**Обеспечение сетевой безопасности совместно с брокерами сетевых пакетов. Пассивные средства безопасности.**

С ростом облачных вычислений и виртуализации современные компьютерные сети становятся всё более уязвимыми и постоянно развиваются, принося с собой новые риски и неопределённости. Давно прошли времена хакерства для удовольствия, хакеры финансово мотивированы и более изощрены, чем когда-либо. Некоторые из них создали хакерские группы, такие как LulzSec и Anonymous, чтобы обмениваться опытом и действовать сообща. Профессионалы информационной безопасности изо всех сил стараются не отставать, пытаясь использовать пассивные (для обнаружения) и активные (для блокировки) инструменты сетевой безопасности. Несмотря на то, что вендоры своевременно разрабатывают и предоставляют инструменты сетевой безопасности для защиты от новейших киберугроз, внедрение этих инструментов является постоянной проблемой по разным причинам. В этой серии публикаций мы опишем наиболее основные средства сетевой безопасности, которые борются с киберугрозами, рассмотрим типичные проблемы при развёртывании и пути их решения с помощью [брокеров сетевых пакетов](https://vk.com/away.php?to=https%3A%2F%2Fhabr.com%2Fru%2Fcompany%2Fdsol%2Fblog%2F490252%2F&cc_key=).

**Пассивные средства безопасности**

Пассивные средства сетевой безопасности применяются для мониторинга и анализа трафика в сети. Такие инструменты работают с копией трафика, полученной со SPAN-портов, ответвителей сетевого трафика (TAP) или брокеров сетевых пакетов (NPB). Пассивный мониторинг не вносит временных задержек и дополнительной служебной информации в сеть. В данное время широко используются такие пассивные средства безопасности, как IDS, Network Forensics, NBA и NTA.



**Система обнаружения вторжений (IDS)**

Система обнаружения вторжений (Intrusion Detection System - IDS) предназначена для мониторинга сетевого трафика на наличие вредоносных программ, эксплойтов и других киберугроз путём использования большого количества сигнатур угроз (иногда называемых правилами). Программное обеспечение IDS может быть развёрнуто на специально построенных устройствах, предоставленном пользователем оборудовании и в некоторых случаях как виртуальные устройства для VMware, Xen и других платформ виртуализации.

В настоящее время в подавляющем большинстве случаев IDS – это режим работы инструментов системы предотвращения вторжений (Intrusion Prevention System – IPS). Другими словами, на сегодняшний день приобрести решение, которое способно выполнять только пассивный мониторинг будет довольно проблематично. IPS относятся к более сложным и дорогим устройствам, однако, как правило, поддерживают активные IPS и пассивные IDS конфигурации в одном решении. Кроме того, компании обычно развёртывают IPS только для пассивного IDS мониторинга, особенно в ядре сети.

В пространстве IDS решений (как конфигурация пассивного мониторинга системы IPS) представлены продукты компаний Positive Technologies, Код Безопасности, Инфотекс, Smart-Soft, Info Watch, Stonesoft, Trend Micro, Fortinet, Cisco, HP, IBM, Juniper, McAfee, Sourcefire, Stonesoft, Trend Micro, Check Point.

**Сетевая форензика (Network Forensics)**

Сетевая форензика (криминалистика) относится к технологии, которая отслеживает, записывает и анализирует трафик компьютерной сети в целях сбора информации, юридических доказательств, а также обнаружения и анализа угроз внутрикорпоративной сетевой безопасности. Эта технология часто описывается как сетевой видеомагнитофон, который записывает (буквально) все пакеты, проходящие через вашу сеть. Программное обеспечение для сетевой криминалистики чаще всего развёртывается на поставляемых поставщиками сетевых устройствах с большими объёмами памяти, но некоторые поставщики предоставляют его как программное решение только для того, чтобы клиенты могли самостоятельно выбрать оборудование для его поддержки.

Производители решений в этом пространстве – MicroOLAP, Гарда Технологии, AccessData, NIKSUN, RSA (NetWitness), Solera Networks.

