УДК 004:056

МАРКИРОВАНИЕ СЕТЕВЫХ ПОТОКОВ

Л. Ю. МОЛЬКОВА
(Петербургский государственный университет путей сообщения Императора Александра I, Россия)

Аннотация. *В данной статье рассматривается важная роль маркирования сетевых потоков для обеспечения эффективного управления трафиком и качеством обслуживания в современных сетевых инфраструктурах. Подчеркивается необходимость идентификации и классификации информационных потоков для оптимизации сети, повышения безопасности и сбора точной статистики. Описываются различные методы анализа трафика, такие как использование инструментов мониторинга, систем обнаружения вторжений, прокси-серверов, а также инновационных решений, например, платформы Remote Topology для визуализации структуры сети и удаленных соединений. Особое внимание уделяется проблемам расшифровки зашифрованного трафика и обработки данных в режиме реального времени. В заключение отмечаются сложности, связанные с интеграцией различных систем маркировки и настройкой политик качества обслуживания, но подчеркивается критическая важность маркирования потоков для повышения производительности и стабильности современных сетей.*

Ключевые слова: *маркирование сетевых потоков, управление трафиком, качество обслуживания, анализ трафика, безопасность сети, мониторинг сети, удаленные соединения, расшифровка трафика, обработка данных в реальном времени.*

В современном мире цифровых технологий, где объем передаваемой информации через Интернет растет стремительно, важно обеспечить эффективную и надежную доставку данных. Управление и оптимизация потоков информации стали основополагающими в обеспечении высокого уровня обслуживания. Методы маркирования сетевых потоков играют ключевую роль в правильном распределении трафика, что необходимо для эффективного функционирования сетевой инфраструктуры в условиях ее постоянной загруженности и разнообразия информационных потоков.

С ростом активности в интернете возникает необходимость в эффективном контроле и управлении сетевой деятельностью. Определение и разделение информационных потоков становится важным элементом в управлении сетевым трафиком, что способствует улучшению обслуживания, обеспечению безопасности

и сбору точной статистики. Маркировка сетевых потоков позволяет идентифицировать трафик по различным параметрам, таким как источник, назначение, протокол, тип сервиса и приложение, что способствует оптимизации сети, увеличению качества обслуживания и соблюдению политик безопасности.

В процессе развития технологических методов анализа трафика происходило постоянное улучшение и интеграция различных элементов. Сравнить это можно с движением по спирали, где каждый новый этап вносит свои усовершенствования и развивается на основе предыдущих достижений. Таким образом, технологии продолжают совершенствоваться и эволюционировать в процессе (рисунок) [1].

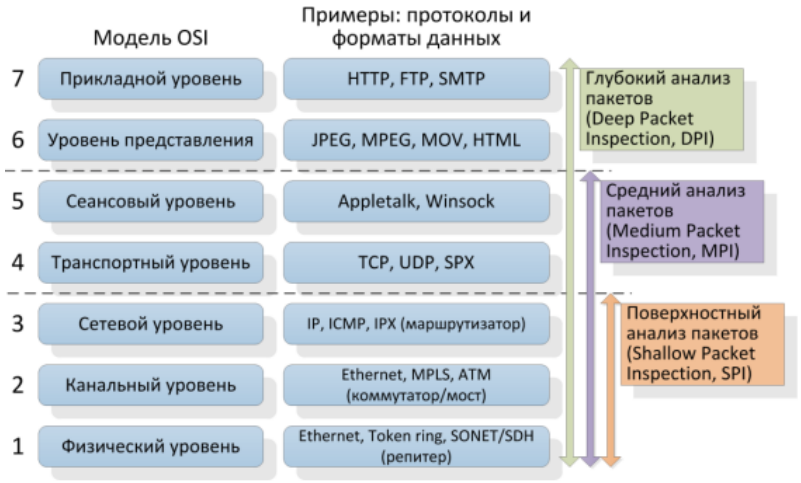

Рисунок. – Уровни развития технологии анализа сетевого трафика по «глубине»

Оптимизация сетевой инфраструктуры достигается благодаря применению тегов на потоки данных в сети, что приводит к улучшению услуг, более эффективному регулированию трафика и сокращению затрат [2].

