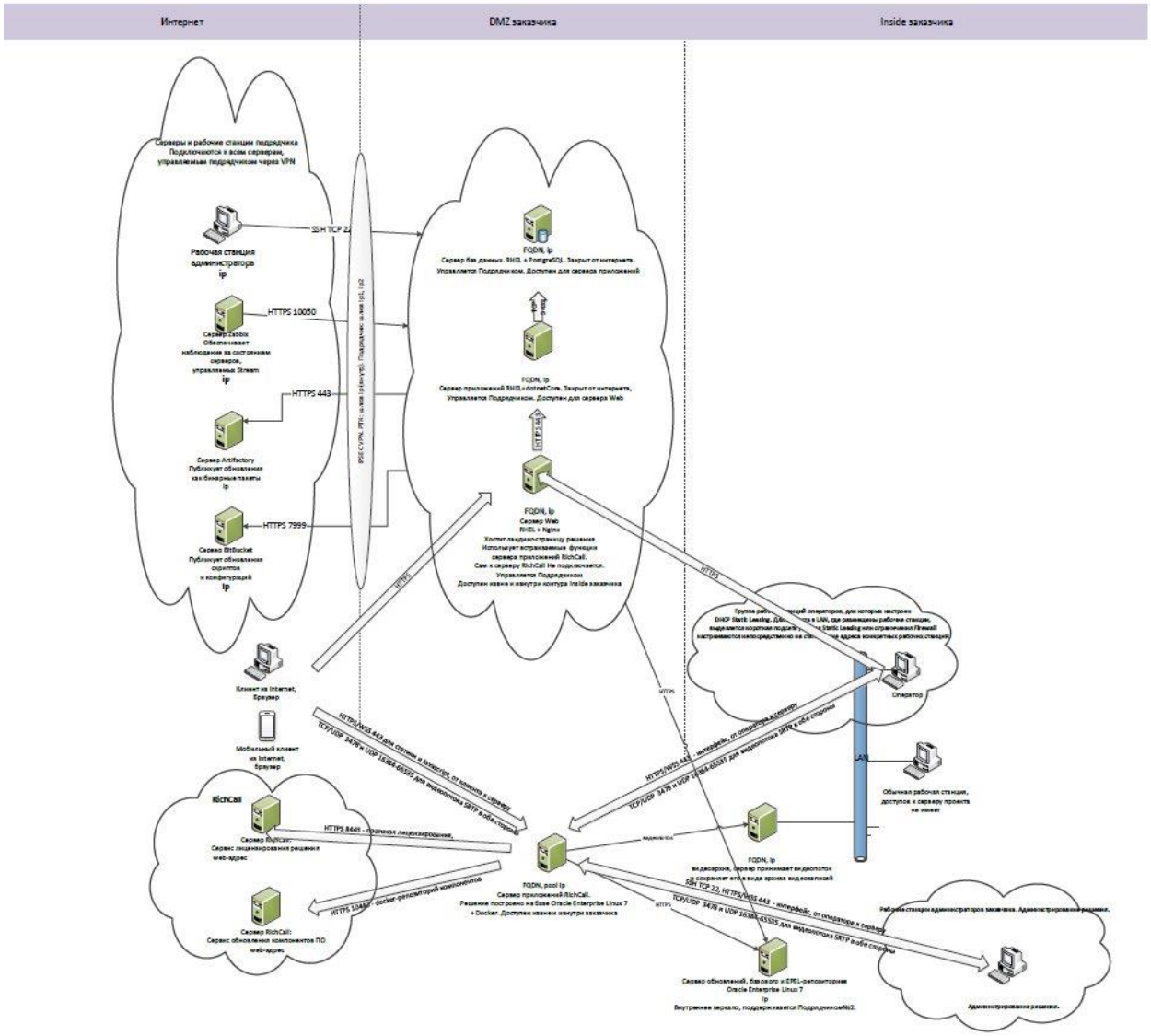
Домашка № 7

Лешков И.А.

Задание №1.

К уроку приложена схема реализации инновационного проекта – продолжение схемы из Урока 6. Составить свою экспертную оценку по поводу наличия угроз и уязвимостей проекта, детализировать аналитическую оценку, аргументировать и предложить варианты защиты от угроз.



