

Описание модуля D: «Технологии защиты и анализа сетевого трафика»

Необходимо настроить межсетевое взаимодействие различных сетей, настроить туннелирование

При выполнении модуля D ставятся следующие цели:

1. Настройка межсетевого взаимодействия с добавлением новых узлов и сохранением работоспособности существующих
2. Настройка туннелирования открытых узлов

При выполнении данного модуля D ставятся следующие задачи:

Задача 2.1. Межсетевое взаимодействие защищённых сетей (со связями «все со всеми»)

Развернуть на Net3-Admin (Сеть 3 межсеть) на ПК рабочее место

Администратора партнёрской сети, создать структуру второй сети:

Рабочее место администратора (БД, ЦУС, УКЦ, Client)

- 1 координатор (HW-VA или координатор Linux),
- 1 узел Admin,
- установите координатор.

Установить и настроить необходимое ПО. Настроить межсетевое взаимодействие между двумя защищёнными сетями, сделать скриншоты всех этапов установки межсетевого взаимодействия.

Проверить взаимодействие узлов, отправив сообщение деловой почты.

Предисловие

По «Задача 2.1» не оговорено, с помощью какого ключа устанавливать межсетевое взаимодействие, вы можете установить при помощи симметричного, так и при помощи асимметричного ключа. Первый вариант легче и быстрее, нам понадобится лишь 1 ключ для двух сетей. Я покажу установку вторым вариантом, потому что именно он использовался на чемпионатах. Если вы выберете для себя первый вариант, то учтите, что вам нужно создать и экспортировать лишь 1 ключ без создания асимметричных, в этом вся разница. При выполнении задач вам уже нужно понимать условную работу УКЦ и ЦУСа, почему иногда нужно создавать ключи и справочники. Если ничего не получается, всегда просматриваете их во время выполнения задачи. Во время выполнения «Задача 2.1» может возникнуть трудность из-за долгой отправки и обработки межсетевой информации, из-за чего начинаешь сомневаться, правильно ли установил и настроил «межсетевое взаимодействие».

Задача 2.1: Решение

Разворачиваем вторую сеть (или третью межсеть).

После разворачивания и установки всего необходимого ПО, заходим в ЦУС. Переходим в «Доверенные сети» и нажимаем «Установить взаимодействие». Выбираем «Я инициатор межсетевого взаимодействия».

