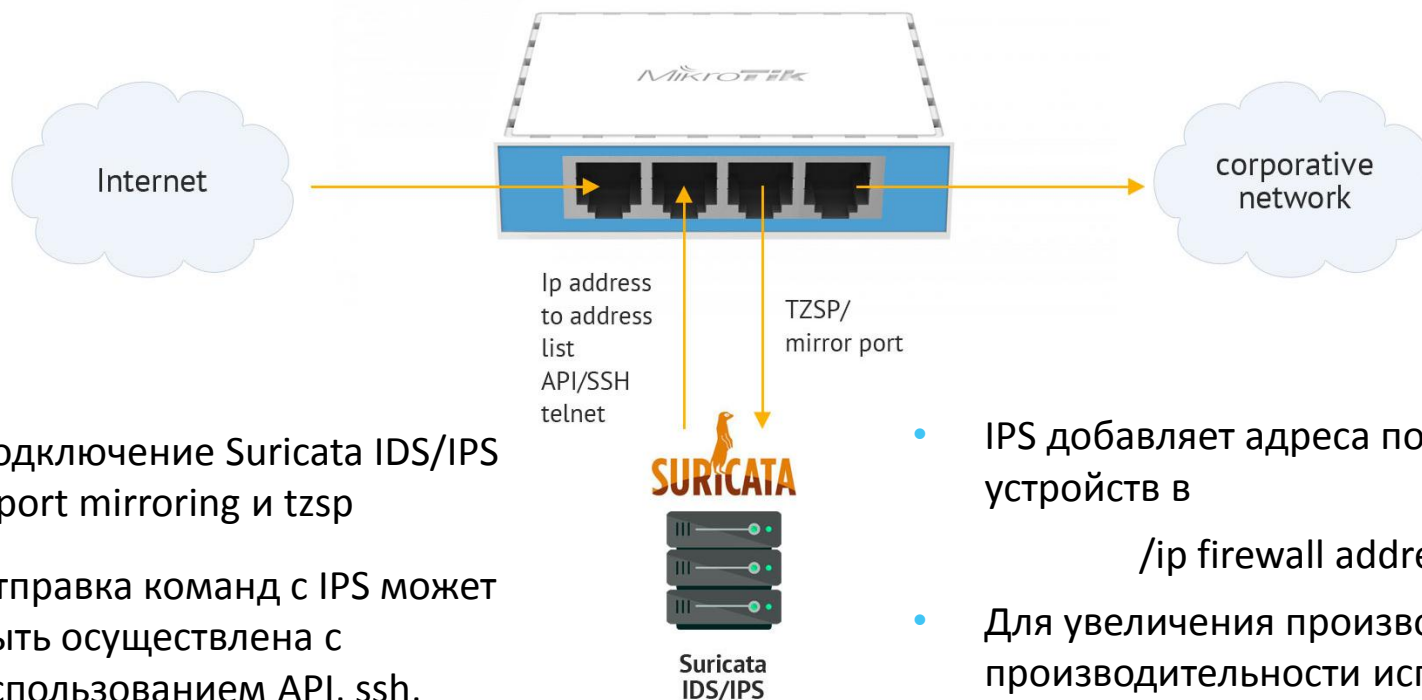


Общие сведения о IPS/IDS

- Задача **IDS (Intrusion Detection System)** состоит в обнаружении и регистрации атак, а также оповещении при срабатывании определенного правила. В отличие от межсетевого экрана, контролирующего только параметры сессии (IP, номер порта и состояние связей), IDS «заглядывает» внутрь пакета (до седьмого уровня OSI), анализируя передаваемые данные.
- **IDS умеют:**
 - выявлять различные виды сетевых атак
 - обнаруживать попытки неавторизованного доступа или повышения привилегий
 - появление вредоносного ПО
 - отслеживать открытие нового порта и т. д.
- **IPS (Intrusion Prevention System)** - система предотвращения атак.
- **IDS** могут самостоятельно перестраивать пакетный фильтр или прерывать сеанс, отсылая TCP RST.

