конференция
РусКрипто

Ежегодная международная научно-практическая конференция

«РусКрипто'2022»

О реализации IPsec маршрутизатора на базе специализированной СБИС

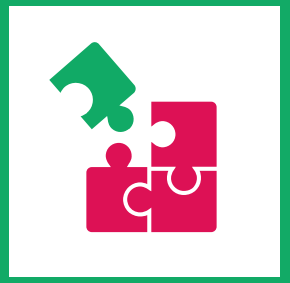
Николай Голиков, главный специалист
Максим Алешин, ведущий инженер
Виктор Фадеев, ведущий инженер
Юрий Сидорин, начальник службы

АО НТЦ «Атлас»

Аппаратная база

- Техпроцесс 65нм
- RISC-32 400 МГц
- MIPS-64 800 МГц

- Пропускная способность 10 Гбит/сек
- 1024 активных соединения
- Протоколы ГОСТ Р. 34.хх

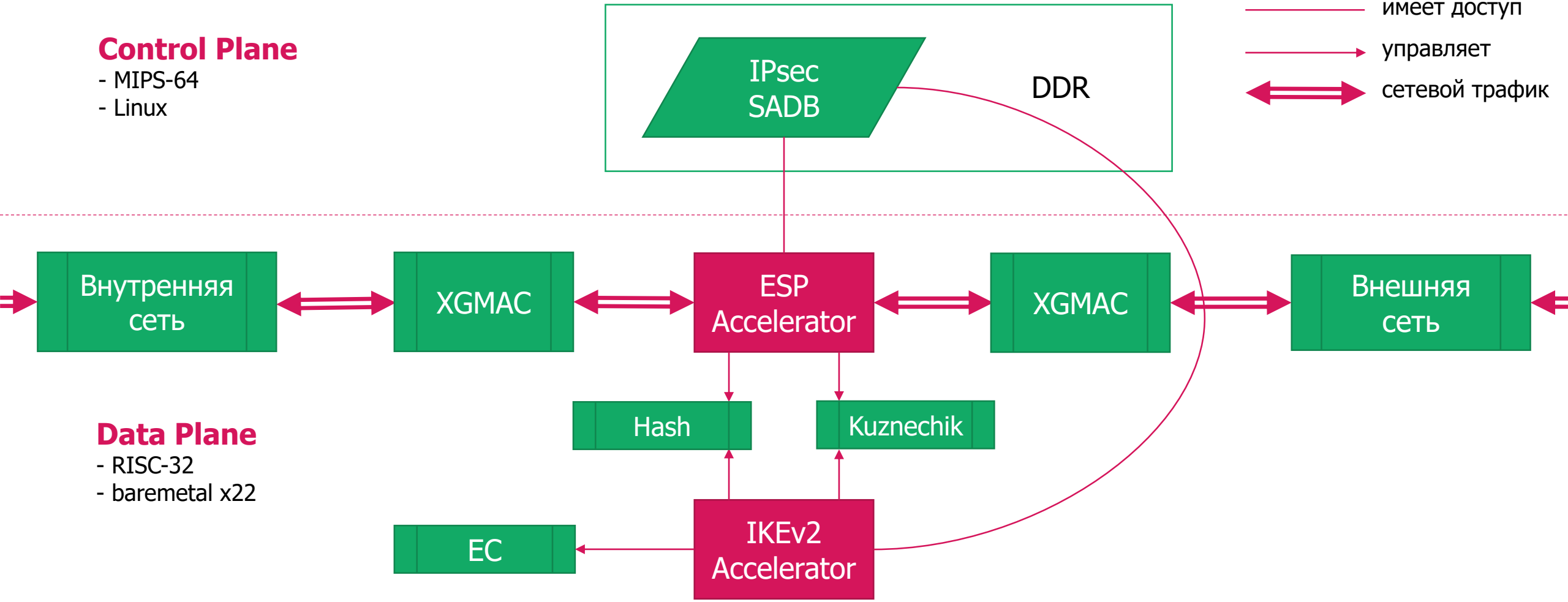


- Собственные криптографические устройства
- Интерфейс 10GbE
- Отказ от использования СФ-блоков foundry-merge

