Расставить IP. Настроить фреймворк. Поставить НАТ и адрес пустой опена, потом исправивить.

Настроить SQL, потом зайти включить его настройки.

Установить ЦУС, настроить его. Скачать УКЦ, поменять пароли. Установить везде клиента.

В ЦУС создать и отправить справочники. В УКЦ создать дистрибутив, зайти в вся сеть – отправить в ЦУС, зайти в пользователи – снять галочку – передать в ЦУС. Раздать ключи. Настроить корд. Изменить IP админ и опен. Отправить справочники. УКЦ – пользователи – поставить галочку – передать в ЦУС. Проверить связь. Установить ЦУС на опен, но не настраивать.

Зайти в клиент на админе – фильтр открытой сети – создать. Название ClientЦУС, пропуск трафика, источники 10.0.0.3, протоколы 9000-9900 - применить.

При входе в ЦУС на опене 10.0.0.2(адм).

Перейти в ЦУС на адм нажать на маленький сертификат – создать пользователя admindb и войти в ЦУС на опен.

Зайти в интернет на админе 10.0.0.1:8080 – как админ – межсетевой экран – локальные фильтры – добавить HTTP8080 – Галочка фильтровать трафик, пропускать - источник 10.0.0.3 – название мой узел – TCP 8080 – сохранить – применить.

Зайти на опене в интернет 10.0.0.1:8080 и ничего…

Аккредитованный режим: УКЦ настройки – программные средства – галочка, автоматезир работа тоже галочка, настроить вбить данные.

(по заданию чуть дальше) Настройки – Программные средства – Функционировать в режиме аккредитованного удостоверяющего центра поставить галочку; Автоматический режим – переходить в автоматический режим работы через 15 мин.

Создание корневого сертификата. УКЦ настройки – администрирование – создать ЛКМ корневой сертификат. Demo.lab [admin@demo.lab](mailto:admin@demo.lab), Казань и тд.

УКЦ – пользователи кроме кордов – Админ, опер, пользователь 2 – стоит галочка, передать в ЦУС ([admin@demo.lab](mailto:admin@demo.lab), Казань и тд.).

Для электронной подписи у пользователя 2 – стоит галочка, создать электронную подпись. Указать файл (УЦ).

Проверить на сетевых узлах опер – передать в ЦУС. Создать/отправить справочники.

УКЦ настройка – публикация данных – скопировать путь – дать общий доступ папке публикейшен.

Настроить переход в автоматический режим (при бездействии администратора): передачу на публикацию и обновление CRL (Действия) с периодичностью 1 день. УКЦ настройка – автомат режим. Действия - Обновлять списки аннулированных сертификатов. (своя сеть) Список аннулированных сертификатов – требуется передать – поставить галочку. (доверенные УЦ) Требуется передать, неактуальные.

Установить Registration Point, Publication Service на опеРЕ.

Заходим в Registration Point – Настройка - Папка ключей сетевого узла – ProgramData – InfoTeCS - Цифры. Войти и закрыть пока.

Сеть-Правой кнопкой мыши-подключение сетевого диска- \\10.0.0.2\Publication (не рабочая версия из видео \\V-1-ADM\Publication). Ввод сетевых учетных данных User-xxXX1234. Потом происходит волшебное подключение.

Далее веселье с FTP-сервером. Устанавливаем Filezilla. I agree, Next…

Connect to Server. Server-Configure-Rights management: Users. Add – User 1. Локальный диск - Создать папку Pub-pubsvr-data. В свойствах папки Pub – Безопасность – все разрешения. Справа Add Virtual path /, Natrive path C:\Pub – Apply. Далее в проводнике прописать ftp://10.0.0.4/ Пользователь User1 Проверить можно ли подключиться к ftp серверу.

В Publication Service зайти с правами администратора Публикации-Добавить-Сертификаты издателей- Тип хранилища FTP-сервер-10.0.0.4 порт 21, абсолютный путь до каталога -/ , Проверить указанные параметры-Готово.

На V-1-Adm зайти в УКЦ, выделить все сертификаты и опубликовать.

На V-1-Oper-CA зайти на ftp-сервер ftp://10.0.0.4/ Если нету опубликованных, то зайти в журнал и обновить. Появятся папки с опубликованными сертификатами.

Заходим в Registration Point-Пользователи-правой кнопкой мыши зарегистрировать пользователя- User 2. User 2- правой кнопкой мыши- сертификаты-создать запрос-далее далее.

На V-1-Adm зайти в УКЦ-Внешние пользователи. Если не приходит опросить транспортный модуль. Ключевой центр-Пользователи-Запросы на дистрибутивы ключей-Удовлетворить-далее далее. Удостоверяющий центр-Запросы на сертификаты-Необработанные запросы-Запросы центров регистрации-Удовлетворить.

На V-1-Oper-CA заходим в Registration Point – Запросы-Запросы на сертификаты-Отправленные-посмотреть чтобы статус был Удовлетворен.

