Сигналтек

LEO

Сетевой фильтр 10 GbE

Многофункциональный сетевой фильтр LEO — аппаратно-программный комплекс мониторинга и фильтрации IP-трафика в соответствии с заданными правилами в режиме реального времени без потерь.

LEO предназначен для решения двух основных типов задач:

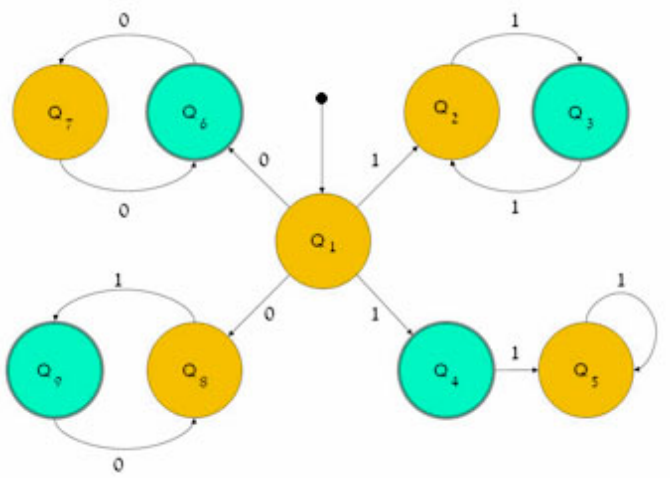
1. Предварительный анализа трафика в сети — определения приоритетных типов трафика, географии используемых ресурсов, нагрузки среднесуточной и в ЧНН.
2. Фильтрация трафика по заданным критериям в режиме реального времени.

Для правильной работы LEO должен в полном объёме получать пакеты, содержащие контентный трафик и служебные управляющие сообщения.

Форм-фактор 1U или 2U в зависимости от решаемых задач.

До восьми 10 GbE портов, каждый из которых может независимо работать на приём (RX) и передачу (TX).

Критерии для правил (matching)



- MAC-адрес
- Порт, диапазон портов
- IP-адрес, IP-IP, подсети (IP + Mask)
- Логин на сервере авторизации
- Тип приложения
- Геолокация
- Регулярные выражения
- Сигнатура

Классификатор приложений

Встроенный классификатор на 180 типов приложений, в том числе:

- почта (pop3, map, smtp, gmail),
- мессенджеры (Oscar, WathsApp, Skype),
- игровые сервисы (WoW, Xbox, Steam, Battlefield и т. д.),
- аудио-, видеопотоки (avi, mpeg, YouTube, RuTube, Quicktime, Realmedia и т. д.),
- шифрованные протоколы (SSL, HTTPS, различные vpn),
- СУБД (Oracle, MySql, PostgreSQL).

  чные виды vpn и т. д.),
- социальные сети.

При необходимости, классификатор может быть доработан под специфические требования заказчика.