Состав системы

Control Plane
- MIPS-64
- Linux

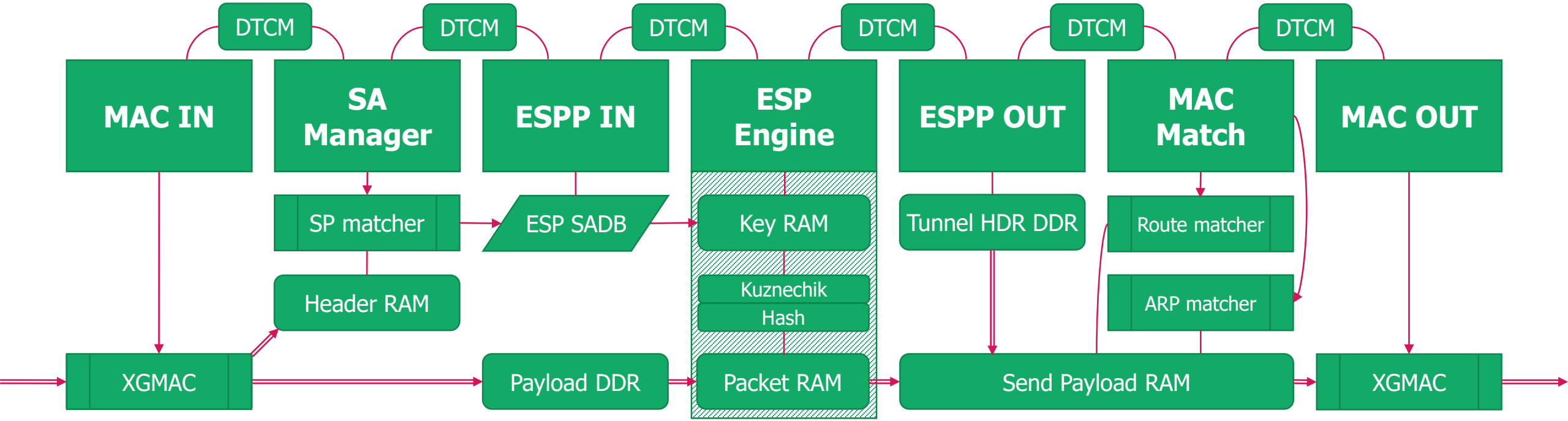
Data Plane
- RISC-32
- baremetal x22



Легенда:
- имеет доступ
- управляет
- сетевой трафик

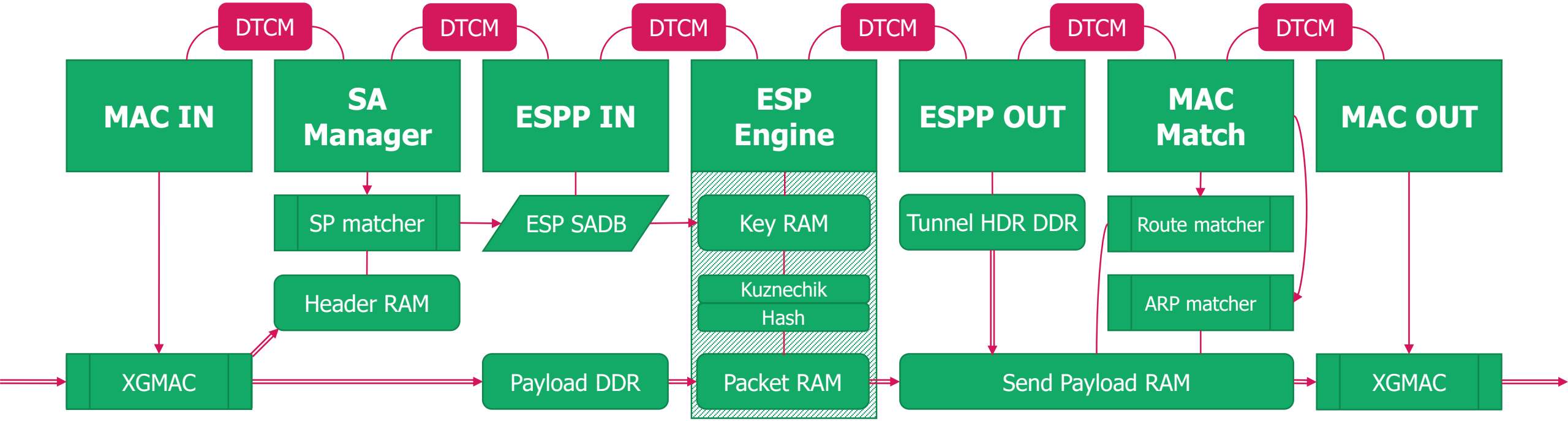
