RTT | Доверие Безопасность Надежность

30-й Юбилейный ТБ ФОРУМ Технологии и Безопасность

Не навреди, не залечи - киберэтика в сети АСУ ТП

Sk Участник

Воробьев Сергей
Менеджер по продукту

2025

RTT

RTT – разработчик и производитель защищенных, безопасных и доверенных сетевых решений.

Мы создаем оборудование, которое позволяет создать основу надежной и функциональной мультисервисной сети передачи данных.

Портфолио: сетевое оборудование.

- Год основания 2009
- Головной офис г. Москва
- Лицензиат ФСТЭК, ФСБ, МО РФ
- Резидент Сколково
- Аккредитованная ИТ-организация
- Входим в перечень ГИСП

15 лет работаем и создаем сетевые решения

Портфолио компании

Сетевое оборудование

- Ethernet-коммутаторы
- Маршрутизаторы
- SFP-модули

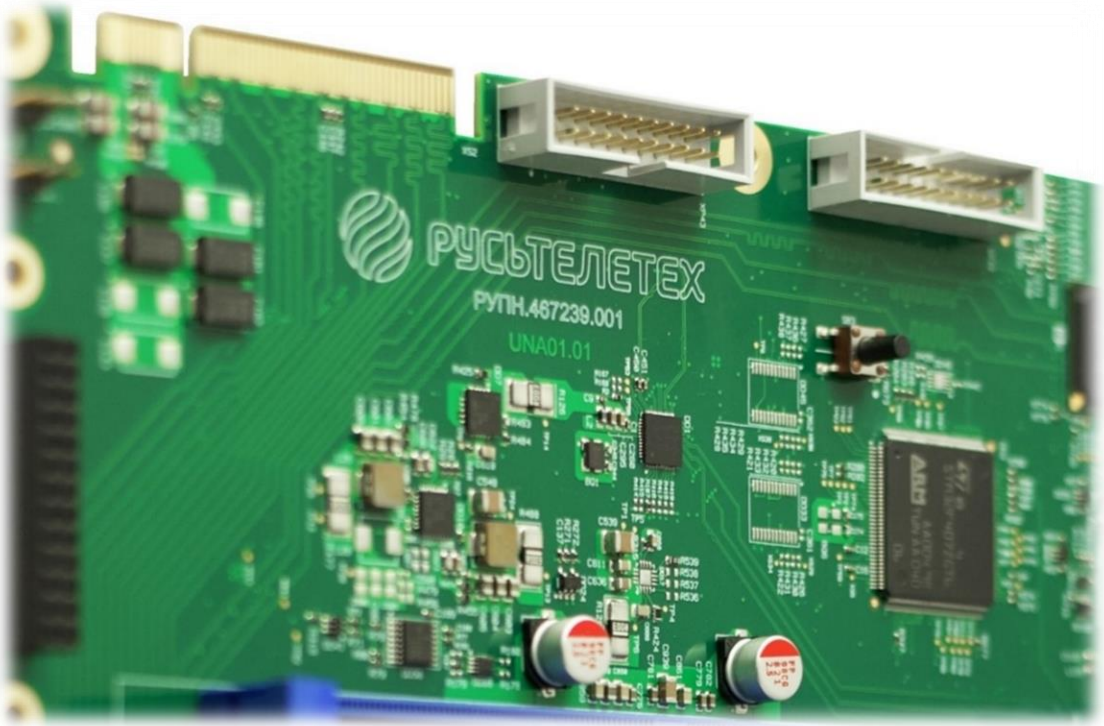
Средства сетевой безопасности

- Универсальные шлюзы безопасности
- Универсальные **промышленные** шлюзы безопасности