**Анализ поведения сети (NBA) и сетевого трафика (NTA)**

Большинство устройств сетевой безопасности размещаются по периметру (за межсетевым экраном) для проверки угроз, поступающих из интернета. Однако мобильные устройства, которые ежедневно приносятся в офис «в кармане», могут содержать вредоносные программы, которые защита периметра может никогда и не увидеть.

Системы анализа поведения сети (Network Behavior Analysis - NBA) обнаруживает угрозы, с которыми сталкивается сеть изнутри, используя NetFlow и другие стандарты потока (cFlow, sFlow, jFlow и IPFIX), чтобы получить базовое значение для нормального сетевого трафика и обнаружить аномалии, такие как распространение вредоносных программ. Системы анализа сетевого трафика (Network Traffic Analysis - NTA) предназначены для перехвата и анализа трафика, а также для обнаружения сложных и целевых атак. С их помощью можно проводить ретроспективное изучение сетевых событий, обнаруживать и расследовать действия злоумышленников, реагировать на инциденты. NTA могут служить отличным источником данных для ситуационных центров информационной безопасности (SOC).

Производители в пространстве NBA и NTA решений – Positive Technologies, Kaspersky, Group-IB, Гарда Технологии, Arbor Networks, Lancope, Riverbed Awake, Cisco, Darktrace, ExtraHop Networks, LogRhythm, Flowmon, RSA, TDS и другие.

**Типичные проблемы развёртывания систем сетевой безопасности**

ИТ-компании сталкиваются с многочисленными проблемами при развёртывании инструментов сетевой защиты, особенно в больших, сложных и географически распределённых сетях. Звучит знакомо? Ниже приведены кейсы, в которых распространённые проблемы систем мониторинга и информационной безопасности решаются с помощью внедрения [брокера сетевых пакетов (NPB)](https://vk.com/away.php?to=https%3A%2F%2Fhabr.com%2Fru%2Fcompany%2Fdsol%2Fblog%2F490252%2F&cc_key=).

**Кейс № 1. Оптимизация сетевой инфраструктуры информационной безопасности**

Современный подход к построению систем информационной безопасности ориентирован на надёжные и экономически эффективные решения, позволяющие уже внедрённым средствам безопасности отслеживать большее количество сегментов сети, повышая её видимость. При этом вновь внедряемые средства безопасности должны иметь доступ к существующим точкам съёма трафика.

Применяемые методы зеркалирования трафика с использованием SPAN-портов или ответвителей сетевого трафика (TAP) имеют свои ограничения и недостатки. Трафик SPAN-портов имеет низкий приоритет и, при повышении нагрузки на коммутаторе, начинает теряться, а при выставлении высокого приоритета, начинает теряться «боевой» трафик, что приводит к более опасным последствиям. Использование TAP позволяет иметь стопроцентную копию трафика, но здесь есть ограничение по количеству возможных точек установки TAP на сетевой инфраструктуре. При увеличении парка средств информационной безопасности, на каждое из которых нужно подавать трафик с одних и тех же сегментов сети, остро встаёт вопрос внедрения их в существующую инфраструктуру.



***Задача:****В компании, где внедрены системы обнаружения вторжений (IDS) и анализа поведения сети (NBA), разворачиваются системы Network Forensics и NTA. Для получения максимальной видимости трафика, съём осуществляется не через SPAN-порты, а через TAP. Трафик от TAP соответствующих сегментов сети необходимо доставить и распределить между четырьмя видами систем информационной безопасности.*

**Решение:**Данная задача легко решается брокером сетевых пакетов, используя который можно агрегировать трафик, полученный через TAP из сегментов сети, оптимизировать (применить функции фильтрации, классификации, дедупликации, модификации) и зеркалировать его, балансируя на соответствующие системы информационной безопасности.

