Технологии кибербезопасности в эпоху IoT

Юрий Широков

С наступлением эры IoT защита от киберугроз и управление сетевой инфраструктурой становятся крайне актуальными задачами. Компания ADLINK предлагает оптимизированную концепцию модульного построения сетевых защитных устройств, повышающую эффективность разработки пользовательских приложений, а также снижающую стоимость их эксплуатации и модернизации.

Мы вступаем в эру Интернета вещей (Internet of Things – IoT), в которой все вещи и устройства будут связаны с сетями Интернет. Сетевой трафик, генерируемый устройствами IoT, также быстро растёт и вследствие расширения диапазона приложений и используемых IoT-устройств становится всё более и более сложным. В то же время всё большее распространение получают облачные вычисления. Ключевой характеристикой облачных вычислений является распределение вычислительных ресурсов по требованию, позволяющее использовать их более эффективно и с меньшими затратами, что приводит к растущей популярности данной концепции среди корпоративных клиентов. Мультитенантная (единая, разделяемая многими пользователями) среда облачных вычислений, а также постоянное создание, миграция и уничтожение виртуальных машин в процессе выполнения запросов на распределение ресурсов приведёт к новым угрозам физической безопасности. Обеспечение безопасности облачных вычислений в эпоху IoT станет огромным вызовом, поскольку традиционные устройства обеспечения безопасности базируются на идее физического разграничения доступа и имеют незначительную динамическую адаптивность, что делает их мало применимыми в среде облачных вычислений. Но в отношении построения оборудования для обеспечения безопасности сети, отвечающего требованиям облачных вычислений, промышленность всё же достигла некоторого прогресса. Например, технология глубокого анализа пакетов (DPI – Deep Packet Inspection) может использоваться для идентификации информации о пользователях и приложениях, породивших сетевой трафик, что даёт возможность точно контролировать поток трафика в сети. Технология программно-определяемых сетей (SDN – Software-Defined Networking) может быть использована для реализации программируемого сетевого трафика, обеспечивая перенаправление трафика и автоматизацию соблюдения безопасности в соответствии с определёнными политиками. Технологию виртуализации сетевых функций (NFV – Network Functions Virtualization) можно использовать для реализации пулов ресурсов безопасности, обеспечивающих общий механизм безопасности для всех пользователей сети. Итак, для эффективной борьбы с угрозами сетевой безопасности в эру IoT следующее поколение оборудования для сетевой безопасности должно быть построено с использованием всех перечисленных технологий.

Унификация DPI – путь к оптимизации

Благодаря массовому росту использования мобильного Интернета выручка от услуг передачи данных составляет всё бóльшую долю от общего дохода операторов связи, которые поэтому придают существенное значение работе служб, связанных с данными. DPI как технология визуализации сетевого трафика стала фундаментальным элементом телекоммуникационной инфраструктуры. После внедрения DPI оператор связи может оптимизировать свой бизнес для предоставления конкретных услуг, а также разрабатывать новые услуги с добавленной стоимостью на основе идентификации пользователей и реализовать защиту сетей гораздо более эффективным образом. До того как была предложена унифицированная концепция развёртывание оборудования DPI осуществлялось с помощью самых разнообразных приложений, к которым было тесно привязано оборудование. По мере увеличения числа приложений DPI в сетях требовалось развёртывать всё больше и больше соответствующего оборудования. Таким образом, унифицированная концепция DPI была предложена с целью сокращения затрат на инвестиции, возникающие в результате многократного дублирования оборудования DPI, благодаря его совместному использованию посредством стандартизации визуализации сетевого трафика. При координации развёртывания оборудования DPI, с точки зрения всей сети, требования DPI унифицируются в ключевых точках сети, а службы DPI совместно используются несколькими приложениями DPI через набор унифицированного серверного API (Application Programming Interface – интерфейс прикладного программирования). Как показано на рис. 1, благодаря совместному использованию оборудования DPI в ключевых точках телекоммуникационной сети унифицированная технология DPI уменьшает дублирование развёртывания оборудования, позволяет оборудованию и при-

