Группа компаний

Реализация устойчивого периметра внешней и внутренней защиты ИТ инфраструктуры компании. Создание непрерывной работы бизнеса в гибридном ИТ ландшафте.

Как у нас было?

- Бэкапирование происходило на сервера, где находились ИС
- Отсутствие мониторинга со стороны ИС и ИБ
- Не было кластеризации основных критических ИС
- Сервера, рабочие станции, сетевое оборудование были в одной локальной сети
- Не было резервирования интернет каналов
- Файрволлы отсутствовали, на периметре сети были только маршрутизаторы
- Контейнер хранения и выдачи паролей отсутствовал
- Не было 2FA при подключении к VPN
- Защита от внешних угроз отсутствовала (в первую очередь от DDOS-атак сайта и клиентского портала)
- Вся инфраструктура заводилась в домен компании (компрометация домена = компрометация всех процессов)

План действий

- Разработать DRP план и организовать бэкапирование по принципу 3-2-1.
- Построить ИТ инфраструктуру во втором ЦОДе для кластеризации бизнес критических ИС.
- Построение мониторинга на базе систем Zabbix, Grafana, SIEM, EDR.
- Всю сеть разделить по VLAN. В основных каналах организовать шифрование IPsec
- Сделать резервирование интернет каналов и заменить маршрутизаторы.
- Установка в ЦОДах фаерволов
- Покупка ПО для хранения ключей.
- Организация 2FA аутентификации.
- Организация защиты от внешних угроз. Выбор ПО.

