RTT

Международный ТБ ФОРУМ Технологии и Безопасность

Жесткое экранозамещение или опыт разработки межсетевого экрана на российском процессоре

14.02.2024

Конференция “Актуальные вопросы защиты информации”

Айбек Абдыманап, исполнительный директор RTT

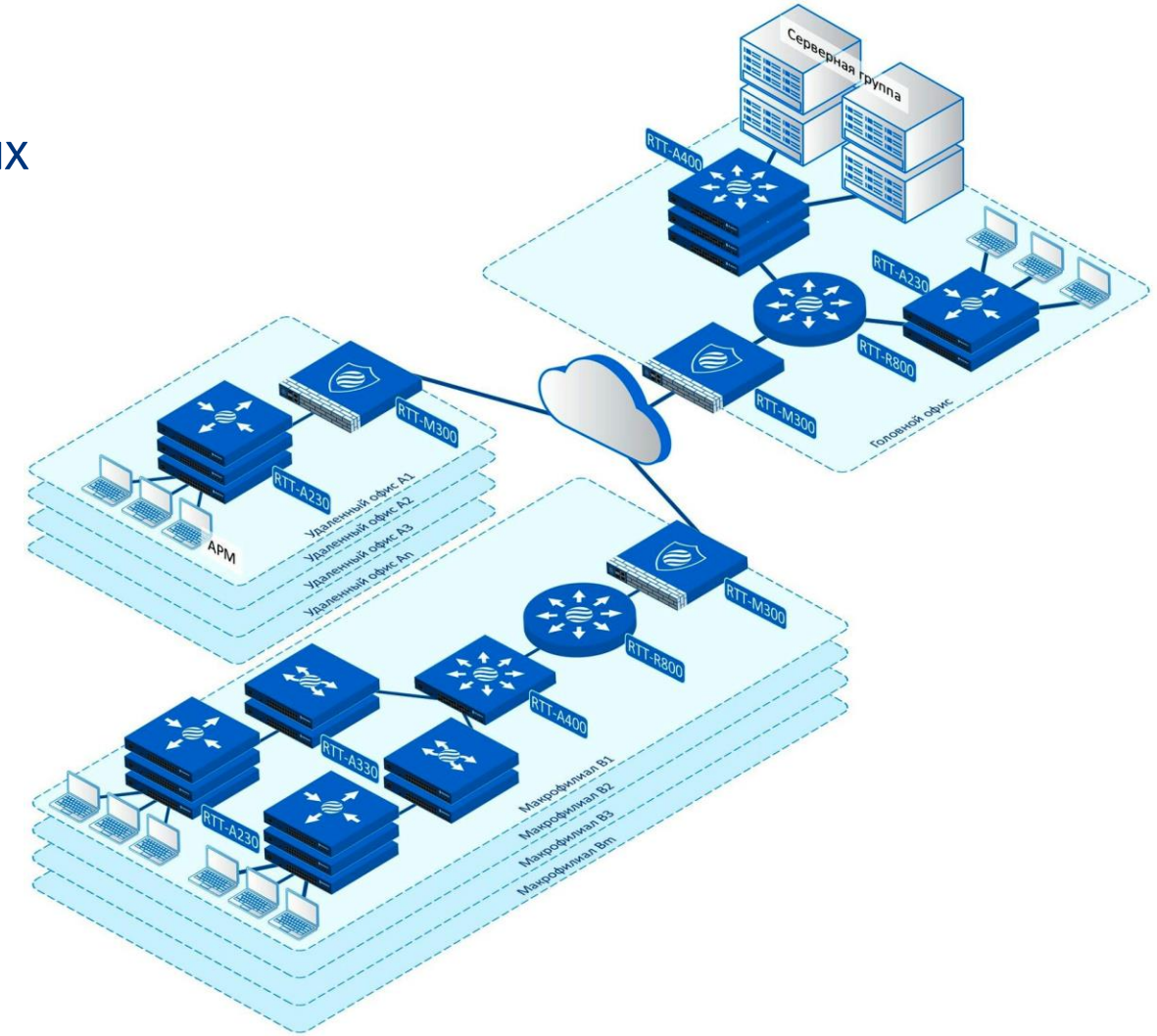
План

1. О компании
2. Почему межсетевые экраны?
3. Почему на российском процессоре?
4. Аппаратные нюансы
5. Программные нюансы
6. Функциональные нюансы
7. Сюрпризы от регулятора и жизни
8. Результаты
9. Дальнейшие планы
10. Вопросы?

