1. Доброго дня, коллеги

Я индивидуальный предприниматель, зовут меня Житков Виталий Петрович

Специализируюсь на построении и сопровождении защищённых информационных систем и являюсь действующим CCSE+

Сегодняшняя презентация о решениях для информационных систем на основе ROS.

1. Сегодня мы поговорим об информационной системе, о способах взаимодействия внутри информационной системы и способах взаимодействия конечных пользователей с информационной системой. Так как мы находимся на MUM, основная тема – ROS.
2. Классическое определение Информационной Системы. И совсем неважно где и кем эта информационная система постороенна.
3. Данная схема очень приблизительно отражает принцип построения информационной системы. Т.е. есть бизнес – владелец информации. Информация может быть территориально распределена. Узлов, где находится информация – множество. Сама по себе информация, которая записана на носителях без представления в читаемый вид не представляет интереса. Т.е. необходимы средства для обработки информации и выдачи результата конечному пользователю. При этом способы взаимодействия с информацией должны подчиняться принципу 3А (доступность, непрерывность, безопасность). Так как для работы с информацией необходимо сетевое взаимодействие, то и оно должно соответствовать принципу 3A. В данной презентации рассматривается реализация принципа 3A на основе оборудования и программного обеспечения mikrotik.
4. Виды информационной системы:
5. Не участвует в презентации
6. Локальная – малый бизнес (краткое описание, плюсы\минусы)
7. Не участвует в презентации
8. Гибридная – средний бизнес (краткое описание, плюсы\минусы)
9. Не участвует в презентации
10. Облачная – средний, крупный бизнес (краткое описание, плюсы\минусы)
11. Не участвует в презентации
12. Локации доступа к информационной системе  
    Дата центр. Специализированный уровень физического и технологического доступа.   
    Офисная сеть. Находится в сфере ответственности компании. Уровень доступа зависит от наличия \ отсутствия регламентов и степени их соблюдения. Степень соблюдения регламентов, в свою очередь зависит от многих факторов. Одни из основных факторов являются:  
    - Уровень понимания руководством и персоналом необходимости соблюдения регламентов доступа к информационной системе.  
    - Уровень компетенции обслуживающего персонала  
    - наличие \ отсутствие программно-аппаратных средств. Затратная часть на реализацию программно-аппаратной части обеспечения информационной безопасности Информационной Системы может быть очень существенная.   
    - Домашняя сеть сотрудников. То происходит в локации доступа зачастую не знает даже владелец локации.  
    Сети общего пользования.   
    - Транспорт  
    - интернет кафе  
    - Сети операторов мобильной связи  
    - Гостиничные сети  
    - Публичные хот споты.  
    Так как данные локации не контролируемы ни в каком виде владельцем информационной системы, то являются наиболее опасными локациями доступа. Поэтому при доступе из подобных мест необходимо обеспечить по возможности контролируемый доступ. Минимальным в данном случае является обеспечение доступа при помощи технологий и протоколов VPN.
13. О чём никогда не надо забывать:   
    Межсетевое экранирование  
    Удалённое взаимодействие посредством VPN
14. Виды межсетевого экранирования:   
    Пакетное межсетевое экранирование на основе источника и получателя.  
    Statefull Inspection – анализ поведения сессий и протоколов.  
    Существует ещё один вид сетевой защиты – Deep Security. Анализ сессий на уровне приложений. Системы IDS\IPS.
15. Краткий обзор вендоров VPN. Слайд в презентации не участвует.
16. Тип поддерживаемых технологий построения VPN туннелей ROS (основные)
17. Тип поддерживаемых технологий построения VPN туннелей ROS (IPSec)
18. Тип поддерживаемых технологий построения VPN туннелей ROS (MPLS)
19. Существуют разные способы построения туннелей. От туннелей на уровне L2 до туннелей уровня L3. ROS поддерживает большинство типов. Можно более детально посмотреть список, скачав презентацию или найти описания в Wiki. Виды туннелей бывают  
    Сеть в Сеть (Site to Site)   
    Клиент к сети (Client to Site)
20. Client to Site
21. Site to Site  
      