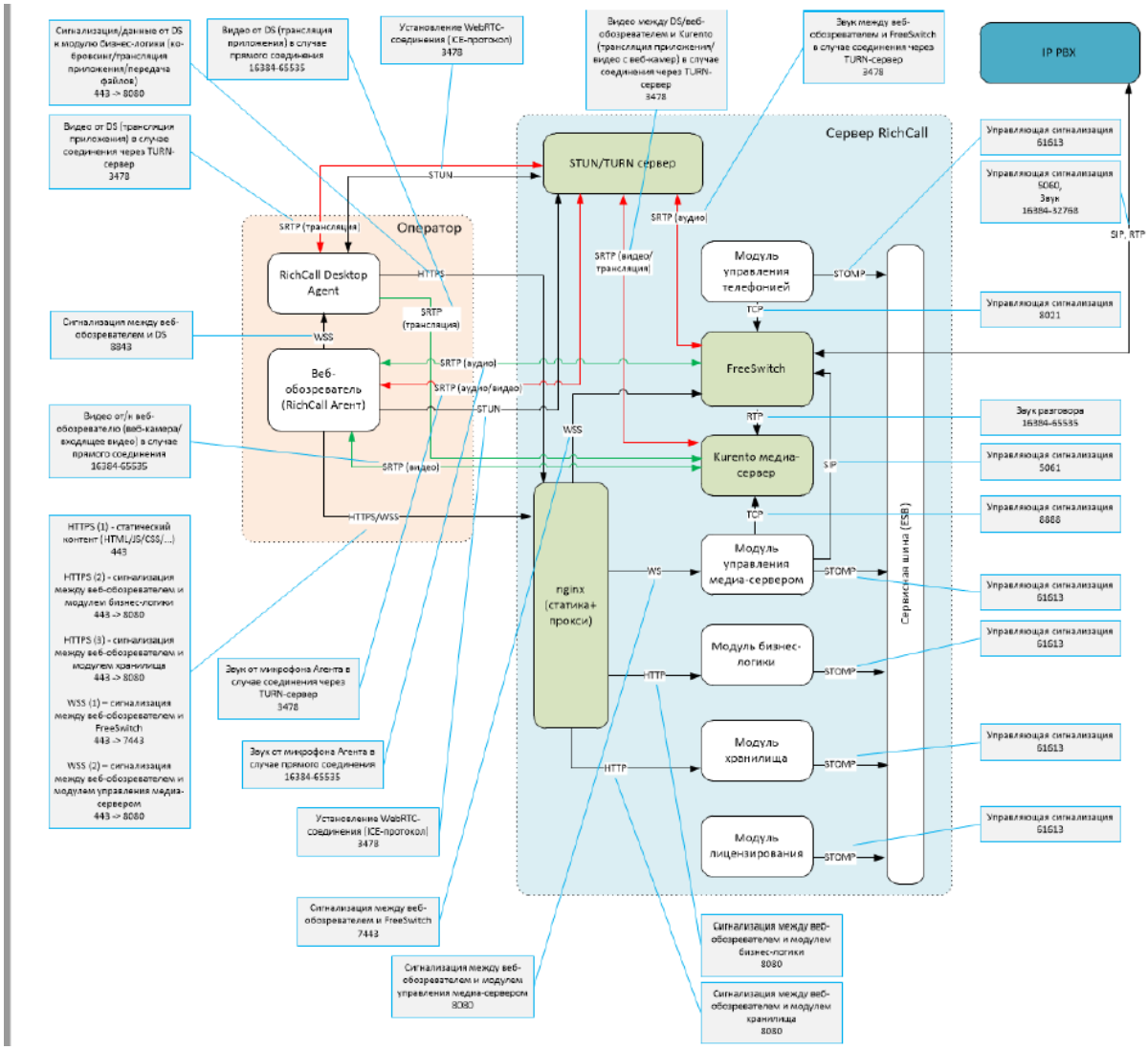


Схема проекта "Виртуальный магазин", страница 3

Для сервера RichCall

направление	порт	пр-кол	описание
Incoming/Outgoing	443	tcp	web (nginx, web)
Incoming/Outgoing	3478	tcp/udp	сигнальный порт для организации TURN/STUN каналов
Incoming/Outgoing	5060	tcp	SIP – сигнальный трафик (FreeSWITCH – корпоративная IP-PBX)
Incoming/Outgoing	16384-65535	udp	rtp медиа-трафик
Outgoing	8443	tcp	Сервис лицензирования[1]
Outgoing	10443	tcp	Сервис обновления[2]

Для внешних клиентов:

направление	порт	пр-кол	описание
Outgoing	443	tcp	web (nginx, web)
Outgoing	3478	tcp/udp	сигнальный порт для организации TURN/STUN каналов
Incoming /Outgoing	16384-65535	udp	rtp медиа-трафик от/к клиенту

Для агентов RichCall:

направление	порт	пр-кол	описание
Outgoing	443	tcp	web (nginx, web)
Outgoing	3478	tcp/udp	сигнальный порт для организации TURN/STUN каналов
Incoming /Outgoing	16384-65535	udp	rtp медиа-трафик от/к агенту

[1] Используется конкретный адрес сервера лицензирования
[2] Используется конкретный адрес сервиса обновления

Глядя на ИС выше, можем наблюдать некую торговую площадку (виртуальный магазин), расположенную в 3-х сегментах: Интернет, DMZ-заказчика и Inside-заказчика с применением облачных решений для обслуживающих серверов и подрядчиков, с организованным VPN-туннелированием, при использовании стандарта безопасности ip-протокола >>> IPSec.