Data Plane

- Синхронный конвейер
- Шифрование и расшифрование организованы зеркально



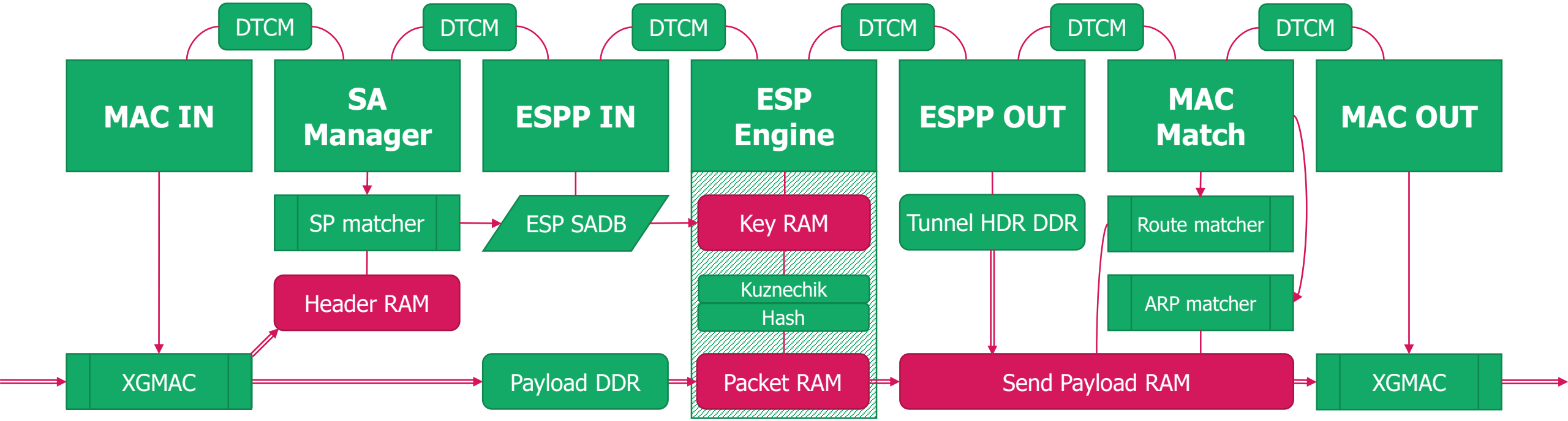
Data Plane DTCM

- Тесно интегрирована с процессорным ядром
- Скорость доступа – 2 такта