Проект разработки межсетевого экрана

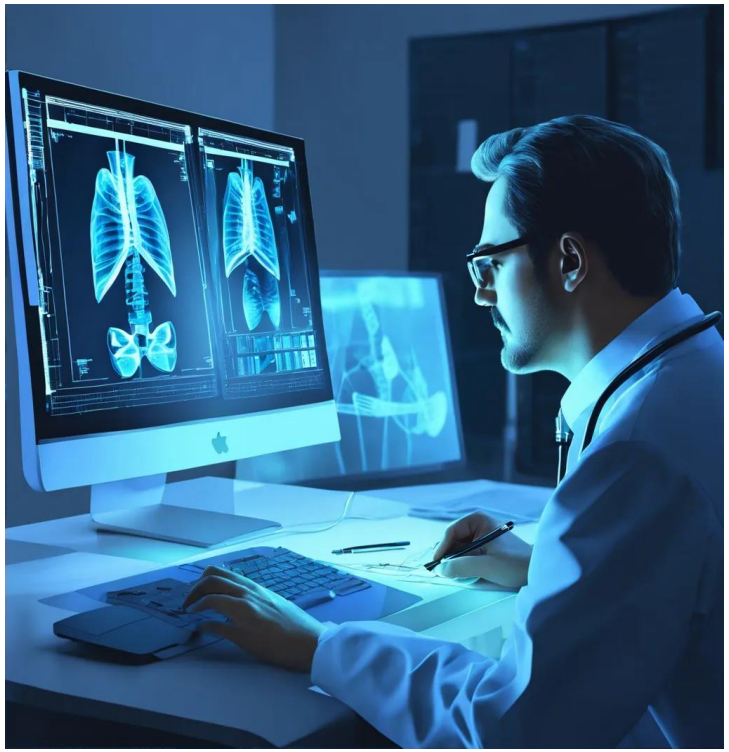
- Название проекта: **UTM RTT- M300**
- Старт проекта: 2020
- 3 серии изделий
- Аппаратная часть собственной разработки
- Программная часть собственной разработки
- 2022 – разработаны и выпущены межсетевые экраны

- 2023 – выпущена серия межсетевых экранов в промышленном исполнении RTT-M300F
- Сертификация ФСТЭК МЭ А4, Д4, СОВ С4, УД4*



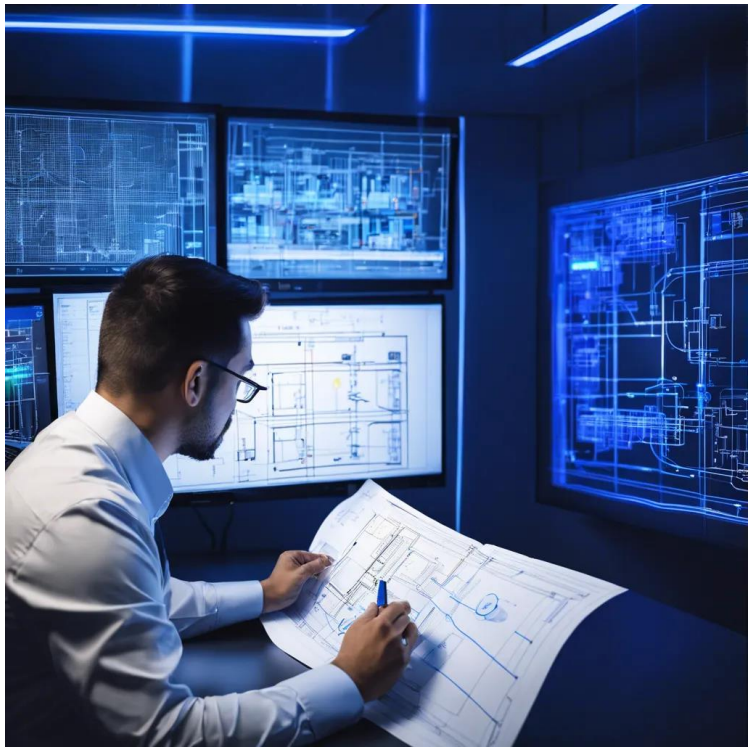
* в работе

Так причем тут киберэтика?



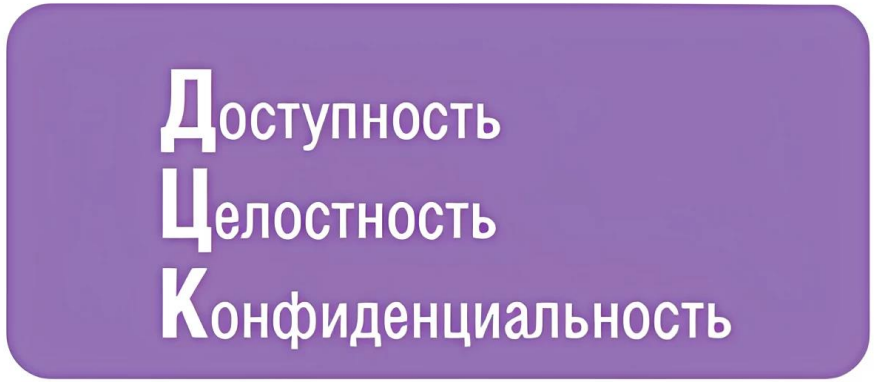
В медицине действует принцип "Не навреди". Врач стремится минимизировать риски лечения, бережно подходить к любым вмешательствам.

