Flowmon
Driving Network Visibility

Техническое руководство:

Мониторинг сети с помощью обогащенных flow-данных

By Pavel Minarik, CTO and Artur Kane, Technology Evangelist

Основное содержание

Цифровая трансформация корпораций во всем мире привела к всеобщей связности и высокоскоростному обмену данными, что сопровождается одновременным ростом производительности сетей. Сетевая инфраструктура при этом становится настолько важной, что обеспечение ее надежности и безопасности абсолютно необходимо для любой организации.

Тем не менее, сети становятся все более абстрактными, описываемыми такими метафорами как «общедоступное облако», нам даже не нужно думать о коммутаторах или маршрутизаторах, не говоря уже об их ручной настройке. Производители сетевого оборудования делают сетевое взаимодействие бесшовным, и соответственно, компетенция инженеров постепенно смещается от использования отвертки до вопросов обеспечения безопасности сети десятков тысяч IoT- устройств. SDN, NFV и виртуализация идут рука об руку с этой тенденцией, позволяя корпорациям сосредоточить свои ресурсы на основном бизнесе, а не на управлении сетью. Это приводит к взрывному росту пропускной способности в корпоративных сетях, а традиционные подходы к мониторингу сети больше не соответствуют реальности. В компании Flowmon мы переосмысливаем старые концепции и стремимся разрушить стены, которые сдерживают прогресс

В этом Техническом руководстве речь идет о нашей уверенности в том, что объединение видимости на уровне flow и на уровне пакетов в одно универсальное решение является технологией, которая будет масштабироваться с учетом будущих требований к производительности и емкости сети. Решение также сохраняет подробную информацию о сетевом трафике и предоставляет отчеты в простой и понятной форме. Вы узнаете, как потоковые данные, часто воспринимаемые как инструмент биллинга и топ-статистики, могут полностью заменить полный пакетный захват и пакетный анализ, и обеспечить непревзойденную масштабируемость, делая шаг в будущее.

История сетевого мониторинга: Пакетный анализ

Пакетный анализ просматривает каждое сообщение для анализа его содержимого. Не происходит агрегации, сжатия или обрезки, и данные хранятся в исходном размере. Поэтому этот метод имеет чрезвычайно высокие требования к производительности и емкости диска. Представьте себе захват сети со средней скоростью 250 Мбит/с. Это эквивалентно загрузке данных со скоростью более 31 МБ в секунду, 1,8 ГБ в минуту, 108 ГБ в час и 2,6 ТБ в день. В случае сетей с пропускной способностью 10 Гбит/с, мы достигли бы невероятных чисел - это было бы более 100 ТБ хранимых данных ежедневно. Однако большие объемы данных не являются единственным недостатком. Основное ограничение пакетного анализа - это зашифрованный трафик. Без ключа шифрования мы не можем понять содержимое любых переданных данных и часто даже не обнаруживаем протокол передачи или приложение. Тем не менее объемы зашифрованного трафика постоянно растут. Непрерывная, полномасштабная запись трафика (с полным пакетным захватом) требует правильного технического оборудования, особенно высокоскоростных накопителей с достаточной пропускной способностью. Такой подход к сетевому мониторингу очень затратный, он подходит только для критической инфраструктуры и сетей с определенными целями. Следует подчеркнуть, что хранение таких данных может быть не единственной проблемой. Как только данные сохраняются, решение любых возникающих проблем требует обширных знаний и большого опыта. Для разрешения большинства сетевых инцидентов компании полагаются на другой подход.