Проблема отсутствия встроенного функционала в RouterOS и варианты решений

1. RouterOS – это классический firewall с некоторыми дополнениями:
 - Layer 7 filter – возможность поиска по регулярным выражениям в 2kb пакета
 - Content filter – функция поиска в нешифрованных пакетах содержимого
 - TLS host - Позволяет сопоставлять трафик https на основе имени узла SNS SNI
 - Возможно настраивать поведенческие фильтры на основании количества соединений и их частоты
2. В RouterOS нет функционала IDS/IPS часть функций можно реализовать на L7/content filtering – что потребует больших трудозатрат и будет достаточно неэффективно
3. Так же подобные настройки снизят производительность нашего firewall



- Подключение Suricata IDS/IPS – port mirroring и tzsp
- Отправка команд с IPS может быть осуществлена с использованием API, ssh, telnet

- IPS добавляет адреса подозрительных устройств в
/ip firewall address list
- Для увеличения производительности используем
/ip firewall raw
- Не забываем про белые списки
- Не забываем тестировать

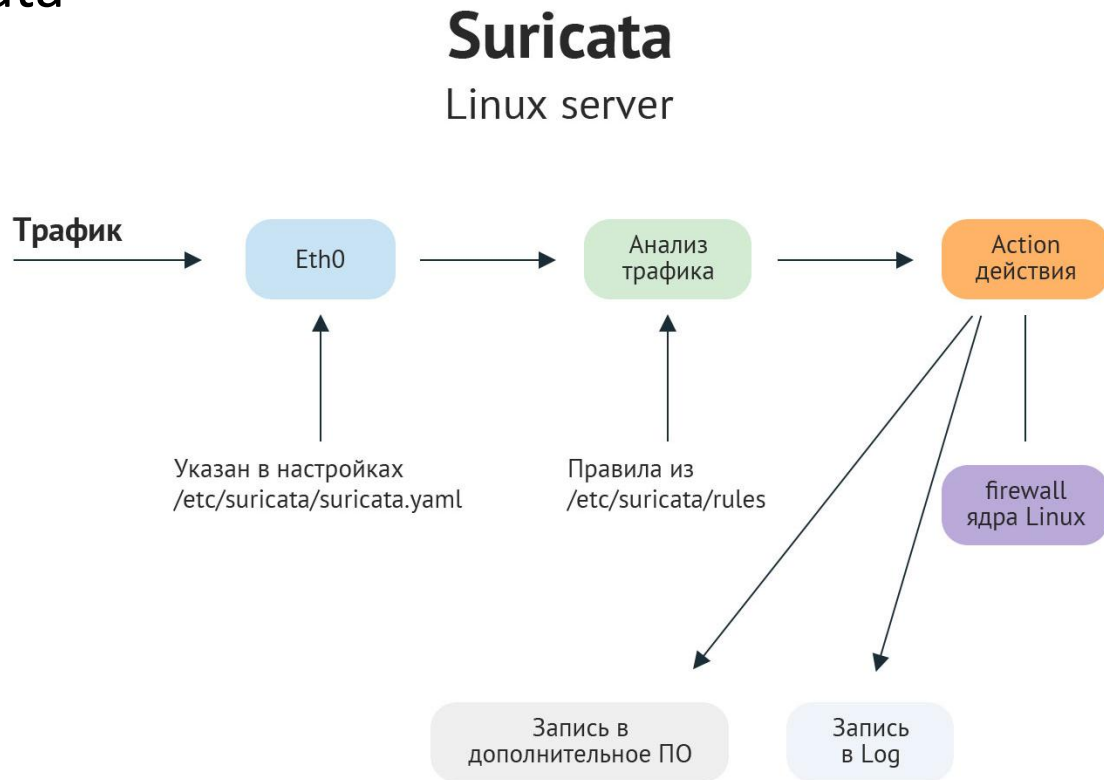
Обзор бесплатного решения Suricata

1. Бесплатное решение IDS / IPS GPLv2
2. Suricata работает в многопоточном режиме
3. Возможность аппаратного ускорения на стороне GPU
4. Поддерживается IPv6
5. Движок автоматически определяет протоколы IP, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB, SMTP и SCTP
6. Интерфейсы и анализаторы, написанные для Snort (Barnyard, Snortsnarf, Sguil и т. д.), без доработок работают и с Suricata
7. Основу механизма детектирования в Suricata составляют правила (rules)
8. Не поддерживает TZSP