О компании

Профиль: оборудование для создания доверенных и защищенных сетевых решений

Факты:
- 15 лет на рынке ИБ
- Лицензиат ФСТЭК, ФСБ, МО РФ
- Резидент Сколково
- Аккредитованная ИТ-организация
- Входим в перечень ГИСП
- 6500+ единиц продукции выпущено
- 260+ довольных заказчиков



Почему решили разработать межсетевые экраны?

Варианты ответов:

A. Потому что идиоты

- В реестре ФСТЭК 129 записей о действующих сертификатах на МЭ
- В отрасли говорят о 30+ вендорах МЭ, NGFW, UTM
- Взялись делать все, включая самых больших (Solar, PT, Kaspersky, etc.)

B. Why not

- Есть опыт – единственные в России коммутаторы с 3-НДВ и 4-МЭ, а они умеют делать фильтрацию L2-L4, приоритизацию, сегментацию, etc.
- Заказчики хотят комплексное сетевое решение: ЛВС + защита по периметру

C. Потому что можем

- Стартовали в 2020, а не после ухода западных «партнеров» в 2022 г.
- Можем сделать продукт с нужной клиенту, но отсутствующей на рынке фичей (фичами)

Почему решили делать на российском процессоре?

Варианты ответов:

A. Потому что идиоты

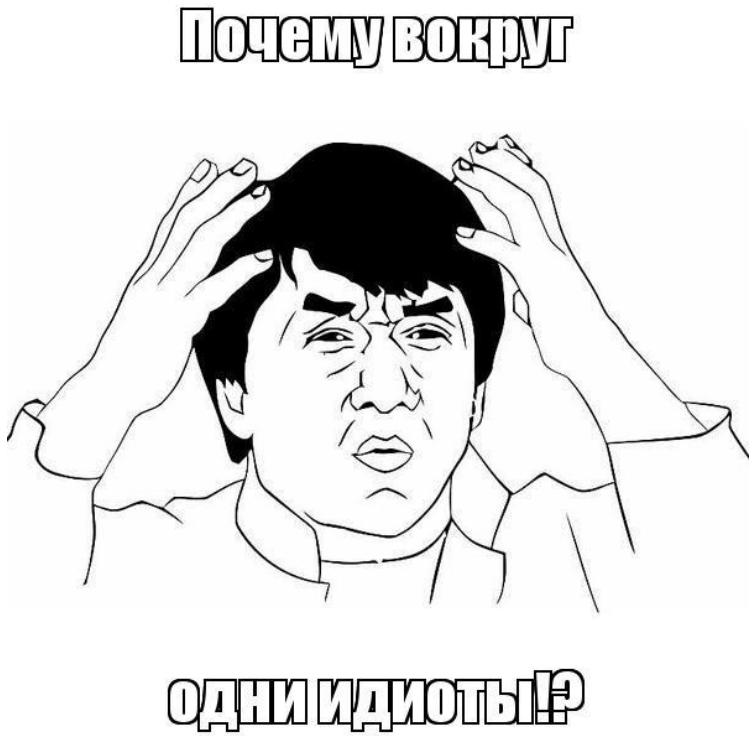
- “Нормальных российских процессоров в природе не существует” ©

B. Потому что регулятор сказал

- Требования доверия (Приказ ФСТЭК № 76 от 02.06.2020):
  - аппаратная платформа из реестра российской продукции
  - процессор из реестра российской продукции (2028)

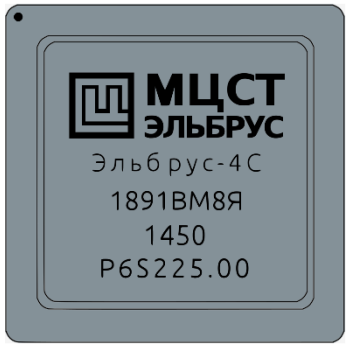
C. Why not

- Есть опыт использования российской ЭКБ в коммутаторах.
- Мы за реальное импортозмащение