Он называется захват пакетов по запросу (on-demand packet capture). При использовании этого подхода мы захватываем пакеты только тогда, когда это необходимо - когда мы имеем дело с проблемами совместимости системы - например, при обнаружении отсутствия или повреждений пакетов. On-demand packet capture является простым методом, доступным для каждого сетевого администратора, но у него есть свои плюсы и минусы. Ограничение этого подхода заключается в том, что администратор должен заранее решить, какой трафик должен сохраняться. Следовательно, нет возможности добраться до архива трафика. Для этого требуется, чтобы сетевой администратор физически переместился (например, в серверную комнату) со своим ноутбуком, подключил его к зеркальному порту или TAP и выполнил запись сетевого трафика. Проблемы могут возникнуть, когда место, где нужно оказаться, находится далеко, а также в оптических сетевых интерфейсах и 10 Гбит-ных инфраструктурах - эти ограничения едва ли можно преодолеть с помощью ноутбука.

Несмотря на то, что потребность в захвате пакетов не пропадает, спрос, однако, безусловно, сокращается. Существует явная проблема масштабируемости, особенно из-за растущего числа устройств, подключенных к сети приложений и услуг, предоставляемых облаком, которые требуют более высокой пропускной способности. Решения для полномасштабной записи и анализа трафика являются очень ресурсоемкими и затратными. Кроме того, существуют технологические ограничения в высокоскоростных сетях и ограниченные возможности использования в случаях, когда трафик зашифрован.

Будущее сетевого мониторинга: Расширенный flow

Когда дело доходит до мониторинга сетевого трафика, устранения неполадок или обнаружения угроз, сетевые инженеры забывают, что в их распоряжении есть два варианта. Первый - это полный захват и анализ пакетов, обеспечивающий полную видимость сети. Другой – анализ flow-данных.

Flow-данные являются абстракцией самого сетевого трафика. Flow-статистика создана на основе совокупности сетевого трафика; она использует IP-адрес источника, IP-адрес назначения, порт источника, порт назначения и номер протокола в качестве атрибутов, которые идентифицируют отдельные записи потока. Содержимое сообщения не сохраняется, и достигаемая скорость агрегирования составляет около 500:1. С помощью информации, перечисленной выше, мы можем проанализировать структуру трафика, определить конечные точки, передающие большие объемы данных, или устранить неполадки в сети и неправильные конфигурации. Другими словами, мы можем справиться с 80% инцидентов в сети, как отмечается в отчетах Gartner с 2013 года.

Очевидно, что flow-данные не содержат достаточно информации для решения некоторых задач. Наоборот, при использовании пакетного анализа, ИТ-отдел обычно перегружен едва управляемыми объемами подробных данных. Когда мы объединяем обе точки зрения и расширяем традиционные flow-данные с помощью информации из уровня приложений, мы можем получить соответствующую информацию о передаче данных, гибкую отчетность и эффективное устранение неполадок в работе, а также автоматическое обнаружение инцидентов безопасности сети. Этот подход называется расширенным flow, использующим гибкость *протокола IPFIX*. Исходя из нашего опыта, можно сказать, что теперь мы можем справиться с 95% сетевых инцидентов с помощью наиболее масштабируемого, экономичного и простого в использовании решения на основе flow-данных.

Наиболее известной реализацией этой технологии является Cisco NBAR2 (Next Generation Network-Based Application Recognition -Распознавание приложений следующего поколения на основе сети). Мониторинг flow-данных сочетается с непрерывным пакетным анализом, который расширяет статистику трафика с помощью названия или протокола приложения. Основываясь на этой информации, современные *flow-коллекторы* позволяют создавать отчеты и анализировать трафик.