Принцип работы Suricata

- Изначально Suricata получает трафик на интерфейс, указанный в настройках `/etc/suricata/suricata.yaml`
- По правилам указанным в файле конфигурации с помощью сигнатур в `/etc/suricata/rules` происходит обработка трафика и детектирование угроз
- Поведение по умолчанию предполагает запись обнаруженных угроз в log
- Так же есть возможность исполнять различные действия



Работа со списками правил Suricata

1. Собственный формат правил rules,
2. Правило состоит из трех компонентов:
 - действие - pass, drop, reject или alert
 - заголовок - IP/порт источника и назначения
 - описание (что искать).
3. В настройках используются переменные, позволяющие, например, создавать счетчики.
4. При этом информацию из потока можно сохранять для последующего использования.

Интеграция с firewall RouterOS

1. На **forum.mikrotik.com** есть реализация интеграции с **routeros**

- PHP скрипт берет ip адреса нарушителей из `/var/log/suricata/fast.log` и добавляет их через API в адрес лист mikrotik
- PHP скрипт берет ip адреса нарушителей из базы данных `barnyard2`(дополнительное ПО) и добавляет их через API в адрес лист mikrotik

2. Прием трафика от mikrotik

- На interface
- TZSP port – требуется виртуальный интерфейс и дополнительное ПО – `trafr` (mikrotik.com) или `tzsp2pcap` (github)

Отправка трафика RouterOS

1. Port mirroring – функция switch

- `/interface ethernet switch set switch1 mirror-source=ether2 mirror-target=ether3`

2. Отправка трафика по протоколу TZSP

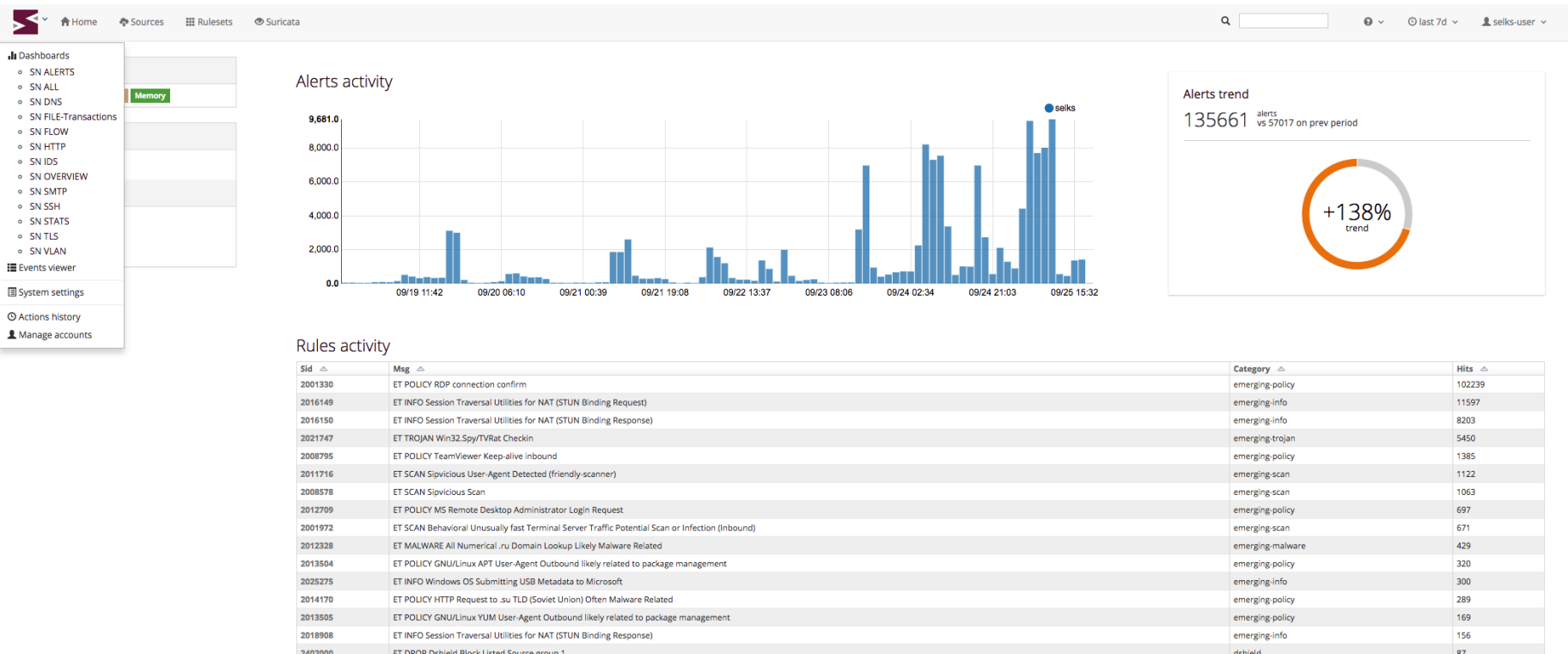
- `/tool sniffer set streaming-enabled=yes streaming-server=192.168.x.x`
- `/ip firewall mangle add action=sniff-tzsp chain=prerouting sniff-target=192.168.x.x sniff-target-port=37008`

