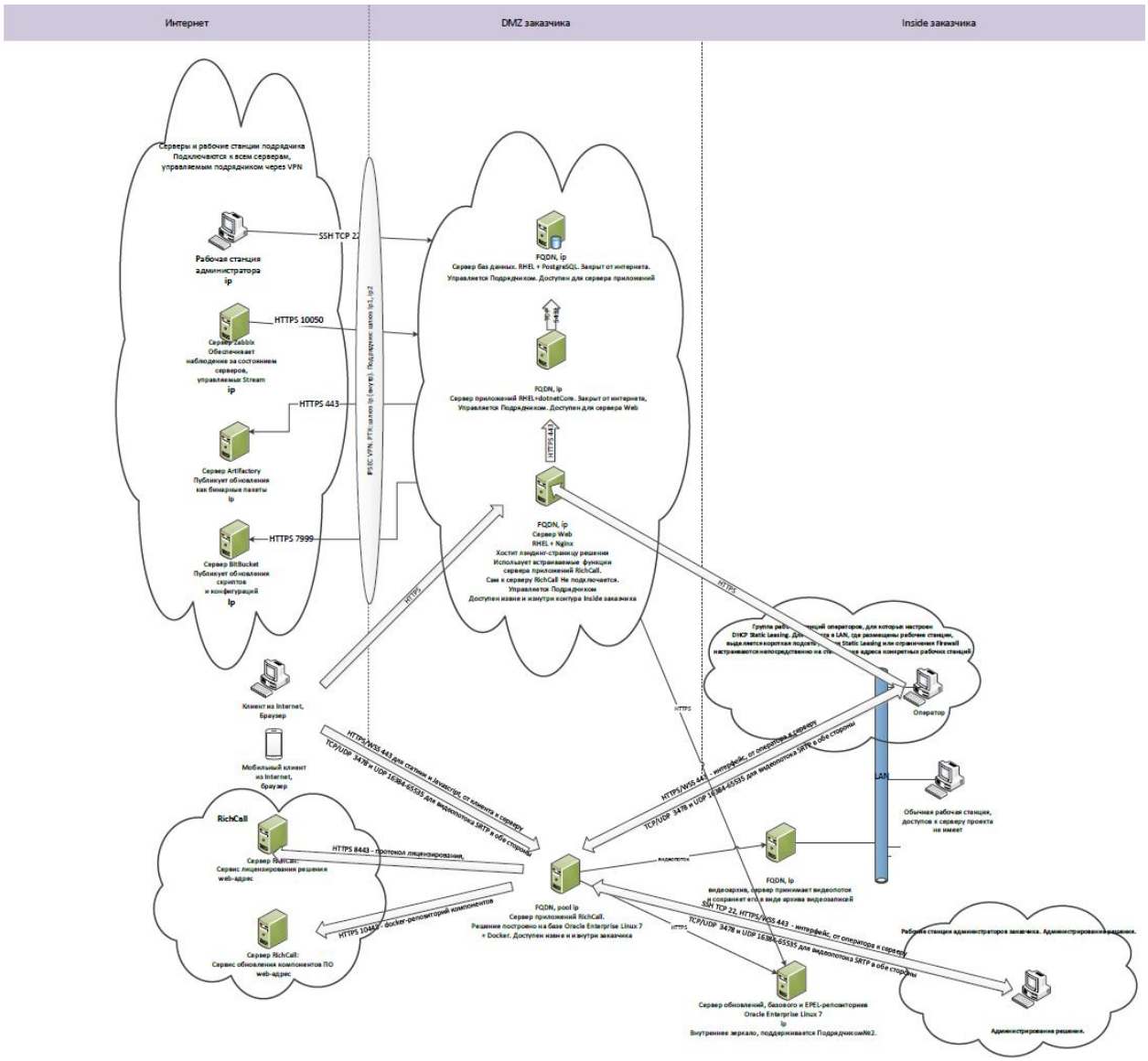
Хананиев Даниил Владимирович
Курс «Подготовка к собеседованию специалиста по информационной безопасности», поток от 20.05.2020
ДЗ № 7



Опять только первая схема. Честно говоря, я не очень понял задания. Что тут еще можно сказать в дополнение сказанному ранее… Даже если посмотреть на эту схему с точки зрения микросервисов в облаке, мы всего лишь экстраполируем нашу предыдущую оценку на новый лад, принципиально ничего нового в схеме мы не видим, если не считать потенциально увеличившиеся риски ИБ из-за добавления еще одного лица – поставщика облачных решений, который имеет как минимум физический доступ к инфраструктуре. Ок, попробую что-нибудь написать, не повторяясь.

1. Решение в облаке, потому в нашей LAN выделяем VLAN для работы именно с этим приложением (там операторы, сервер обновлений, администраторы, видеоархив), vpn к облаку и к серверу приложений RichCall (будем считать, что он тоже в облаке).
2. От провайдера облачных услуг сертификаты ISO, выполнение ругуляторных требований и результаты последнего аудита.

3. Уязвимые данные в облаке – сервер баз данных и видеархив. Т.е. необходим контроль данных и управление их жизненным циклом. Все тот же принцип AAA, шифрование трафика, логи, SIEM, etc.
4. Точки входа – сервер web и RichCall. Все тоже AAA, шифрование трафика, двухфакторная аутентификация, аудит, логи, etc.
5. Контроль кода веб-приложения, пентестинг.
6. И полный контроль, аудит всех узлов, впрочем я уже это писал, сеть (IPS), сервера, рабочие станции, антивирус, почта, все централизованно приходит в SOC, любого уровня, от опенсорсной системы сбора и анализа логов до монструозной SOAR.