PROFITAP

White Paper

NETFLOW МЕТАДАННЫЕ АНАЛИЗ ПАКЕТА

В чем разница?

Какой метод подходит мне?

Каковы преимущества и недостатки каждого метода?

VISIT WWW.PROFITAP.COM

ВВЕДЕНИЕ

С каждым годом ИТ-инженерам приходится прикладывать все больше усилий для контроля сетевого трафика. Увеличились скорость и объем трафика, снизилась стоимость сетевого подключения. Если раньше мы только мечтали о 40 Гбит/с каналах, то сегодня они стали реальностью. Но эта тенденция сопровождается ростом атак, взломов, проникновений. Большинство ИТ-специалистов понимают, что сейчас самое время внедрять систему мониторинга, если они еще этого не сделали. Как это сделать?

Существует три принятых подхода к сбору данных, проходящих по сети, и формированию отчетности: NetFlow (или любой другой вид мониторинга на основе потока), пакеты и метаданные. Какой метод подходит для вашей среды?

В этом документе анализируются методы мониторинга, рассматриваются их сильные и слабые стороны, а также целесообразность их использования при различных обстоятельствах.

Первый рассматриваемый метод, считающийся золотым стандартом – анализ данных пакетов.

ГЛУБОКИЙ АНАЛИЗ ПАКЕТОВ

Анализ пакетов дает наиболее подробную информацию. Остальные два метода используют, фактически, данные пакетов для генерирования статистики. С помощью данных пакетов можно измерить расстояние между метками времени последовательных пакетов, время ответа сервера и расшифровать поток для просмотра полезной нагрузки приложения.

ЗА: отличная детализация

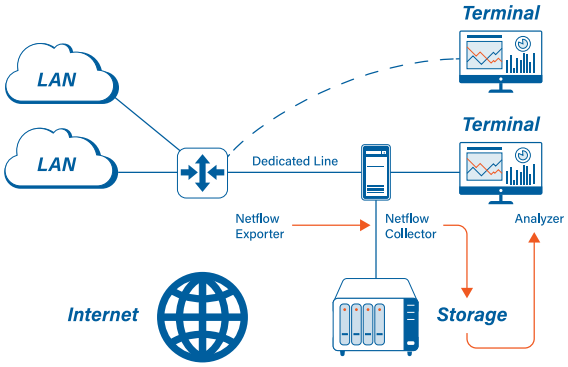
В пакете содержится все. При возникновении проблемы можно просмотреть каждый бит, байт и заголовок и получить полную картину. Некоторые проблемы можно увидеть только с помощью сырых данных, которые действительно показывают детальную картину и позволяют полностью проанализировать ситуацию. Например, если проблема возникла из-за низкого значения MSS в TCP, данные пакета позволят не только увидеть это, но и сопоставить с соответствующими ICMP-сообщениями.

ПРОТИВ: большой объем данных!

Легко потерять иголку в стоге пакетов. Данные пакетов очень объемны, их трудно анализировать, особенно при захвате трафика высокоскоростных каналов. Например, при захвате трафика 10Гбит/с канала, используемом на 50% своей мощности, в течение 5 минут, размер файла захвата составит почти 200 Гбайт. Это затрудняет исторический анализ при разрешении проблем хотя бы потому, что сложно хранить такой объем данных за несколько часов или дней.

При анализе данных пакета требуются навыки, опыт и терпение. Этот метод дает наиболее подробные сведения, но цель анализа должна оправдывать средства.

NETFLOW
(или другие методы на основе потоков)



При анализе сетевого трафика не всегда нужны подробные данные. Иногда достаточно высокоуровневой статистики, это зависит от целей анализа. NetFlow представляет собой сводные данные IP-трафика, которые генерируются сетевыми устройствами и отправляются в коллекторы, где преобразуются в красивые графики данных трафика.

ЗА: долгосрочный мониторинг, простое представление данных

Потоки предоставляют статистику в объеме, достаточном для обнаружения вторжения, идентификации наиболее активных пользователей сети и причин большого трафика. Для этого нет необходимости в глубоком анализе каждого пакета потока. Большинство решений анализа потоков выделяют IP-адреса, номера портов TCP или UDP, значения DiffSrv, время потока, длительность потока и количество данных в потоке. Большинство таких систем мониторинга позволяют просмотреть данные потоков за дни, недели или даже месяцы.