SELKS

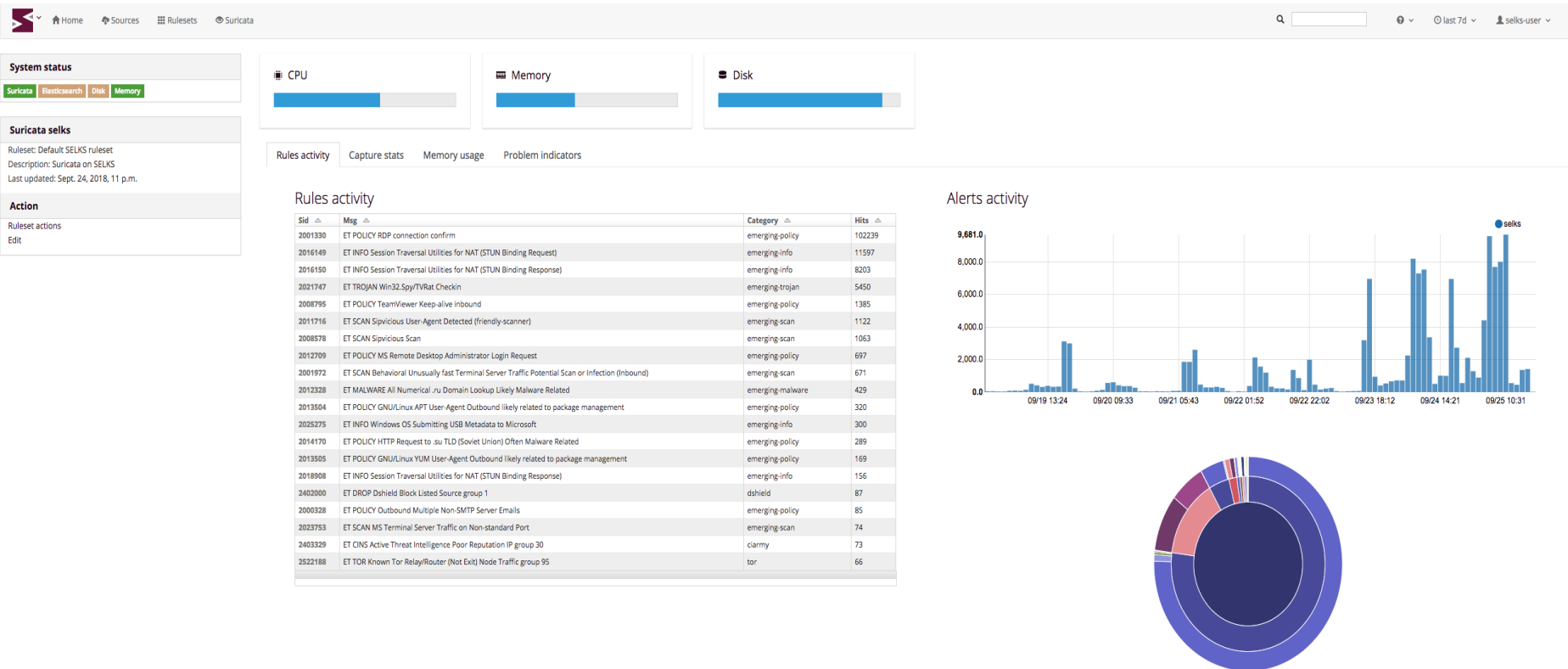


1. Бесплатное готовое решение для работы с suricata
2. Selks состоит из
 - Suricata – IDS/IPS движек
 - Elasticsearch 5.5.2 – поисковый движок
 - Logstash 5.5.2 – сбор логов и последующая их обработка
 - Kibana 5.5.2 – веб интерфейс для отображения данных из Elasticsearch
 - Scirius – веб интерфейс для управления suricata и навигации по kibana
 - EveBox – альтернативный веб интерфейс для управления событиями suricata
3. Поставляется в виде готового iso образа.