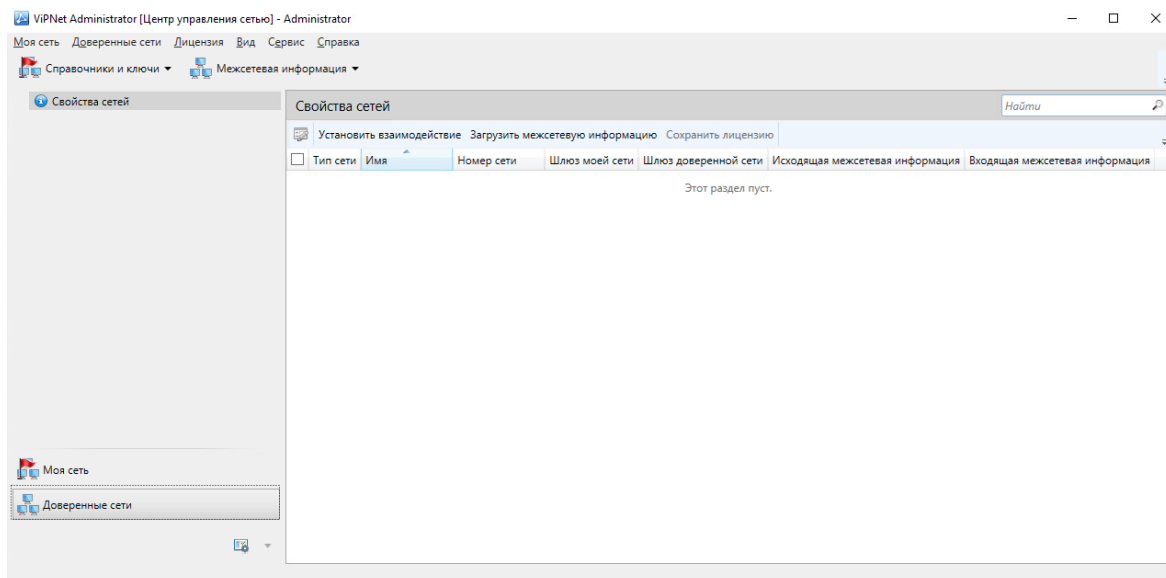


Рисунок 1 – Доверенные сети

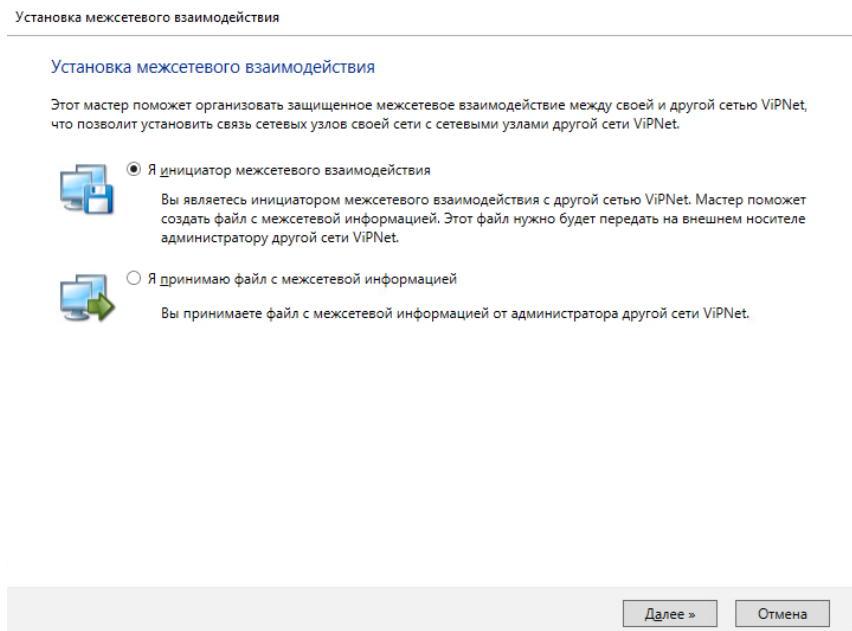


Рисунок 2 – Установка межсетевого взаимодействия

Задаем номер и имя сети, нажимаем «Выбрать» для выбора координатора.

Установка межсетевого взаимодействия

Задайте информацию о другой сети ViPNet и координатор для связи с ней

Введите номер сети ViPNet, с которой вы хотите установить межсетевое взаимодействие, и имя, под которым она будет отображаться в Центре управления сетью.

Номер сети: 12845

Имя сети: Сеть 2

Описание:

Выберите шлюзовый координатор своей сети ViPNet, через который будет осуществляться связь с другой сетью ViPNet.


Координатор: 

Рисунок 3 – Информация о другой сети ViPNet

Выбираем подходящий координатор, через который вы установите связь с координатором из второй сети. Убедитесь, что шлюз будет соответствовать выбранному координатору, нажимаем «ОК».

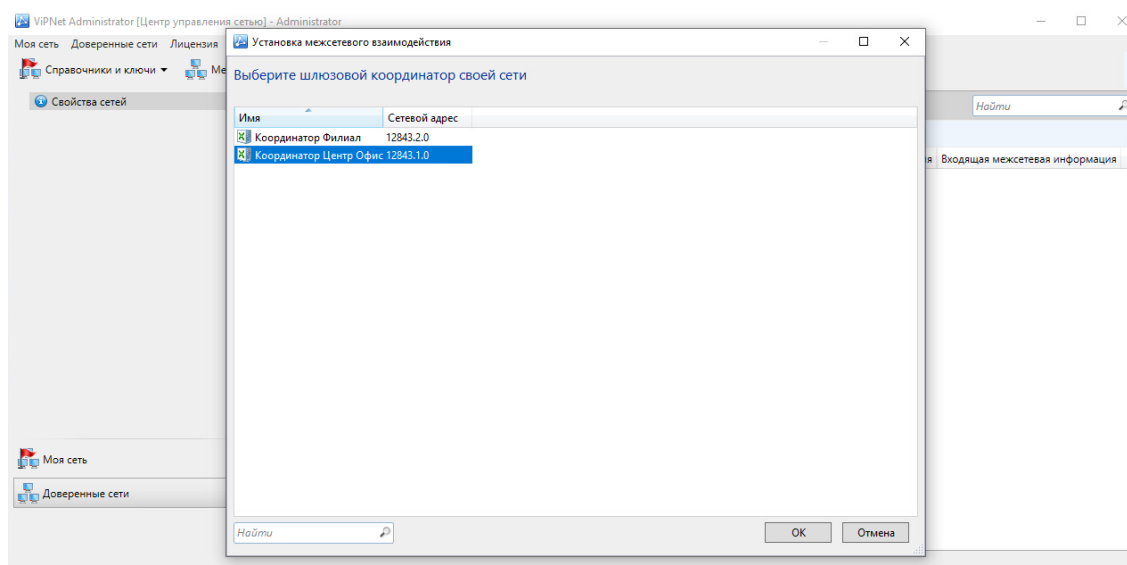


Рисунок 4 – Выбор шлюзового координатор

Нажимаем «Добавить», выбираем все сетевые узлы. Далее указываем всех пользователей для связей «все со всеми». Нажимаем «Далее» → «Далее».