Аппаратные нюансы

1. **Выбор процессорной платформы**
   - Просто МЭ никому не нужен, все хотят комбайн (NGFW, UTM)
     Ищем нормальный процессор общего назначения (FPGA, ASIC не обсуждаем)
   - Тогда выбор невелик: Байкалы, Скифы, Эльбрусы
   - По совокупности критериев выбрали Baikal-M
2. **Это ARM**
   - Программная экосистема сильно меньше, чем у систем на x86
   - Адаптация и оптимизация ПО под эту архитектуру
3. **Это ARM64**
   - Много оперативки – это плюс
   - Экосистема еще меньше – это минус
4. **Это ARM64 8 ядер по 1,5 ГГц**
   - Балансировка нагрузки (Control plane + Data Plane) по ядрам
   - Приоритизация ресурсов, например, под логгирование
5. **Это относительно новый процессор**
   - Все «детские» болезни (SDK, драйверы, Errata, документация)



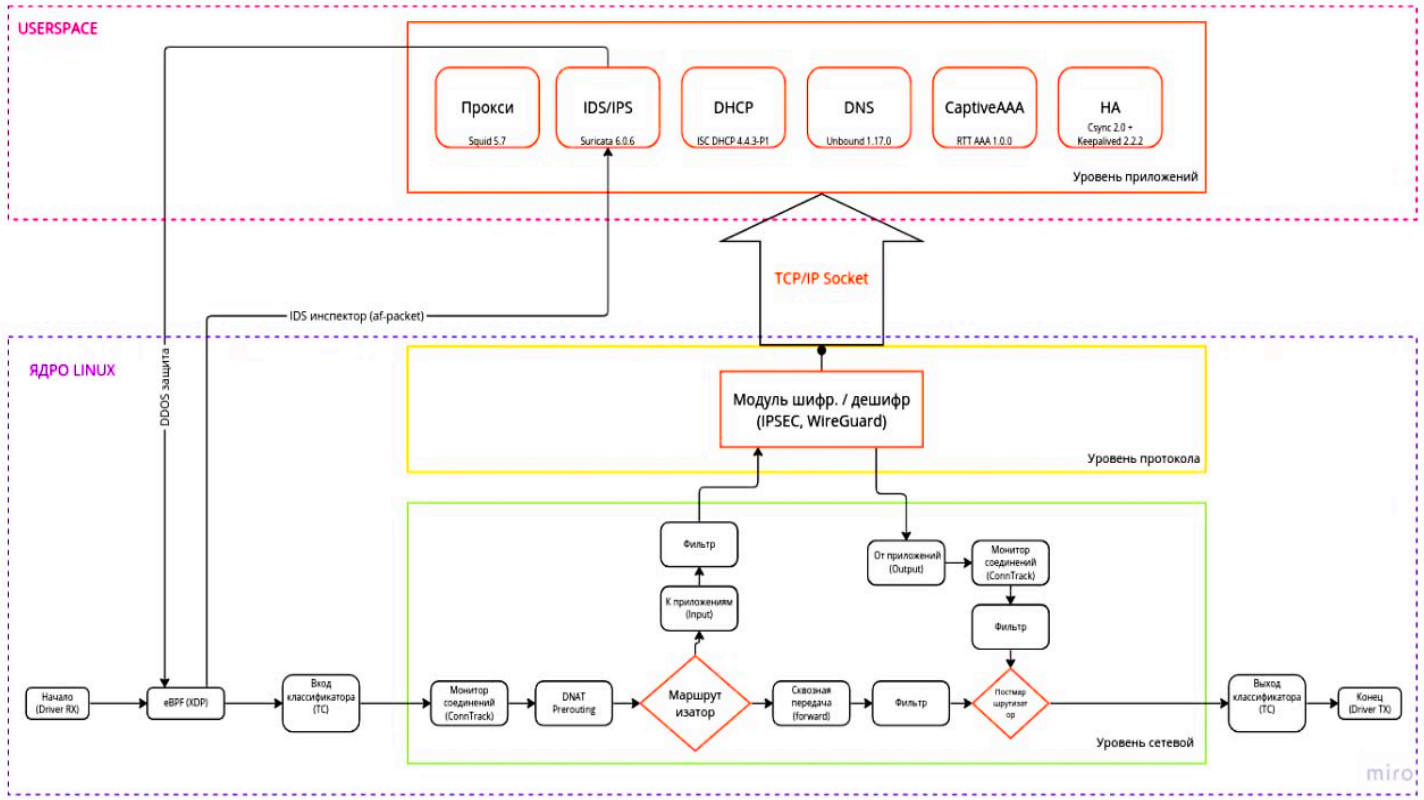
Программные нюансы

1. **Выбор ОС**
   - Оптимальный путь – следовать за SDK на ЦПУ, значит Linux.
     Поддержку других ОС чип-вендор пока не предлагает
2. **Выбор движка файрволла**
   - По совокупности критериев выбрали OPNsense. Но он на FreeBSD!
   - Замена Packet Filter (FreeBSD) на Netfilter (Linux).
     И всего остального
   - В итоге от выбранного движка остался только графический интерфейс
3. **Поддержка от чип-вендора**
   - Не самые свежие ядра Linux
   - Не все драйверы для периферии
   - Тех поддержка по багам или кастомизации

