neutrino | foresight

Neutrino Foresight

Руководство Администратора

Июнь 2024

Содержание

Введение

Neutrino Foresight представляет собой передовое решение в области мониторинга и анализа сетевых взаимодействий на базе протокола Netflow, основная задача которой повысить общую эффективность бизнес сервисов, работы сети, снизить издержки на ее поддержку и решение инцидентов.

В отличие от других, Neutrino Foresight используя анализ потока данных тщательно регистрирует, обрабатывает и анализирует обширный набор параметров NetFlow, дополненный обогащением SNMP, геолокационными данными и информацией о пользователях.

В основе функциональности Foresight лежит современный и удобный интерфейс, гармонично сочетающийся с его сложными внутренними механизмами. При поддержке нашего собственного языка запросов в сети (FQL), Foresight выходит за пределы обычных ограничений, представляя собой универсальный и отлично настраиваемый инструмент, созданный для удовлетворения разнообразных требований к управлению вашей сетью и контроля работы бизнес-сервисов. В мире, где ключевую роль играют точность и гибкость, Foresight выступает в роли маяка, направляя бизнес к беспрецедентным инсайтам и технологической устойчивости.

Ниже приведен список некоторых задач, которые можно решить путем анализа протоколов Netflow, sFlow, IPFIX:

- Определение сбоев в сети: контролируйте тысячи портов в сети, чтобы выявить медленные серверы и сбои в работе сети.
- Мониторинг трафика: статистика по сетевому трафика в режиме реального времени, включая использование пропускной способности, протоколов, приложений и соединений.
- Планирование сети: исторические тенденции и тренды использования трафика можно использовать для определения пропускной способности сети.
- Обнаружения вторжений: распознавайте сетевые атаки и аномалии в сети
- Профилирование маршрута: можно определить скорость потока для каждого маршрута.
- Учет трафика: предоставление подробной статистики о приложениях, используемых в сети.

Архитектура

Neutrino Foresight представляет комплексную систему мониторинга, обогащающую данные NetFlow для более глубокого анализа и понимания сетевой активности, а также обеспечивающую расширенные возможности идентификации и контроля ресурсов в сети. Архитектура этого продукта привносит передовые технологии, обеспечивая эффективный сбор, хранение, анализ и представление данных сетевого трафика.

Ключевые Компоненты Системы:

1. **Модули Сбора Данных и обогащения:**
    - Поддержка NetFlow, sFlow, IPFIX.
    - SNMP-опрос сетевых устройств.
    - Интеграция DNS для разрешения имен.
    - Добавление геолокационных данных.
    - Идентификация хостов.
2. **Долгосрочное Хранение (база данных):**
    - Система предоставляет механизмы для долгосрочного хранения данных, обеспечивая возможность последующего анализа и выявления трендов.
3. **Выявление аномалий в сети (Anomaly Detection):**
    - Система предоставляет возможности по выявлению различных аномалий в сети.
4. **Управление Через WEB Интерфейс:**
    - Администраторы могут легко управлять настройками через современный WEB интерфейс, обеспечивая удобное управление и мониторинг.

Гибкая Установка:

Система разработана с учетом гибкости установки, что позволяет развертывать компоненты на одном сервере, отдельных серверах или виртуальных машинах. Кроме того, она может быть интегрирована в кластер Kubernetes, обеспечивая масштабируемость и отказоустойчивость.

Поддержка Операционных Систем:

Все компоненты системы могут быть установлены на современные операционные системы Linux таких как Ubuntu, Rocky Linux, CentOS, а также Astra Linux и Red OS. Дополнительно, за исключением базы данных, компоненты могут быть развернуты на операционной системе Windows Server.

Механизмы Обогащения:

Система реализует механизмы обогащения статистики NetFlow. Текущая версия включает следующие интеграции и обогащения:

- DNS Reverse Lookup

- SNMP Polling
- Геостатистика
- Active Directory Polling
- Приложения
- Приложения. App ID из статистики NGFW PaloAlto
- Пользователи User ID из статистики NGFW PaloAlto

Верхнеуровневая Архитектура:

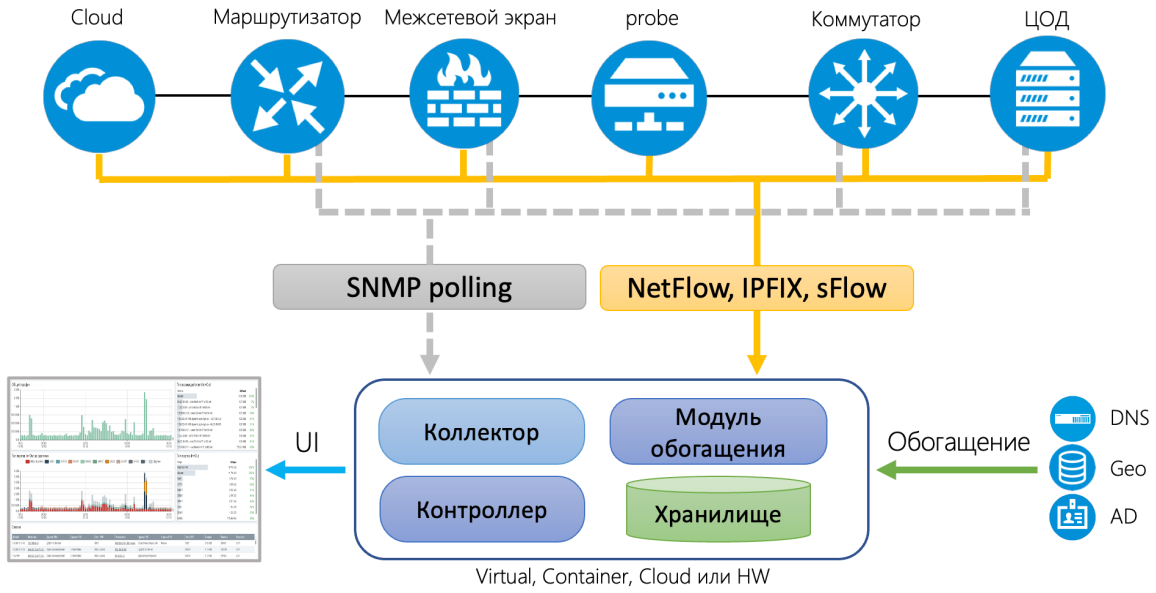
В схеме ниже представлена верхнеуровневая архитектура решения, демонстрирующая взаимодействие ключевых компонентов в системе.

Neutrino Foresight - это не просто инструмент мониторинга, а полноценная платформа, предназначенная для эффективного управления и анализа сетевой активности, обеспечивая беспрецедентный уровень контроля и безопасности.

Для обеспечения работы Neutrino Foresight задействованы следующие модули:

- Коллектор;
- Модуль обогащения;
- Хранилище;
- Контроллер.

Архитектура системы представлена на схеме:



Используемые порты и интеграции

Для корректной работы системы необходимо предусмотреть доступность следующих портов:

- UDP/2055, 6343 – для приема NetFlow, sFlow и IPFIX
- TCP/22, 80, 443, 9092 – для администрирования

Помимо этого, система в процессе своей работы обращается к следующим элементам системы:

- По SNMP обращается к сетевым устройствам для получения справочной информации;
- По LDAP обращается к AD для аутентификации пользователей;
- По DNS обращается к DNS серверам для получения имён хостов.

Требования к вычислительным ресурсам

Спецификация аппаратной платформы, на которой будет устанавливаться система, зависит от необходимой глубины хранения, входящего потока Netflow и уровня производительности. Для помощи с определением спецификации аппаратной платформы обратитесь к технической поддержке Neutrino.

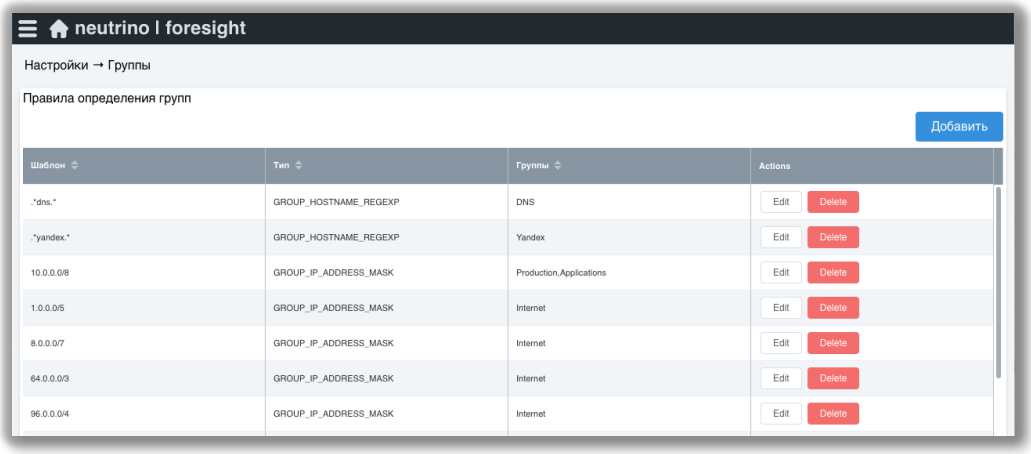
Первоначальная настройка

Первоначальная настройка системы включает три основных шага:

1. Настройка групп
2. Настройка опроса маршрутизаторов, МСЭ и коммутаторов по протоколу SNMP
3. Настройка DNS Reverse Lookup

Группы

В данном разделе рассматривается процесс определения групп для последующего отслеживания, формирования отчетов и Дашбордов. Раздел «Группы» доступен в подменю раздела Меню > Настройки > Группы.



Система поставляется с одной заранее определенной группой: «Internet». Эта группа описывает все публичные подсети и используется на вкладке Обзор для отображения использования ресурсов Интернет в компании.

Группа Other. Все хосты, которые не попали под созданные группы, будут отображаться в группе Other.

Типы Групп. В рамках системы реализовано два основных типа группировки, предоставляющих гибкость выбора в соответствии с потребностями конечного пользователя:

1. **По IP-адресам:**

Этот тип группировки позволяет организовать хосты и подсети на основе их IP-адресов. Пользователь может создавать группы, объединяя устройства с определенными IP-адресами, что облегчает отслеживание и мониторинг в контексте сетевых адресов.
Для группировки хостов по IP адресам используется Тип Группы - GROUP_IP_ADDRESS_MASK

2. **По имени хоста:**

Второй тип группировки базируется на именах хостов, что позволяет пользователям организовывать устройства в группы в соответствии с их именами. Это особенно полезно в случаях, когда удобство идентификации устройств по их именам превалирует над использованием IP-адресов.

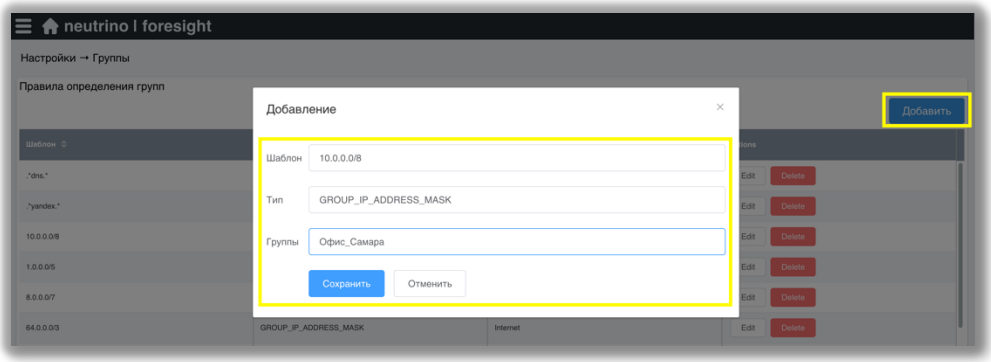
Для группировки хостов по их именам используется Тип Группы - GROUP_HOSTNAME_REGEXP

Добавлять и создавать новые группы необходимо на основе общих характеристик хоста, таких как его функция, принадлежность к внутренней или внешней сети или физическое местоположение. Хосты, выполняющие одну и ту же функцию, или хосты, находящиеся в одном и том же месте, могут быть удобно отслежены в виде графиков и таблиц.