    Примеры решений на основе ROS
22. Построение сети загородного дома.  
    Три этажа  
    Общая площадь 1800 квадратных метров + двор, который тоже необходимо покрыть бесшовным роумингом.  
    Стены кирпичные. Каждая стена с обеих сторон облицована двойной металлической решёткой.   
    Взяли ноутбук с Proximity картой и три точки доступа. Произвели обследование беспроводного покрытия дома.  
    Общее число необходимых точек доступа получилось четырнадцать штук с учётом двора. На двор пошло две уличные точки доступа. В доме 13 точек доступа и MikroTik Cloud Router Switch CRS125-24G-1S-2HnD-IN в качестве пограничного маршрутизатора, межсетевого экрана, cAPMan контролера. Ресурсов вполне хватило. Прекрасное соотношение цена\качество. ISP подключили SFP. Правда пришлось согласовывать с ISP режим подключения (1 Gb Full Duplex) последней мили. Пару SFP приобретали отдельно. Один модуль выдали ISP. После этого провайдер пошёл на встречу и всё настроил со своей стороны.  
    Были другие подобные проекты в которых вопрос подключения по оптике с провайдером согласовать не удалось. В этих проектах использовали медиа конвертор, выданный ISP . То есть в медиа конвертор пришла сто мегабитная оптика, перешла в медь. Медь подключили в Ethernet порт.  
    Тринадцать портов из двадцати четырёх ушло на коммутацию точек доступа. Остальные сетевые порты были использованы для подключения принтеров, телевизионных панелей, IP приставок. Нескольких Ethernet розеток.  
    В качестве точек доступа использовали hAP AC Lite  
    Два диапазона  
    PoE in  
    Четыре свободных Ethernet порта.  
    Небольшой размер.  
    Прямоугольная форма   
    Прекрасно разместили в технологических люках.  
    Для обеспечения питания точек доступа использовали две 8 портовые PoE панели с внешними блоками питания.  
    По просьбе клиента выбрали и смонтировали вызывную панель на входной калитке.  
    Возможные способы взаимодействия с вызывной панелью.  
    Смонтированные видео терминалы внутри дома.  
    SIP телефоны, расставленные по дому с возможностью видео звонков.  
    Сматрфоны, планшеты.  
    GSM телефоны.
23. Классическая реализация гибридной схемы информационной системы.   
    Компоненты :   
    Облачная инфраструктура  
    Офисная сеть  
    Удалённые пользователи.  
    Так как облачная инфраструктура расположенная в ЦОД, который обладает высоким уровнем SLA и предоставляет услуги по резервированию каналов связи, электропитания, то разумнее точку входу и подключения располагать там.  
    В офисной сети уровень SLA однозначно меньше. Чем в ЦОД. Поэтому площадка может быть использована для обеспечения рабочих мест сотрудников. Конечно можно всё разместить и на площадке офиса, но тут будет необходимо решить вопросы с резервированием каналов связи, электропитания, резервированием аппаратных платформ, климат-контролем, резервным копированием. Необходимо наличие высококлассного персонала, у которого высокий уровень заработной платы.  
    Покупка и обновление аппаратных ресурсов.  
    Покупка и обновление программного обеспечения.  
    То есть содержать полностью информационную систему на своих ресурсах и обслуживать ей экономически невыгодно. Очень высокий уровень TCO (совокупная стоимость владения).   
    Это классическая схема используется чаще всего.   
    В офисе ЛВС. Необходимое сетевое оборудование. Рабочие места офисных пользователей.  
    Файловый сервер (обычно Linux + Samba + Kerberos). Иногда резервный контролер домена и сервер IP-телефонии.
24. Часто при выполнении бизнес-задач необходимо решать более сложные вопросы.  
    В качестве примера.  
    Бизнес оказывает услуги по контролю физического и автомобильного доступа на придомовые территории в Москве и Подмосковье.  
    Необходимо решать задачи по контролю за удалёнными объектами.  
    Изначально бизнес попробовал обойтись сетевым оборудованием дешёвого домашнего сегмента. Не получилось. Домашнее сетевое оборудование не является даже полу промышленным.   
    Бизнесу было предложено перейти на сетевое оборудование Микротик.  
    Запустили пилотный проект.  
    Через два месяца пилотного проекта было принято решение полностью перейти на сетевое оборудование Микротик.  
    Следующий вопрос. Который необходимо было решить – консолидировать сервисы используемые бизнесом.  
    Изначально заказчик хотел все сервисы консолидировать у себя на площадке в офисе.  
    Совместно провели расчёт бюджета, необходимого на реализацию данного желания заказчика.   
    Заказчик увидел ИТОГО бюджета.   
    У него возник вопрос, «Как реализовать необходимые и достаточные мероприятия с существенным уменьшением конечной стоимости.  
    Было предложена реализация в облачной инфраструктуре.  
    Опять совместно посчитали стоимость бюджета.  
