

1. На схеме видим порядка 8 сетей. Первым делом надо составить план по адресации всех сетей и составить план сегментации.
2. Если для подключения между сетями используется сеть интернет, то данные сети необходимо оснастить на границах файрволлами типа Cisco ASA или Firepower. Для подключения между сетями предпочтительно использовать IP-VPN подключения или шифрованные IP-SEC туннели. На данных файрволлах можно было поднять сервис VPN и использовать его, вместо отдельного VPN концентратора. Чем меньше устройств в цепочке, тем выше отказоустойчивость.
3. В идеале придерживаться подключения кабель провайдера –> файрволл/vpn -> маршрутизатор.
4. В ЦОДе надо разнести адресацию дополнительно, к примеру, АД, почта, MSSQL в одной сети, сервер приложений и сервер статистики в другой сети. Данная сегментация поможет отлавливать запросы между этими сетями.
5. Сервер приложений и сервер Branch Hub использует кучу портов, необходимо проанализировать их все и оставить только защищенные и только те, которые используются в работе.
6. Аналогичная ситуация между сервером статистики и сервером Branch Hub. Убрать незащищенные порты и перенастроить.
7. Далее общие рекомендации. Провести пентест (ISO 27001, OWASP) на наличие открытых портов как на границах периметра, так и внутри каждой сети.
8. Установить SIEM систему для анализа и сбора журналов со всех сетевых устройств для обнаружения несанкционированных действий.
9. Установка антивирусного ПО на всех серверах и рабочих станциях.
10. Исключить прямого подключения партнерского канала связи на прямую в нашу локальную сеть.
11. Возможно следует разрешить подключение к серверу Branch Hub только через реверс прокси и исключить прямое подключение по ip-адресу.