Итак, совершенно логичным является тот факт, что – это торговая площадка, с огромным клиентским насыщением, а соответственно с огромным количеством чувствительной информации (конфиденциальные данные пользователей, коммерческая тайна заказчика, и.т.д), как в текстовом, так и видео/аудио контакты. Поэтому, здесь обязательно нужно задуматься о:

- Наложении норм российского законодательства в области обеспечения защиты информации (ФСТЭК), а также о внедрении норм различных «бестпрактисов» для обеспечения ИБ на каждом из уровней.
- Внедрение технических мер защиты (на схеме они отсутствуют), таких как:
  - Фаерволлы (к примеру сервер Rich Call и сервер Web, к которым есть прямой доступ из внешней сети).
  - Внедрить ids/ips системы для защиты, к примеру, от DDos-атак (тут есть явная угроза, так как открыто слишком много портов для видеопотока SRTP в обе стороны), например, настроить динамическую маршрутизацию через BGP на уровне провайдера – метод “blackhole”(метод позволяет полностью прекратить поток трафика на атакуемый сервер и снять нагрузку с каналов AS и провайдера).
  - Также задуматься о поднятии SIEM-системы.
  - Обязательное применение СКЗИ (для всех типов данных)
  - Антивирусное ПО для серверных и пользовательских решений
  - Строгое разграничение доступа
  - Провести пентест и сканирование всей архитектуры на наличие уязвимостей
  - Задуматься о выделении отдельной области для хранения и бэкапирования данных.
  - Наличие серверов обновлений наводит на мысль о необходимости применения анализаторов кода для контроля за содержимым репозиториев и своевременного эффективного патчинга возможных уязвимых мест.
- По первому рисунку ещё обратить внимание на открытые порты и необходимость использования SSH, к примеру.
- Что касается внутрянки серверов и 2-го рисунка, то стоит обратить внимание на незащищенные протоколы и соединения с модулями бизнес-логики (HTTP, WS не годятся). Также между модулем FreeSwitch и медиа-сервером использовать более защищенный SRTP.
- Также задуматься о стандартных портах и возможности их замены на нестандартные.

- Касаемо правил фаерволлинга (рис.3), задуматься о необходимости двухсторонних соединений, особенно, касаясь внешних пользователей и агентов RichCall
- Вместе с тем, как уже упоминал выше, подумать о внедрении защиты от DDoS-атак, касаемо наличия SRTP медиа-траффика.

Теперь, немного коснёмся инновационных тенденций в IT. Как я уже описывал в практике к уроку, в данном проекте можно задуматься о:

- ✓ Безопасности и конфиденциальности “BigData” (больших данных) путём внедрения усиленной и стойкой криптозащиты любых потоков данных, гранулированного контроля доступа, мониторинга безопасности в режиме реального времени, итд.
- ✓ Корреляция веб и мобильных приложений, проверка на уязвимости последних, согласно «бестпрактисам» >>> OWASP, грамотная конфигурация компонентов серверов и баз данных, обеспечение многофакторки, итд.
- ✓ В проекте присутствуют облачные решения (“Cloud services”), поэтому здесь важно обеспечить централизованное управление и следовать стандартам и best practice, а также проводить регулярный пентест, с целью обнаружения точек входа потенциальных злоумышленников, итд.
- ✓ Проект предполагает присутствие систем виртуализации и контейнеризации, а посему, проведение автоматизированной проверки уязвимостей контейнеров, обеспечение контроля доступа, использование API и другие меры необходимы для предотвращения или смягчения последствий угроз и атак на платформы виртуализации, ядро системы, итд.

И в заключение, хотелось бы отметить то, что важно понимать, что внедрение соответствующих СЗИ и их взаимодействие, должно происходить без конфликтов и конечно же не мешать, и не отсекать излишне пользовательский траффик, и как следствие, задуматься о тех мощностях, которые позволили бы равномерно распределить нагрузку и позволить всем легитимным пользователям беспрепятственно получать доступ ко всей необходимой информации.

Так как, в конечном итоге, именно наличие пользователя-клиента определяет успешность бизнеса.

//Done… ☺