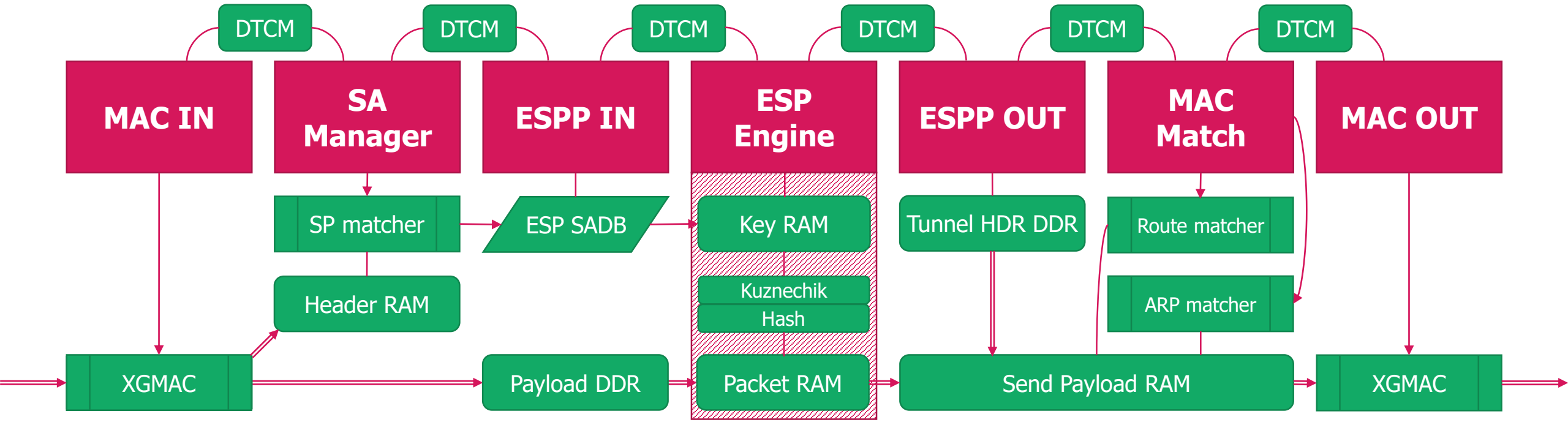
Data Plane RAM

- Хранят промежуточные данные
- Скорость доступа – 6 тактов



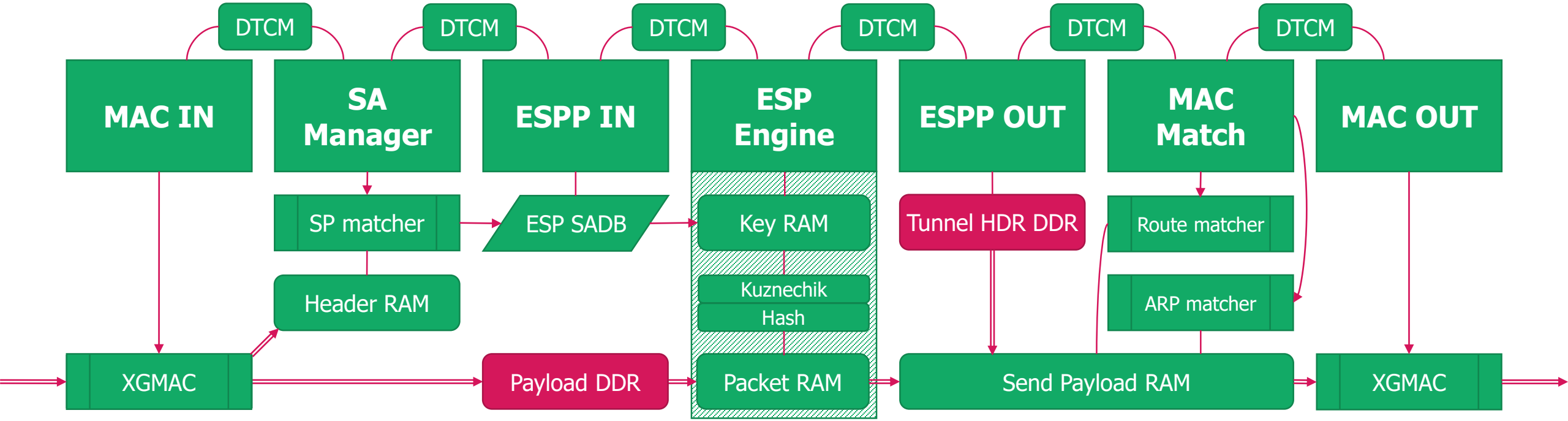
Data Plane

- 7 составных частей совершают определенное действие по цепочке