ПРОТИВ: нет полезных данных пакета, времени приема-передачи в сети и времени ответа сервера

NetFlow объединяет поток пакетов в одном направлении в единую статистику, поэтому не фиксирует время, что нужно для измерения времени приема-передачи или задержки между последовательными пакетами. Не собираются также детали заголовка, такие как флаги TCP, размер окна и параметры процедуры установления соединения (handshake), критичные для диагностики комплексных проблем.

Короче говоря, если цель мониторинга трафика заключается в наблюдении за трафиков в течение длительного периода для проведения расследований и обеспечения безопасности, NetFlow – идеальный выбор.

МЕТАДАННЫЕ

Этот метод является золотой серединой между вышеперечисленными. Данные пакета собираются анализатором, сортируются, разбираются, индексируются и даже сохраняются (в некоторых случаях). Затем генерируются графики и статистика о сетевом трафике, его использовании, полосе пропускания и даже производительности приложений. Эти данные и статистика хранятся длительное время. Этот метод предоставляет данные уровня анализа пакетов для диагностики большинства общих проблем, не требуя обработки больших объемов данных.

ЗА: Больше данных по сравнение с NetFlow, но без сложностей метода анализа пакета, длительное хранение в индексированном виде

Этот метод позволяет отслеживать и представлять в виде графиков статистику, такую как iRTT, время ответа приложений, время повторной передачи TCP и коды ответов DNS, позволяя инженерам обнаруживать болевые точки. При возникновении потребности в дополнительной информации, например в расшифровке трафика, можно отфильтровать и экспортировать пакеты для целенаправленного подробного анализа.

ПРОТИВ: аппаратные ресурсы, потеря данных

Использование метода требует мощных аппаратных ресурсов для проведения анализа в реальном времени, что часто очень затратно. Преобразование пакетов в долгосрочные метаданные, требует больших вычислительных мощностей. Есть также риск потери данных или генерации избыточных метаданных, особенно на высокоскоростных каналах.