Одним из наиболее распространенных протоколов связи является HTTP или его зашифрованная версия HTTPS. Сегодня он используется для предоставления доступа к некоторым веб-сайтам, но это не единственная его функция. Протокол также является основой связи между компонентами бизнес-систем или приложениями, работающими с конфиденциальными данными (например, электронными банковскими операциями). Определив этот протокол передачи, мы можем расширить статистику flow-данных с помощью основных составляющих HTTP-запроса: имени хоста или информации URL. Благодаря SNI (Server Name Indication - Распознавание имени сервера) мы можем получить информацию об имени хоста, даже если используется протокол HTTPS. Точно так же мы можем получить другую информацию из HTTP-коммуникации; например, название операционной системы и ее версии, идентификация браузера и его версии или тип устройства в случае мобильных телефонов. И это только один пример из многих протоколов, для которых мы можем использовать информацию L7 без необходимости ручного анализа данных. Тем не менее, flow-данные могут быть расширены чем-то, возможно, даже более мощным в современном мире, а именно, Мониторингом производительности сети (NPM). Показатели NPM могут существенно помочь в устранении неполадок с производительностью сети. Используя показатели Server-Response-Time и Round-Trip-Time, мы можем различать задержки в сетевой инфраструктуре (например, неисправную точку доступа) и задержки на сервере (например, из-за недостатка аппаратных ресурсов). Такая информация крайне важна для быстрого устранения неполадок в сети. Показатели задержки и jitter особенно интересны, когда мы используем VoIP-звонки или видеоконференции, поскольку они могут указывать на плохое качество звука и видео.

Когда мы говорим о передаче больших объемов данных, нас интересует в основном количество повторных передач TCP, которые могут указывать на проблемы на физическом уровне (например, помехи, неисправный порт), а также низкая скорость передачи данных или беспорядочные пакеты, что может указывать на сбои в каналах связи.

А когда этот уровень информации все еще неисчерпывающий, *Flowmon* позволяет запускать полный захват пакетов по требованию. Это можно сделать вручную или автоматически при обнаружении события. Когда это происходит, фильтр захвата определяется системой автономно, сокращая объем захваченных данных до абсолютного минимума, сохраняя только необходимую часть трафика. Очевидно, что это можно сделать удаленно в любой части сети на скорости 100 Гбит/с; что недостижимо с помощью Wireshark или WinPCAP.

Преимущества *flow-мониторинга* и анализа уровня приложений очевидны. Мы получаем более подробную информацию о передаче данных, улучшенные возможности анализа трафика. В то же время мы сохраняем отличную степень сжатия статистики сетевого трафика по сравнению с исходным объемом трафика для масштабирования до нескольких 100ГБ сетей. Кроме того, система агрегирует наиболее важную информацию, поэтому она может быть сразу доступна, без необходимости ручного обработки данных с анализом пакетов. Это приводит к значительному сокращению Mean-Time-To-Resolve, и в то же время требует меньше навыков, необходимых для использования решения. С Flowmon всегда можно вести полномасштабную запись трафика, если необходимо, используя ту же платформу.

Почему стоит выбрать flow, а не packet? Экономические и технические преимущества

В предыдущей части этого Технического руководства мы выявили различия между непрерывным захватом пакетов и flow-данными в контексте использования этих технологий для успешного мониторинга сетевого трафика. Давайте обобщим преимущества расширенного flow в сравнении с пакетным захватом:

- Из-за среднего соотношения сокращения необработанного трафика к требуемому объему хранения для соответствующих записей flow, равного 500:1 (в отличие от пакетного анализа 1:1), технология flow является гораздо более масштабируемой.
- Бюджетные требования к технологиям пакетного анализа редко позволяют осуществлять мониторинг всего объема сетевого трафика. Таким образом, он осуществляется только для мониторинга критически важных систем, в отличие от flow-анализа, который покрывает весь трафик корпоративной сети, охватывая дата-центры и cloud по стандартной схеме.
- *Устранение неполадок* в основном не проводится в режиме реального времени. Часто в корпорациях несколько дней уходит на то, чтобы администратор сети рассмотрел зарегистрированный инцидент. При ограниченном сроке хранения данных ретроспективный анализ был бы невозможен. Flow-мониторинг может легко обеспечить хранение трафика за несколько недель или месяцев, поэтому вы можете легко расставить приоритеты в своей работе и сосредоточиться на ретроспективном анализе в любой момент, когда вы выполнили более важные задачи.
- Беспроблемное развертывание, интеграция с существующим сетевым оборудованием, совместимость с широким спектром источников flow, быстрое обучение администраторов - вот лишь некоторые из многих аргументов, почему так просто внедрить flow-технологию в вашу сеть и получить мгновенную выгоду.