Далее заходим в сертификаты и все приостанавливаем. Транспортный модуль на опере и админе чтобы быстрее пришло. На V-1-Adm в УКЦ-Удостоверяющий центр-Запросы на аннулирование сертификатов-выделяем все и удовлетворить. В Registration Point на V-1-Oper-CA Сертификаты-Статус Приостановлен. Далее аннулируем сертификаты.

На V-1-Adm зайти в УКЦ - Удостоверяющий центр-Необработанные запросы-Удовлетворить. В Registration Point на V-1-Oper-CA Сертификаты-Статус Аннулирован.

На V-1-Adm установить CA Informing, запустить Настройки Способ выдачи уведомлений– сохранять в папку – создать папку на рабочем столе CA, Свойства сообщений с уведомлениями: Отображаемый адрес OperCA@demo.lab, Отображаемое имя OperCA, OperCA@demo.lab , База данных удостоверяющего центра: Тип базы данных – SQL Server УКЦ 4x , Строка подключения к базе данных

Data Source=10.0.0.3\winnccsql;Initial Catalog=ViPNetAdministrator;User:Id=KcaUser;Password=Number1;

Кросс сертификаты можно не настраивать, если в задании нет.

Путь сохранения отчетов – созданная папка CA. Проверить настройки!

Отчеты-Добавить-Сохранить файл с сертификатами, Путь для сохранения – СА, Фильтрация сертификатов E-MAIL, город, имя (по заданию) – ОК. Выполнить. Проверяем отчет в папке СА. СНАПШОТ

На V-1-Oper-CA TSP-OCSP Service скачать. В поиске найти Создание запроса на сертификат. Шаблон сертификата: Для TSP-сервера

Адрес электронной почты: TSP@demo.lab Подразделение: IT

Город: Казань Область: Республика Татарстан Страна: RU

Сохранение запроса в файл: создать папку на рабочий стол TSP. Сформировать запрос в созданную папку. Затем скинуть файл в общую сетевую папку Publication или можно этот файл с запросом через флешку перенести на V-1-Adm. Далее в УКЦ - Удостоверяющий центр – Внешние пользователи – Загрузить и обработать запрос – на флешке выбрать файл с запросом TSP – Издать сертификат. Файл с изданным сертификатом перекинуть на V-1-Oper-CA. На V-1-Oper-CA открыть ViPNet CSP – Добавить контейнер - Инициализация контейнера ключей – Папка на диске – Созданная папка TSP – ок. Установить сертификат – Сертификат изданный на админе – далее, далее – ок. Настройка параметров – Запустить TCP – Действия – Настроить сервер – Серийный номер 01 00 00 00 00 00 00 00. Создать – Идентификатор объекта политики – 1.2.643.100.1.2.3 Закрыть и заново открыть. Установить сертификат: кликнуть по нему – локальный компьютер – поместить все сертификаты в следующее хранилище – Личное- Готово. Службы УЦ – Службы TCP – Выбрать сертификат – Должен появиться сертификат, выбрать его.

На V-1-Adm в УКЦ – Пользователи - Пользователь 2 – Считать ключи скомпрометированными - Да. Пароль – Сменить. Сетевые узлы – Выбрать Admin, CoordSub, Пользователь 2 (те, у кого статус ключей требуется создать) – Создать и передать в ЦУС. Затем заходим в ЦУС – отправить справочники и ключи – ТОЛЬКО НА ПОЛЬЗОВАТЕЛЯ 2. На V-1-Adm в УКЦ – Пользователи – Пользователь 2 – Ключи пользователя – Создать и сохранить РНПК в файл – на рабочем столе создать папку РНПК – ОК. Пользователь 2 – Создать и передать ключи в ЦУС. Потом переходим в ЦУС – Отправить справочники и ключи - ТОЛЬКО НА ПОЛЬЗОВАТЕЛЯ 2.

На Client 2 подергать транспортный модуль. ViPNet Client должен вылететь и потухнуть все узлы.

На V-1-Adm в УКЦ – Сетевые узлы – Oper CA, CoordOffice (статус CRL неактуальные) – Создать и передать ключи в ЦУС.

На Client 2 должно выйти предупреждение – срок действия текущего пароля пользователя истек сменить пароль – пароль сохранить в файл. Далее предупреждение – текущий сертификат электронной подписи недействителен – выбрать другой demo.lab. Далее установка корневого сертификата – ОК.

На V-1-Adm в ЦУС – Отправить справочники и ключи – Отправить на весь список. На V-1-Adm в ViPNet Client должен потухнуть Пользователь 2. Далее на Client 2 должно все восстановиться, все узлы должны гореть. На админе тоже. Вуаля.

3. CA Informing.

C:\ProgramData\Infotecs\ViPNet Administrator\KC\Key management\Certificates Issuers - Папка с кросс-сертификатами на AdminCA.

Data Source=10.14.0.2\winnccsql;Initial Catalog=ViPNetAdministrator;User Id=KcaUser;Password=Number1; - Строка подключения к базе данных.