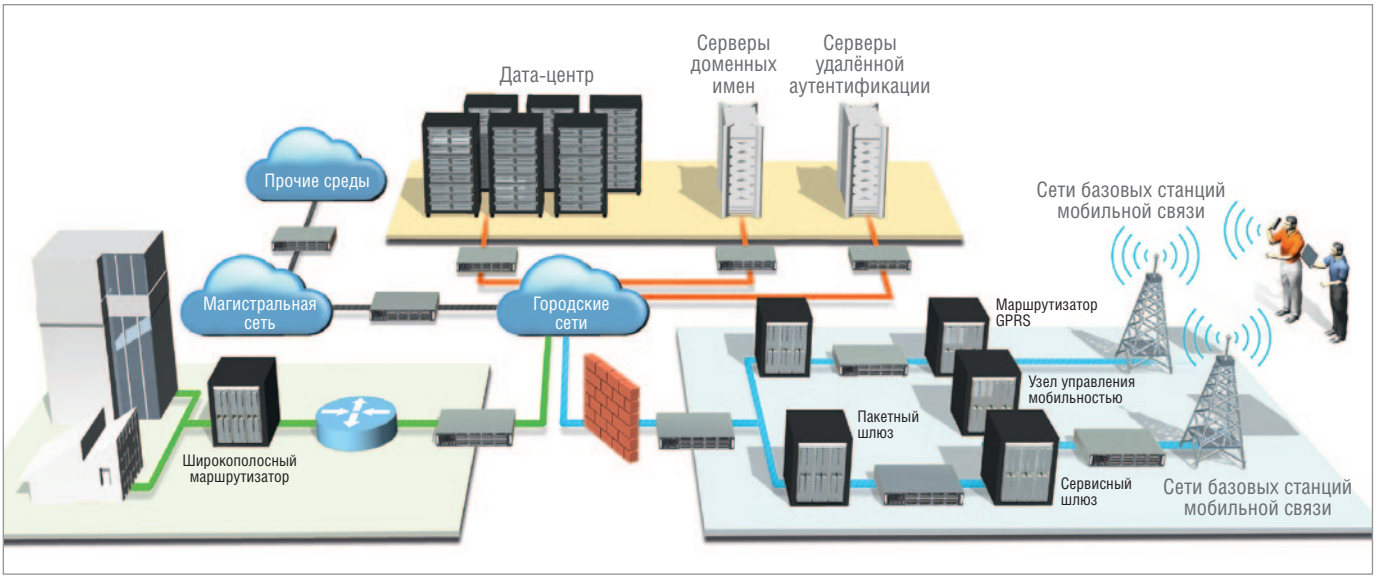

Рис. 1. Структура современных сетей передачи данных

ложениям DPI развиваться независимо друг от друга и значительно расширяет возможности для внедрения приложений DPI. В следующих разделах статьи требования к унификации оборудования DPI будут проанализированы с разных точек зрения.

Производительность важна

В настоящее время сети 4G обеспечивают достаточную пропускную способность для тысяч постоянно меняющихся мобильных приложений, а также многочисленных приложений для социальных сетей, всё больше и больше насыщаемых различными функциями. Однако с подключением к телекоммуникационной сети огромного количества IoT-устройств типы сетевого трафика станут ещё разнообразнее. Ценность вклада оборудования DPI в основном зависит от того, сколько типов трафика оно может идентифицировать. Это является основой всех новшеств в приложениях DPI верхнего уровня. Аналитические возможности оборудования DPI зависят от программного обеспечения и в ещё большей степени – от вычислительной производительности аппаратной платформы DPI. Только высокая производительность вычислений может гарантировать, что оборудование DPI сможет идентифицировать больше типов трафика в режиме реального времени.

Для решения проблем безопасности в мультитенантной среде широко используются технологии туннелирования, такие как VXLAN (Virtual Extensible LAN – виртуальная расширяемая локальная сеть). VXLAN – это технология инкапсуляции, которая переупаковывает фреймы Ethernet 2-го уровня OSI (уровень данных) в протокол UDP (User Datagram Protocol – протокол пользовательских датаграмм) 4-го уровня (транспортный уровень) и таким образом помогает преодолеть ограничения размеров таблицы MAC и пространства идентификаторов VLAN ID. Поскольку устройства сетевой безопасности часто связаны в единую цепочку, для обработки проходящего через них сетевого трафика все они должны поддерживать VXLAN. Удаление и добавление заголовков VXLAN требует значительных ресурсов процессора и существенно снижает общую производительность сетевого защитного оборудования. Решение этой проблемы заключается в использовании дополнительного аппаратного ускорения. Кроме того, для повышения безопасности облачных вычислений всё более широко используются технологии шифрования. Как и в VXLAN, процесс шифрования сетевого трафика также потребляет значительные ресурсы ЦПУ и может быть реализован с помощью дополнительных аппаратных блоков. Когда процессор избавлен от этих ресурсоёмких задач, он может сосредоточиться на ключевой задаче DPI более эффективно и результативно.

