Обзор решения

iRZ Агрегация

Содержание

1. Общие сведения **3**
2. Функции и возможности **4**
2.1. Агрегация каналов 4
2.2. Отказоустойчивость 4
2.3. Балансировка и маршрутизация 4
2.4. Безопасность 4
2.5. Управление и мониторинг 4
3. Примеры применения **5**
3.1. Пример 1 5
3.2. Пример 2 5
3.3. Пример 3 5
4. Заключение **6**

1. Общие сведения

iRZ Агрегация – это программное решение для объединения нескольких независимых каналов связи в единый высокопроизводительный туннель со стабильным соединением.

Продукт предназначен для корпоративных заказчиков, которым критически важна непрерывность передачи данных: промышленных предприятий, транспортных компаний, операторов видеонаблюдения, финансовых организаций и прочих.

iRZ Агрегация поставляется в виде виртуальной машины, совместимой с системами виртуализации (VMware, Microsoft Hyper-V), и управляется через ОС **irzOS**. Работает на роутерах iRZ с операционной системой irzOS.

2. Функции и возможности

2.1. Агрегация каналов

Система объединяет несколько каналов связи (мобильные, Ethernet, Wi-Fi) в один логический туннель. Это позволяет **суммировать пропускную способность** каждого из каналов за исключением затрат на поддержание функционирования туннеля – итоговая скорость соединения возрастает.

2.2. Отказоустойчивость

При нестабильном соединении обеспечивается **непрерывная работа приложений** (видеопотоков, систем удаленного управления, промышленных контроллеров). Это достигается за счет автоматического перераспределения трафика по оставшимся каналам в случае отказа одного из них.

2.3. Балансировка и маршрутизация

Нагрузка динамически распределяется между каналами на основе их текущего состояния (задержка, загрузка, качество сигнала). Поддерживается гибкая политика маршрутизации для приоритизации критичного трафика.

2.4. Безопасность

Используются безопасные методы аутентификации клиентов, шифрование служебных данных. Система **пропускает любой протокол шифрования**, включая VPN-протоколы (IPSec, OpenVPN, WireGuard) и протоколы безопасности (TLS/SSL для HTTPS), без конфликтов и снижения производительности.

2.5. Управление и мониторинг

Удобное управление через **понятный веб-интерфейс irzOS**, сбор статистики по каналам. Доступна подробная техническая документация для ИТ-специалистов.

3. Примеры применения

3.1. Пример 1

Проблема: при использовании одного канала обрыв связи распознается системой как аварийный сигнал, что приводит к ложным остановкам производства.

Задача: непрерывная передача показаний датчиков (давление, температура, вибрация) с удаленных объектов.

Решение: агрегация двух независимых каналов обеспечивает штатную передачу данных даже при отказе одного из них. Логический туннель скрывает физическую структуру каналов, исключая интерпретацию разрыва как сигнала аварии.

3.2. Пример 2

Проблема: разрыв соединения в момент транзакции приводит к отклонению операции, потере клиента и рискам несоответствия требованиям PCI DSS к доступности инфраструктуры.

Задача: стабильная авторизация платежей в условиях слабого покрытия или перегруженных вышек.

Решение: объединение нескольких сотовых линий гарантирует непрерывность TCP-соединения. Трафик автоматически перераспределяется на работающий канал без разрыва сессии авторизации.

3.3. Пример 3

Проблема: при обрыве канала без агрегации туннель перестраивается, что вызывает задержки и потерю контекста сессии.

Задача: организация защищенного туннеля для инженерных бригад, видео-инспекций или удаленного доступа к серверам.

Решение: агрегация сохраняет туннель активным независимо от состояния физических каналов. Непрерывность передачи сохраняется даже при непредсказуемой деградации качества связи.

4. Заключение

iRZ Агрегация — это промышленное решение для задач, где недопустимы простои связи или потеря данных.

С внедрением системы:

- **повышается надежность** сервисов (автоматика, беспилотный транспорт, видеонаблюдение);
- **растет эффективность** использования имеющихся каналов связи без замены инфраструктуры;
- операционные **риски снижаются** за счет автоматического переключения при отказах.

Рекомендуется к внедрению на объектах с высокими требованиями к доступности сети, а также в сценариях, где требуется увеличение пропускной способности без перехода на дорогостоящие выделенные линии.