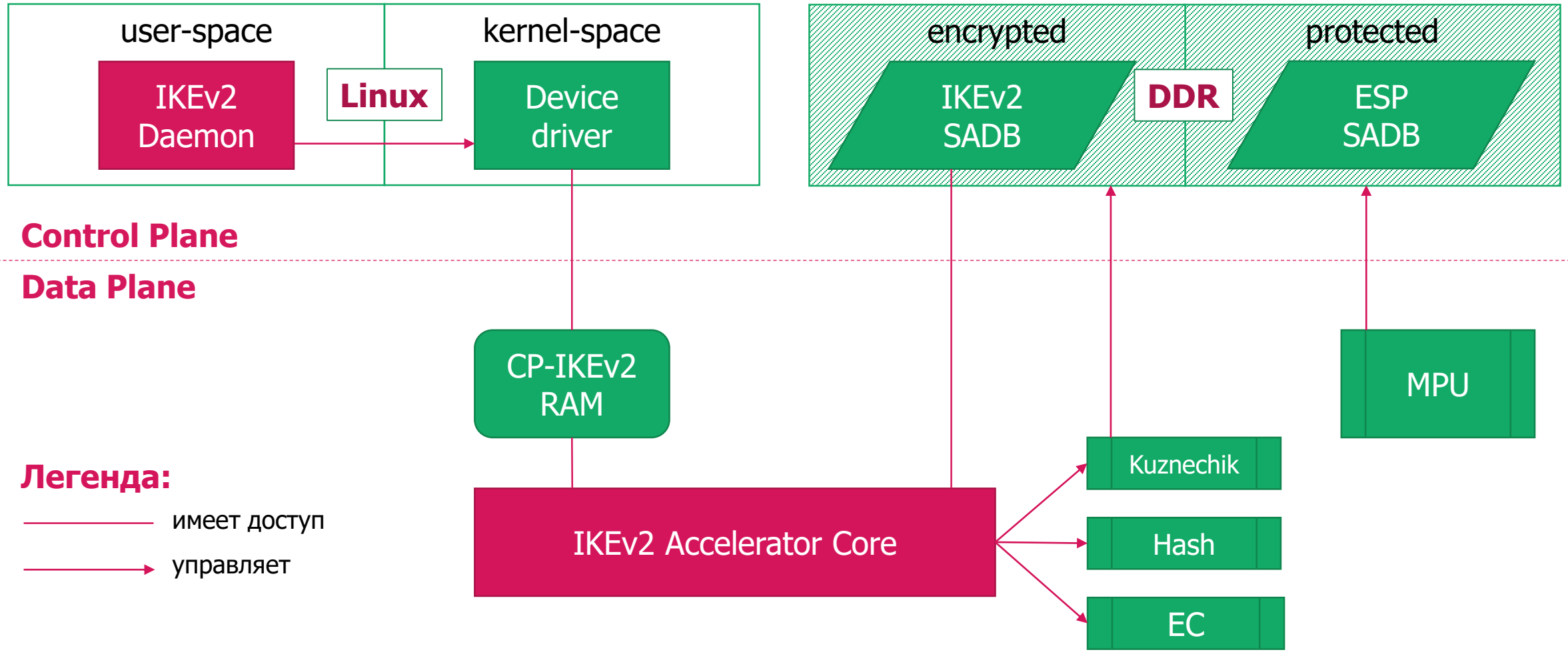


Data Plane DDR

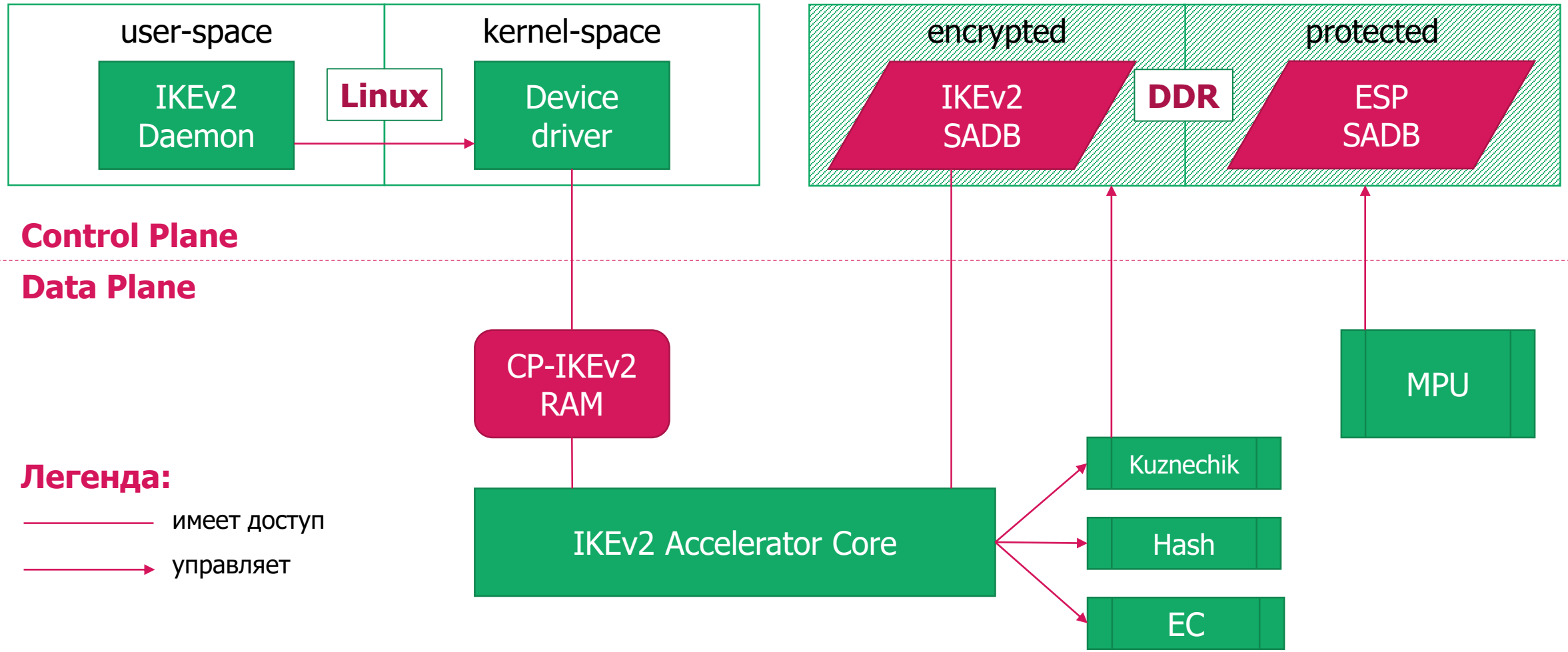
- Содержит тела принятых пакетов и туннельные заголовки
- Доступ к данным только через DMA с фильтром