В современном мире угрозы в сфере кибербезопасности растут с каждым днем, и поэтому процесс защиты информации становится все более важным. Система, которая помогает классифицировать данные по различным критериям с использованием специальных меток, может эффективно управлять ресурсами и обеспечивать безопасность передачи информации. Такой подход позволяет отражать кибератаки и обеспечивать надежность и доступность данных.

Метки в сетевых потоках обеспечивают продвинутое регулирование качества обслуживания, известного как QoS [3]. Данные по степени важности распознают и упорядочиваются сетевыми механизмами в системе, где осуществляется преимущественная обработка для важных потоков, таких как передача голоса и видео.

Эффективное распределение потоков данных по сети обеспечивается метками, учитывающими различные требования к пропускной способности. Это содействует стабильному и безопасному передаче информации, а также снижает вероятность перегрузок, возникающих из-за высокой нагрузки.

Такой подход не только оптимизирует работу сети, но и улучшает качество коммуникационных услуг, повышая удовлетворенность пользователей и обеспечивая более рациональное использование ее пропускной способности.

Методы анализа сетевого трафика [4]:

Для эффективного контроля над безопасностью, производительностью и стабильностью сетей необходимо тщательно следить за входящим и выходящим трафиком. В аспекте управления HTTP-соединениями, важно отметить несколько аспектов:

1. Для обеспечения безопасности данных и выявления подозрительных действий в сети, сетевые администраторы могут воспользоваться инструментами анализа трафика, такими как wireshark, nagios, prtg, solarwinds и прокси-серверы. Функция глубокого анализа трафика (dpi) включена в фаерволы, а также в системы мониторинга логов, что способствует контролю параметров работы сети. Сотрудничество между системами мониторинга и другими инструментами безопасности повышает эффективность выявления угроз. Однако для успешного наблюдения требуются четкие правила и опытные эксперты.

2. В реальном времени анализируются данные об активности пользователей в интернете, собранные из веб-трафика и интерфейсов сети. Перехваченная информация о действиях пользователей направляется в центральную базу данных для удобного доступа и глубокого анализа. Инструменты мониторинга используются для выявления аномалий в текущих событиях, а также для исследования исторических данных с целью обнаружения общих тенденций и раскрытия прошлых инцидентов.

Обеспечение безопасности и управления инцидентами включает в себя интеграцию с другими системами, учитывая при этом законодательные стандарты о конфиденциальности и защите данных. Регулярное обновление и планирование технологических и процессуальных аспектов необходимы для поддержания актуальности в условиях сетевых угроз.

3. Созданная система Remote Topology представляет собой инновационное решение, предназначенное для анализа структуры сети и удаленных соединений, включая технологии telnet, ssh, vmware remote console (vmrc) и vnc. Она функционирует путем сбора данных о сеансах через специально настроенное логирование на различных устройствах и серверах, а также через API и точки интеграции, предоставленные vmware и vnc. Все собранные сведения попадают в центральное хранилище, где они обрабатываются и структурируются при помощи инструментов, таких как logstash, что в дальнейшем облегчает их анализ.

Инструменты, такие как kibana или grafana, используются для создания информационных панелей, визуализирующих обработанную информацию. Эти панели не только показывают динамику и статистику дистанционных соединений, но и отображают структуру сети и её компоненты, что способствует улучшению

управления и понимания сетевыми ресурсами. Для повышения уровня безопасности рекомендуется использовать инструменты IDS/IPS для обнаружения и предотвращения вторжений, а также специализированные средства для выявления активности, свидетельствующей о несанкционированном доступе или отклонениях от нормы.