Баланс между вмешательством и бездействием



Системы АСУ ТП можно представить как сложный "живой организм". Нарушение работы одного "органа" может привести к сбоям всей системы.

Три Основных Принципа Информационной Безопасности



Главная задача - обеспечить
непрерывность (доступность)
технологического процесса

Как проявляется нарушение доступности?

Инцидент с подводной платформой Deepwater Horizon 2010 год.

Данные о повышении давления поступали с запозданием, и это создало впечатление, что ситуация под контролем. Но произошел взрыв…. И дальнейший разлив нефти в Мексиканском заливе

Авария на химическом заводе Сент-Луис, 2021 год.

Произошел аварийный выброс химиката в атмосферу. Причиной этому послужила неправильная настройка системы контроля давления в резервуаре, которая не была синхронизирована с обновленной системой.

Инцидент на заводе по производству удобрений в Порт-Лаваке в 2022 году

Авария произошла в результате утечки аммиака, и ее причины были связаны с нарушениями в функционировании АСУ ТП.

Безопасности много не бывает….. Но…

Требования:

ИТ.МЭ.Д4.ПЗ Выбор момента идентификации **FIA_UID.1.2**

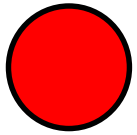
Замечание по применению: должна быть предусмотрена возможность выполнения определенных действий без прохождения процедуры идентификации с целью максимальной оперативности. Примером таких действий является переведение МЭ в состояние, не оказывающее влияние на функционирование автоматизированной системы управления.

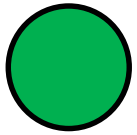
Выполнение требований:

Не влиять на штатный режим функционирования **(режим “пропускать всё”, если оказываем негативное влияние)**

Что еще влияет на доступность?

Не мешайте нам работать!





“Не мешайте нам работать!”

“Нам нужно надежное решение — оборудование, которое не нарушит наши технологические процессы."

Что еще влияет на доступность?

Надежность аппаратной платформы

- Пассивное охлаждение
- Резервированный блок питания
- Расширенный диапазон температур
- Стойкость к ЭМС
- ….

  и т.д.

Специализированный функционал ПО

Требования ФСТЭК

- FPT_FLS.1 Сбой с сохранением безопасного состояния
- FPT_RCV.2 Автоматическое восстановление

- **FRU_FLT.2** Ограниченная отказоустойчивость

Дополнительные требования

- Удаленная диагностика и контроль параметров
- ….

Промышленной сети - промышленный межсетевой экран!

Универсальные шлюзы безопасности серии

RTT-M300

Серия RTT-M300

RTT-M300

- Защита сетей небольших организаций
- Слот под карты расширения
- Активное охлаждение
- Модуль питания 220 В (AC)