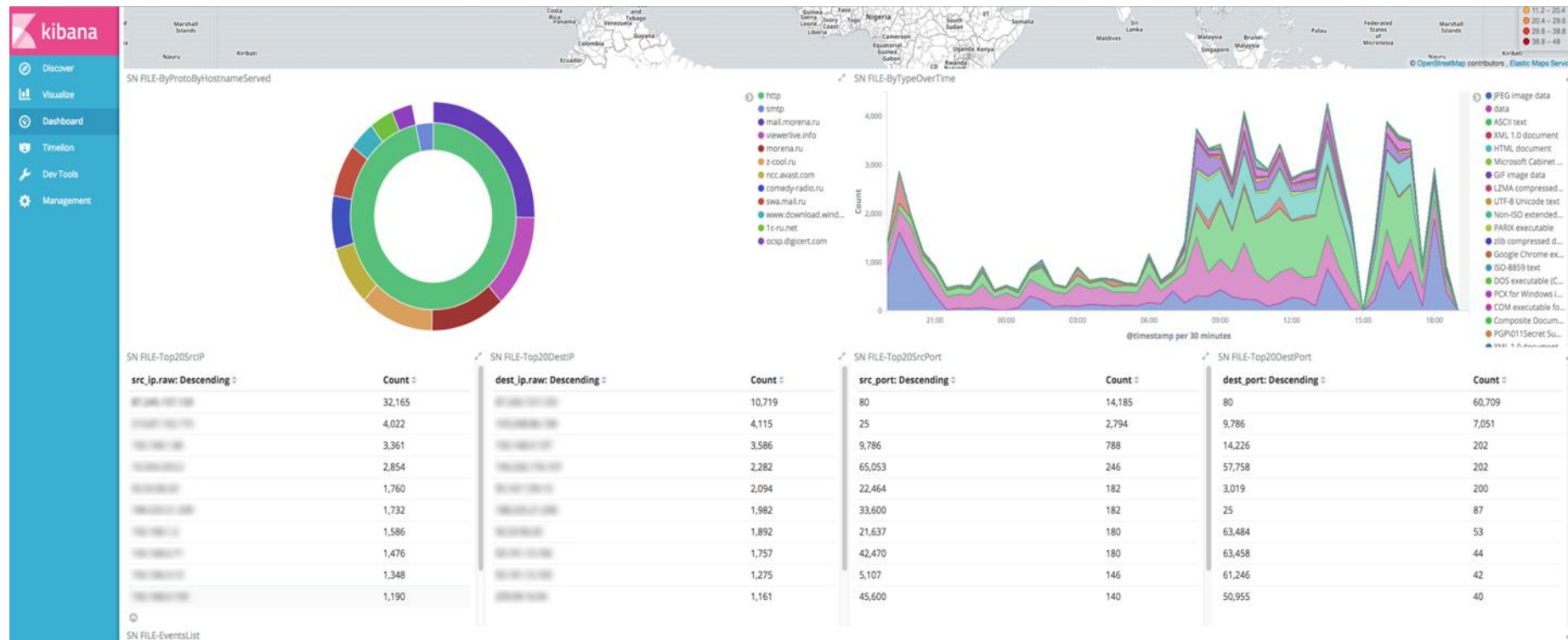
SELKS



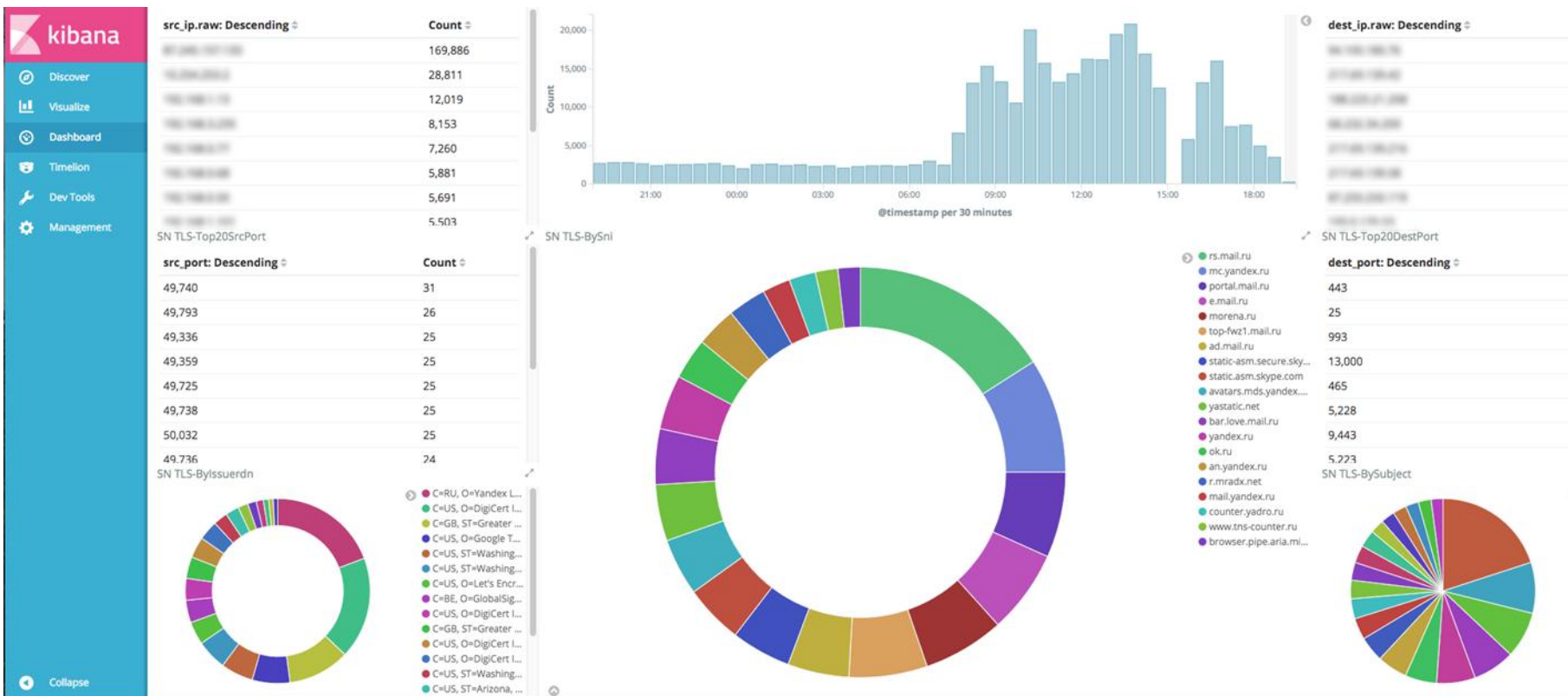
SELKS



SELKS



SELKS



Результаты работы suricata в сети

1. Обнаруженные угрозы

- Несколько пропущенных вирусов
- Обнаружено нецелевое использование ресурсов сети интернет
- Обнаружено ПО отправляющее логины и пароли без шифрования
- Заблокированы торренты
- Заблокирован teamveawer
- Заблокированы различные сканеры портов

2. Оптимизация firewall

Общие рекомендации по внедрению и проблемы

1. После установки системы ее не стоит включать сразу в боевом режиме
2. Стоит запустить детектирование угроз локальной сети на отдельной группе устройств
3. Возможны ошибочные срабатывания правил
4. Добавлять белые списки возможно в исключениях правил mikrotik firewall или в suricata rules
5. Обязательно делайте белые списки – ip адреса gateway, адреса различных поставщиков услуг и тд
6. Система не должна ломать работы чего либо в сети – если это не так, то отключаем блокировки и разбираемся в чем дело
7. Периодически стоит проверять работу системы



БЕСПЛАТНЫЙ ВЕБИНАР

НАСТРОЙКА SURICATA + MIKROTIK

3

октября
в 11:00

СРЕДА



СПАСИБО ЗА ВНИМАНИЕ

Приходите на наши курсы по
Mikrotik и Asterisk

*Mikro***Tik**