Гибкость не противоречит унификации

В целях абстрагирования приложений DPI верхнего уровня от оборудования DPI нижнего уровня и для обеспечения требуемого масштаба развёртывания и совместимости приложений DPI с различным аппаратным обеспечением унифицированный интерфейс DPI определяет требования к поддержке аппаратного интерфейса. В зависимости от места развёртывания в телекоммуникационной сети оборудование DPI нуждается в поддержке входящего/исходящего сетевого трафика в сетях 1G/10G WAN/LAN, 2.5G/10G POS или 100 GbE. Для работы оборудования DPI в составе сети необходимые сетевые интерфейсы должны быть встроены в него непосредственно, а реализация с использованием внешних сплиттеров, коммутаторов или преобразователей протоколов запрещена, чтобы исключить дополнительный риск от добавленных устройств. Следовательно, помимо обеспечения достаточного количества входных/выходных портов и полосы пропускания обработки унифицированное оборудование DPI также должно обеспечивать гибкую конфигурацию сетевого ввода-вывода, то есть требуется возможность выбора соответствующих интерфейсных модулей для адаптации к различным местоположениям развёртывания.

Поддержка SDN

Для поддержки различных приложений DPI верхнего уровня унифицированное оборудование DPI должно обеспечивать не только общую идентификацию протоколов и статистические функции, но и строгую логику управления потоком. Для реализации детального управления трафиком, необходимого приложениям верхнего уровня, оборудование DPI должно поддерживать управление потоком на основе идентифицированного сетевого трафика, а также гарантировать минимальную пропускную способность, возможности ограничения максимальной пропускной способности, пропуска и блокиро-

вания потоков. Для приложений сетевой безопасности важно также, чтобы оборудование DPI поддерживало параметры белого и чёрного списков на основе метаданных потока, таких как адрес источника, адрес назначения, номер протокола, порт источника, порт назначения, имя домена, идентификатор пользователя. Если эти функциональные требования реализуются с помощью традиционных методов, не только функциональная реализация становится непрозрачной, но также значительно ограничиваются и возможности для последующей модернизации. Для классификации потока трафика на основе многомерных метаданных может быть использована технология SDN. Промышленность пытается внедрить технологию SDN, с помощью которой можно установить различные стратегии управления потоком данных, для преодоления трудностей размытия границ безопасности в виртуализированной среде. SDN может направлять целевой сетевой трафик на устройство виртуальной сетевой безопасности путём перенаправления и агрегирования потока. И когда виртуальная машина мигрирует, технология SDN с её глобальной гибкостью и программируемостью может помочь реализовать автоматическую миграцию соответствующих сетевых политик безопасности. Когда логика службы DPI построена на основе архитектуры SDN, становятся доступны не только функции анализа DPI, а ещё и статистика, управление, мультиплексирование и централизованное управление безопасностью.

Доступность «пять девяток»

Итак, оборудование DPI как элемент телекоммуникационной сети будет становиться всё более и более важным. Как и в других частях телекоммуникационной инфраструктуры, унифицированное оборудование DPI должно обеспечить доступность 99,999%. Для этого основные сервисные компоненты оборудования DPI, такие как вычислительные и коммутационные блоки, должны обеспечивать соответствующее «горячее» резервирование. Такие компоненты системы, как блоки питания и вентиляторные модули, должны обеспечивать соответствующую избыточность и поддержку онлайн-замены в случае сбоев. Кроме того, для оборудования DPI, которое необходимо объединить в цепочку, должен быть обеспечен обход в случае потери питания или сбоя. В таких ситуациях канал связи, обеспечивая непрерывность обслуживания, может автоматически переключиться от основного блока к блоку байпаса.