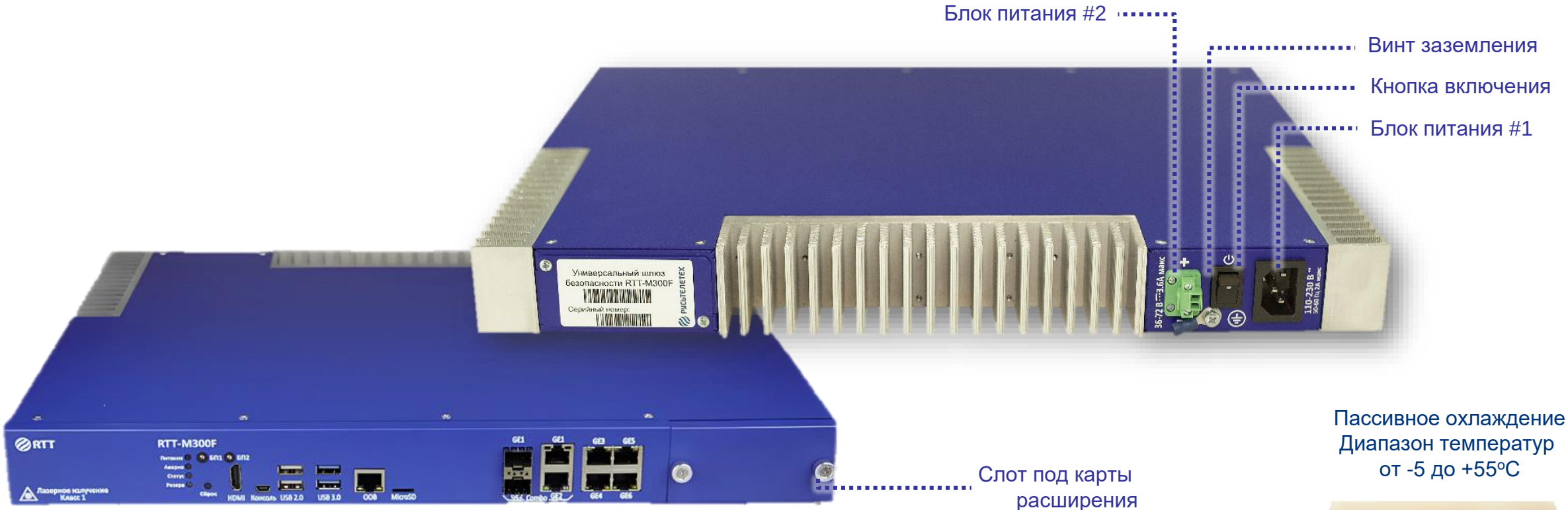
RTT-M300F

- Защита сетей АСУТП и объектов КИИ
- Диапазон рабочих температур -5 …+55 °C
- Пассивное охлаждение
- Резервированный модуль питания

RTT-M300E

- Защита корпоративных сетей
- 2 слота под карты расширения
- Поддержка до 18 портов GE
- Резервированный модуль питания Hot Swap

RTT-M300F (конструктив)



Пассивное охлаждение
Диапазон температур
от -5 до +55°C

RTT-M300 (карты расширения)

M300-NM- 8G

Порты

– 8 x10/100/1000Base-TX
– 4 x10/100/1000Base-TX
– Flow Control

M300-NM-4G-S

L2 –функционал

– IEEE 802.1Q VLAN (Tag-based)
– Flow Control
– QoS
- Storm control
– Loop protection

Безопасность

-IEEE 802.1x
-Port Security
-ACL rules

M300-NM-2XG

Порты

– 2x10GE SFP+
– 2x1GE SFP

RTT-M300F (система питания)

Резервированный блок питания

Характеристики по питанию:

- Входное напряжение питания:

  AC (85… 264 В) ~ 47…63Гц
  DC (120… 264 В)

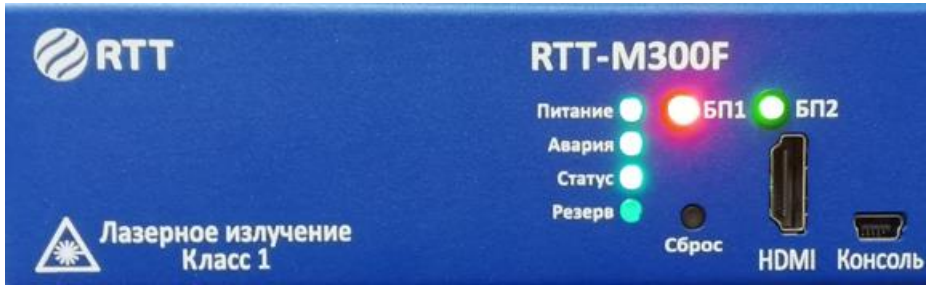
- Архитектура DPA
- Контроль температуры
- Индикация состояния системы питания и каждого блока в отдельности

- Удаленный контроль температуры и статуса через SNMP v3

- Настраиваемый старт устройства

RTT-M300F (диагностика аппаратной части)

- Контроль загрузки процессора
- Контроль температуры процессора
- Контроль состояния портов
- Контроль состояния блоков питания




```
ubuntu@UbuntuWest:~$ snmpget -v3 -l authPriv -u RTT -a MD5 -A Rusteletech -x
DES -X Rusteletech 172.16.20.56 .1.3.6.1.4.1.37293.2.2.12.1.1.5.0

iso.3.6.1.4.1.37293.2.2.12.1.1.5.0 = STRING: "{\"term1\": \"38.4\", \"term2\":
\"38.7\", \"ps1\": 1, \"ps2\": 1}"
```

Производительность и аппаратная платформа

ЦПУ	ARM архитектура (BaikalM и др.)
ОЗУ	До 32 Гбайт, 2400 МГц DDR4
ПЗУ	До 2 ТБ, SATA 3.0
Сетевые интерфейсы	4xGE (RJ45), 2xGE Combo (RJ45/SFP),
Порт OOB	RJ45
Консольный порт	mini USB
Карты памяти	Слот micro SD
Интерфейсы	2xUSB 2.0, 2xUSB 3.0, 1xMiniUSB, HDMI 2.0
Форм-фактор	1RU (монтаж в стойку 19”)