**Кейс № 2. Оптимизация использования средств информационной безопасности**

Стандартные устройства сетевой безопасности поставляются с фиксированным количеством интерфейсов для осуществления одновременного мониторинга нескольких сегментов сети. Однако после того, как эти интерфейсы полностью заполняются, компании вынуждены покупать дополнительные единицы средств безопасности.



***Задача:****Компания имеет систему обнаружения вторжений (IDS) с четырьмя интерфейсами 10GbE. Трафик для мониторинга снимается с четырёх сегментов сети, при этом пиковая нагрузка на IDS не более 40%. Со временем инфраструктура сети увеличилась, и возникла необходимость дополнительно отслеживать два новых сегмента.*

**Решение:** С расчётом на дальнейшее развитие сети и отказа от закупки дополнительной IDS в виду 40% загрузки существующей системы, решать эту задачу рациональнее с помощью брокера сетевых пакетов. В данном случае использование пакетного брокера продиктовано еще и уменьшением проблем, связанных с решением вопросов выделения места в стойке, обеспечения электропитания и кондиционирования. Брокеры сетевых пакетов могут агрегировать трафик из нескольких сегментов сети, а затем оптимизировать (выполняя функции фильтрации, классификации, зеркалирования, балансировки, дедупликации, модификации) этот трафик перед маршрутизацией в IDS. Брокеры сетевых пакетов, как правило, дешевле средств обеспечения безопасности, что позволяет компаниям разумно использовать денежные средства и материальные ресурсы, одновременно повышая отказоустойчивость и производительность инструментов.

**Кейс № 3. Использование инструментов безопасности 1G в современных сетях**

Стандарт компьютерной сети 10-гигабитный Ethernet (10GbE или 10G) был впервые опубликован в 2002 году, но достиг критической массы к 2007 году. С тех пор 10G стал основой для крупных компьютерных сетевых инфраструктур и магистралей. Уже сейчас широко распространяются стандарты 40G/100G, а в недалёком будущем придут стандарты 200G/400G.

Практически каждая крупная компьютерная сеть имеет десятки, а то и сотни, инструментов мониторинга безопасности волоконной сети 1G. Эти устройства в зависимости от модели могут иметь возможность проверять более 1 Гбит/с трафика, но инструменты, оснащённые интерфейсами 1G, физически не могут подключаться к сетям 10G/40G/100G.



***Задача:****Компания модернизирует инфраструктуру сети для увеличения пропускной способности каналов внедрением нового сетевого оборудования и линий связи. На замену интерфейсам 1G приходят интерфейсы 10G/40G/100G. Существующая система информационной безопасности состоит из средств с интерфейсами 1G. Необходимо обеспечить функционирование существующей системы информационной безопасности на новой инфраструктуре.*

**Решение:** Брокеры сетевых пакетов решают эту задачу путем агрегирования, балансировки нагрузки и оптимизации трафика (минимизация нецелевого трафика и дедупликация) из сетей 10G/40G/100G в существующие инструменты безопасности 1G. Это решение не только продлевает срок службы существующих инструментов 1G (что откладывает расходы на их замену), но и максимизирует их производительность и отказоустойчивость.

Таким образом, применение брокеров сетевых пакетов решает следующие задачи:

* увеличение количества точек контроля/мониторинга;
* возможность подключения нужного количества средств контроля/мониторинга трафика;
* оптимизация использования средств информационной безопасности;
* исключение влияния средств ИБ на отказоустойчивость сети;
* обеспечение совместимости интерфейсов в инфраструктуре ИБ;
* повышение видимости сети для средств ИБ.

Из приведенных выше кейсов отлично видно, насколько просто решаются проблемы, так часто встречающиеся при построении систем информационной безопасности, выводятся на новый уровень механизмы доставки и повышения видимости трафика, повышается производительность и отказоустойчивость всей системы в целом при применении брокеров сетевых пакетов. В следующей части мы поговорим об активных средствах обеспечения сетевой безопасности, а также разберём типовые кейсы по их интеграции в сетевую инфраструктуру компании.