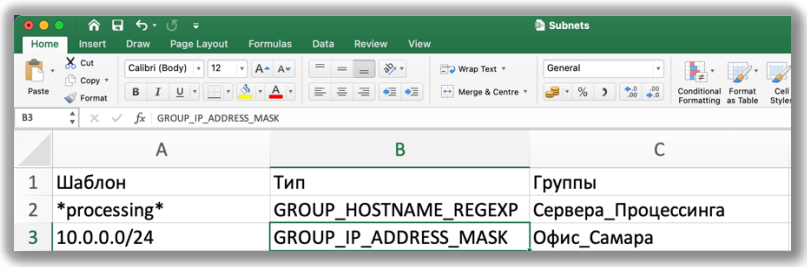
В целях эффективного мониторинга в различных сценариях возможно включение одного и того же хоста, подсети или имени хоста в несколько различных групп.
Например, хост может быть в группе «Приложения» и в группе «База_Данных».

Создание группы
Вы можете воспользоваться любым из следующих подходов для создания группы хостов:

- Ручное создание группы. Вы можете задавать вручную атрибуты хостов - Шаблон, Тип (По IP адресам или по имени хоста) и Название Группы, которые определяют группу.



- Импорт файла в систему. Вы можете определить список групп в файле, а затем импортировать файл в систему. Структура файла должна иметь следующий формат и должна быть подготовлена в виде csv файла:



Изменение и удаление групп
Для изменения атрибутов группы - Шаблон, Тип и Название Группы - необходимо нажать Edit напротив выбранной группы.
Для удаления группы необходимо нажать Delete.

SNMP

Для удобства работы со статистикой, система обогащает данные NetFlow статистикой получаемой по протоколу SNMP. Выполняется SNMP polling сетевых устройств.
Система Neutrino Foresight выполняет SNMP Polling для двух задач:

1) опрос маршрутизаторов, МСЭ и других сетевых устройств по протоколу SNMP Version 2c и 3 для обогащения данных по интерфейсам, с которых система получает Netflow.

При SNMP polling система опрашивается сетевое устройство по следующим атрибутам:

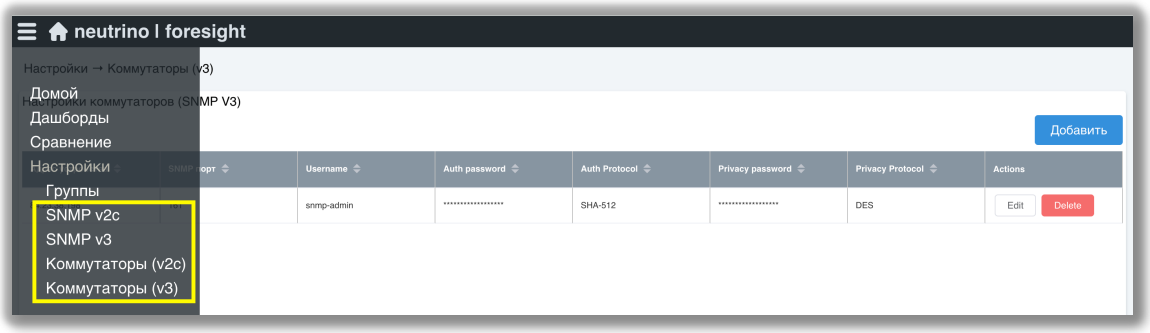
- Device Name – имя сетевого устройства
- Description (ifAlias) – описание интерфейса ifAlias
- Description (ifDescr) – описание интерфейса ifDescr
- MAC Address – MAC адрес интерфейса
- Type – Тип интерфейса
- Inbound/Outbound Speed – Входящая и Исходящие скорости на интерфейсе
- MTU – Maximum transmission unit на интерфейсе.

2) Опрос коммутаторов для определение сетевого интерфейса, к которому подключен хост. Полученные данные отображаются в отчетах по хосту. Выполняется опрос ARP таблицы коммутатора и имя коммутатора. Данный опрос необходим для более быстрого траблшутинга проблем, когда есть задача определить к какому коммутатору и порту коммутатора физически подключен хост, который генерирует аномальный трафик.

Дополнительно к этому за счет использования встроенных возможностей Операционной Системы, на которой установлена система Neutrino Foresight, возможна отправка SNMP traps в случае возникновения проблем, например, увеличением CPU, потребления RAM и других параметров работы сервера. Настройка SNMP Traps зависит от выбранной Операционной Системы и в данной документации не рассматриваются.

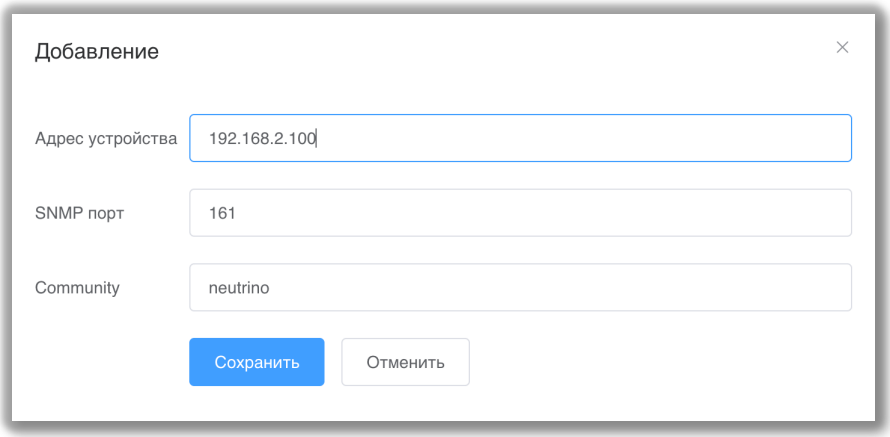
Настройка SNMP

Для настройки SNMP polling необходимо зайти в основное Меню и выбрать соответствующий раздел.
Для опроса маршрутизаторов, МСЭ и других сетевых устройств необходимо выбрать раздел SNMP и необходимую версию SNMP v2c или v3. Для опроса коммутаторов необходимо выбрать раздел Коммутаторы и необходимую версию SNMP v2c или v3, как показано на скриншоте ниже.



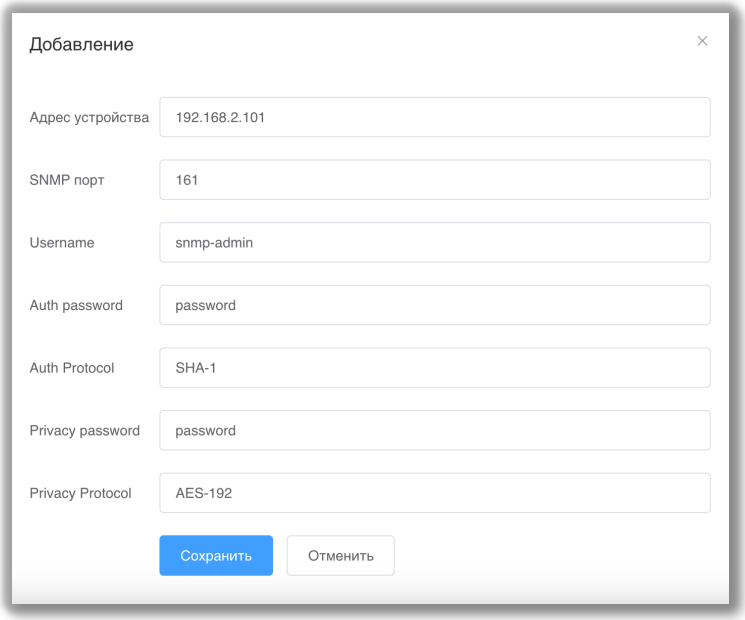
SNMP v2c

Для настройки SNMP v2c необходимо указать IP адрес устройства, SNMP порт и Community.



SNMPv3

Для настройки SNMP v3 необходимо указать IP адрес устройства, SNMP порт, Username, Auth password, Auth protocol, Privacy password и Privacy protocol, как показано на скриншоте ниже.



Поддерживаемые Authentication Protocols:

- SHA-1
- MD5
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Поддерживаемые Privacy Protocols:

- AES-128
- AES-192
- AES-256
- DES
- 3DES
- AES-192_3DES (AES-192 с 3DES расширением)
- AES-256_3DES (AES-192 с 3DES расширением)

DNS. Reverse lookup

Для удобства работы со статистикой, система обогащает данные NetFlow доменными именами хостов. Для этого выполняется обратный просмотр DNS (*reverse DNS lookup*), что позволяет определить имя узла по его IP-адресу с помощью PTR-записи.
Для успешной работы данного типа обогащения необходима PTR записи или. Pointer для хостов в настройках DNS сервера – указатель, служат как обратное отображения IP-адресов в именах хостов.
IP адреса DNS серверов для задачи reverse DNS lookup необходимо указать в конфигурационном файле. Путь файлу конфигурации DNS <путь до микросервиса обогащения>/application-prod.yml

```
netflow:
 analyzer:
  enricher:
   enrichers:
    hostname:
     dns:
      rps: 100
     resolver:
      type: dnsJava
      dns-servers-address: 8.8.8.8,8.8.4.4
```

Обогащение доменными именами хостов происходит в тот момент, когда Neutrino Foresight принимает записи Netflow. По умолчанию выполняется не более 100 запросов в секунду – параметр **rps**, что позволяет исключить перегрузку локального DNS сервера. При необходимости, количество запросов к DNS серверу может быть увеличено. Увеличение обращений необходимо в том случае, если у администратора системы есть задача всегда работать с доменными именами.

Пользовательский интерфейс

В рамках разработки пользовательского интерфейса уделяется особое внимание применению передовых методик и лучших практик по взаимодействию пользователя с системой Neutrino Foresight. Структура интерфейса пользователя делится на два ключевых раздела:

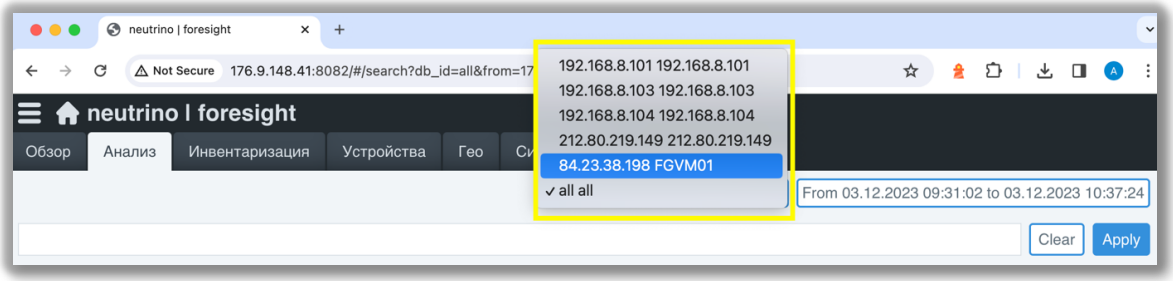
1. Раздел Настроек и Управления: Переход в этот раздел осуществляется путем нажатия кнопки "Меню". В данном разделе пользователь имеет возможность проводить настройку и управление параметрами системы.
2. Раздел Мониторинга и Анализа Статистики: Этот раздел включает в себя несколько вкладок, каждая из которых предоставляет специфичные функции:
    a. Обзор
    b. Анализ
    c. Инвентаризация
    d. Устройства
    e. Гео
    f. Система

    Ниже приведено подробное описание каждой вкладки.

