Сервер расширенного функционала BCOM-TA-ADV (BCOM-TA-vADV)

Общая информация



В современных сетевых архитектурах для обработки входящего трафика требуются многочисленные инструменты киберзащиты и мониторинга, получающие информацию от многих устройств видимости сети, включая TAP, порты SPAN и устройства BCOM-TA (BCOM TAP Aggregation). Объемы и разнообразие этого трафика могут значительно влиять на производительность этих инструментов. Дублированные пакеты могут перегружать приложения кибербезопасности и мониторинга до пределов их вычислительной мощности, тогда как пакеты с несколькими заголовками (например, MPLS, VLAN тегами, ERSPAN и т. д.) часто не распознаются этими инструментами и обычно отбрасываются.

Расширенные функции сетевой обработки, которые изначально связаны с процессорной мощностью, такие как дедупликация, потребляют много ресурсов центрального процессора и не должны выполняться на устройстве захвата или агрегации трафика. Сервер расширенного функционала BCOM-TA-ADV является пакетным брокером нового поколения за счет использования передового, высокопроизводительного, модульного и масштабируемого оборудования ODM, которое можно настроить в соответствии с пропускной способностью сети. Этот уникальный подход устраняет ограничения производительности оборудования и позволяет выполнить самые высокие требования к оборудованию и производительности.

Сервер расширенного функционала BCOM-TA-ADV - единственный пакетный брокер на рынке, который предлагает сетевые интерфейсы 100G в компактном форм-факторе 1U. Устройство основано на мощном сверхплотном, надежном и универсальном стоечном сервере высотой 1U, который можно масштабировать с использованием дополнительных вычислительных мощностей и памяти в соответствии с задачами, выполняемыми пакетным брокером.

Образ ПО BCOM-TA-vADV для развёртывания в виртуальных средах позволяет выполнять задачи по фильтрации, агрегации, обработке трафика в сценариях, когда применение аппаратного решения невозможно или нецелесообразно.

Преимущества

- Доступный брокер сетевых пакетов с высокой производительностью
- Мощная и масштабируемая серверная архитектура, которая отвечает требованиям производительности
- Агрегация, фильтрация, удаление заголовков, дедупликация, маскирование данных, обрезка размера пакета, вставка временных меток, захват трафика, дефрагментация, белые и черные списки, фильтрация на основе URL, строк и регулярных выражений, Net-Flow/IP-FIX
- Масштабируемость решения (серверная платформа с гибкими конфигурациями, которые отвечают требованиям к производительности)
- ПО, адаптированное для быстрого развёртывания в виртуальных средах

- Широкий выбор трансиверов, оптики и кабелей, поддерживающих интерфейсы 1G, 10G, 25G, 40G, 100G
- Агрегация и перенаправление сетевого трафика с выбранных входных портов на выходные порты для дальнейшей обработки
- Оптимизация производительности инструментов за счет исключения из обработки ненужного сетевого трафика с использованием условной фильтрации по MAC-адресам, Ether-Type, IP-адресам, TCP портам, UDF), белых/черных списков и расширенной фильтрации на уровне строки / URL / регулярных выражений
- Отслеживание пути пакета за счет добавления тега VLAN, указывающего его входной порт (маркировка портов)
- Сокращение требуемых ресурсов инструментов агрегирования и фильтрации за счет удаление заголовков протоколов MPLS, VLAN, PPP, QinQ, VN-TAG, GRE, GTP, ERSPAN, VxLAN, GENEVE, PBB, Cisco Fabric
- Максимальное повышение производительности инструмента за счет исключения дублированных пакетов, собранных из нескольких точек сбора (дедупликация)
- Защита конфиденциальных данных путем их перезаписи перед отправкой в инструменты (маскирование данных)
- Повышение эффективности мониторинга и анализа сетевых данных за счет уменьшения размера пакета и сохранения только необходимого фрагмента пакета для дальнейшей обработки
- Повышение видимость сети за счет возможности вставки временных меток на уровне наносекунд
- Запись трафика в формате PCAP в соответствии с фильтром для дальнейшего анализа
- Сбор фрагментов пакета в цельный пакет (дефрагментация)
- Генерация Net-Flow или IP-FIX для приложений мониторинга и безопасности
- Выполнение глубокой инспекции пакетов и идентификации тысячи протоколов на Уровне 7
- Репликация трафика, позволяющая нескольким инструментам производить анализ одного и того же трафика
- Фильтрация по параметрам внутреннего туннеля (GTP, VxLAN, L2TP)
- Обеспечение связности пакетных брокеров на нескольких площадках с помощью протоколов L3GRE и NVGRE
- Отслеживание пакетов, соответствующие определенному «окну» во входящем трафике
- Распределение трафика между несколькими инструментами анализа для сокращения числа требуемых лицензий (подписок) средств кибербезопасности и мониторинга
- Генерация метаданных для серверов Syslog
- Управление Web UI, CLI, SNMP, Netconf, REST API

Сценарии использования

- Удаление дублированных пакетов для оптимизации производительности приложений безопасность и мониторинг
- Расширение возможностей пакетного брокера
- Единое устройство с базовым и расширенным функционалом пакетного брокера
- Удаление меток MPLS для мониторинга сетей MPLS
- Маскирование конфиденциальной и частной информации о клиентах
- Обеспечение видимости сети для виртуального сетевого трафика
- Перенаправление виртуального сетевого трафика на инструменты мониторинга в физических и / или виртуальных средах

- Возможность использование инструментов физического мониторинга при миграции в виртуальные среды
- Оптимизация использования инструментов виртуального и физического мониторинга за счет фильтрации данных
- Обеспечение баланса между физическими и виртуальными инструментами мониторинга

Информация для заказа

Наименование	Описание
B4T-TA-ADV-50-HW	Сервер расширенного функционала BCOM-TA-ADV с предустановленным ПО BCOM-TA-ADV (Сетевые интерфейсы 4*10/25G или 2*100G)
B4T-TA-ADV-50-SW	Лицензия на ПО расширенного функционала BCOM-TA-ADV для сервера ADV-50. Производительность до 50 Гбит/с
B4T-TA-vADV-10-SW	Лицензия на ПО расширенного функционала BCOM-TA-ADV (BCOM-TA-vADV) для развертывания в виртуальных средах. Производительность до 10 Гбит/с
B4T-SUP-TA-ADV-50-HW1	Сервисная техническая поддержка для сервера B4T-TA-ADV-50-HW, 1 год
B4T-SUP-TA-ADV-50-HW3	Сервисная техническая поддержка для сервера B4T-TA-ADV-50-HW, 3 года
B4T-SUP-TA-ADV-50-HW5	Сервисная техническая поддержка для сервера B4T-TA-ADV-50-HW, 5 лет
B4T-SUP-TA-ADV-50-SW1	Сервисная техническая поддержка ПО BCOM-TA-ADV, 1 год
B4T-SUP-TA-ADV-50-SW3	Сервисная техническая поддержка ПО BCOM-TA-ADV, 3 года
B4T-SUP-TA-ADV-50-SW5	Сервисная техническая поддержка ПО BCOM-TA-ADV, 5 лет
B4T-SUP-TA-vADV-10-SW1	Сервисная техническая поддержка ПО BCOM-TA-ADV (BCOM-TA-vADV), 1 год
B4T-SUP-TA-vADV-10-SW3	Сервисная техническая поддержка ПО BCOM-TA-ADV (BCOM-TA-vADV), 3 года
B4T-SUP-TA-vADV-10-SW5	Сервисная техническая поддержка ПО BCOM-TA-ADV (BCOM-TA-vADV), 5 лет