    Договорились с облачным провайдером о тестовом периоде (по сути финансовых каникулах) для реализации пилотного проекта по консолидации сервисов.  
    Запустили пилотный проект.  
    Через два месяца заказчик решил, что сервисы, расположенные в облачной инфраструктуре его полностью устраивают   
    В результате получилась следующая схема (слайд 25);  
    На всех объектах используется различное оборудование Микротик.  
    Аппаратные платформы:  
    От MikroTik hAP Lite Tower   
    До MikroTik SXT 4G kit  
    В среде виртуализации изначально использовали Микротик x86. Но в какой то момент заметили, что очень высокая утилизация узла при увеличении сетевого трафика. При загруженности 100 мегабитного канала примерно на 60% утилизация узла составляла около 90%.  
    В процессе траблшутинга было выяснено, что платформа x86 в среде виртуализации поддерживает только сетевые адаптеры Legacy.  
    Приняли решение перевести центральный сетевой узел в среде виртуализации перевести с платформы x86 на платформу CHR.  
    Как только перевели, сменив тип сетевых адаптеров с Legacy на Synthetic всё пришло в норму.  
    Со временем выяснилось, что ширины канала в 100 мегабит не хватает. В основном трафик шёл от видео в HD качестве. Одна камера берёт примерно от 1,5 до 2,5 мегабит.  
    Понятно, что видео шло только когда происходило обращение к камере или, когда срабатывал датчик движения.   
    Вышли из положения не расширением канала у облачного провайдера, а арендой ещё одного 100 мегабитного линка.
25. Упрощённая схема взаимодействия внутри информационной системы. Которая получилась в результате.
26. На некоторых объектах было проблематично проложить витую пару или оптику. Просто ФСО не давало разрешение. Было предложено внутри сетевое взаимодействие с использованием беспроводных мостов.  
    В качестве примера:   
    Район Кутузовского проспекта.  
    Использовали уличные 5 Ггц беспроводные мосты. На некоторых устройствах беспроводной сети, для уменьшения затрат пришлось увеличить уровень лицензии с L3 до L4. Превратив устройство из компонента сетевого моста в полноценную точку доступа. К такому устройству возможно подключить более одного устройства беспроводным методом. Это позволило уменьшить на 4 штуки количество устройств, используемых для организации беспроводных линков.
27. Что получилось в результате.  
    Всё это работает исключительно на оборудовании Микротик.  
    были попытки перейти на убикьюти. Но в результате отказались от этого. Причины была исключительно одна – надёжность работы. Оборудование убикьюти греется и часто приходится или приезжать перезагружать (ибо оборудование просто становится недоступным), либо просить это сделать кого-то на объекте, либо колхозить стороннее решение для удалённой перезагрузки оборудования. Например GSM розетки.
28. Продолжение
29. Продолжение
30. Продолжение
31. И последний слайд.  
    Построение географически распределённого сетевого кластера га основе CHR.  
    Для некоторых видов бизнеса необходима постоянная работа с клиентами. Одним из методов взаимодействия бизнеса со своими клиентами является системы лояльности.  
    Система по сути работает в режиме real time.  
    Работоспособность данной системы должна быть высокой. Уровень SLA должен быть не менее 98%. Даже учитывая сетевую доступность.  
    Компания, занимающаяся системами лояльности. периодически теряла свои сервисы. из-за сетевой недоступности. Основная причина недоступности сервисов – заказная DDoS атака.  
    Обратились к облачному провайдеру с просьбой решить вопрос с доступностью сервисов.  
    Облачный провайдер обратился с этим вопросом ко мне.  
    Решение должно быть недорогим, работоспособным.  
    Произвели обследование проблемы.  
    Два географически распределённых ЦОДа в Москве.  
    ЦОДы согласно правилам построения ЦОД имеют несколько входящих линий оптики, приведённых не пересекающимися трассами. У каждого ЦОДа свои подключения.  
    Между ЦОДами облачный провайдер согласовал и проложил две независимые нитки «серой оптики».   
    Предложил решение.  
    Инициировали пилотный проект на площадках в обоих ЦОДах  
    Две недели пилотный проект тестировали в стресс тестах.  
    Предложили решение конечному заказчику.  
    Согласовали с заказчиком этапы и время внедрения.  
    Произвели внедрение.  
    Система работает более шести месяцев.  
    Суть решения.  
    На уровне L3 работает BGP, что позволяет обеспечивать доступность маршрутов.  
    Уровень L2 серой оптики обеспечивает работоспособность VRRP.  
    Для обеспечения доступности сервисов VRRP настроен на всех сетевых интерфейсах кластера.  
    Да, можно было поднять реализацию BGP, непосредственно на сетевых маршрутизаторах CHR. Установленных в разных ЦОД, но в результате не получился бы полноценный кластер. Да и ресурсов бы понадобилось гораздо больше, чем при построении VRRP кластера.