Элементы навигации:
В системе предусмотрены два ключевых элемента навигации, применимых во всех разделах, где отображается статистика:

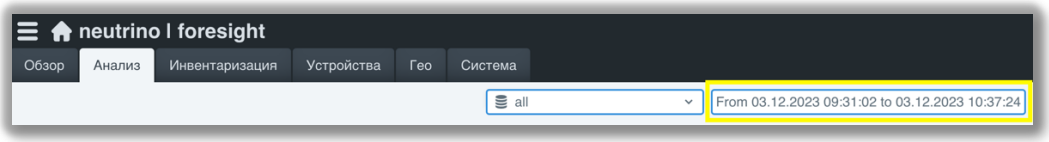
- **Выбор источника статистики NetFlow:**

Для облегчения навигации в системе реализована возможность выбора источника статистики NetFlow из выпадающего списка.

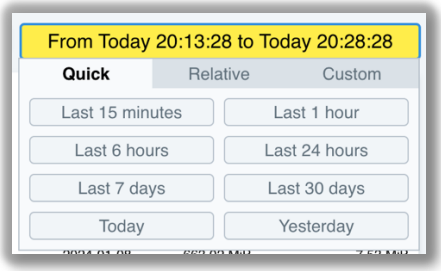


- **Выбор временного интервала:**

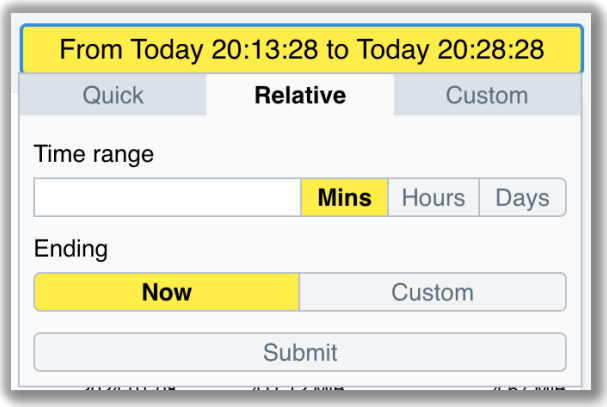
Для удобства пользователей доступен выбор различных временных интервалов для отчетов.



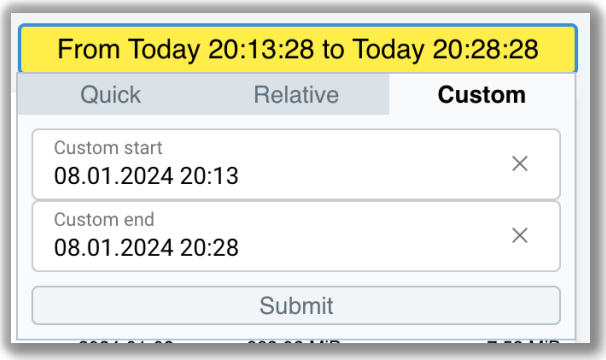
Быстрый выбор времени: последние 15 минут, 1 час, 6 часов, 24 часа, 7 дней, 30 дней, сегодня и вчера.



Выбор относительного времени.

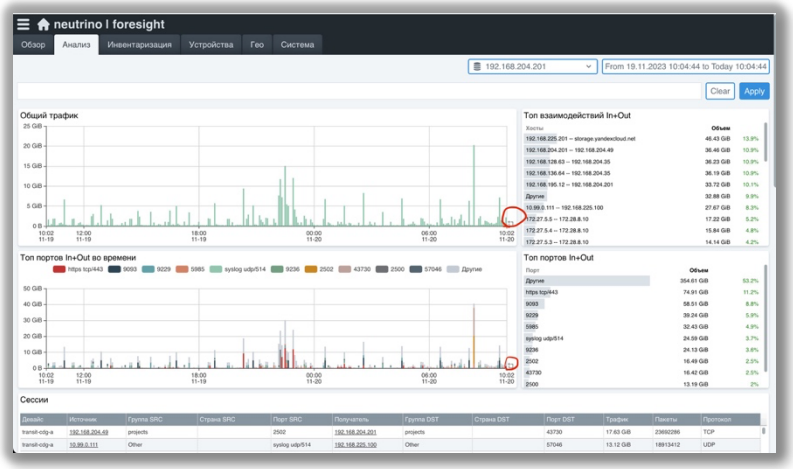


Выбор произвольного временного интервала для создания индивидуальных отчетов с учетом специфических задач, параметров и временных рамок.



- **Механизм Zoom-In:**

В отчетах системы внедрен механизм zoom-in, который позволяет выделять область на графике и автоматически пересчитывать статистику за выделенный временной интервал. Для использования этого механизма необходимо нажать на соответствующую иконку в правом нижнем углу графика, затем, удерживая левую кнопку мыши, выделить желаемую область на графике и отпустить кнопку мыши. Эта функция доступна на графиках в разделах: Анализ, Хост, Порт, Интерфейс.



- **Drill Down переходы**

В системе реализованы сценарии переходов Drill Down между отчетами, которые позволяют пользователям более детально исследовать статистику на различных уровнях: Интерфейс, Порт, Хост и Гео статистика.

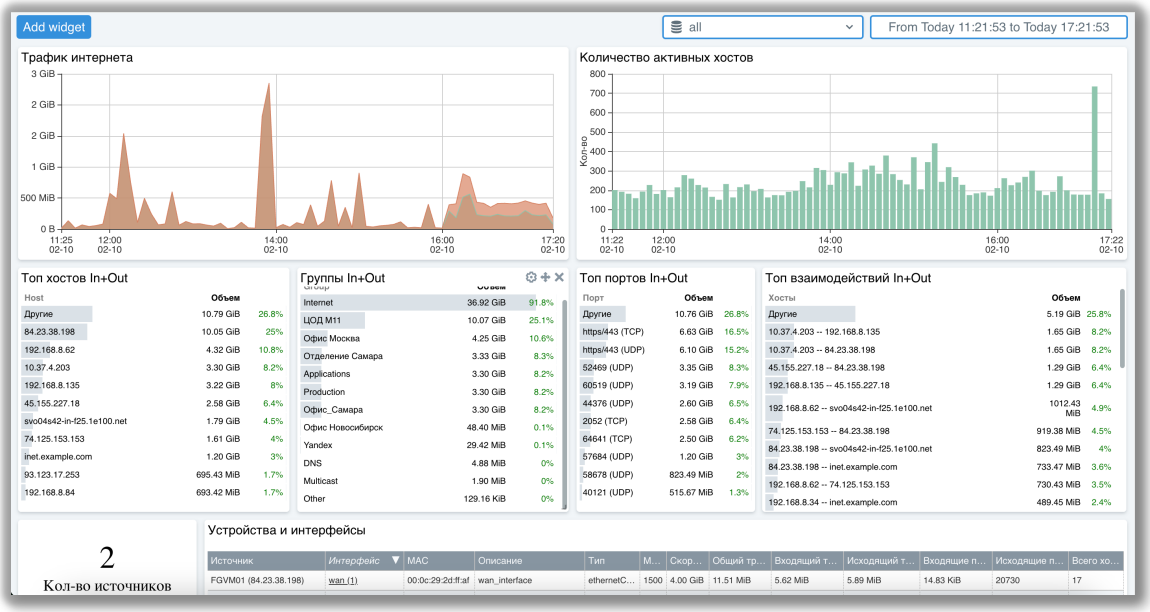
1. **Интерфейс**: При просмотре общей статистики по сетевым интерфейсам, пользователь может использовать функцию Drill Down, чтобы получить подробную информацию о конкретном интерфейсе. Это включает в себя данные об использовании полосы пропускания, ошибки и другие связанные параметры.
2. **Порт**: Механизм Drill Down также распространяется на уровень портов, где пользователь может более детально изучить статистику сетевых портов. Это может включать в себя данные о трафике, соединениях, аномалиях и других характеристиках конкретного порта.
3. **Хост**: Для анализа активности конкретных хостов в сети, механизм Drill Down позволяет перейти к детальной статистике по каждому хосту. Это включает в себя информацию о группах, в которые входит хост, передаче данных, запросах и других параметрах, связанных с конкретным хостом.
4. **Гео-статистика**: Механизм Drill Down раскрывает географическую статистику, позволяя пользователям изучать происхождение трафика и активность на глобальном уровне. Это включает в себя информацию о странах, регионах и других географических аспектах сетевой активности.

Для выполнения перехода Drill Down следует выполнить нажатие на объект интереса, что в свою очередь вызовет открытие новой вкладки с соответствующим отчетом. В процессе перехода Drill Down пользователь непрерывно сохраняет связь с контекстом предыдущего отчета. Например, при генерации отчета по интерфейсу "Wan" пользователь может осуществить переход на порт 443, что приведет к автоматическому открытию новой вкладки с отчетом по данному порту в контексте интерфейса "Wan".

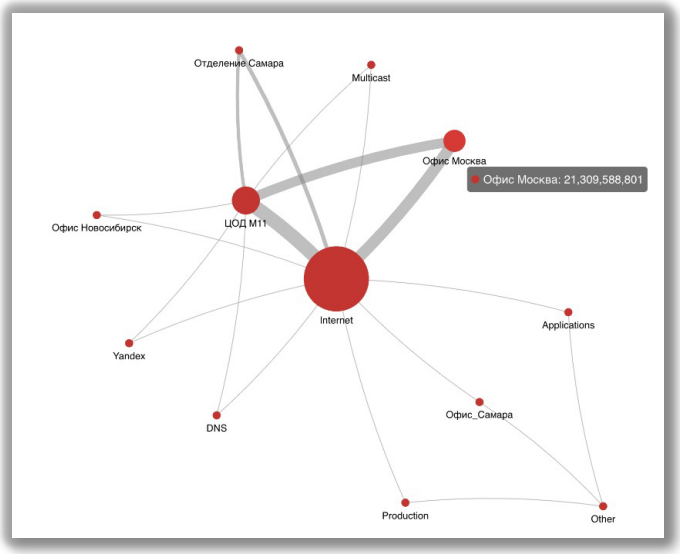
Этот гибкий механизм Drill Down предоставляет пользователям возможность глубже исследовать данные в различных контекстах, что обеспечивает более точное и всестороннее понимание состояния сети.

Обзор

Раздел "Обзор" – это первоначальная страница пользовательского интерфейса, предоставляет комплексную информацию о текущем состоянии сетевого трафика при подключении к системе мониторинга. На данной вкладке предоставляется доступ к ключевым параметрам, таким как объем потребляемого интернет-трафика, количество активных хостов в сети, а также статистика ТОП-хостов, ТОП-групп, ТОП-транспортных портов и ТОП-взаимодействий. Дополнительно предоставляется информация о количестве экспортеров и сетевых интерфейсах, что обеспечивает общее представление о текущем состоянии сети.