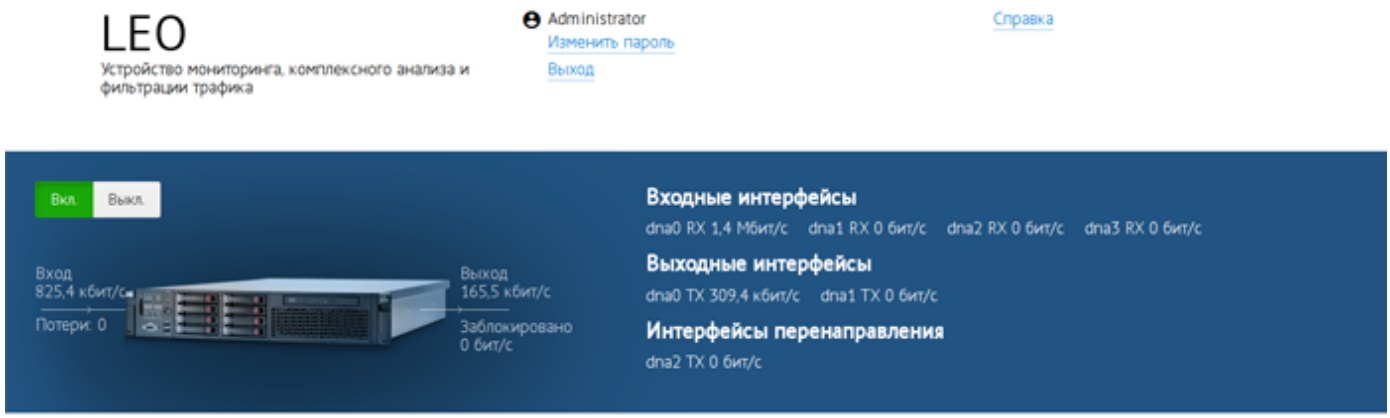
Классификатор стран

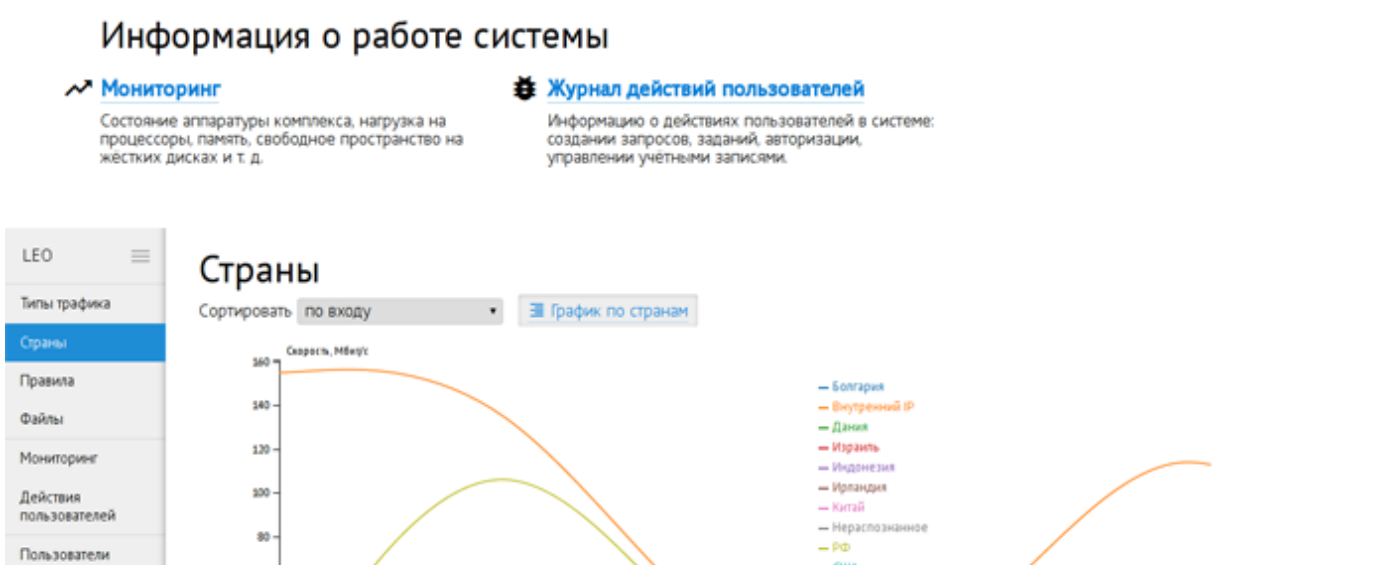
Встроенный классификатор стран на основе базы данных геолокации. Классификация входящего и исходящего трафика на страну. Накопление статистики по странам.