- Уровень детализации, обеспечиваемый пакетным анализом, делает возможным проведение подробной судебной экспертизы. Компании обращаются к технологии flow, чтобы минимизировать время, необходимое для выявления первопричин, и получить больше времени на их устранение, используя удобные информационные панели и возможности детализации.
- Чрезмерная детализация пакетного анализа означает более высокие издержки, более низкую масштабируемость и намного более высокий требуемый набор навыков для управления им. При этом только небольшой процент собранных данных является актуальным. С другой стороны, расширенный flow хранит наиболее интересную и важную информацию, так что с ее помощью можно разрешить 95% сетевых инцидентов. Кроме того, Flowmon обеспечивает *полный пакетный захват по требованию* для остальных случаев.
- Пакетный анализ был построен с учетом неограниченной видимости. Это хорошо подходит для трудоемкой судебной экспертизы. С целью скорейшего восстановления обычных бизнес-процессов корпорации обращаются к Flowmon для получения аналитики рабочих процессов и автоматизации для упрощения решения.
- С увеличением объемов зашифрованного трафика, пакетный анализ становится бесполезным. При экспорте flow-данных из зашифрованного трафика Flowmon фокусируется на незашифрованных IP-заголовках, что помогает устранить 80% инцидентов. Кроме того, он использует различные методы для извлечения информации из уровня приложений, который скрыт для других инструментов.
- Поставщики общедоступных облачных сервисов не разрешают подключаться к своей сети для полного пакетного анализа. Однако, как облачные провайдеры, так и виртуальные гипервизоры часто экспортируют flow-данные, совместимые с Flowmon, что обеспечивает бесперебойную работу и внедрение качественного сетевого мониторинга.

Примеры применения

Устранение неполадок с использованием пакетного захвата

Допустим, что у нас есть инструмент анализа пакетов с продолжительным захватом. Будем надеяться, что запущенный буфер хранит необходимые данные. К счастью, мы можем загрузить PCAP, который содержит трафик с IP-адреса 192.168.222.87 и открыть трафик в Wireshark.

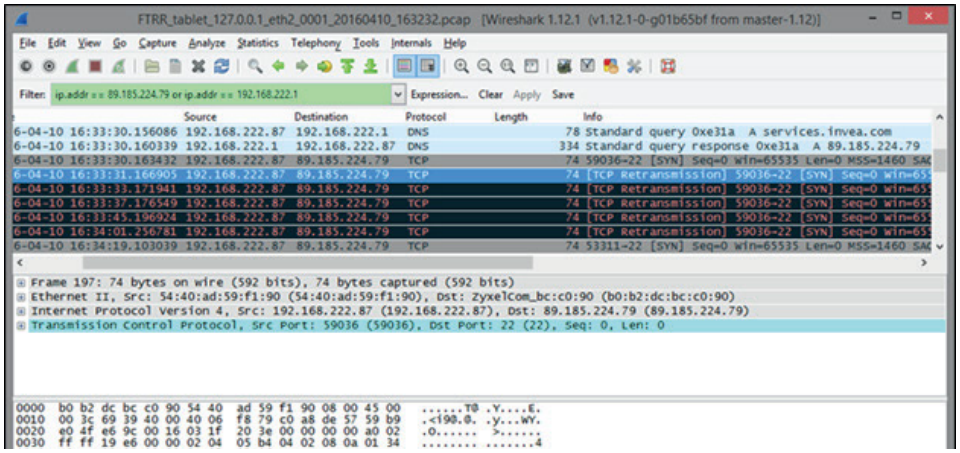

Рисунок 1: Анализ сетевого трафика в Wireshark.