Модульность и масштабируемость

Данные порождаются пользователем, а затем последовательно передаются через локальную сеть доступа, глобальные, региональные и магистральные сети. Поэтому трафик можно контролировать, если оборудование DPI установлено в ключевых точках сетевой инфраструктуры, через которые проходят данные. Согласно унифицированной спецификации DPI от China Mobile, эти ключевые точки развёртывания можно определить так: сторона пользователя, транзит через глобальную сеть, транзит через региональную сеть и межсетевой трафик. Требуемые внешние сетевые интерфейсы, как и объёмы сетевого трафика, в этих ключевых точках различны, поэтому одно устройство не сможет оптимально удовлетворить различным требованиям во всех точках развёртывания. Однако, чтобы уменьшить общую стоимость владения и резервные мощности для модернизации на будущее, очень многие поставщики услуг DPI всё же предпочли бы одну масштабируемую платформу, которая сможет работать с большинством сценариев развёртывания. Методология решения этой дилеммы заключается в принятии модульного аппаратного дизайна и поддержке линейного расширения для вычислительных блоков.

Платформы сетевой безопасности ADLINK Technology

Компания ADLINK предприняла большие усилия для полного понимания требований DPI и безопасности облачных вычислений в эпоху IoT и представила серию компьютерных платформ CSA, удовлетворяющих этим требованиям. Благодаря интеграции высокопроизводительных возможностей обработки DPI и поддержке NFV, SDN и аппаратных ускорителей серия продуктов CSA создаёт хорошую основу для разработки следующего поколения сетевых защитных систем. Требования к производительности оборудования унифицированных DPI для телекоммуникаций или облачных вычислений растут. В то же время ожидается, что на оборудовании DPI для повышения его функциональности и адаптивности будет поддерживаться SDN. Кроме того, существует тенденция к стандартизации вычислительных платформ на основе продуктов COTS (Commercial off the Shelf – готовый коробочный продукт). Серия продуктов CSA (Cyber Security Appliance) компании ADLINK разработана и построена с учётом этих тенденций. Благодаря интеграции специальных требований следующего поколения устройств сетевой безопасности на открытых вычислительных платформах платформы CSA помогут провайдерам сетевой безопасности в создании сервисов, соответствующих требованиям безопасности DPI и облачных вычислений в эпоху IoT.

OCCERA от ADLINK

Открытая вычислительная базовая эталонная архитектура OCCERA (Open Computer Carrier-grade Edge Reference Architecture) обеспечивает распределение ресурсов по требованию для удовлетворения ключевых потребностей облачных вычислений. Облачные вычисления требуют модернизации оборудования ИКТ (информационных и коммуникационных технологий) в соответствии с недавними техническими достижениями в области мобильного Интернета, центров обработки данных и обработки больших данных. Облачные вычисления становятся основной моделью предоставления услуг будущего, в результате чего рынок традиционных ИКТ претерпевает огромные изменения. Конструкция традиционного оборудования ИКТ обычно основывалась на старой методологии проектирования, которая объединяла вычислительные ресурсы, ресурсы хранения и ввода-вывода в единый физический объект в соответствии с начальными максимальными требованиями. Это часто требовало переделки существующего оборудования для адаптации к требованиям нового прикладного устройства, иногда ради совсем незначительных изменений. Модульность построения устройств по концепции OCCERA проиллюстрирована на рис. 2. Основной концепцией облачных вычислений является предоставление ресурсов по требованию. Это означает, что вычислительные ресурсы, ресурсы хранения и ввода-вывода можно гибко комбинировать для удовлетворения требований приложения. Для реализации концепции необходимо, чтобы вычисления, хранение и ввод-вывод были разделены на независимые функцио-