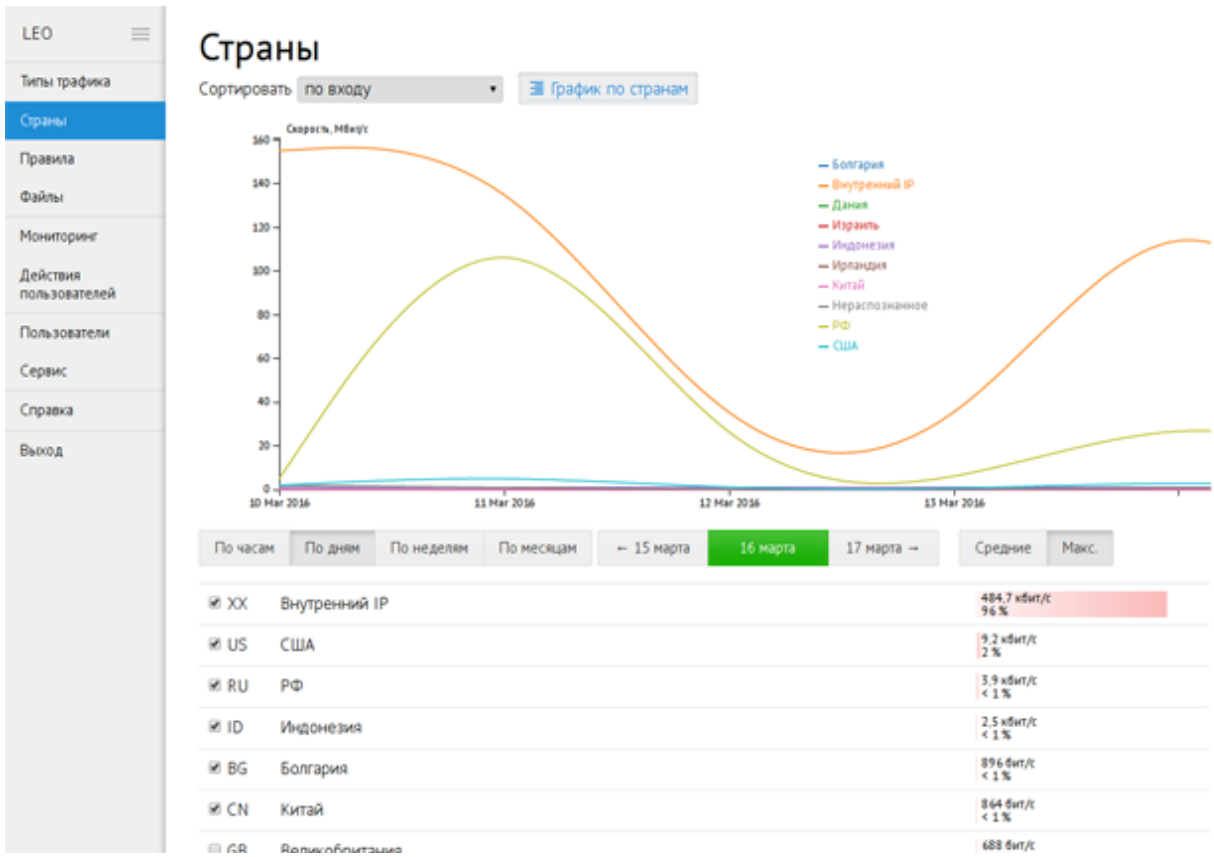
Действия

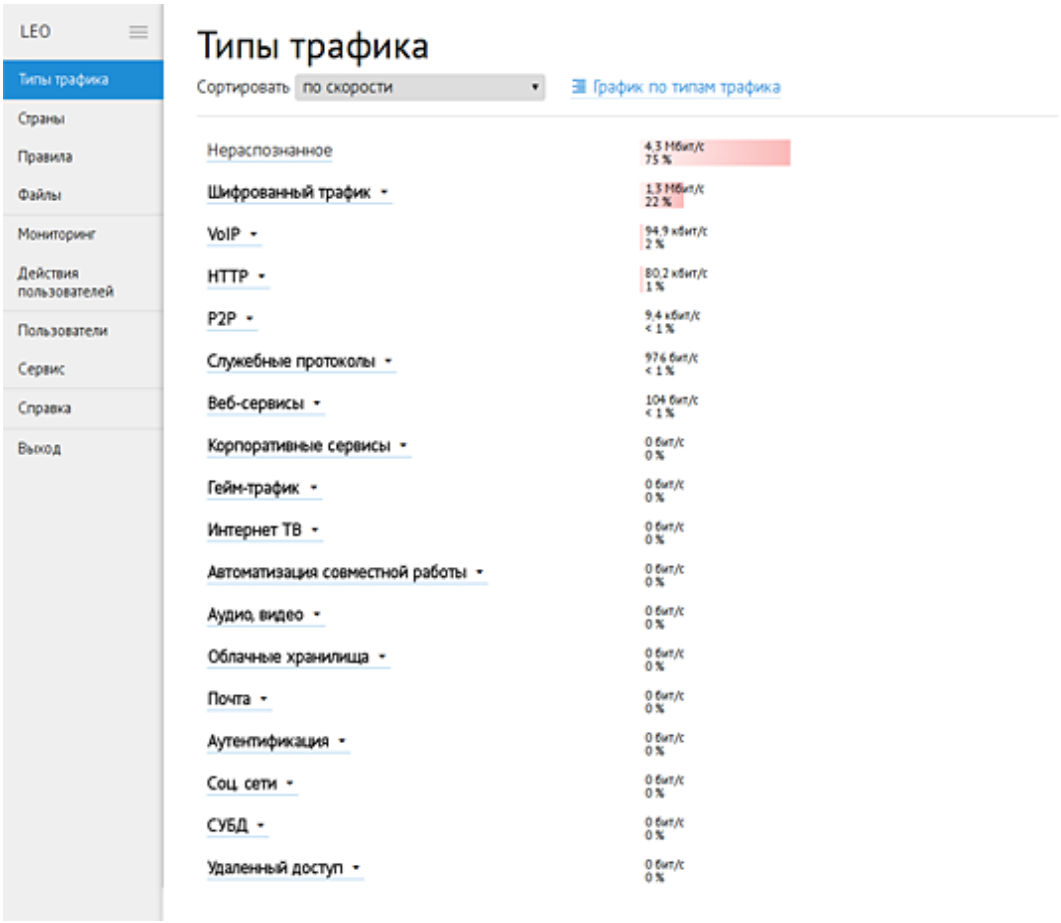
- **Блокировка** используется при установке LEO «в разрыв» для фильтрации из выходного потока нежелательных типов трафика.
- **Запись**. При необходимости можно записать определённый вид трафика в файл для анализа с использованием стороннего программного обеспечения. Например, можно открыть запись в Wireshark.
- **Перенаправление трафика**. Можно выделить из основного потока часть трафика и отправить в свободный сетевой интерфейс, например, для обхода фильтрации или подачи на устройство мониторинга.

Скриншоты


LEO
Устройство мониторинга, комплексного анализа и фильтрации трафика
Administrator
Изменить пароль
Выход
Справка
Вкл.
Выкл.
Вход
825,4 кбит/с
Потери: 0
Выход
165,5 кбит/с
Заблокировано
0 бит/с
Входные интерфейсы
dna0 RX 1,4 Мбит/с
dna1 RX 0 бит/с
dna2 RX 0 бит/с
dna3 RX 0 бит/с
Выходные интерфейсы
dna0 TX 309,4 кбит/с
dna1 TX 0 бит/с
Интерфейсы перенаправления
dna2 TX 0 бит/с
Типы трафика
Распознавание 180 типов трафика. Для каждого типа трафика можно назначить правило.
Страны
Классификация трафика по 240 странам. Для каждой страны можно назначить правило.
Правила