IKEv2 ускоритель



IKEv2 ускоритель



Элемент IKEv2 SADB

- Элемент БД – это множество байтовых строк, которые являются ключевым материалом
- Три основных типа строк по уровню доступа:
  - защищенная строка;
  - только для чтения;
  - открытая строка.
- Примеры расширенного типа строк:
  - закрытый ключ Диффи-Хеллмана;
  - открытые ключи Диффи-Хеллмана обоих строн;
  - SPI ответчика и инициатора.

Работа с элементам IKEv2 SADB

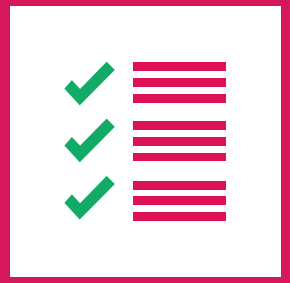
- IKEv2-A должен выполнять операции:
  - генерация случайного числа;
  - генерация ключевой пары Диффи-Хеллмана;
  - экспорт ключей из IKEv2 SADB в ESP SADB;
  - и т.п.
- Каждая команда из Control Plane в IKEv2-ускоритель содержит расширенный тип строки.
- Успех выполнения зависит только от основного типа и размера строки.

Пример операции

Генерация открытого ключа Диффи-Хеллмана на основе закрытого ключа:

- открытый ключ:
  - размер 64 или 128 байт;
  - основной тип – строка «только для чтения»;
- закрытый ключ:
  - размер 32 или 64 байта;
  - основной тип – «защищенная строка».

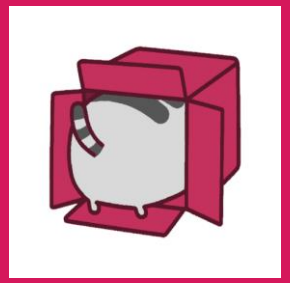
Программная база



Жесткая политика выравнивания данных:

- для Data Plane – 32 бита;
- для Control Plane – 64 бита;
- для DMA – 128 бит.

Используются inline функции и кольцевые буферы



Размер baremetal прошивок Data Plane составляет от 8Кб до 32Кб

Производительность

IKEv2

Размер EC	SA/сек	Такты
512 бит	252	1 625 396 825
256 бит	474	864 135 021

ESP

Блок	Шифров.	Расшифров.
MAC IN	436	429
SA Manager	427	377
ESPP IN	408	409
ESP Engine	447	431
ESPP OUT	277	244
MAC MATCH	253	280
MAC OUT	431	437
Сумма	3 178	3 213
В среднем	454	459

Вопросы

???