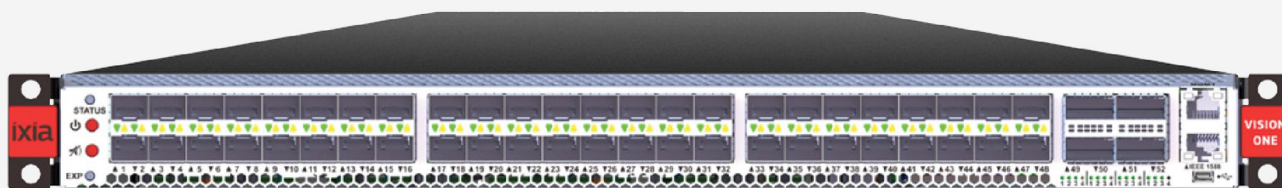


# ВЫСОКОПРОИЗВОДИТЕЛЬНЫЙ ИНТЕЛЛЕКТУАЛЬНЫЙ БРОКЕР СЕТЕВЫХ ПАКЕТОВ



Брокер сетевых пакетов Vision ONE компании Ixia гарантирует полную видимость сетевого трафика для устройств информационной безопасности (ИБ), что является необходимым условием надежной защиты сети. В этом брокере компания Ixia сконцентрировала самые передовые возможности контроля трафика, включая возможности процессора Ixia ATI (Application and Threat Intelligence). Среди них – дешифровка трафика SSL с учетом состояния сеансов (stateful) и глубокий анализ пакетов (DPI), выходящий далеко за рамки простой проверки совпадения с регулярным выражением и обеспечивающий точную идентификацию трафика приложений. Также Vision ONE выполняет различные функции обработки пакетов (например, их дедупликацию, усечение (trimming), снабжение временными метками) и балансировку нагрузки на включаемые в разрывы линий связи (inline) устройства ИБ (межсетевые экраны, IPS и др.). Данный брокер может работать как с inline-устройствами, так и с внеполосными (out-of-band) устройствами ИБ или мониторинга (IDS, устройства записи сетевого трафика и др.) одновременно.

## Основные достоинства Vision ONE

- **Отказоустойчивая установка inline-устройств ИБ.** Благодаря этому, пользователи могут устанавливать системы IPS, устройства DLP и подобные средства, не создавая угрозы потери доступа к сетевым сервисам в случае отказа этих inline-устройств.
- **Эффективное обнаружение скрытых угроз.** Обеспечивается дешифровкой SSL-трафика и отправкой расшифрованного текстового контента на одно или несколько устройств анализа трафика.
- **Обработка пакетов без их потерь.** Для повышения эффективности использования устройств ИБ и других анализирующих трафик средств Vision ONE выполняет функции AFM, включая дедупликацию и усечение пакетов, а также удаление их заголовков. Благодаря аппаратной реализации этих функций, обработка пакетов выполняется на полной линейной скорости портов без потерь пакетов.

- **Точная идентификация трафика приложений.** Реализуется с помощью функционала DPI, который также позволяет классифицировать трафик на основе географического расположения (например, можно отбирать трафик, поступающий из определенного региона) и данных о мобильном устройстве. Имеется возможность генерации записей NetFlow.
- **Экономичная масштабируемость.** Обеспечивается функционалом балансировки нагрузки, дающим возможность постепенно наращивать производительность системы анализа трафика, не переходя на более высокопроизводительные устройства анализа.
- **Экономия стоечного пространства** – благодаря малой высоте корпуса, равной 1U.
- **Уменьшение риска, связанного с переходом на виртуализированные среды.** Возможно объединение трафика, поступающего от физических и виртуальных (vTap) ответвителей, что позволяет получить полную картину функционирования сети.
- **Оптимизированная многопользовательская работа.** Ролевой контроль доступа, самый простой в отрасли графический пользовательский интерфейс и эффективный компилятор фильтров гарантируют, что пользователи не будут мешать друг другу, одновременно работая с данным устройством.

## Спецификация

### Гибкость использования портов

- 4 порта 40GbE QSFP+, могут быть сконфигурированы как 16 портов 10GbE.
- Все порты двунаправленные и не блокируемые.
- Обработка пакетов на полной линейной скорости на всех портах.
- Фильтрация пакетов по содержимому их заголовков L2–L4:
  - L2: MAC, VLAN, MPLS или Ethertype.
  - L3: адреса источника, назначения IPv4 или IPv6, DSCP, IP-протокол.
  - L4: номера портов, TCP Control.
- Возможно подключение inline- и out-of-band-устройств.

### Интеллектуальная обработка пакетов на полной линейной скорости

- Модифицирует каждый пакет на полной линейной скорости, выполняя функции Advanced Feature Module (AFM) – дедупликацию, удаление заголовка, усечение пакета, прикрепление временной метки, защиту порта 1GbE от всплесков трафика и маскирование данных.
- Может гибко распределять общую пропускную способность 160 Гбит/с между портами, выделяя ее частями по 10 Гбит/с.