В нижней части раздела "Обзор" находится схема/карта взаимодействий между группами хостов. На данной схеме отображается взаимодействия между группами за выбранный интервал времени и по выбранному экспортеру. На схеме размер отображаемой группы и связи между группами зависит от объема передаваемого трафика в обоих направлениях.

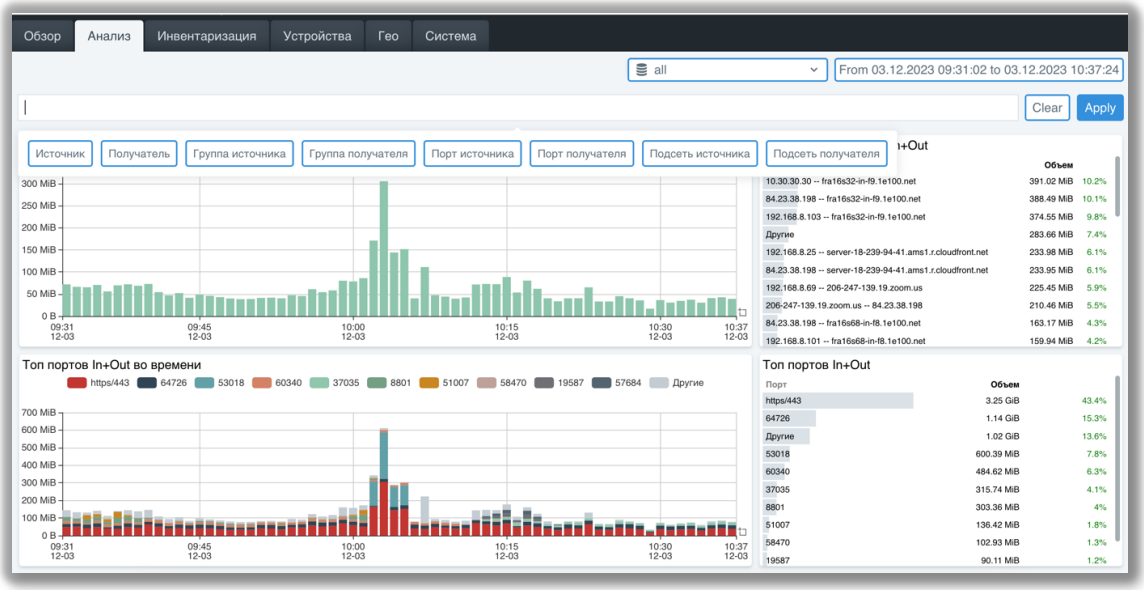


При выявлении аномального трафика пользователь может воспользоваться функционалом "Drill Down", осуществляя переход к детализированной статистике по конкретному хосту, порту, группе или сетевому интерфейсу. Этот функционал предоставляет возможность провести более глубокий анализ возможных аномалий и принять соответствующие меры для их решения. Данный инструментарий позволяет оперативно реагировать на потенциальные угрозы или нештатные ситуации, повышая эффективность системы мониторинга.

Анализ

Раздел "Анализ" предназначен для проведения специфических запросов, связанных с детальным анализом сетевого трафика и формирования соответствующих отчетов. Эти запросы позволяют получить статистику для конкретных хостов-отправителей, направлений передачи данных, определенных портов и временных интервалов. Этот раздел основан на использовании языка запросов Foresight Query Language (FQL).

Использование Foresight Query Language (FQL)
FQL предоставляет пользователю возможность формировать сложные запросы, учитывая различные параметры сетевого трафика. Пользователь вводит запросы на языке FQL в "Строке Поиска".
Для облегчения этого процесса при наведении на "Строку Поиска" предоставляются наиболее часто используемые шаблоны запросов, такие как "Источник", "Получатель", "Группа Источника", "Группа Получателя", "Порт Источника", "Подсеть Источника", "Подсеть Получателя". Выбор соответствующей подсказки добавляет соответствующую запись FQL в строку поиска, которую пользователь может редактировать по необходимости.



Использование результатов запросов FQL

Сформированные FQL запросы могут быть использованы для создания виджетов на Дашбордах, предоставляя наглядное представление данных в реальном времени. Кроме того, запросы могут быть использованы на вкладке «Сравнение» для более детального анализа и сравнительного изучения данных.

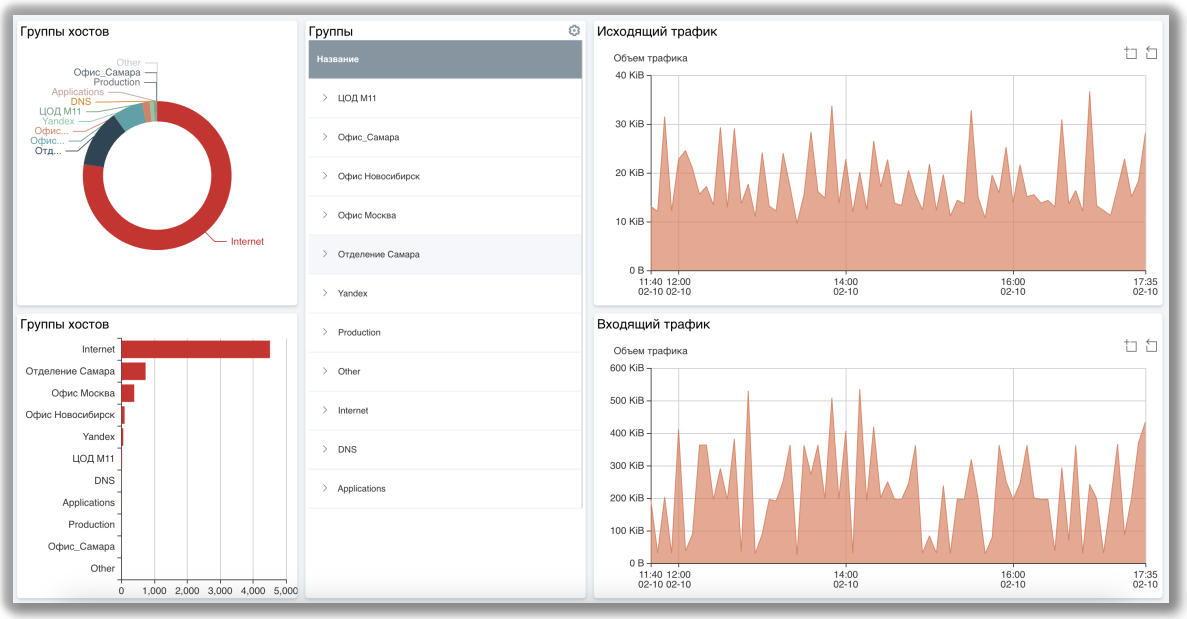
Инвентаризация

Раздел «Инвентаризация» представляет собой центральный источник информации о всех активных хостах в корпоративной сети. Основной целью данного раздела является увеличение эффективности отчетности путем использования группировки хостов и выявления потенциально утерянных, забытых или неизвестных узлов в организации, путем анализа хостов входящих в группу Other.

Группы хостов могут отображать принадлежность к географическому расположению (например, офис, филиал) или функциональному назначению (например, серверы, приложения). Это обеспечивает более наглядное представление об активах и их роли в сетевой инфраструктуре.

Группировка хостов осуществляется на основе заранее заданных параметров IP-подсетей или адресов и доменных имен, которые могут быть указаны в виде регулярных выражений. Создание и настройка групп хостов выполняется в разделе "Группы", доступном в подменю "Меню > Настройки > Группы".

После определения групп хостов и сбора статистики NetFlow система автоматически обновляет данные. Для каждой указанной группы хостов отображается количество активных узлов. Пользователи имеют возможность просмотра списка хостов, входящих в выбранную группу, а также получения общей информации о входящем и исходящем трафике для конкретного хоста в заданный временной интервал.



Для более детального анализа данных предусмотрен механизм Drill Down: двойное нажатие на интересующую группу активирует механизм, который предоставляет подробный отчет о выбранной группе хостов.

Устройства

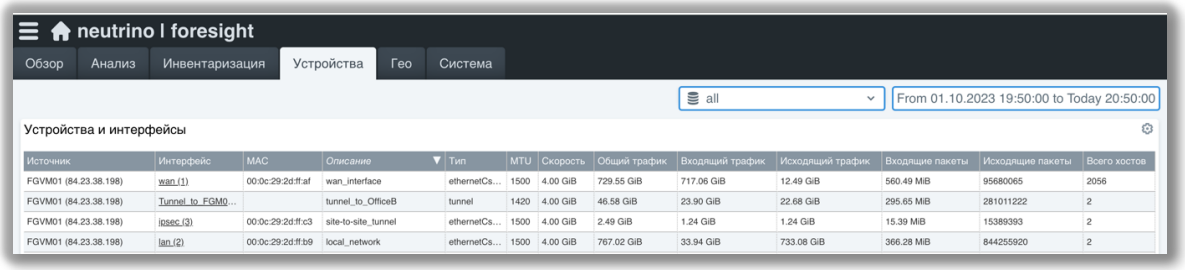
Раздел "Устройства" предоставляет перечень экспортеров и соответствующих сетевых интерфейсов, сопровождаемых SNMP-метриками, такими как:

- Device Name: Имя устройства.
- Description (ifAlias): Описание (ifAlias) интерфейса.
- Description: Описание интерфейса.
- MAC Address: MAC-адрес устройства.
- Type: Тип интерфейса.
- Inbound/Outbound Speed: Скорость входящего/исходящего трафика.
- MTU (Maximum Transmission Unit): Максимальный размер передаваемого пакета.

Статистика по интерфейсам включает следующие параметры, извлекаемые из NetFlow и рассчитываемые для выбранного временного интервала:

- Общий трафик
- Входящий трафик
- Исходящий трафик
- Входящие пакеты
- Исходящие пакеты

По умолчанию страница "Устройства" отображает все сетевые интерфейсы и устройства, на которых настроен экспорт статистики NetFlow. Для просмотра информации по конкретному устройству, необходимо выбрать его из контекстного меню.



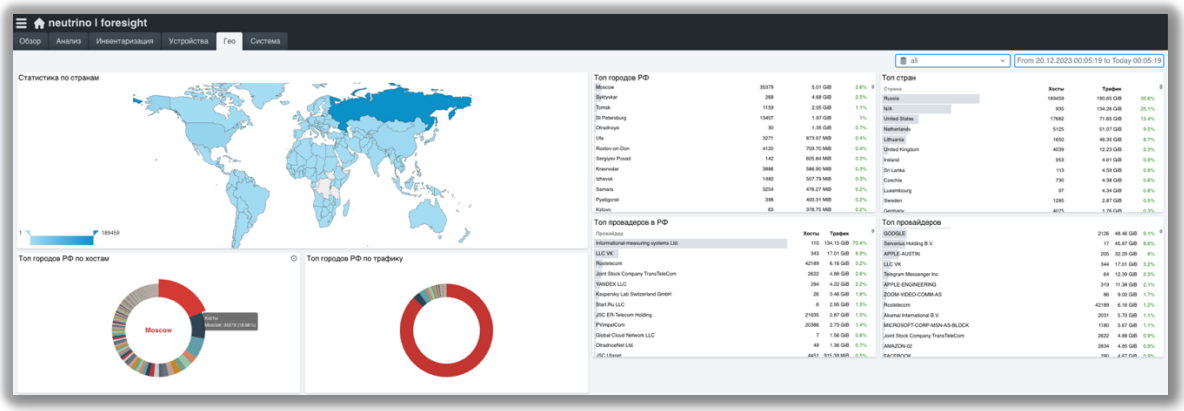
Источник	Интерфейс	MAC	Описание	Тип	MTU	Скорость	Общий трафик	Входящий трафик	Исходящий трафик	Входящие пакеты	Исходящие пакеты	Всего хостов
FGVM01 (84.23.38.198)	wan (1)	00:0c:29:2d:ff:af	wan_interface	ethernetCs…	1500	4.00 GiB	729.55 GiB	717.06 GiB	12.49 GiB	560.49 MiB	95680065	2056
FGVM01 (84.23.38.198)	Tunnel_to_FGM0…		tunnel_to_OfficeB	tunnel	1420	4.00 GiB	46.58 GiB	23.90 GiB	22.68 GiB	295.65 MiB	281011222	2
FGVM01 (84.23.38.198)	ipsec (3)	00:0c:29:2d:ff:c3	site-to-site_tunnel	ethernetCs…	1500	4.00 GiB	2.49 GiB	1.24 GiB	1.24 GiB	15.39 MiB	15389393	2
FGVM01 (84.23.38.198)	lan (2)	00:0c:29:2d:ff:b9	local_network	ethernetCs…	1500	4.00 GiB	767.02 GiB	33.94 GiB	733.08 GiB	366.28 MiB	844255920	2

При клике на интересующий интерфейс срабатывает механизм "Drill Down", который раскрывает подробный отчет по выбранному сетевому интерфейсу, предоставляя более глубокий анализ данных.