Список правил установленных на устройстве. Добавление правил по IP-адресу, порту, сигнатуре и т. д.
Файлы
Список pcap-файлов записанных в результате срабатывания правил.


Информация о работе системы
Мониторинг
Состояние аппаратуры комплекса, нагрузка на процессоры, память, свободное пространство на жёстких дисках и т. д.
Журнал действий пользователей
Информацию о действиях пользователей в системе: создании запросов, заданий, авторизации, управлении учётными записями.


LEO
Типы трафика
Страны
Правила
Файлы
Мониторинг
Действия пользователей
Пользователи
Сервис
Справка
Выход
Страны
Сортировать
по входу
График по странам
Скорость, Мбит/с
Болгария
Внутренний IP
Дания
Израиль
Индонезия
Ирландия
Китай
Нераспознанное
РФ
США
10 Мар 2016
11 Мар 2016
12 Мар 2016
13 Мар 2016
По часам
По дням
По неделям
По месяцам
← 15 марта
16 марта
17 марта →
Средние
Макс.
XX Внутренний IP 484,7 кбит/с 96 %
US США 9,2 кбит/с 2 %
RU РФ 3,9 кбит/с < 1 %
ID Индонезия 2,5 кбит/с < 1 %
BG Болгария 896 бит/с < 1 %
CN Китай 864 бит/с < 1 %
GB Великобритания 688 бит/с



Мониторинг и статистика

- Мониторинг в реальном времени
- Долговременное накопление и агрегация статистики
- Статистика по типам трафика
- Статистика по странам