Функциональные нюансы

Вечный дует Kernel Space vs User Space

- Каждое приложение в своей песочнице – это плюс.
- Основная обработка сетевого пакета происходит в ядре, т.е. медленно – это большой минус!
- Требуется рефакторинг (DPDK, VPP, FPGA, ASIC, etc.)



Сюрпризы от регулятора и жизни

От регулятора

- Конец 2022 г. – требование о применении российской аппаратной платформы сдвигается на 2024, далее – неизвестно
- Март 2023 г. – выход требований к ММЭ (NGFW)

От жизни (после 24.02.2022)

- Нет тех. поддержки от вендоров сетевых контроллеров (Marvell, etc.)
- Закупка интеллектуальной ЭКБ только через третьи страны (Intel, Marvell, STM, etc.)
- Производство Baikal-M и всех других российских чипов на зарубежных фабриках – это большой квест
- «Геопространственные» данные (GeoIP) с учетом новых территорий
- Отказ ClamAV и др. работать в РФ

Наши результаты

Универсальные шлюзы безопасности

- **RTT-M300** – для корпоративных сетей.
  RTT-M300F – для промышленных сетей.
- Первая подсерия на процессорах Baikal-M.
  В roadmap'е выпуск на других ЦПУ
- Аппаратная часть собственной разработки.
  Универсальная сетевая платформа
- Программная часть собственной разработки.
  Кроссплатформенное решение
- Сейчас идет сертификация ФСТЭК
  МЭ А4, Д4, СОВ С4, УД4

Функциональные возможности

Комплексная защита сетевой инфраструктуры:

- Межсетевое экранирование (Firewall)
- Защита от вторжений (IDS/IPS)
- Журналирование трафика (Logging)
- Анализ и инспекция пакетов (LiteDPI)
- Проксирование трафика (Proxy)
- Трансляция сетевых адресов (xNAT)
- Создание «частных» сетей (VPN)
- Потоковая антивирусная защита (AV)
- Аутентификация (AAA)
- Кластеризация (HA)
- Маршрутизация (RIP, OSPF, ECMP, xBGP)
- Сервер DHCP, DNS, NTP

Система и управление:

- Полное управление через Web-интерфейс
- Подключение по SSH
- Мониторинг служб и платформы
- Резервные копии системы и сервисов
- Обновление из доверенного репозитория
- Журналирование системы
- Резервирование (CARP)
- Экспорт/импорт настроек
- Оповещение об обнаруженных ошибках
- Доверенная загрузка системы
- Автоматическое восстановление после сбоев