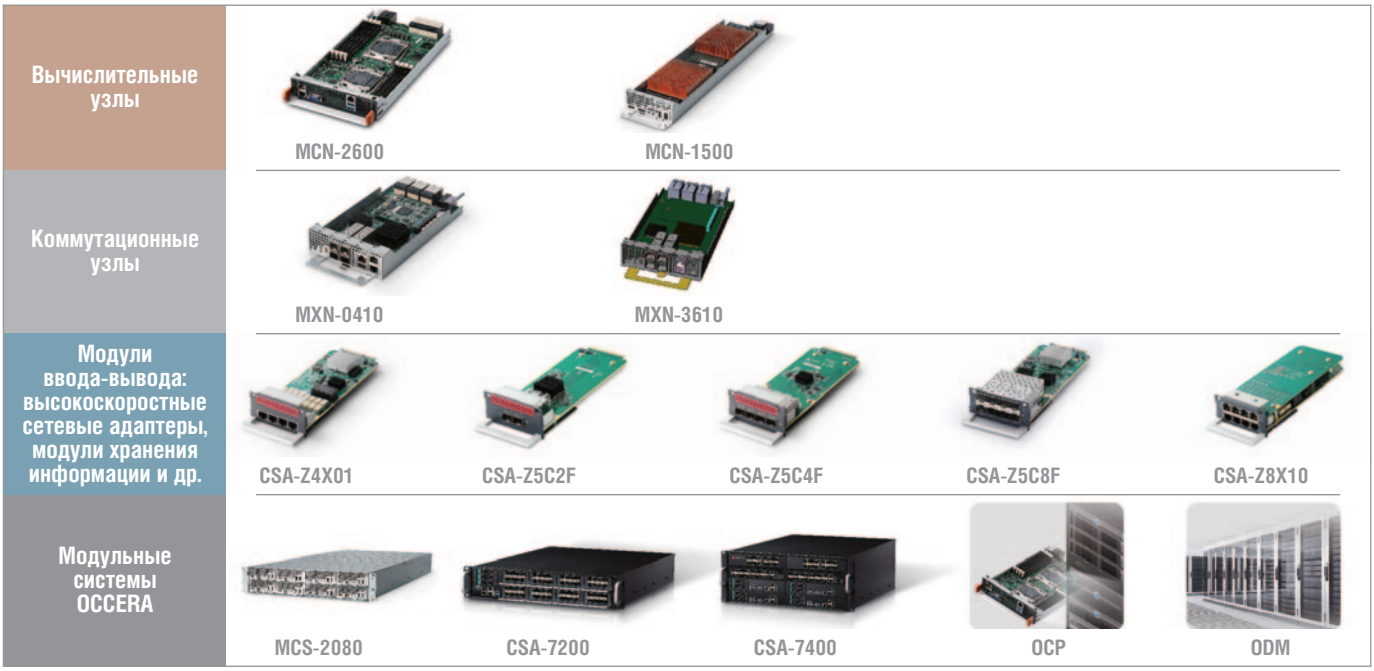

Рис. 2. Модульная платформа OCCERA

нальные модули ещё на стадии проектирования. Затем, исходя из требований конкретного приложения, эти независимые функциональные модули компонуются и объединяются в конкретный аппаратный объект. Архитектура OCCERA от ADLINK Technology была создана для реализации этой концепции. Она ассимилировала новейшие технологии Интернет-центров обработки данных, особенно последние достижения в области NFV и SDN, обеспечив возможности преобразования вычислительной инфраструктуры ИКТ и плавного перехода к OCP. В то же время OCCERA интегрировала и аспекты традиционного промышленного вычислительного оборудования, такие как модульные архитектуры, аппаратное ускорение и стандарты проектирования операторского уровня. OCCERA позволяет применять новейшие технологии NFV и SDN к промышленным вычислениям, сохраняя при этом ключевые функции традиционных промышленных вычислений, давая возможность поставщикам видео, сетевой безопасности и телекоммуникационного оборудования легко и эффективно вступить в эру облачных технологий.

В табл. 1 перечислены требования следующего поколения DPI и облачных вычислительных продуктов безопасности в левой колонке и соответствующие им функции, реализованные на продуктах линейки CSA в правой колонке. Для обеспечения высокой пропускной способности, требуемой для продуктов сетевой безопасности следующего поколения, а также поддержки новейших от-

Таблица 1

Требования к оборудованию сетевой безопасности и соответствующие свойства продуктов серии CSA