## Работа с inline-устройствами

- Поддерживает параллельное (для балансировки нагрузки) и последовательное подключение inline-устройств, а также любые комбинации этих видов подключения.
- Для выявления отказавших inline-устройств с целью автоматического преодоления отказов используются одноуровневая (single-stage) и многоуровневая (multi-stage) передача heartbeat-пакетов.
- Два режима преодоления отказа:
  - Перераспределение сессий с отказавшего inline-устройства по всем активным inline-устройствам.
  - Переключение всех активных сессий с отказавшего inline-устройства на резервное inline-устройство.

## Возможности процессора Ixia ATI (Application and Threat Intelligence)

- Реализует функционал DPI для классификации трафика по типу приложения, географическому расположению, информации об устройстве и сервис-провайдере.
- Регулярное обновление сигнатур приложений посредством подписки на сервис ATI.
- Дешифровка трафика SSL. Поддерживаемые шифры:
  - 3DES,
  - RC4,
  - AES,
  - SHA1/521/384/256/224,
  - MD5.
- Поддержка дешифровки SSL/TLS:
  - Версии SSL/TLS: SSL3.0, TLS1.0, TLS1.1 и TLS1.2.
  - Обмен асимметричными ключами: RSA и ECDH.
  - Симметричные ключи: AES, 3DES и RC4.
  - Алгоритмы хэширования: SHA и MD5.
  - Максимальное число одновременных сессий: более 1 000 000.
  - Хранение частного ключа: в зашифрованном виде с атрибутом write only.
- Проверка совпадения с регулярным выражением.
- Маскирование данных для защиты секретных сведений, например данных, обеспечивающих идентификацию личности, или информации о номерах кредитных карт.
  - Целевое поле идентифицируется с помощью заданного пользователем регулярного выражения.
  - Имеются заданные по умолчанию регулярные выражения для маскирования данных, которых чаще всего требуется скрывать (например, номеров кредитных карт).
- Может быть выполнено множество операций над сессиями, соответствующими правилам отбора трафика.
  - Передача всех соответствующих пакетов на устройство анализа трафика.
  - Генерация записей Enhanced NetFlow v9/v10 и IPFIX для отправки их на некоторое число (до 10) коллекторов.
  - Простое ценообразование с подпиской на ATI, обеспечивающей обновление функционала и сигнатур приложений.

### Управление

- Поддержка SNMP v1, v2 и v3.
- Возможность временной синхронизации с использованием протокола PTP (Precision Time Protocol).
- Поддержка локальной аутентификации, а также аутентификации по протоколам RADIUS и TACACS+.
- Гибкие функции контроля доступа.
- Мониторинг и протоколирование событий.
- Syslog.
- Возможность автоматизации управления посредством RESTful API.

### Электропитание

- Два заменяемых в «горячем» режиме блока питания переменного или постоянного тока.
- Напряжение питания:
  - переменное: 100...240 В;
  - постоянное: 40...60 В.
- Номинальный потребляемый ток:
  - 1,5 А при переменном напряжении 240 В;
  - 12,5 А при постоянном напряжении 53 В.
- Максимальный потребляемый ток:
  - 7,7 А при переменном напряжении 100 В;
  - 19,25 А при постоянном напряжении 40 В.
- Тепловыделение при 100%-ной нагрузке трафиком: 660 Вт/2252 BTU/ч.

### Механические характеристики

- 19-дюймовое шасси высотой 1U.
- Габаритные размеры (Ш x Д x В): 445 x 750 x 45 мм.
- Масса: 16,5 кг.



Группа компаний БАКОТЕК – официальный дистрибьютор Ixia в Украине, Республике Беларусь, Азербайджане, Грузии, Армении, Казахстане, Кыргызстане, Молдове, Таджикистане, Туркменистане и Узбекистане.  
[www.bakotech.com](http://www.bakotech.com), [ixia@bakotech.com](mailto:ixia@bakotech.com), +38 044 273 33 33.

#### IXIA WORLDWIDE

26601 W. AGOURA ROAD  
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)

1.877.367.4942

(OUTSIDE NORTH AMERICA)

+1.818.871.1800

(FAX) 818.871.1805

[www.ixiacom.com](http://www.ixiacom.com)

#### IXIA EUROPE

CLARION HOUSE, NORREYS  
DRIVE MAIDENHEAD SL6 4FL  
UNITED KINGDOM

SALES +44.1628.408750

(FAX) +44.1628.639916

#### IXIA ASIA PACIFIC

101 THOMSON ROAD,  
#29-04/05 UNITED SQUARE,  
SINGAPORE 307591

SALES +65.6332.0125

(FAX) +65.6332.0127