Для обеспечения безопасности сети и соблюдения политик важно регулярно проводить проверки и анализ данных сессий. Необходимо создать системы, которые будут автоматически блокировать подозрительные действия и интегрировать их с управлением инцидентами. Проект Remote Topology предлагает централизованный обзор удаленного доступа и активности в сети, что способствует повышению контроля над безопасностью сети.

4. Расшифровка данных, передаваемых по защищенным туннелям HTTP и HTTPS, представляет собой сложную задачу из-за встроенных функций безопасности. Однако, с применением определенных прокси-серверов, способных расшифровывать информацию, можно успешно обойти эту проблему. Процесс начинается с установки специального корневого сертификата компании на все устройства, подключенные к сети. После расшифровки информацию можно анализировать, классифицировать и повторно защищать шифрованием. Важно помнить о необходимости соблюдения юридических норм, политик безопасности и конфиденциальности, а также организации надежного аудита и контроля за всем процессом.

5. Для эффективной обработки информации, поступающей из запросов и ответов в режиме реального времени, необходимо использовать специальные приемы и стратегии:

1) Начнем с того, чтобы исследовать и анализировать данные, используя API для отслеживания активности информации.

2) Затем необходимо провести процесс синхронизации, включающий в себя применение специализированных инструментов для структурирования данных в рамках существующих систем.

3) В последующем этапе необходимо провести непосредственное исследование и обработку данных, применяя инструменты потокового анализа для обеспечения оперативности и точности.

На первом этапе проводится анализ, после чего следует этап документирования и сохранения информации. Важно обеспечить защиту данных в процессе их обработки и хранения, соблюдая нормативные требования. Затем систему необходимо развивать и адаптировать к растущим объемам данных, обеспечивая ее расширение. Наконец, последним шагом становится надзор, включающий системы наблюдения и реагирования на необычные ситуации.

Анализ данных и обучение моделей путем использования передовых технологий с целью выявления потенциальных рисков и закономерностей.

Вопреки тому, что маркировка сетевых потоков представляет собой ключевой инструмент для обеспечения высококачественного управления данными и повышения уровня безопасности, она сопровождается рядом сложностей. Эти сложности включают в себя задачи по интеграции многообразных систем и устройств, которые выполняют функции классификации и маркировки трафика, а также трудности, связанные с настройкой и обслуживанием политик качества обслуживания (QoS) в пределах сетевой инфраструктуры.

В современном мире, где передача информации занимает центральное место, использование маркировки сетевых потоков становится ключевым фактором для улучшения производительности сети. Этот метод не только способствует более эффективному распределению сетевых ресурсов, но и обеспечивает высокий уровень качества обслуживания, стабилизирует передачу данных и позволяет точно контролировать приоритетность различных потоков данных. В общем, маркирование потоков выступает как фундаментальный инструмент для усовершенствования данных и сетевых операций в эпоху, когда эффективность передачи информации становится критически важной.

ЛИТЕРАТУРА

1. Гетьман А.И., Евстропов Е.Ф., Маркин Ю.В. Анализ сетевого трафика в режиме реального времени: обзор прикладных задач, подходов и решений. – ИСПРАН, 109004, Россия, Москва, 2015. – С. 1–52.
2. Соколов И. А. и др. Проекты цифрового транспорта с глобальными навигационными спутниковыми системами – путь к построению интегрированных систем цифрового транспорта // International journal of open information technologies. – 2019. – Т. 7. – №. 1. – С. 49–77.
3. Знамени О. Т. К., Мусатов В. К. Разработка метода оценки показателей производительности межсетевых экранов при функционировании в условиях приоритизации трафика. – 2018. – Москва. – С.1–19.
4. Уймин А. Г. Автоматическое маркирование сетевого трафика браузера для анализа и классификациина примере платформы "Remotetopology" // T-Comm-Телекоммуникации и Транспорт. – 2022. – Т. 16. – № 12. – С. 17–22.