Производительность и аппаратная платформа

Межсетевой экран, 1000 правил, UDP 1500B	2500 Мбит/с
Межсетевой экран, 1000 правил, EMIX, логирование, счетчики	580 Мбит/с
Межсетевой экран, 1000 правил, EMIX + COB IDS, 50K сигнатур	320 Мбит/с
Межсетевой экран, 1000 правил, EMIX + COB IPS, 50K сигнатур	30 Мбит/с
Максимальное число конкурентных TCP-сессий, 1000 CPS	265K
Максимальное число новых TCP-сессий в секунду	2K

REFOS

AAA
- Управление группами пользователей
- Сквозная аутентификация по локальной БД, Radius , LDAP
- Многопользовательская аутентификация

DPI
- Инспекция протоколов
- Raw offset для своих правил
- Правила фильтрации отдельных типов сообщений

СОВ
- Обнаружение аномалий в трафике
- Anti-DDOS
- Обновляемая база уязвимостей
- Визуализация найденных угроз

Веб-прокси
- HTTP-proxy
- Фильтрация URL
- Собственный список фильтрации URL/IP
- Проверка почтовых сообщений
- Проверка сертификатов SSL

Сетевые функции
- Поддержка IPv4/IPv6
- xNAT (DNAT, SNAT, PAT)
- NTP/SNTP
- DHCP-сервер/клиент
- DNS-сервер
- Маршрутизация RIP, OSPF, BGP, BFD
- Профилирование трафика

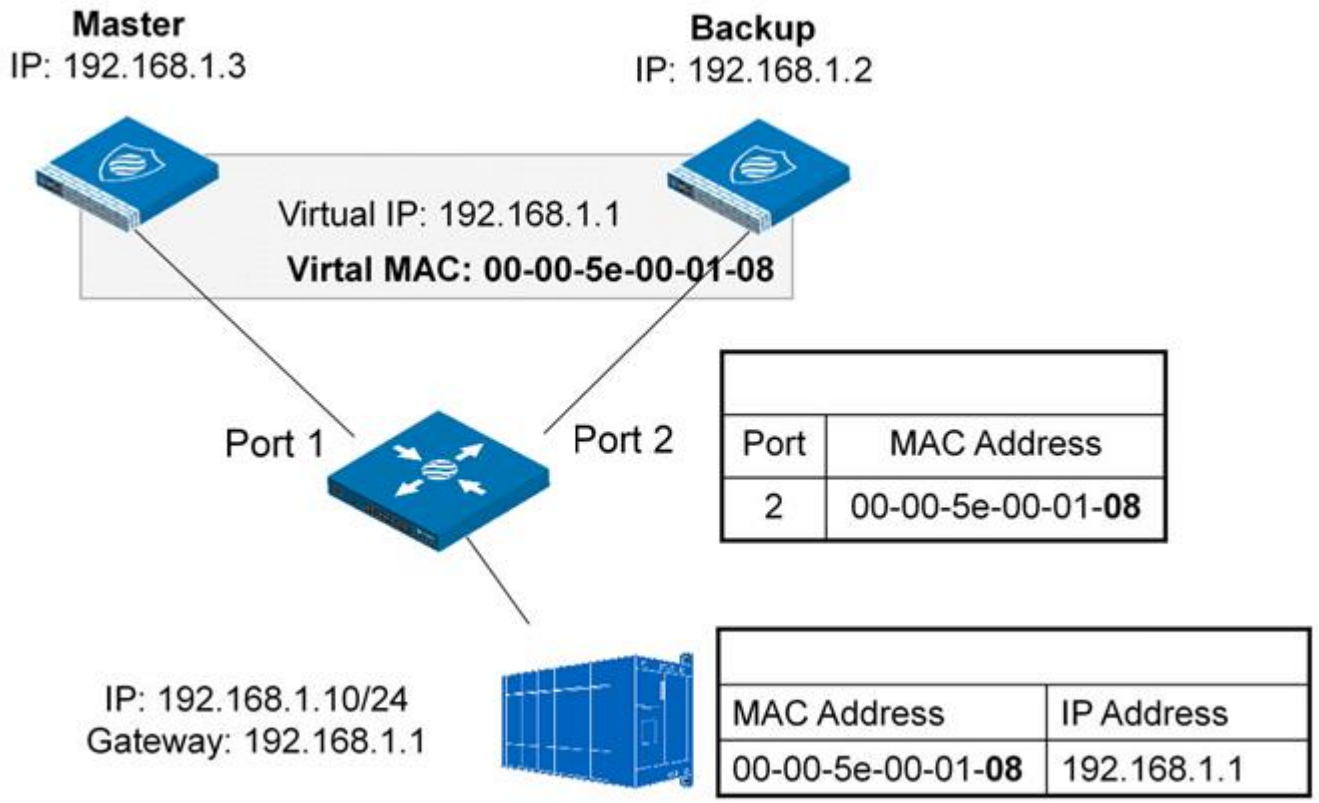
Система и управление
- Полное управление через Web
- Подключение по SSH
- Мониторинг служб
- Работа в режиме кластера (Active/Active, Active/Passive)
- Автоматическое восстановление