Требования к оборудованию сетевой защиты	Возможности продуктов CSA
Обеспечение высокопроизводительной аналитики DPI для визуализации сетевого трафика	Продукты серии CSA имеют дизайн с высокой плотностью, что позволяет вдвое увеличить вычислительную плотность обычного стоечного сервера. Новейшее программное обеспечение Intel® DPDK, Open vSwitch (OVS) и ПО nDPI интегрировано в продуктах CSA с ПО ADLINK PacketManager, которое оптимизирует среду выполнения и помогает достичь пропускной способности данных, в 10 раз превышающей пропускную способность стандартной среды Linux
Обеспечение гибких сетевых операций ввода-вывода для адаптации к различным сценариям приложений	Продукты CSA среднего уровня имеют модульную конструкцию ввода-вывода, что позволяет пользователям выбирать разные платы ввода-вывода для комплектации необходимых портов и обеспечения пропускной способности. Продукты CSA высшего уровня обеспечивают двойное 64G-соединение между всеми узлами ЦП через встроенный высокопроизводительный коммутатор, который также поддерживает 64 порта 10G каскадных линий связи и может поддерживать другие типы портов каскадных линий связи путём настройки мезонинной платы ввода-вывода
Поддержка технологии NFV для обеспечения распределения ресурсов безопасности по требованию	Продукты CSA реализуют новейшие технологии виртуализации от Intel, включая VT-x, VT-d, VT-c и PCIe SR-IOV, что обеспечивает отличную производительность виртуализации. Кроме того, для обеспечения работы платформы NFV под ключ Intel® ONP и Wind River Titanium Server также интегрированы и проверены на продуктах CSA
Поддержка технологии SDN для обеспечения управления потоками данных	Вычислительные узлы продуктов CSA поддерживают Open vSwitch с Data Plane Development Kit (OvS-DPDK) и протокол OpenFlow. Узлы коммутатора используют микросхему коммутатора с непосредственной обработкой потока, что обеспечивает большую гибкость для включения различных агентов SDN
Обеспечение технологии инкапсуляции VXLAN и криптооборудования для освобождения ресурсов ЦП	Сетевые средства ввода-вывода и коммутационные узлы продуктов CSA имеют встроенные модули аппаратного ускорения для VXLAN, перегрузки сегмента TCP (TSO), перегрузки контрольной суммы IP и т.д. Требования к шифрованию и дешифрованию также могут быть достигнуты путём расширения с помощью модулей Intel® QAT и FPGA на зарезервированном порте PCIe
Модульная конструкция, поддержка линейной масштабируемости и высокая доступность операторского уровня	Продукты CSA доступны в различных форм-факторах (1U, 2U и 4U) и обеспечивают модульность и масштабируемость благодаря архитектуре OCCERA для адаптации к различным потребностям развёртывания. Продукты ADLINK CSA также обеспечивают путь эволюции к OCP и поддерживают линейную масштабируемость при развёртывании центров обработки данных. Более того, продукты CSA могут соответствовать требованиям высокой доступности телекоммуникационных приложений благодаря избыточным конструкциям с возможностью «горячей» замены

