



СИСТЕМА АНАЛИЗА СЕТЕВОГО ТРАФИКА

Система анализа сетевого трафика предназначена для сбора данных о прохождении сетевого трафика и анализа пропускной способности сетей передачи данных Ethernet.

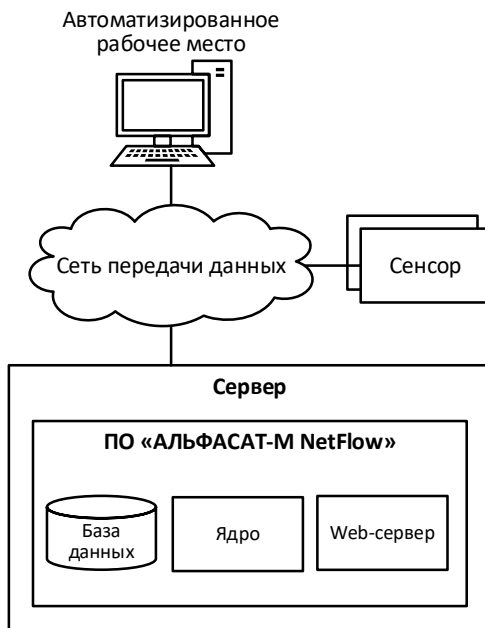
Решаемые задачи:

- Поиск проблемных мест в сети передачи данных;
- Поддержка принятия решений о модернизации сети;
- Анализ эффективности использования сети передачи данных.

Функции:

- Сбор по протоколу NetFlow и хранение статистических данных о сетевом трафике;
- Представление оператору данных в виде графиков и таблиц с возможностью оперативного анализа;
- Обеспечение быстрого поиска, сортировки и отбора данных;
- Формирование отчетов;
- Разграничение доступа пользователей к данным.

Структура системы



- Сенсор – программное средство, обеспечивающее сбор статистических данных о проходящем через оборудование сети передаче данных сетевом трафике (реализуется в составе оборудования сети передачи данных).
- Сервер – аппаратно-программный комплекс с установленным ПО «АЛЬФА САТКОМ NetFlow», обеспечивающий сбор данных о сетевом трафике с сенсоров, сохранение их в базу данных (БД), подготовку отчетной документации.
- Автоматизированное рабочее место – аппаратно-программный комплекс, обеспечивающий управление процессом анализа сетевого трафика.

Сервер функционирует под управлением свободно распространяемых операционных систем семейства Linux (Astra Linux, Ubuntu Server, CentOS) и системы управления базами данных (PostgreSQL).

Взаимодействие пользователя с системой осуществляется через Web-интерфейс.

Технические характеристики

Перечень данных, собираемых о трафике:

- IP-адрес источника;
- IP-адрес назначения;
- Порт источника для UDP и TCP;
- Порт назначения для UDP и TCP;
- Тип и код сообщения для ICMP;
- Номер интернет-протокола транспортного уровня, инкапсулированного в протокол IP;
- Входящий и исходящий сетевой интерфейс;
- Время начала и конца потока;
- Количество байт и пакетов в потоке.

Общество с ограниченной ответственностью «АЛЬФА САТКОМ СИСТЕМС»

105005, Россия, г. Москва, Аптекарский пер. д.4, стр.1

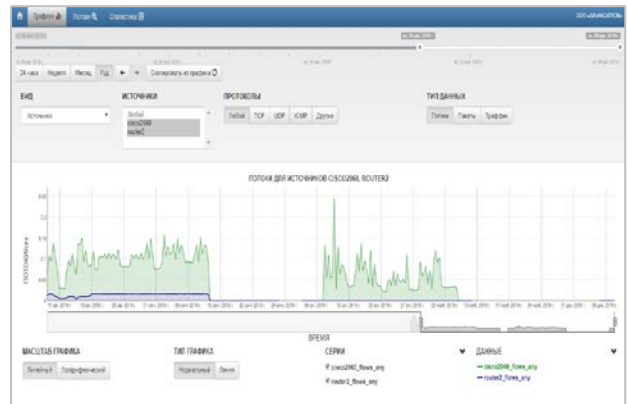
Tel.: +7(495) 729 4322; E-Mail: info@alfasatcom.ru



Пользовательский интерфейс

Графики потоков

Графики содержат агрегированные данные о сетевом трафике, сгруппированные по виду (устройства, протоколы, порты), сетевому оборудованию (устройствам, поддерживающим протокол NetFlow), протоколам (TCP, UDP, ICMP и др.) и типу данных (поток, пакеты, трафик).



Начальное время - окончание	Квантовое время - результат измерения	Предопределенность	Адрес источника	Адрес назначения	Порт источника	Протокол	Всего байтов	Входящие байты	Исходящие байты	Исходящие байты
2019-05-16 07:23	2019-05-06 07:29:48	4224792.761	1.187.0.0	82.0.2.1	0	TCP	120718420	2232126344	0	0
2019-05-05 07:08:45	2019-05-06 07:29:48	0.114	19.8.228.250	20.208.0.0	24	TCP	163772878	139608	0	0
2019-05-16 06:10	2019-05-06 07:29:48	4224792.881	26.229.0.0	8.8.8.0	0	TCP	179629636	161772878	0	0
2019-05-05 07:08:45	2019-05-06 07:29:48	0.420	6.9.1.187	222.180.0.0	0	TCP	120718420	139612	0	0
2019-05-05 07:08:45	2019-05-06 07:29:48	129.076	0.0.0.0	8.8.8.24	0	ICMP	1619424	4078412	0	0
2019-05-16 14:08:18	2019-05-06 07:29:48	4732791.287	0.0.0.0	8.24.16.0	197	TCP	205273620	179629636	0	0
2019-05-17 12:44:42	2019-05-06 07:29:48	4732792.550	2.11.0.24	27.1.0.0	43499	TCP	179629636	179629636	0	0
2019-05-05 07:08:45	2019-05-06 11:12:30	7471.181	208.186.20.236	8.8.8.8	4366	TCP	16784512	2546	0	0
2019-05-05 07:08:45	2019-05-06 11:24:43	87236.564	36.216.105.236	8.8.202.57	189	UDP	362347	217	0	0

Статистика

Позволяет просматривать суммарную статистику по трафику, проходящему через контролируемое сетевое оборудование (IP-адрес источника, IP-адрес назначения, наименование протокола, порт назначения, количество байт в потоке) за выбранный период времени.

Потоки

Позволяет просматривать в табличном виде информацию о потоках IP-трафика, проходящих через настроенные интерфейсы контролируемого сетевого оборудования (время начала и окончания передачи потока, продолжительность передачи потока, IP-адрес источника, IP-адрес назначения, порт источника, порт назначения, протокол передачи, число пакетов, количество байт на входящем и исходящем интерфейсах).

Адрес источника	Адрес назначения	Протокол	Порт назначения	Всего байт
192.168.0.0	16.9.0.200	UDP	8000	1070284164700
192.168.0.0	16.9.0.200	UDP	8000	1070284164700
192.168.1.2	16.9.0.200	TCP	8000	4056413170341
192.16.45	16.9.0.200	UDP	8000	502011874156
192.16.45	16.9.0.200	TCP	8000	2228160180910
192.168.0.0	16.9.0.248	UDP	5480	57272110810
192.16.249	192.168.0.0	ICMP	0	16784512120
192.168.0.0	16.9.0.248	UDP	0	16784512120
192.16.249	192.168.0.0	ICMP	55540	16784512120
192.168.0.0	16.9.0.200	UDP	8000	16784512120