На рисунке выше мы видим связь между пользователем и services.invea.com. Домен services.invea.com правильно соотносится с IP-адресом 89.185.224.79, но, после получения ответа от DNS, пользователь попытался установить сеанс TCP без ответа от внешнего IP-адреса. Мы должны проверить настройки брандмауэра, чтобы определить, разрешена ли эта коммуникация. Вторая проблема связана с несуществующим доменом, который запрашивает компьютер пользователя. Мы видим, что update.invea.com не существует, что, вероятно, подразумевает неправильную конфигурацию пользователя, а не проблему, связанную с сетью.

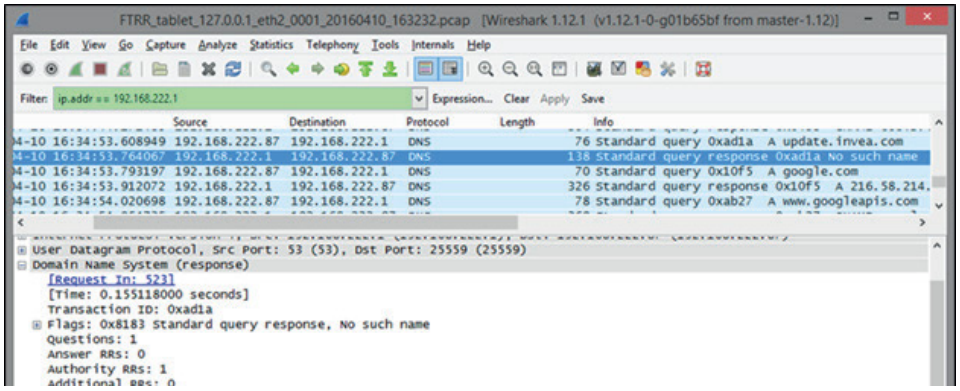

Рисунок 2: Хост-запросы для обнаружения несуществующего домена.

Устранение неполадок с использованием Расширенного flow

Допустим, у нас есть установленный *Flowmon Probe* и *Flowmon Collector*, который хранит в истории несемплированную и неагрегированную статистику трафика за несколько недель. Итак, мы можем напрямую создать запрос по поводу DNS домена services.invea.com.

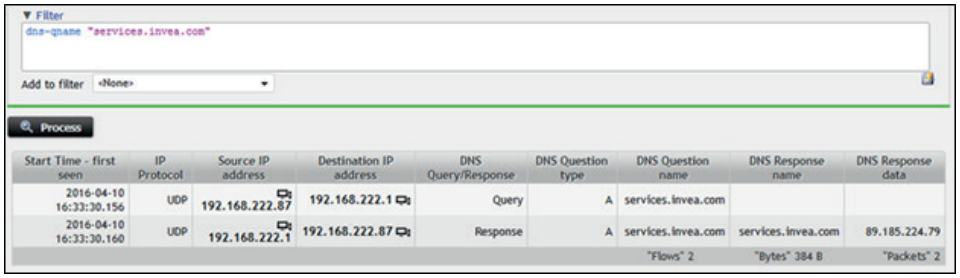

Рисунок 3: Фильтрация в трафике DNS - статистика потоков, расширенная информацией DNS.

Мы можем видеть IP-адрес, предоставленный DNS-сервером, в качестве ответа и легко проверить трафик, идущий на этот IP-адрес. Это возможно, потому что потоки от зонда, соответствующего серверу DNS, расширены самой важной информацией уровня L7 из протокола DNS.