RTT-M300x Аппаратные конфигурации

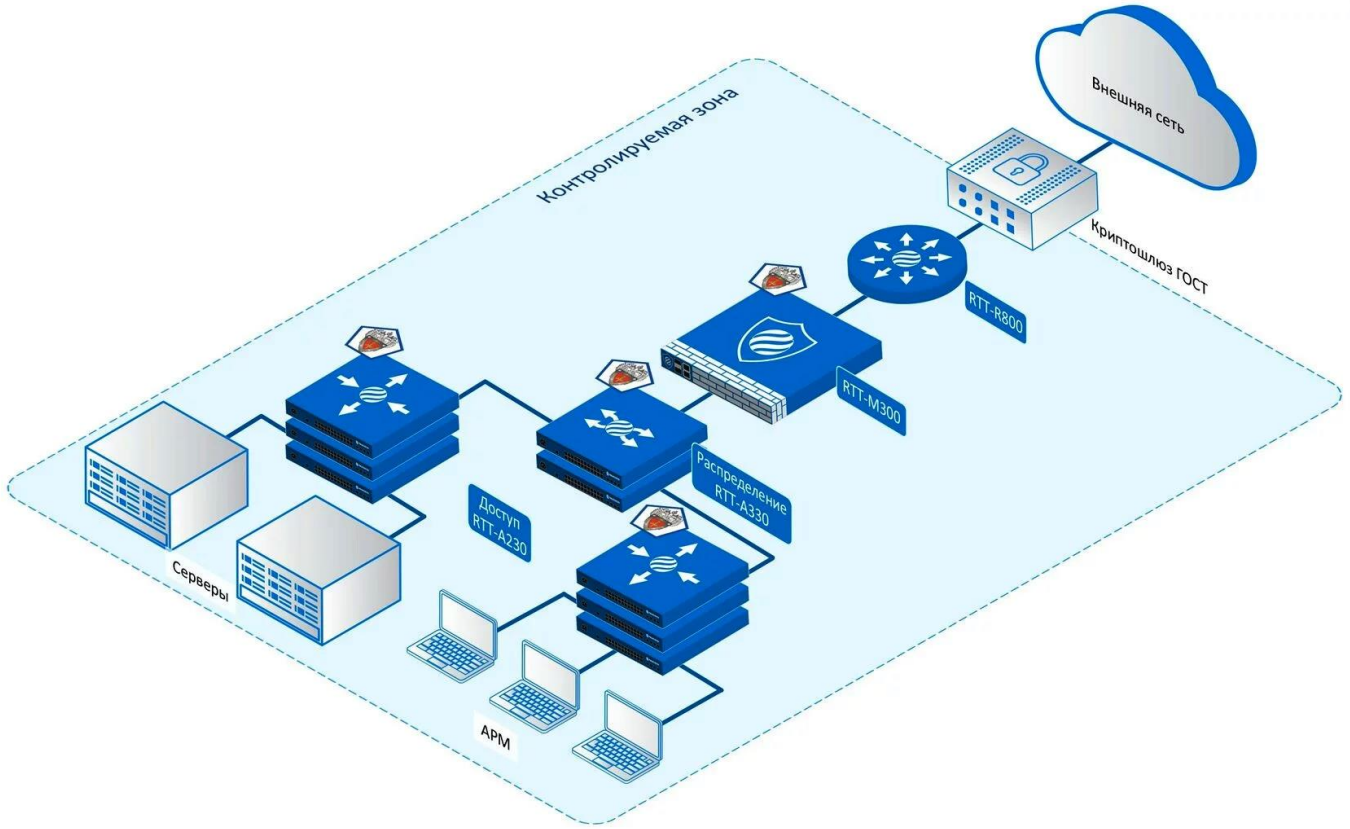
Характеристика	Значение	
Наименование (модель)	RTT-M300	RTT-M300F
Форм-фактор	1U (19” Rack unit)	
Центральный процессор	Baikal-M1000, 8-core 1,5 GHz ARM Cortex-A57	
ОЗУ	До 32 Гбайт (до 4 модулей DIMM) 2400 МГц DDR4	
ПЗУ	2 порта SATA 3.0	
Сетевые интерфейсы	4 x GE, 2 x 10GE (SFP+), 2 x GE Combo	
Карты расширения	8xGE (RJ45), 2x10GE (SFP+), 4xGE Switch*	
Порт OOB	1 x FE (RJ45)	
Влагопылезащищенность	IP20	IP30
Пассивное охлаждение	Нет	Да
Диапазон рабочих температур	-5°C … +45°C	-5°C … +55°C
Габариты	444 × 44 × 383 мм	444 × 44 × 403 мм
Вес	Не более 5 кг	Не более 7 кг
Электропитание	115 – 240 В, 50Гц, не более 1 А	
Резервное питание*	1+1 Hot plug	18-72 В DC, не более 5 А

Производительность

Характеристика	Значение	
Размер пакета, байт	64	1500
Количество правил фильтрации	100	
Пропускная способность в режиме фильтрации L4, Мбит/с	120	2500
Пропускная способность в режиме фильтрации L4, кпак/с	205	300
Пропускная способность в режиме фильтрации + Lite DPI (на примере 100 правил IP drop + 5 правил offset drop), Мбит/с	120	2500

RTT-M300x. Roadmap

- Кластеризация active/active + балансировка трафика
- Контентная фильтрация, L7
- Интеграция с SOC
- VPN с ГОСТ
- Функции L2 (LACP, VLAN и т.д.)
- Полноценный API для HTTPs
- Браузер логов
- Средства миграции сторонних конфигураций
- Рефакторинг по производительности
- Далее до ∞



А ты доверяешь своей сети?

www.ртт.рф +7 (495) 234-9777 info@rusteletech.ru