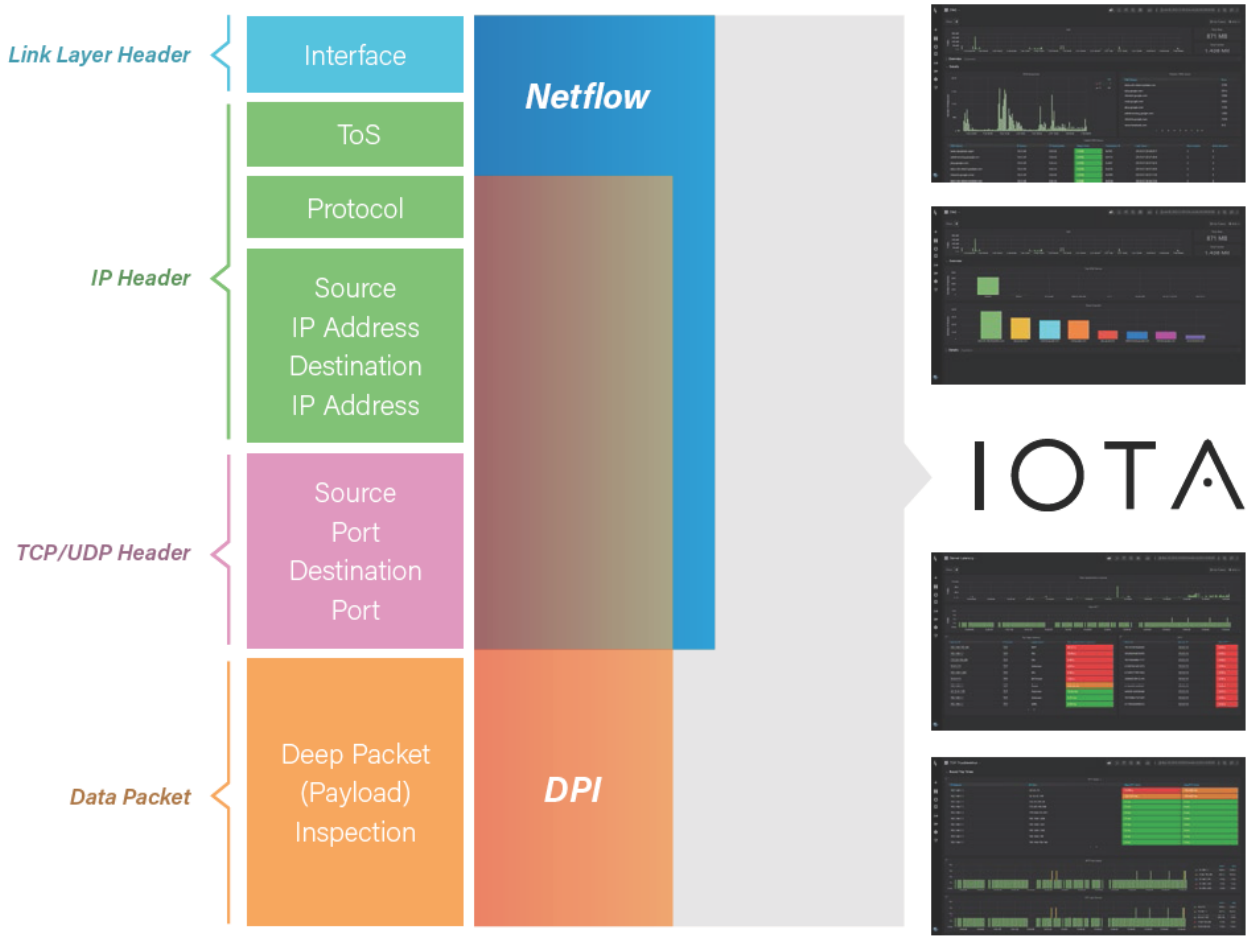
ОБЪЕДИНЯЯ ЛУЧШЕЕ

IOTA берет достоинства этих трех методов анализа и объединяет их в одном, компактном, переносном и экономически эффективном инструменте. Решение IOTA использует мощные возможности анализа пакетов, направляя данные на зашифрованный жесткий диск размером 1 ТБ (возможно подключение внешнего устройства хранения) и одновременно анализируя входящие данные в реальном времени.

Важные данные для анализа производительности и расследований отображаются и анализируются на встроенных информационных панелях. Полоса пропускания, производительность DNS, метрики TCP, задержка приложений, User Experience и многое другое можно отслеживать на настраиваемых экранах, предназначенных для отображения нужных данных при диагностике проблем. Это позволяет сетевым инженерам любого уровня проактивно и реактивно, быстро и легко разрешать сетевые проблемы.

При поиске следов проникновения или взлома во время расследования инцидента можно просмотреть трафик, отфильтрованный по потоку сеанса, GeoIP-местоположению или потреблению полосы пропускания. При решении проблемы низкой производительности статистика уровня пакета, такая как задержка сети, метрики TCP и время ответа сервера, могут помочь с определением коренной причины. Если требуется детальная информация на уровне пакетов, то поможет отфильтрованный и экспортируемый файл трассировки.

С IOTA вы получаете подробные данные анализа пакетов, простоту использования NetFlow и мощные возможности метаданных на одном экране без крупных финансовых затрат.



PROFITAP

Profitap разрабатывает и производит аппаратные и программные решения, которые помогают обеспечить полный доступ и прозрачность вашей сети. Эти решения сетевой прозрачности разработаны для защиты, проведения расследований, захвата пакетов и мониторинга производительности сети и приложений.

Сетевые решения Profitap помогают избежать простоя сети, обеспечить дополнительную безопасность в существующих и новых сетях в любой точке мира, правомерно перехватывать данные приложений и снижать сложность сети. Все инструменты сетевого мониторинга Profitap демонстрируют высокую производительность, безопасность и простоту использования, обеспечивают прозрачность и доступ к сети 24/7.

Будучи экспертом в области сетевого мониторинга, компания выпускает продукты, которые становятся стандартами отрасли, характеризующаяся высокими требованиями.

Продуктами компании пользуются свыше 1000 клиентов из 55 стран мира. Решения Profitap стали must-have для крупных компаний, в том числе из списка Fortune 500.

PROFITAP HQ B.V.
HIGH TECH CAMPUS 9
5656 AE EINDHOVEN
THE NETHERLANDS
sales@profitap.com
www.profitap.com

Profitap
@Profitap
profitap-international