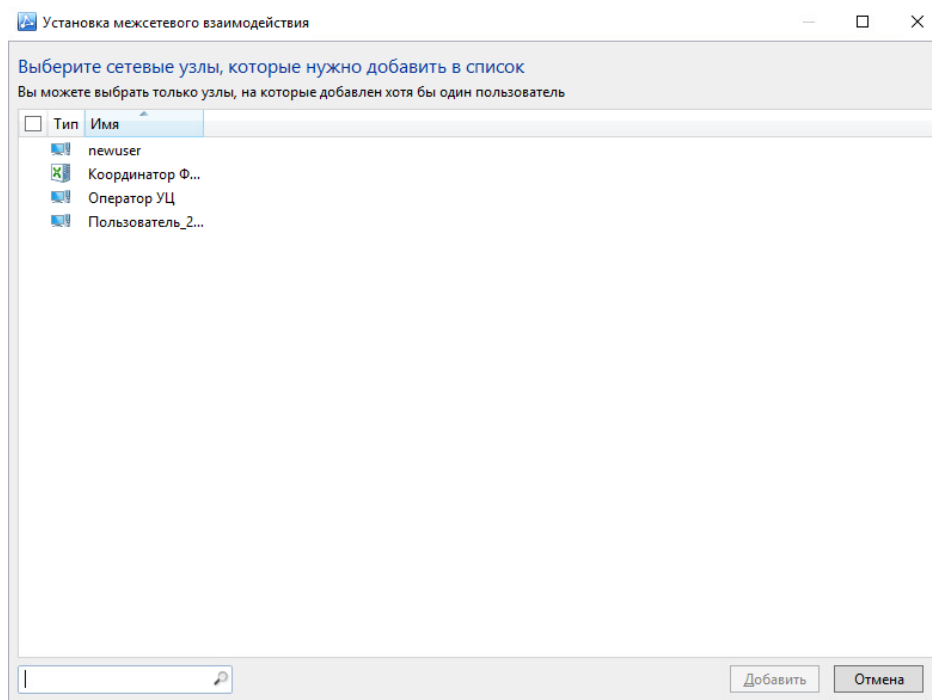


Рисунок 5 – Выбор сетевых узлов

Указываем удобный путь для нашего файла (он нам пригодится) и продолжаем установку.

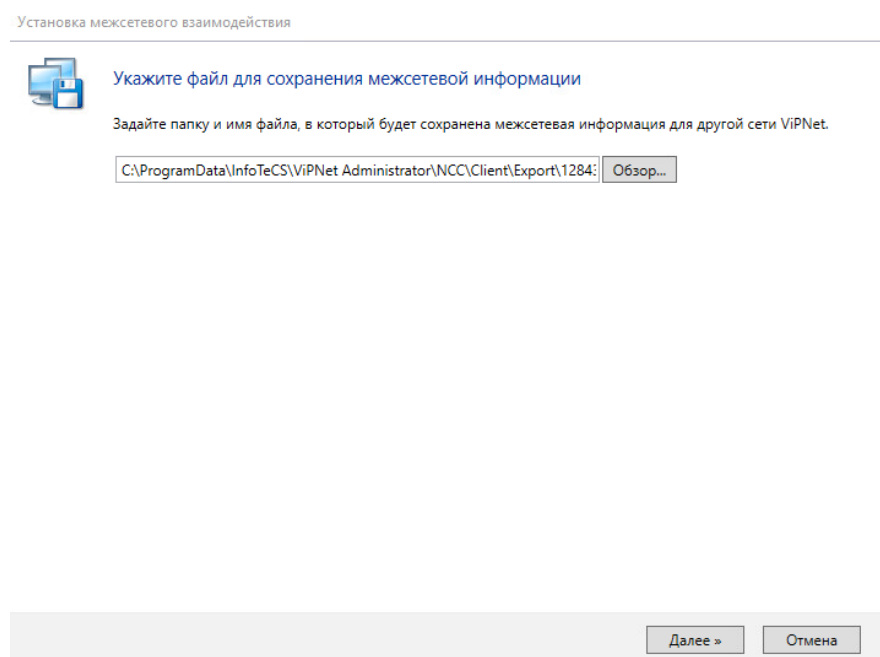


Рисунок 6 – Указание файла для сохранения межсетевого взаимодействия

После сохранения межсетевой информации переходим в УКЦ.

В УКЦ переходим в «Асимметричные мастер-ключи», нажимаем «Создать» → «Создать мастер-ключ» → «Да».