Таблица 2

Платформы сетевой безопасности ADLINK Technology

CSA-5100/5200 **1U/2U–платформа для монтажа в стойку**  Платформа сетевой безопасности, подходящая для малых и среднемасштабных проектов	CSA-5100/5200 разработана для сценариев безопасности приложений низкого и среднего уровня, обеспечивая подходящую платформу сетевой безопасности для малых и средних предприятий (МСП). На базе четырёх слотов расширения ввода-вывода на этой платформе может быть реализовано до 32 портов 10G SFP+. Основные характеристики CSA-5100/5200: ● Поддерживает семейство процессоров Intel® Xeon® E3 v3, четыре слота памяти DDR3 для памяти объёмом до 32 Гбайт; ● Четыре слота расширения поддерживают гибкие конфигурации сетевого ввода-вывода, адаптируемые к различным сценариям доступа к сети. ● Плата процессора и модули расширения ввода-вывода поддерживают обход локальной сети, допуская автоматический и ручной режимы работы. ● CSA-5100 имеет один разъём mSATA и один 2,5″ слот для жёсткого диска; CSA-5200 предоставляет четыре 2,5″ или 3,5″ слота для жёстких дисков, отвечающих различным требованиям к хранилищу. ● CSA-5200 имеет слот расширения PCIe x4 Gen2, что позволяет добавлять аппаратные ускорители, такие как карты Intel® QAT и FPGA
CSA-7200 **2U-платформа на базе архитектуры OCCERA**  Многоцелевая платформа сетевой безопасности с богатым выбором интерфейсов ввода-вывода	ADLINK CSA-7200 – высокопроизводительная двухпроцессорная платформа с Intel® Xeon® E5 v3 имеет до 64 портов 10G SFP+ благодаря восьми модулям сетевого интерфейса (NIM). Разработана для использования в качестве устройства сетевой безопасности следующего поколения. *Основные характеристики CSA-7200*: ● Восемь слотов NIM гибко поддерживают интерфейсы ввода-вывода, адаптируемые к различным сложным сценариям подключения. ● Расширенные функции обхода локальной сети; режимы обхода каждого NIM могут быть установлены независимо через меню BIOS; 12 слотов памяти DDR4 объёмом до 192 Гбайт удовлетворяют высоким требованиям к памяти при обработке сетевых пакетов. ● Три 2,5″ отсека для жёстких дисков SATA с возможностью «горячей» замены, поддерживает дополнительное расширение хранилища данных через PCIe или M.2. ● Один слот расширения PCIe x8 Gen3, позволяющий добавлять устройства аппаратного ускорения, такие как карты Intel® QAT и FPGA. ● Интеллектуальное управление системой, совместимое со спецификацией IPMI v2.0, поддерживает SOL и адаптивное изменение скорости вращения вентиляторов
CSA-7400 **4U высокопроизводительная платформа на базе архитектуры OCCERA**  Высокопроизводительная платформа сетевой безопасности с высокой вычислительной плотностью	ADLINK CSA-7400 – это высокопроизводительная вычислительная платформа высокой плотности, поддерживающая четыре процессора Intel® Xeon® E5 v3, образующих узлы, соединённые двумя модулями коммутатора с резервированием. CSA-7400 обеспечивает бесперебойную доставку услуг через вычислительные узлы с «горячей» заменой и коммутационные модули и подходит для создания высокопроизводительных межсетевых экранов следующего поколения и виртуализированных телекоммуникационных элементов. Основные характеристики CSA-7400: ● Построена на основе открытой вычислительной эталонной архитектуры (OCCERA). ● Семейство процессоров Intel® Xeon® E5-2600 v3/v4. Платформа высокой плотности 4U с четырьмя двухпроцессорными системами Intel® Xeon® E5 v3/v4. ● Модули с двумя коммутаторами обеспечивают 2 внутренних канала Ethernet 50 Гбит/с для каждого вычислительного узла. ● Пропускная способность Ethernet 2×400 Гбит/с, пропускная способность PCIe 2×200 Гбит/с, общая пропускная способность 1,2 Тбит/с. ● Гибкие комбинации ввода-вывода посредством выбора салазок коммутатора (MXN-3610, MXN-4100) и сети. ● Интерфейсные модули (NIM-1610, NIM-0440). ● Расширенное управление шасси. ● Резервирование питания переменного/постоянного тока (N + 1)

крытых компьютерных и коммуникационных технологий в продуктах CSA ADLINK реализован аппаратный дизайн высокой плотности. Это гарантирует богатый набор новых функций, позволяющих пользователю легко справляться с проблемами сетевой безопасности эпохи Интернета вещей. В табл. 2 приведены для примера основные параметры трёх платформ серии CSA.

Платформы ARiP

Для достижения максимальной совместимости в рамках всей продуктовой линейки и снижения совокупной стоимости владения платформы CSA разработаны в соответствии с модульной концепцией. Компания ADLINK также создала и интегрировала необходимые программные компоненты и промежуточное ПО с открытым исходным кодом, сокращая усилия клиентов по разработке. В итоге ADLINK Technology представила интеллектуальные платформы с поддержкой приложений ARiP (Application Ready Intelligent Platform) для сетевой безопасности. Это программное обеспечение PacketManager для платформ CSA, объединяющее популярное ПО с открытым исходным кодом, такое как DPDK (Data Plane Development Kit – набор драйверов и библиотек для быстрой обработки сетевых пакетов) и nDPI (библиотека с открытым кодом LGPLv3 для глубокой инспекции сетевых пакетов, базирующаяся на Open-DPI), предназначенное для обработки сетевых пакетов. Оптимизируя среду выполнения, PacketManager помогает в развитии сетевых приложений безопасности, которые требуют DPI, классификации потоков, фильтрации, переадресации, балансировки нагрузки и шифрования/дешифрования. Для обеспечения функциональности NFV под ключ в решение ADLINK CSA интегрированы продукты Intel® ONP (Open Network Platform – открытая сетевая платформа) и Wind River Titanium Server (платформа с поддержкой разработок NFV), которые построены на основе DPDK для обеспечения высокой пропускной способности. Платформа ADLINK включает также поддержку SDN. Для аналитики DPI на основе больших данных интегрирован также Apache YARN (Yet Another Resource Negotiator – ещё один планировщик ресурсов), работоспособность которого проверена на платформах CSA. PacketManager и интегрированные программные стеки сторонних компаний повышают производительность платформ CSA; а также предоставляют богатый набор функций для настоящих и будущих приложений сетевой безопасности. Благодаря этому пользователи могут разрабатывать на основе продуктов CSA решения для защиты DPI и облачных вычислений и ещё быстрее выводить новые продукты на рынок (рис. 3). Удалённое управление и энергоэффективность являются обязательными функциями при развёртывании продуктов для обеспечения сетевой безопасности в центрах обработки данных. Про-