Концептуальная схема сети

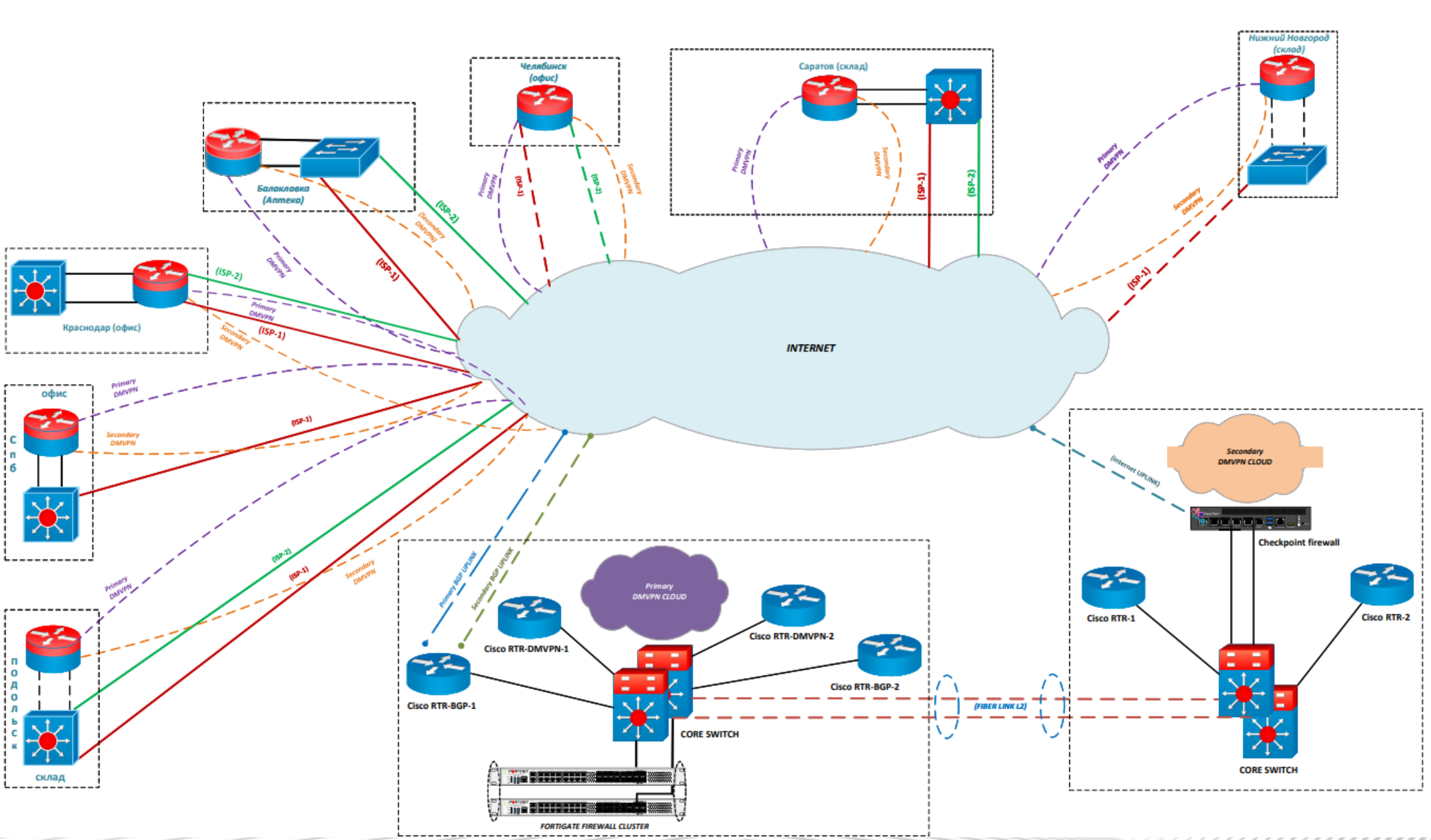
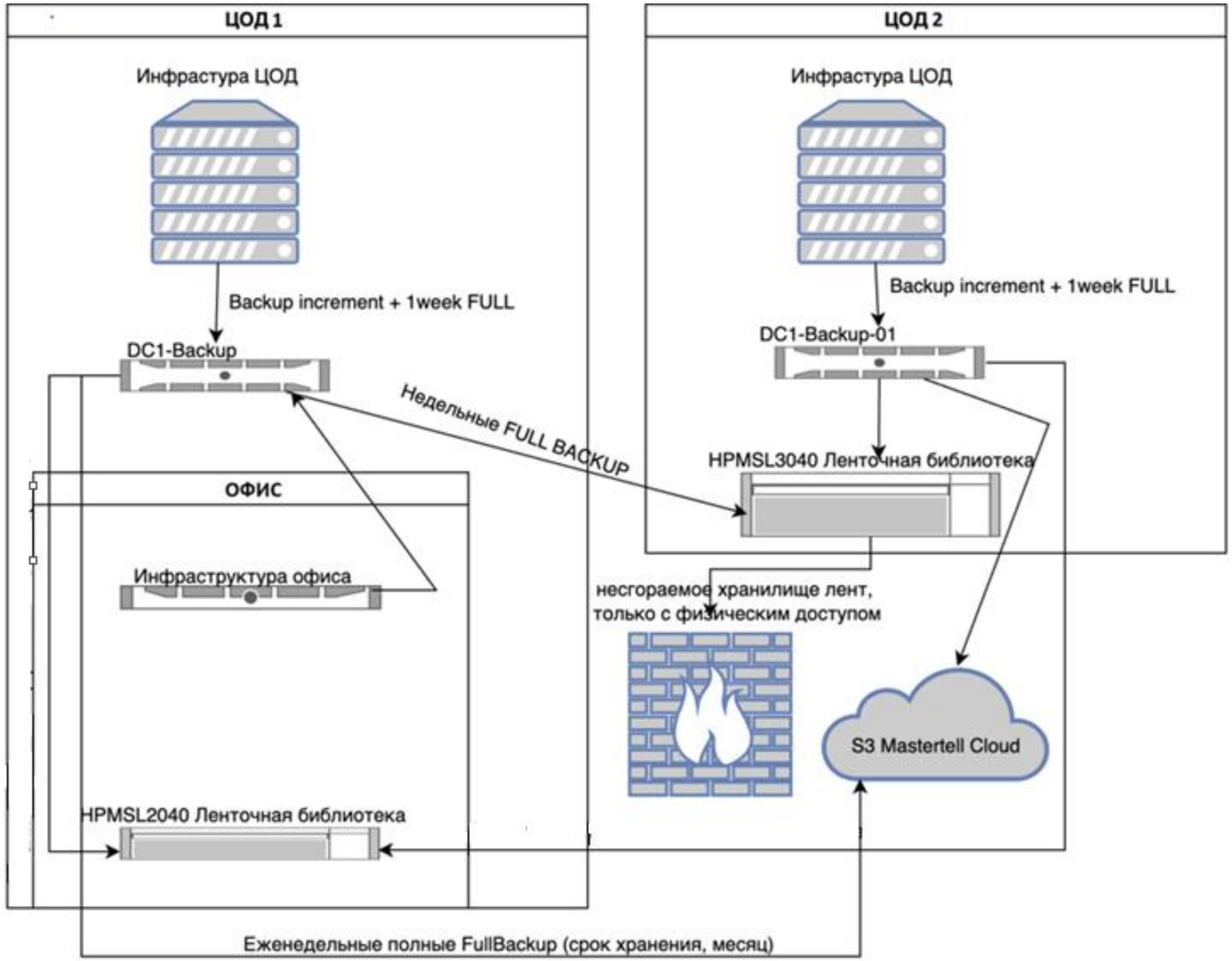


Схема бэкапирования 3-2-1.



Итоги работы