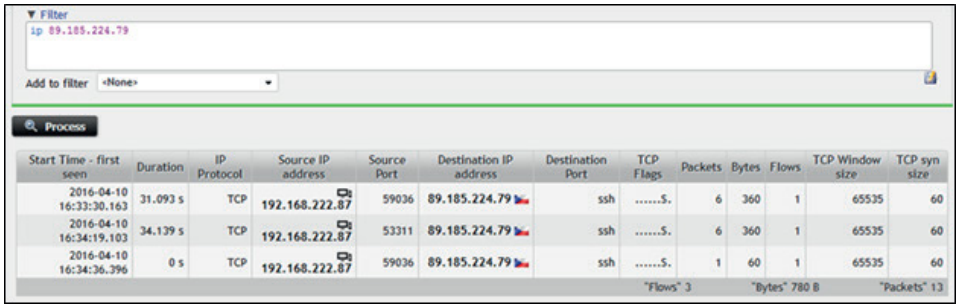

Рисунок 4: Фильтрация взаимодействия пользователя с внешним сервисом.

Хост не получает никакого ответа.

Я вижу, что только пакеты SYN передаются в сеть без ответа от внешнего IP-адреса, что подразумевает необходимость проверки правил брандмауэра. Помимо общей информации L3 / L4, у меня есть представление о конкретных элементах TCP, таких как размер сегмента TCP (окна) по умолчанию, что может помочь устранить неполадки в сеансе TCP.

Несуществующий домен также находится в этом flow. Домен update.invea.com не существует, поэтому DNS-сервер отвечает «NXDomain».

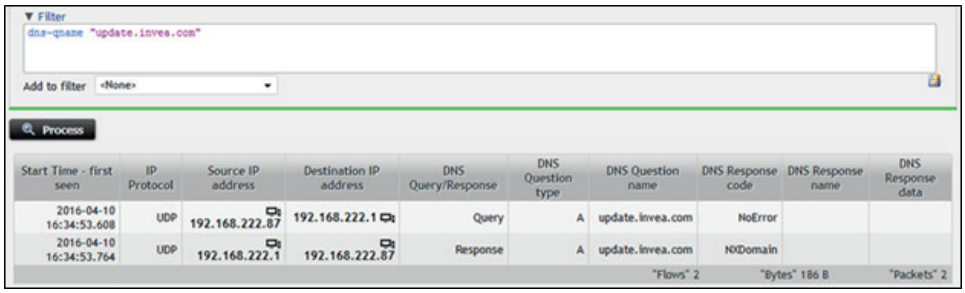

Рисунок 5: Фильтрация в трафике DNS - поиск NXDomain в коде ответа DNS

Обзор проекта:
Инструмент выявления первопричин

Представим отдел инженеров уровня Level 3+ банка, в котором насчитывается 50 тысяч сотрудников. Эти инженеры сосредоточены на анализе первопричин сетевых инцидентов, которые до этого не могли быть решены. Например, чтобы выяснить, почему прерывалось VPN-соединение между клиентом и банком, которые находятся на разных континентах. Очень часто работа инженеров состоит в том, чтобы проанализировать в Wireshark петабайты данных, генерируемых сотнями различных систем в сложной и неоднородной среде. И это как раз та ситуация, когда один из клиентов Flowmon попросил нас предоставить альтернативное и более эффективное решение для борьбы с операционными инцидентами.

Важно сказать, что наш клиент построил целую платформу, чтобы помочь им с сетевыми операционными задачами. Она была основана на инструменте для непрерывного захвата пакетов, специализированном программном обеспечении с открытым исходным кодом для flow мониторинга и инструменте на основе SNMP, отображающем карты передачи данных в режиме реального времени. Вскоре стало ясно, что обслуживание, техническая поддержка и модернизация решения для повседневной работы были слишком дорогими и отнимали много времени. Поэтому они искали технологию на основе NetFlow/IPFIX для замены оригинального решения. IT департамент банка искал решение, которое полностью заменило бы оригинал. Несмотря на то, что бюджет был согласован, выбор был не так прост, как кажется на первый взгляд. Во время тестирования решений разных производителей, выявленные проблемы иногда заключались в агрегировании данных или в отсутствии виртуализации, но во всех случаях это была медлительность с точки зрения времени, необходимого для предоставления результатов измерений.