Гео

Система Neutrino Foresight обладает функциональностью обогащения собираемой статистики NetFlow данными гео-локации. Реализована возможность предоставления информации о странах, городах Российской Федерации, а также о национальных и международных провайдерах.

Обогащение Гео-данными
На странице "Гео" системы отображается статистика, предоставляющая географический анализ использования информационных ресурсов. В случае использования экспорта NetFlow с сетевых устройств и наличия публичных IP-адресов в статистике, система автоматически обогащает данными гео-локации. Этот процесс охватывает запросы из локальной сети к публичным сервисам в интернете, а также запросы от внешних источников к публичным сервисам компании.



Применение фильтров и Дашборды
Отображаемые виджеты на странице "Гео" могут быть включены в Дашборды системы с возможностью предварительной настройки необходимых фильтров с использованием языка FQL. Это предоставляет пользователям гибкость в анализе данных и создании персонализированных отчетов.

Примеры использования
Страны: Визуализация распределения сетевого трафика по странам позволяет выявить географические особенности активности.

Города Российской Федерации: Анализ сетевых взаимодействий внутри страны для выявления основных центров активности.

Провайдеры Российской Федерации: Идентификация влияния провайдеров на сетевой трафик внутри страны.

Провайдеры международные: Мониторинг взаимодействия с международными провайдерами для оптимизации глобальной сетевой инфраструктуры.

Эти возможности обеспечивают более глубокий и широкий анализ сетевой активности, повышая эффективность мониторинга и обеспечивая более точные данные для принятия управленческих решений.

Система

Раздел "Система" предоставляет обширную информацию о управлении дисковым пространством системы, предназначенным для хранения данных о потоках трафика. В данном разделе также предоставляется статистика использования диска в зависимости от типов данных (для различных механизмов агрегации), а также отслеживается динамика получения сетевых потоков от экспортеров NetFlow.

Вкладка "Система" включает в себя четыре основных раздела:

1. **Распределение дискового пространства:**

Этот раздел определяет, как система использует дисковое пространство для хранения данных о потоках трафика с различным разрешением/агрегацией. В данном контексте отображается объем выделенного дискового пространства для системы и оставшегося пространства. При достижении предела выделенного объема, система автоматически перезаписывает наиболее старые данные.

2. **Статистика хранения по типам данных:**

В данном разделе отображается объем данных, занятый определенными типами данных. Типы данных определяют временные интервалы отчетности, при которых устройство автоматически переключается между различными разрешениями. Например, можно проследить, что один тип данных (детализации/агрегации) за 1 минуту занимает 1 ГБайт. Также предоставляется информация о различных типах тип детализации/агрегации за определенный период времени. Важно отметить, что система предоставляет возможность перераспределения дискового пространства для различных типов тип детализации/агрегации, обеспечивая сохранение информации на более продолжительный период времени.

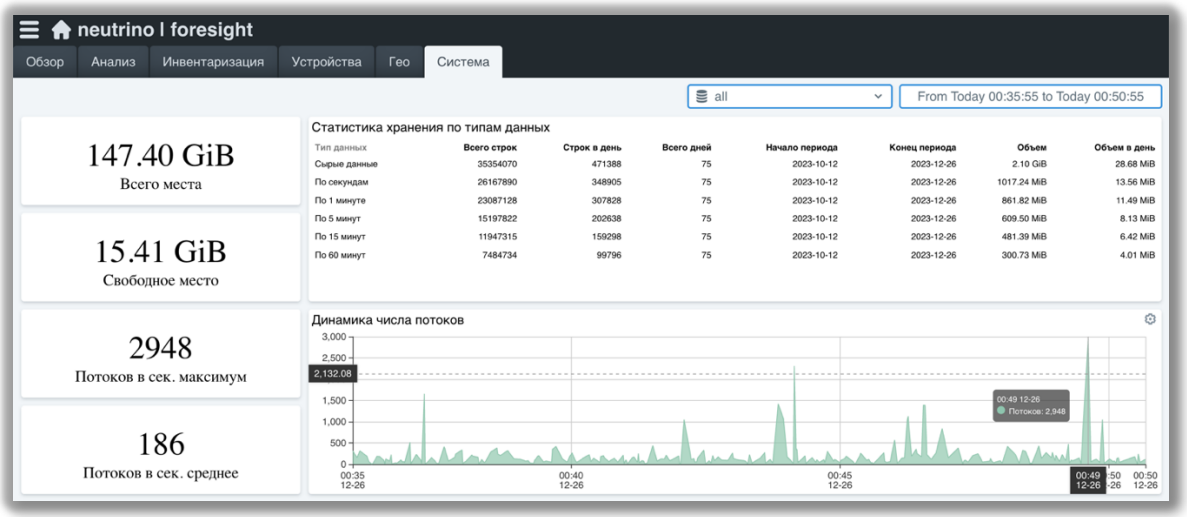
3. **Максимальное и среднее число потоков в секунду:**

Этот раздел предоставляет информацию о лицензировании системы в соответствии с максимальным числом потоков в секунду. Также отображается среднее число потоков в секунду, что может быть полезным для анализа нагрузки и эффективности системы.

4. **Динамика числа потоков:**

Здесь представлен график распределения потоков NetFlow, поступающих в систему от всех источников. Этот график отражает динамику изменения потоков во времени и является важным инструментом для мониторинга и анализа сетевой активности.

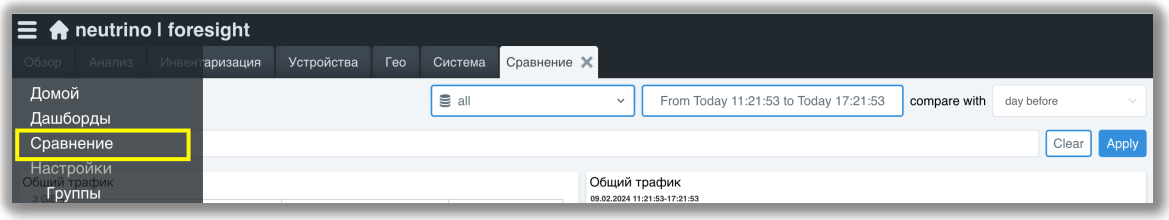
Данные разделы обеспечивают детализированный обзор функциональности системы мониторинга NetFlow, позволяя эффективно управлять и анализировать потоки трафика в сети.



Более детально про механизм агрегации статистики описано в разделе [Агрегация статистики]

Сравнение «До и После»

Neutrino Foresight предоставляет уникальную функциональность в виде механизма сравнения статистики до внесения изменений и после. Этот инструмент направлен на обеспечение эффективного мониторинга и оценки воздействия внесенных изменений на сетевую инфраструктуру. Раздел Сравнение доступен в основном Меню системы.



Процесс сравнения:

1. Выбор временного интервала: Пользователь определяет временной интервал в верхнем меню, включающий период до внесения изменений. Это обеспечивает точность сравнения и дает возможность оценить долгосрочное воздействие изменений.
2. Выбор периода для сравнения: Пользователь выбирает период времени для сравнения, такой как день назад, неделю назад, или определенный пользователем период, начинающийся в определенное время в прошлом. Данные для периода в прошлом отображаются в правом разделе меню.
3. Фильтрация статистики: для создания уникального запроса доступны фильтры с использованием языка FQL, аналогичные вкладке "Анализ".

Отображение статистики:
Система автоматически извлекает статистические данные до и после внесения изменений, включая информацию о потоках, использовании пропускной способности и других ключевых параметрах.

Визуализация результатов:
Полученные данные представляются в удобочитаемой форме через графики, диаграммы и сводные таблицы. Это обеспечивает пользователям легкость сопоставления метрик до и после изменений в сетевой активности.

Преимущества механизма сравнения:

1. Объективная оценка изменений: Возможность сравнивать статистику до и после изменений обеспечивает объективную оценку воздействия изменений на сетевую среду.
2. Сокращение времени анализа: Автоматизированный процесс сравнения значительно сокращает время анализа, что крайне важно в динамичной сетевой среде.
3. Быстрое выявление проблем: Возможность оперативно выявлять неожиданные изменения в сетевой активности после внесения изменений позволяет оперативно реагировать на потенциальные проблемы.

Механизм сравнения статистики до и после изменений в системе мониторинга Netflow является мощным инструментом для поддержки прозрачности и эффективности управления сетевой инфраструктурой.

Foresight Query Language (FQL)

Этот раздел описывает язык запросов FQL - Foresight Query Language, далее FQL. FQL это мощный и гибкий язык запросов к базе данных Neutrino Foresight для решения специфических или узконаправленных задач при работе с системой.
FQL используется в трех раздела системы:

1. Вкладка Анализ
2. Вкладка Сравнение
3. На Дашбордах, для фильтрации статистики Виджетов.