Межсетевой экран
- Stateful/Stateless Firewall
- Фильтрация по гео-признаку
- Изменение политики фильтрации

Антивирус
- Работа с внешними антивирусами

RTT-M300 Кластеризация (резервирование)

- Полное резервирование устройства
- Синхронизация конфигурации
- Поддержка режимов active/active, active/passive
- Синхронизация сессии
- Виртуальный IP и **MAC**



Port	MAC Address
2	00-00-5e-00-01-**08**

MAC Address	IP Address
00-00-5e-00-01-**08**	192.168.1.1

Нет периода обновления ARP-таблиц на конечных устройствах, что позволяет организовать бесшовное резервирование

RTT-M300 (DPI промышленных протоколов)

- **MODBUS/TCP**
- **IEC 104**

- Устаревшая архитектура:
- Легкость сканирования и идентификации:
- Уязвимость к физическим атакам
- Отсутствие шифрования:
- слабая или отсутствие аутентификации:
- и т.д.

Дополнительные фокусные цели

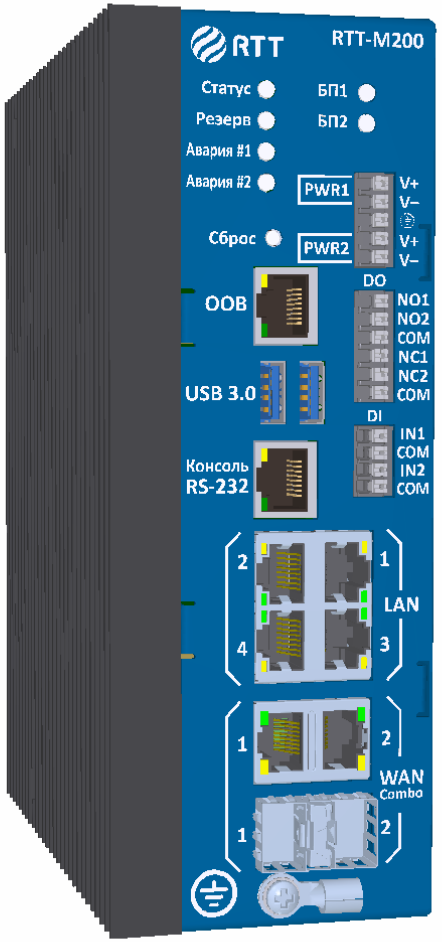
сделать инструмент понятным и простым в применении

- Акцентировать параметры на фильтрацию нужных полей

- Применение шаблонов

  - ❑ Проверка полей пакета данных согласно спецификации
  - ❑ Проверка работы протокола обмена
  - ❑ Только чтение
  - ❑ Только чтение/запись

RTT-M200 (анонс)



Производительность	До 3 Гбит/с (UDP)
Количество и тип портов 10/100/1000Base-T	4 - RJ45 (LAN) 2 – SFP (COMBO)
Консольный порт	RS-232
USB-порт	2 шт. type A
DI	2 шт.
Релейные выходы	2 шт. NI/NO
Тип питания	DC, 12..48 В
Наличие резервированного блока питания	да
Габариты оборудования	160(Г) X 190(В) x 70(Ш) мм
Тип монтажа	Din рейка 35 мм
IP	40
Диапазон рабочих температур	–5°... +55° С (пассивное охлаждение)
Диапазон температур хранения	–40°... +75° С
Относительная влажность	5...95 %

Ждем Вас на стенде!

павильон 2, зал 10, стенд С 20

Вопросы?

Благодарим за внимание!

Воробьев Сергей
Менеджер по продукту
RTT
тел: +7-495-234-9-777 доб. 250
e-mail: s.vorobyev@rusteletech.ru

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

RTT