Решение, которое было бы идеальным, должно:

- предоставлять не только контекстно-зависимые панели инструментов верхнего уровня, но и те, которые позволяют выполнять детализацию любого flow вручную.
- не агрегировать хранимые данные и сохранять необработанные потоки в течение всего срока хранения.
- не обязательно должно зависеть от своих собственных датчиков, поскольку они не могут быть привязанными к одной технологии из-за их неоднородной среды.
- быть виртуализированным, чтобы управление и миграция были максимально гибкими.
- совмещать flow мониторинг с полным захватом пакетов по требованию.
- что наиболее важно, обеспечивать вывод измеренных статистических flow-данных быстрее, чем платформа, которую они создали самостоятельно десять лет назад на основе инструмента с открытым исходным кодом.

Затем команда наткнулась на Flowmon, который полностью соответствовал их потребностям. Начиная с пилотного проекта, Flowmon стал основным инструментом. Главным инструментом по выявлению первопричин. Теперь инженеры начинают с панели инструментов, переходят к статистике верхнего уровня, углубляются в уровни NetFlow, а затем сосредотачиваются только на небольшой части трафика, где они могут выполнять полный захват пакетов.

Заключение

Динамичное развитие и разнообразие современных сетей бросают вызов преобладающему подходу к сетевому мониторингу. Сталкиваясь с увеличением скорости сети, пробелами в видимости, вызванных миграцией в облако, IoT и программно-определяемыми сетями, решения по захвату пакетов пытаются принести ожидаемые результаты быстро и по разумной цене.

Решения по пакетному захвату были разработаны в то время, когда было трудно предположить динамику развития современных сетевых сред. В настоящее время они хорошо работают в отдельных примерах, но они не могут справиться с гибкостью, масштабируемостью и простотой использования потоковых данных в большинстве случаев повседневного использования, с которыми сталкиваются сетевые инженеры. Мы продемонстрировали пример использования, когда данные потока с расширенной видимостью одинаково эффективны для полного пакетного захвата и пакетного анализа. С другой стороны, справедливо сказать, что даже с расширенной видимостью на уровне flow вы все равно можете столкнуться с проблемами, когда анализ PCAP неизбежен.

Мы во Flowmon Networks верим, что объединение видимости уровней потоков и пакетов в одном универсальном решении - это технология, которая сможет быть масштабирована с учетом будущих потребностей в производительности и емкости. Итак, давайте проводить непрерывный flow-мониторинг и пакетный захват, когда это необходимо. В конце концов, вы, скорее всего, увидите, что необходимость анализировать PCAP гораздо ниже, чем вы ожидаете.

Попробуйте Flowmon и посмотрите, как это может помочь вашей организации.

О Flowmon Networks

Павел Минарик

Технический директор Flowmon Networks

Как технический директор Flowmon Networks, Павел отвечает за технологическую дорожную карту, дизайн и разработку продуктов, а также за техническую поддержку и проекты клиентов по всему миру.

Артур Кейн

Технологический евангелист Flowmon Networks

Артур Кейн работает технологическим евангелистом Flowmon Networks. Он отвечает за обучение бизнес-партнеров компании и за повышение осведомленности о технологиях Flowmon.

Flowmon Networks позволяет предприятиям уверенно управлять и защищать свои компьютерные сети. Благодаря нашей высокопроизводительной технологии мониторинга сети и аналитическому поведенческому анализу IT-специалисты во всем мире получают абсолютную прозрачность сетевого трафика для повышения производительности сети и приложений и борьбы с современными киберугрозами.

Увлеченные технологиями, мы находимся в авангарде разработки средств сетевого мониторинга NetFlow/IPFIX - высокопроизводительного, масштабируемого и простого в использовании.

Крупнейшие в мире компании, поставщики интернет-услуг, государственные учреждения или даже небольшие и средние компании полагаются на наши решения для контроля своих сетей, поддержания порядка и преодоления сомнений.

Дистрибьютор Web Control DC

info@web-control.ru

+7 495 925 7794