Ниже перечислены основные запросы FQL в системе:

Значение фильтра	Тип фильтра	Пример
date	Дата	
time_received	Дата и время	
sequence_num	Числовое значение	
sampling_rate	Числовое значение	
flow_direction	Числовое значение	
sampler_address	Фиксированное числовое значение	
time_flow_start	Дата и время	
time_flow_end	Дата и время	
bytes	Числовое значение	
packets	Числовое значение	
src_ip	строка или имя	
dst_ip	строка или имя	
etype	Числовое значение	
proto	Числовое значение	proto = 6
src_port	Числовое значение	src_port = 6003
dst_port	Числовое значение	dst_port = 443
in_if	Числовое значение	in_if = 1
out_if	Числовое значение	
src_mac	Числовое значение	
dst_mac	Числовое значение	
src_vlan	Числовое значение	
dst_vlan	Числовое значение	
vlan_id	Числовое значение	vlan_id = 5
ingress_vrf_id	Числовое значение	
egress_vrf_id	Числовое значение	

ip_tos	Числовое значение	ip_tos = 34
ip_ttl	Числовое значение	
tcp_flags	Числовое значение	
icmp_type	Числовое значение	
icmp_code	Числовое значение	
ipv6_flow_label	Числовое значение	
src_as	Числовое значение	
dst_as	Числовое значение	
next_hop	строка или имя	
next_hop_as	Числовое значение	
src_net	Числовое значение	
dst_net	Числовое значение	
bgp_next_hop	строка или имя	
bgp_communities	Числовое значение	
as_path	Числовое значение	
has_mpls	Числовое значение	
mpls_count	Числовое значение	
mpls_1_ttl	Числовое значение	
mpls_1_label	Числовое значение	
mpls_2_ttl	Числовое значение	
mpls_2_label	Числовое значение	
mpls_3_ttl	Числовое значение	
mpls_3_label	Числовое значение	
mpls_last_ttl	Числовое значение	
mpls_last_label	Числовое значение	
mpls_label_ip	строка или имя	
observation_domain_id	Числовое значение	
observation_point_id	Числовое значение	
sampler_host	строка или имя	
dst_host	строка или имя, имя хоста, если мы смоги сделать обратный DNS lookup	
src_host	строка или имя, имя хоста, если мы смоги сделать обратный DNS lookup	
sampler_ip	строка или имя	sampler_ip = '10.200.233.54'
src_ip	строка или имя	
dst_ip	строка или имя	
sampler_name	строка или имя	
dst_name	строка или имя	
src_name	строка или имя	

src_groups	строка или имя	
dst_groups	строка или имя	
src_country	строка или имя	
src_city	строка или имя	
src_asn	Числовое значение	
src_aso	строка или имя	
dst_country	строка или имя	
dst_city	строка или имя	
dst_asn	Числовое значение	
dst_aso	строка или имя	
App ID (для Palo Alto)	TBD	TBD
User ID (для Palo Alto)	TBD	TBD

При FQL запросах возможно использование логических операторов AND, OR, IN, а также применение операторов сравнения = , >, < , in, not, like (неточное соответствие), % (любая последовательность символов).
Пример использования оператора AND:

```
(src_ip = '192.168.89.242') AND (dst_ip = '192.168.205.251')
```

Например, ... IN (..., ..., ...) – вхождение во множество, аналог оператору OR, используется когда стоит задача анализировать трафик сразу по нескольким портам, адресам, группам, странам и тп. Пример:

```
dst_port in (443,80,8080)
dst_city in (Moscow, Samara, Novosibirsk)
```

Примеры использования like (неточное соответствие), при использовании этого оператора нужны кавычки.
Источник трафика – IP или имя хоста

```
src_name like 'ya.ru' или src_name like '192.168.8.69'
```

Получатель трафика – IP или имя хоста

```
dst_name like 'ya.ru' или dst_name like '192.168.8.69'
```

Группа источника или получателя трафика

```
has(src_groups, 'ЦОД М11') или has(dst_groups, 'ЦОД М11')
```

Подсеть Источника

```
isIPAddressInRange(src_ip, '192.168.8.0/24')
```

Подсеть Получателя

```
isIPAddressInRange(dst_ip, ‘10.10.0.0/14’)
```

Пример использования оператора %(любая последовательность символов):
Если указать

```
like Yandex%
```

это будет соответствовать любому значению после Yandex. Например, после Yandex могут быть следующие соответствия: Yandex.ru, Yandex.org.
Оператор % может использоваться в начале, в середине или в конце строки.

Дополнительные примеры:

Отобразить трафик для конкретного хоста в обоих направлениях, проходящих через определенный интерфейс.

```
(dst_name = 'host_name' OR src_name = 'host_name') AND sampler_ip = 'x.x.x.x'
```

Посмотреть данные по взаимодействию двух групп между собой по всем экспортерам

```
(has(src_groups, 'group_name_A') and has(dst_groups, 'group_name_B'))  or
(has(src_groups, 'group_name_B') and has(dst_groups, 'group_name_A'))
```

Посмотреть по двух группам с привязкой к конкретному серверу, на который они обращаются

```
(has(src_groups, 'group_name_A') or has(dst_groups, 'group_name_A')) and (dst_name =
'host_name_A' OR src_name = 'host_name_A')
```

Отобразить статистику по определенным интерфейсам для одного экспортера

```
(sampler_ip = ’x.x.x.x’ AND (in_if = 3 OR out_if = 3))
```

Отобразить статистику по нескольким определенным интерфейсам для одного экспортера. Требуется для анализа статистики, например, для интерфейсов типа LAG.

```
(sampler_ip = ’x.x.x.x’ AND (in_if = 3 OR out_if = 3 OR in_if = 5 OR out_if = 5))
```

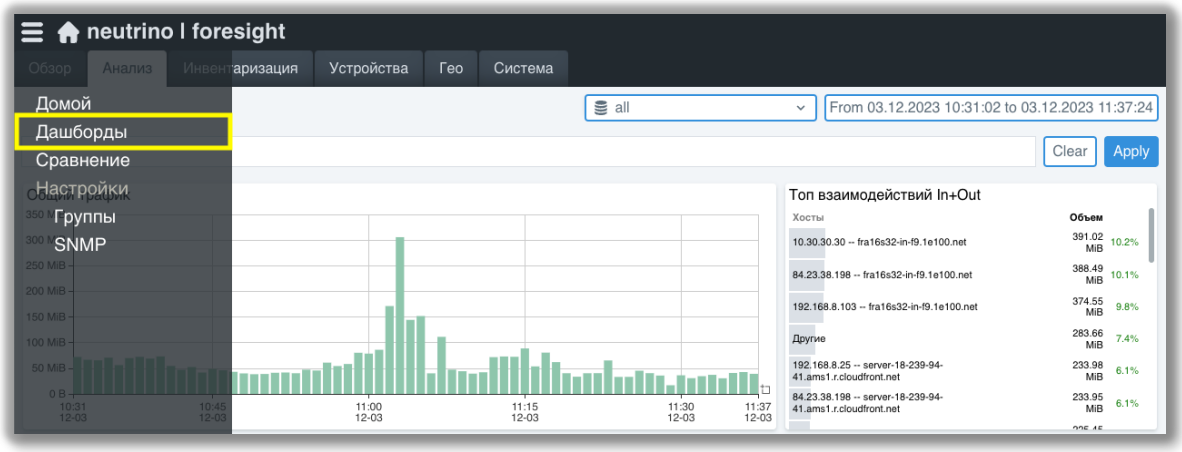
Вернуть фильтр виджета к дефолтному значению

```
1=1
```

Дашборды

Дашборды – это визуальное представление данных, разработанное для быстрого анализа информации о сетевом трафике и повышения информационной осведомленности.
Дашборды состоят из различных Виджетов – объектов с графическим представлением конкретных данных, которые можно добавлять, редактировать, располагать, удалять или изменять по вашему усмотрению.
Дашборды используются для различных задач – анализ работы определенного бизнес-сервиса, загрузка каналов определенных маршрутизаторов и МСЭ.
Neutrino Foresight позволяет пользователям настраивать несколько Дашбордов.

Дашборды созданные пользователем, доступны для использования в Меню.



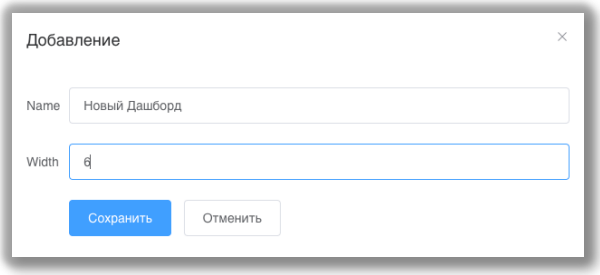
В данном меню представлена таблица со всеми Дашбордами, созданными пользователем в системе.

Создание Дашборда.
Для создание нового Дашборда, необходимо нажать «Добавить»
Далее необходимо указать:

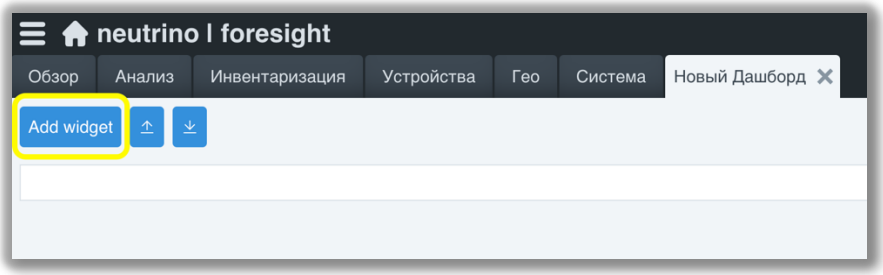
- Наименование Дашборда – Name. Задается уникальное имя Дашборда.
- Ширину Дашборда – Width.

Ширина Дашборда является ключевым параметром, подлежащим настройке с учетом разрешения экрана, на котором осуществляется его отображение. Данная характеристика напрямую влияет на визуальное восприятие и эффективность использования Дашборда. Рекомендуется учитывать разрешение экрана в процессе

определения ширины Дашборда. Для обеспечения оптимального пользовательского опыта и избежания горизонтальной прокрутки рекомендуется установка ширины Дашборда таким образом, чтобы он полностью адаптировался к разрешению экрана.



Далее созданный Дашборд необходимо наполнить Виджетами. Нажимаем кнопку «Add widget»

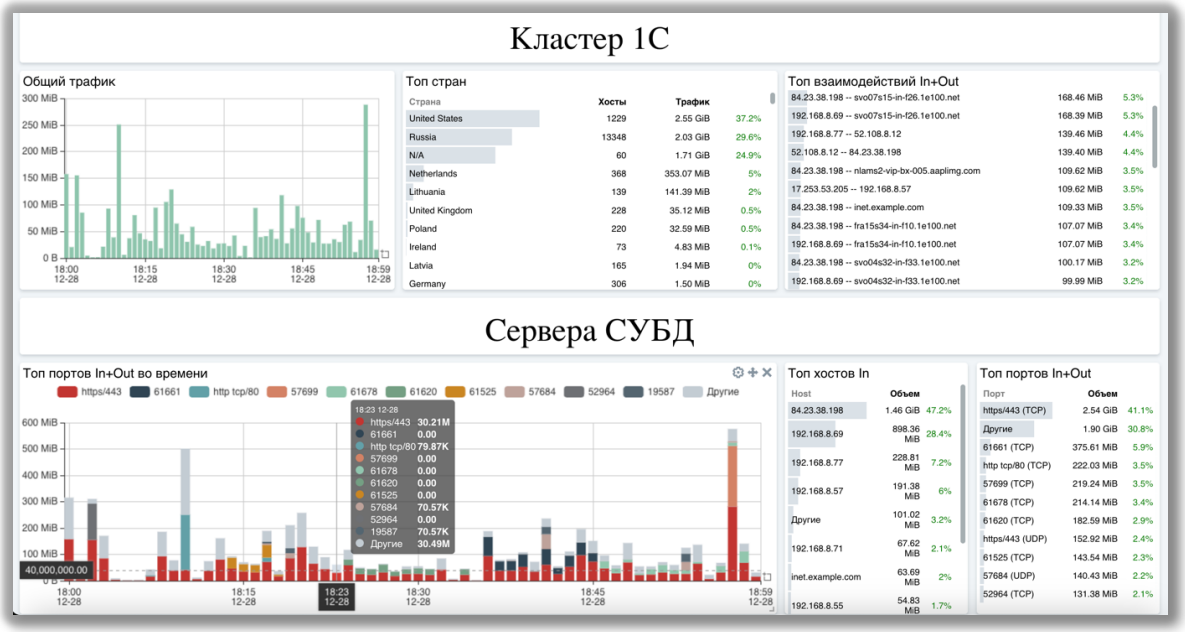


Удаление Дашборда

Для удаления Дашборда необходимо перейти на список Дашбордов, найти необходимый и нажать Delete.