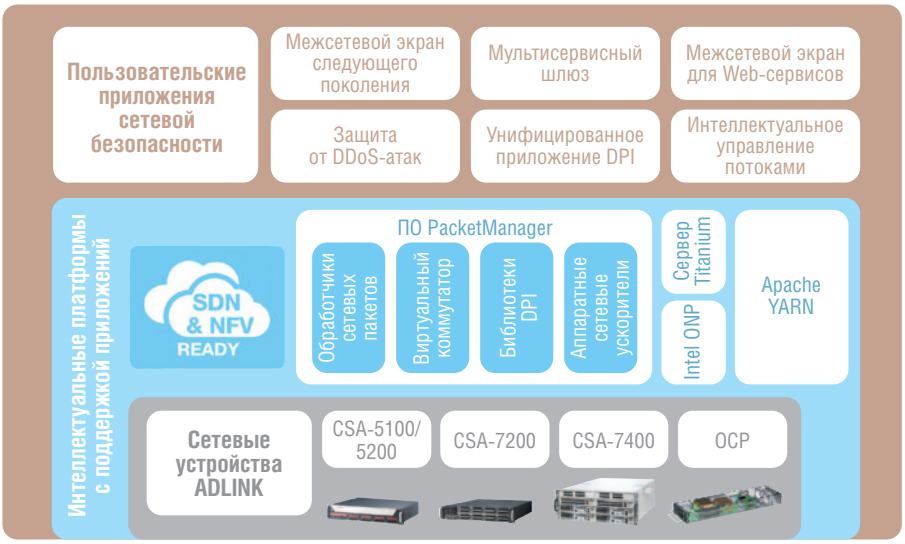

Рис. 3. Платформы CSA ARiP от ADLINK Technology

дукты CSA как среднего, так и высшего уровня поддерживают спецификацию IPMI v2.0 (Intelligent Platform Management Interface – интеллектуальный интерфейс управления платформой), позволяющую удалённо контролировать рабочее состояние вычислительных узлов, блоков питания и вентиляторных блоков. С целью снижения энергопотребления в продуктах CSA реализовано адаптивное управление скоростью вращения вентиляторов на основе IPMI и интеллектуального управления ресурсами ЦП с помощью Intel® Node Manager. Высокодоступные производительные платформы ARiP отвечают требованиям сетевой безопасности для промышленного IoT и учитывают новые тенденции в области сетевой безопасности. Очень важным их преимуществом является и то, что они построены на открытых компьютерных технологиях.

Заключение

Ведущий поставщик платформ в индустрии встраиваемых вычислений тайваньская компания ADLINK работает на рынках США, Великобритании, Сингапура, Китая, Японии, Кореи и Германии. Продукты ADLINK в настоящее время доступны в более чем 40 странах на пяти континентах. Данный факт является лучшим подтверждением конкурентоспособности её продукции. В данной статье мы привели лишь небольшой пример разработок компании, чей спектр интересов помимо коммуникационных технологий охватывает приложения для искусственного интеллекта, медицины, транспорта, машинного зрения и многих других отраслей. По всем вопросам применения и закупки обращайтесь к официальному представителю ADLINK в России – компании ПРОСОФТ. ●

Статья подготовлена по материалам компании ADLINK

E-mail: textoed@gmail.com