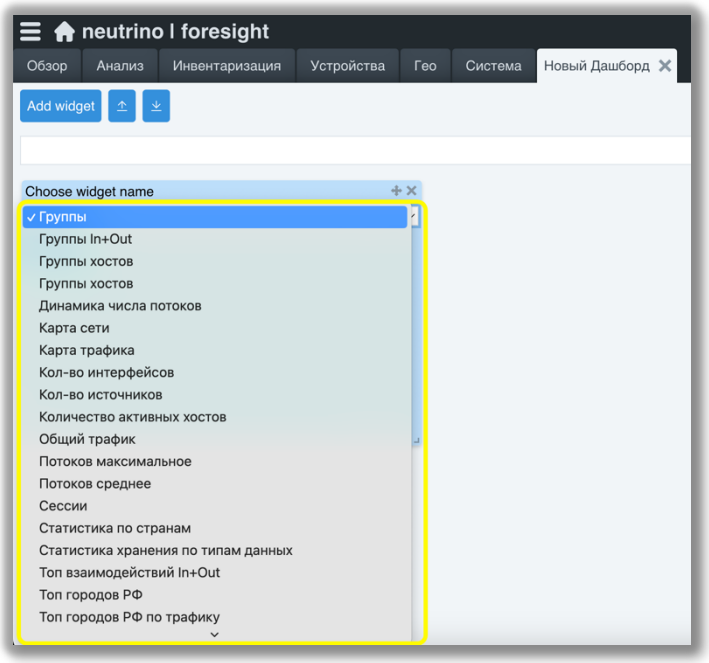
Виджеты

Виджеты – это объекты с графическим представлением конкретных данных, которые можно добавлять, редактировать, размещать, удалять или изменять по своему усмотрению.



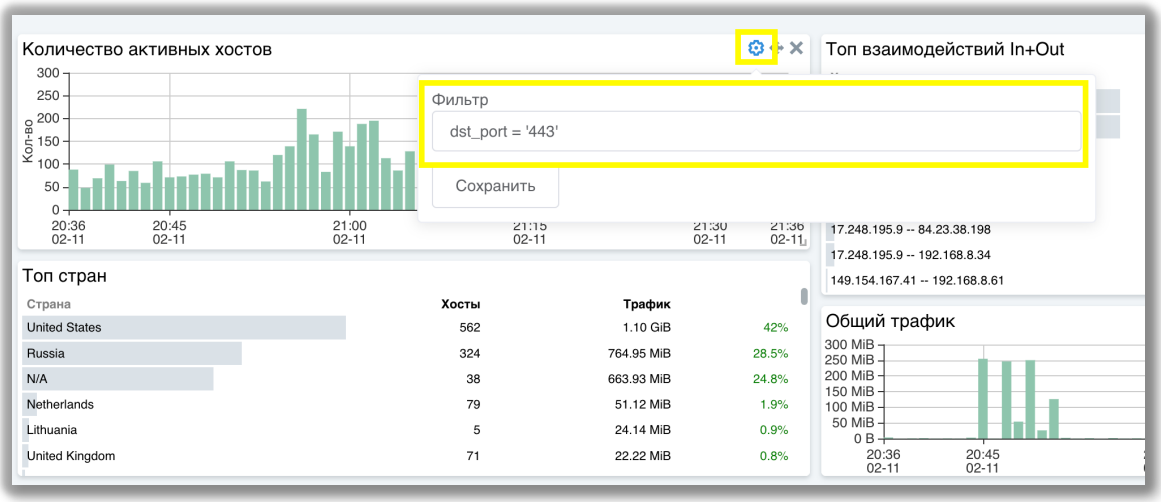
В системе доступны следующие виджеты

1. Группы
2. Группы In+Out
3. Группы Хостов
4. Группы Хостов
5. Динамика числа потоков.
6. Карта Сети
7. Карта Трафика
8. Кол-во Интерфейсов
9. Кол-во Источников
10. Количество активных хостов
11. Общий трафик
12. Потоков максимальное
13. Потоков среднее
14. Сессии
15. Статистика по странам
16. Статистика хранения по типам данных
17. Топ взаимодействий In+Out
18. Топ городов РФ
19. Топ городов РФ по трафику



По умолчанию виджет отображает общую статистику для всей системы. Для создания виджета под определенную задачу, например применительно для определенной группы, порта, страны и тп, необходимо использовать FQL.

Для этого, после добавления виджета на Дашборд, необходимо нажать на колесико настроек виджета и добавитьFQL фильтр, как показано на скриншоте ниже.



Агрегация статистики

Для работы система собирает «сырые» потоки NetFlow, как правило в крупных компаниях за несколько дней могут собираться миллиарды записей. Для эффективной работы с большим количеством записей и быстрого построения отчетов в системе реализован механизм оптимизации с различным уровнем агрегации – 1 секунда, 1 минута, 5 минут, 15 минут, 60 минут.
Разрешение данных представляет собой временной интервал, представленный каждой точкой данных, собранной для отчета. Например, если отчет создается за последний день, то он будет построен на основе записей, агрегированных за интервалы в 5 минут.

Агрегация позволяет повысить производительность, когда есть задача анализа информации за длительный промежуток времени. Анализ сырых данных необходим для проведения детального анализа и расследования точечных инцидентов.

Обычно при разборе сетевых потоков по интересующему инциденту в сети, администраторы системы запускают отчет за большой период, для которого автоматически устанавливается соответствующую агрегация. Использование низкого разрешения данных в отчетах позволяет вам быстрее запускать отчет и получать ответ на вопрос. Затем администраторы сужают временной интервал отчета только до времени инцидента и запускают отчет за десятки минут, где используется высокое разрешение данных 1 секунда или 1 минута, что обеспечивает наивысшее разрешение.

Уникальной особенности агрегации статистики в Neutrino Foresight являет тот факт, что при агрегации не происходит потери данных при построении отчета, как в некоторых аналогичных системах.

Автоматическая детализация данных в отчетах, агрегация
Система устанавливает интервал разрешения данных в зависимости от выбранного временного интервала отчета или Дашборда.
Разрешение доступно для временных интервалов до минимального временного интервала следующего уровня разрешения. Например, предположим, что минимальные временные интервалы для:

- разрешения 1 секунда установлены на 15 минут,
- разрешения 1 минута установлены на 6 часов,
- разрешения 5 минут установлены на 3 дня,
- разрешения 15 минут установлены на 8 дня,
- разрешения 60 минут установлены на 8+ дней.

Это означает, что:

- Отчеты с временными интервалами менее 16 минут будут использовать разрешение 1 секунда.
- Отчеты с временными интервалами от 16 минут до 6 часов 59 минут будут использовать разрешение 1 минут.
- Отчеты с временными интервалами от 6 часов 59 минут до 3 дней будут использовать разрешение 5 минут.

- Отчеты с временными интервалами от 3 дней до 8 дня, будут использовать разрешение 15 минут
- Отчеты с временными интервалами от 8 дней, будут использовать разрешение 60 минут

При агрегации система суммирует объем переданных данных для идентичных хостов и портов. Другие системы могут попросту не отображать часть статистики, так как агрегируют именно записи NetFlow. Например, если какой-то хост создавал небольшой сетевой трафик пол года назад, мы сможем его увидеть в Neutrino Foresight, в других система этой статистики может не быть.

Статистика хранения по типам данных

Тип данных	Всего строк	Строк в день	Всего дней	Начало периода	Конец периода	Объем	Объем в день
Сырые данные	35354070	471388	75	2023-10-12	2023-12-26	2.10 GiB	28.68 MiB
По секундам	26167890	348905	75	2023-10-12	2023-12-26	1017.24 MiB	13.56 MiB
По 1 минуте	23087128	307828	75	2023-10-12	2023-12-26	861.82 MiB	11.49 MiB
По 5 минут	15197822	202638	75	2023-10-12	2023-12-26	609.50 MiB	8.13 MiB
По 15 минут	11947315	159298	75	2023-10-12	2023-12-26	481.39 MiB	6.42 MiB
По 60 минут	7484734	99796	75	2023-10-12	2023-12-26	300.73 MiB	4.01 MiB

Система выполняет агрегацию данных в режиме реального времени. При построении отчетов, дашбордов и в зависимости от выбранного диапазона времени система определяет какой уровень агрегации необходимо использовать для оптимального построения отчета с точки зрения скорости и детализации.
При необходимости администратор может задать различные политики для разных типов агрегированных данных в зависимости от задач длительного хранения разного типа статистика.

Воздействие на отчеты о трафике
Объем переданных данных в отчетности о трафике не будет отличаться в зависимости разрешения данных в отличие от других решений NetFlow мониторинга. Все уровни агрегации будут включать все соединения. Например, предположим, что были зафиксированы следующие соединения:
Хост A --> Хост B
Хост A --> Хост C
Хост C --> Хост A
При всех уровнях агрегации мы увидим все данные для всех трех хостов в отличие от решений конкурентов, у которых бывает, что при разрешении в 5 минут и больше отслеживаются только наиболее активные хосты и пары хостов.

REST API

Система Neutrino Foresight поддерживает подключение внешних систем по REST API с авторизацией для экспорта/выгрузки необходимых данных и статистики на внешнюю систему. Дополнительно поддерживается доступ к базе данных с помощью запросов.

Пример API запроса:

```
curl http://localhost:8092/api/v1/query/databases --user "user:user"
```

Требования к каналу связи.

Экспорт статистики NetFlow потребляет незначительную долю емкости канала связи, ориентировочно 1-3%. Ниже представлены замеры нагрузки на канал связи, которые были сделаны на лабораторном стенде, где передается около 50 FPS. Принято допущение, что в случае увеличения кол-ва FPS, объем передаваемых данных будет линейно расти.

- 500 FPS -> по сети ориентировочно передается 500 Кбайт в минуту

Для большего кол-ва потоков объем передаваемых данных линейно растет:

- 1000 FPS -> по сети ориентировочно передается 1000 Кбайт (1 Мбайт) в минуту
- 2000 FPS -> по сети ориентировочно передается 2000 Кбайт (2 Мбайт) в минуту

Примеры настройки экспорта NetFlow

Элтекс ESR-Series

Выбираем интерфейс, статистика по которому будет экспортироваться

```
esr(config)# interface gigabitethernet 1/0/1
esr(config-if-gi)# ip netflow export
```

Настраиваем параметры экспорта

```
esr(config)# netflow active-timeout 60
esr(config)# netflow inactive-timeout 60
esr(config)# netflow version 9
```

Указываем адрес и порт коллектора

```
esr(config)# netflow collector x.x.x.x
esr(config-netflow-host)# port 2055
```

Активируем netflow на маршрутизаторе

```
esr(config)# netflow enable
```

Применяем изменения

```
esr# commit
```

Configuration has been successfully committed

```
esr# confirm
```

Configuration has been successfully confirmed

Проверка:

```
esr# show netflow configuration
Netflow configuration:
Global state:     Enabled
Version:         9
Maxflows:        10001
Refresh rate:     10
Inactive timeout:  15
Host: 115.0.0.10  Port: 2055
```

```
esr# show netflow statistics
Flows: active 9 (peak 34 reached 1d4h20m ago), mem 3841K
Hash: size 491496 (mem 3839K). InHash: 760 pkt, 339 K, InPDU 4, 160.
Processed rate   Bits/s        Packets/s
--------------   --------------   ---------------
Current              5142            2
1 Min Avg             4921            0
5 Min Avg             4874            0
Export: Rate 0 bytes/s; Total 3952 pkts, 3 MB, 28818 flows; Errors 2 pkts; Traffic lost 0
pkts, 0 Kbytes, 0 flows.
```

CheckPoint

Вы можете выполнить конфигурацию Checkpoint NetFlowV9, выполнив следующую команду:

```
add netflow collector ip X.X.X.X port 2055 export-format Netflow_V9 srcaddr Y.Y.Y.Y is-enabled true
```

Fortinet FortiGate

Добавляем адрес и порт коллектора

```
config system netflow
   set collector-ip <ip>
   set collector-port <0-65535>
   set source-ip <ip>
   set active-flow-timeout 60
   set inactive-flow-timeout 60
end
```

Включаем Netflow на интерфейсе

```
config system interface
   edit <interface name>
   set netflow-sampler {disable | tx | rx | both}
end
```

Проверка конфигурации

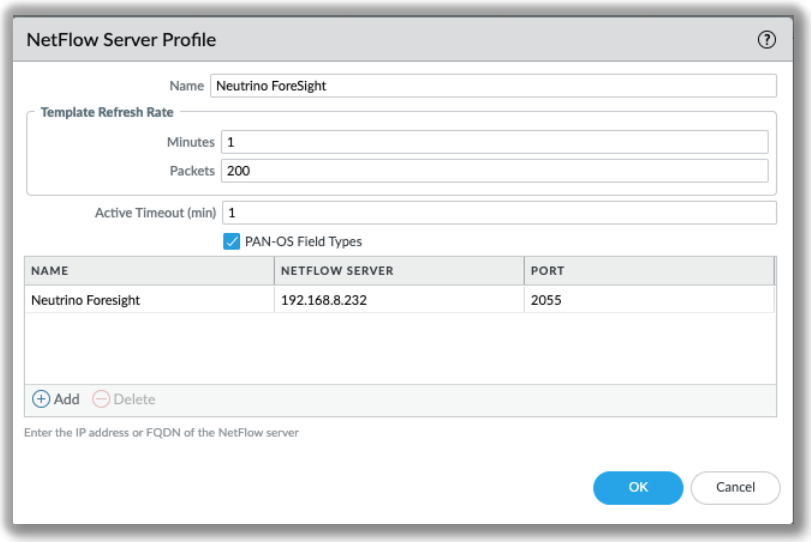
```
diagnose test application sflowd 3
diagnose test application sflowd 4
```

PaloAlto

Для настройки NetFlow на устройстве Palo Alto необходимо выполнить два шага:

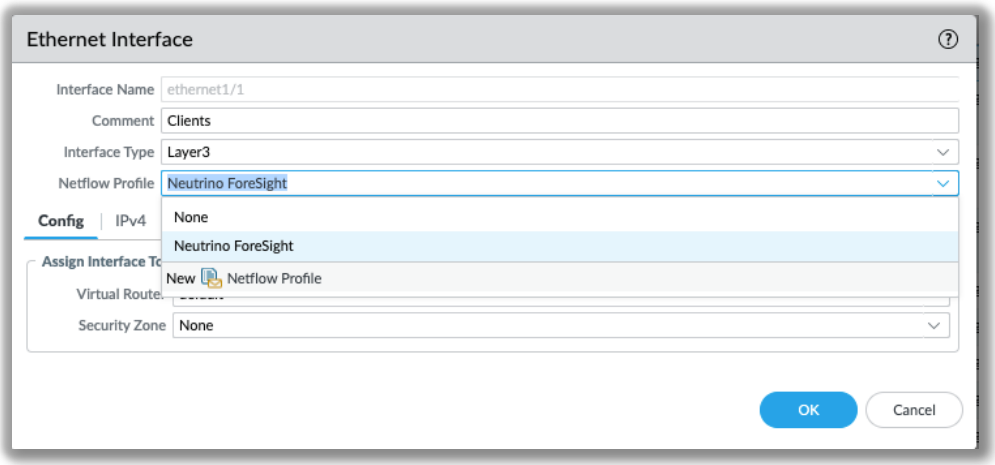
1) Настроить профиль сервера NetFlow: определяет частоту экспорта вместе с серверами NetFlow, которые будут получать экспортированные данные.
2) Назначить профиль сервера Netflow на интерфейс: весь трафик, проходящий через этот интерфейс, экспортируется на указанный сервер NetFlow.

Шаг 1
Для определения профиля сервера NetFlow (NetFlow server profile) вам необходимо перейти к Device > Server Profiles > NetFlow в графическом интерфейсе. Здесь вы увидите следующие настройки:



Name : введите имя для настроек NetFlow.
Template Refresh Rate : укажите количество минут или количество пакетов, после которых обновляется шаблон NetFlow (мы рекомендуем 1 минуту; диапазон пакетов 1–600, по умолчанию 20).
Active Timeout : укажите частоту экспорта записей данных для каждого сеанса (мы рекомендуем 1 минуту).
Export PAN-OS Specific Field Types: экспортировать поля, специфичные для PAN-OS, такие как App-ID и User-ID, в записях Netflow.
Server Name: укажите имя для идентификации сервера.
Server: укажите имя хоста или IP-адрес сервера.
Port: укажите номер порта для доступа к серверу (по умолчанию 9996).

Шаг 2
После того, как мы настроили профиль NetFlow, следующим шагом будет назначение профиля на интерфейс, для этого перейдите в Network > Interfaces > Ethernet. Откройте настройки интерфейса, с которого необходимо выполнить экспорт статистики.



Щелкните ссылку интерфейса на вкладке Ethernet и укажите профиль NetFlow.
После того, как вы настроите эти два шага, потоки будут экспортированы на сервер Nutrino Foresight, который автоматически обнаружит устройство и начнет создавать для вас отчеты.

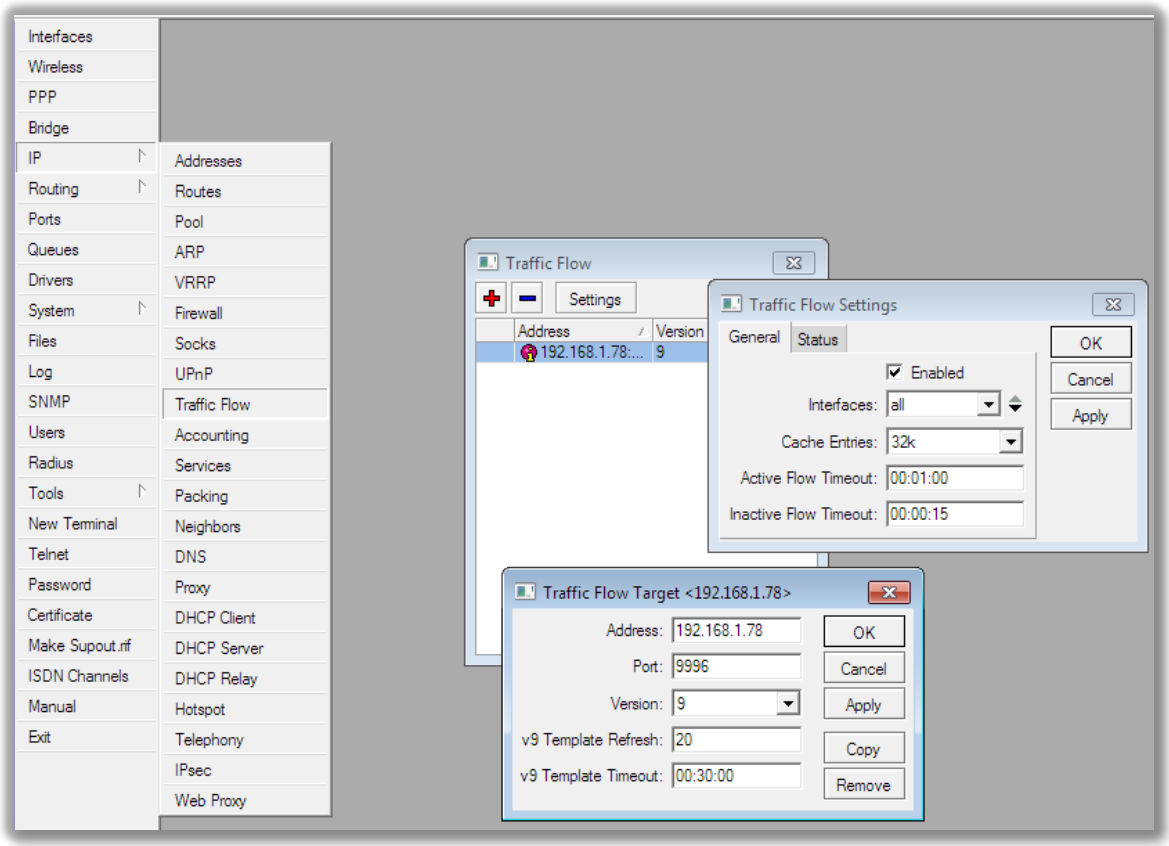
MikroTik

Настройка MikroTik выполняется из командой строки. Необходимо включить Traffic Flow и определиться с каких интерфейсов осуществлять сбор. Далее указать адрес и порт системы Neutrino Foresight, а также версию NetFlow.

```
/ip traffic-flow set enabled=yes
interfaces=ether1
*указан интерфейс 1, либо можно указать =all для сбора NetFlow со всех интерфейсов.

active-flow-timeout=1
inactive-flow-timeout=1
/ip traffic-flow target add address=X.X.X.X
port=2055
version=9
```

Либо тоже самое используя утилиту WinBox, для настройки Traffic Flow левом меню откройте пункт IP и выберите Traffic Flow. Необходимо включить Traffic Flow, поставив галочку напротив Enabled и выбрать желаемый интерфейс для сбора информации. После этого переходим на вкладку Targets и добавляем параметры коллектора, достаточно внести IP адрес, порт и версию. После этого нажимаем на кнопку Apply. После этого роутер начнет отправлять информацию на Neutrino Foresight.



Cisco Nexus 9000 series (sFlow)

1. Включить sFlow Feature

```
switch(config)#feature feature sflow
```

2. Задать sampling rate

```
switch(config)#sflow sampling-rate 4096
```

Диапазон от 4096 до 1000000000, sampling-rate = 0 отключает sampling.

3. Задать максимальный размер sampling size - максимальное количество байтов, которые следует скопировать из выборочного пакета

```
switch(config)#sflow max-sampled-size 256
```

Диапазон от 64 до 256 байтов

4. Задать counter poll interval

```
switch(config)#sflow counter-poll-interval 60
```

Диапазон от 0 до 2147483647, counter poll interval = 0 отключает counter sampling

Здесь указывается максимальное количество секунд между последовательными выборками счетчиков, связанных с источником данных.

5. Задать адрес и порт Neutrino Foresight, IP адрес устройства и интерфейсы, с которых необходимо собирать sFlow

```
sflow collector-ip <Neutrino Foresight IP address>
sflow collector-port 6343
sflow agent-ip <Any L3 interface IP>
sflow data-source interface <interface name>  // для всех интерфейсов, с которых
необходимо отправлять статистику sFlow.
```

sFlow диагностика

```
show sflow – отобразить глобальную конфигурацию sFlow
show sflow statistics – отобразить статистику sFlow
clear sflow statistics – очистить статистику sFlow
show running-config sflow[all] – отобразить текущую конфигурацию sFlow
```