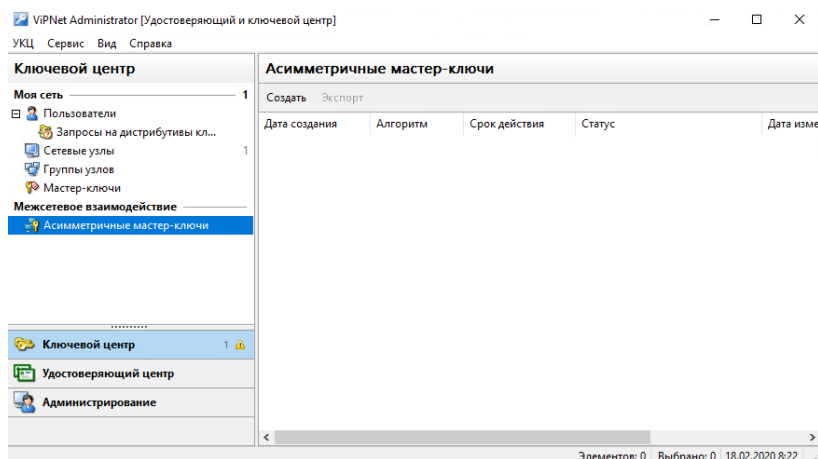


Рисунок 7 – Асимметричные мастер-ключи

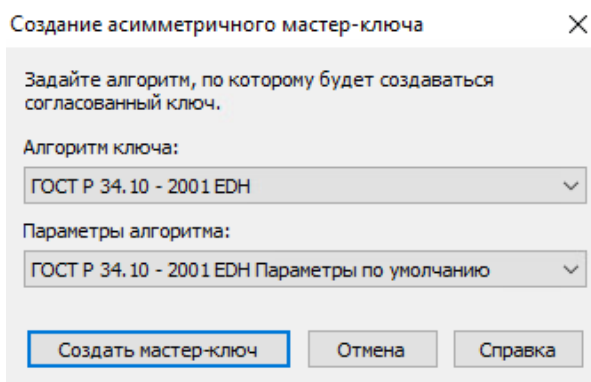


Рисунок 8 – Создание асимметричного мастер-ключа

Кликаем по нашему созданному ключу ПКМ → «Экспорт».
Экспортируем в удобное нам место, после экспорта еще раз кликаем по нему ПКМ → «Текущий».

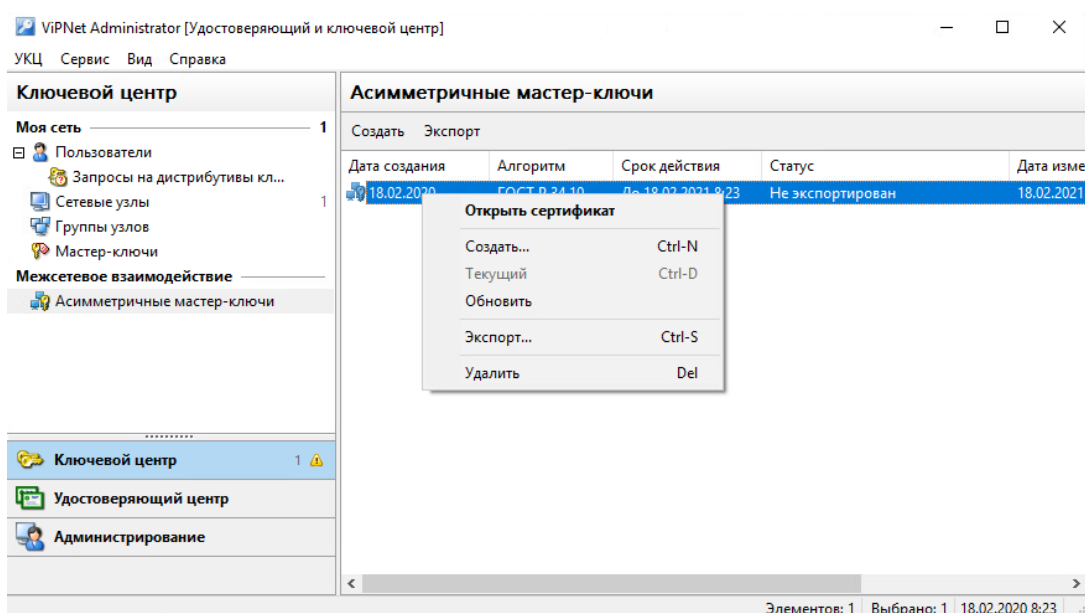


Рисунок 9 – Экспорт ключа

Передаем наш ключ и файл с межсетевой информацией на виртуальную машину второй нашей сети, с которой хотим установить межсетевое взаимодействие.

Заходим в ЦУС, переходим в «Доверенные сети» и нажимаем «Установить взаимодействие». Выбираем «Я принимаю файл с межсетевой информацией» → «Установить взаимодействие». Выбираем координатор.

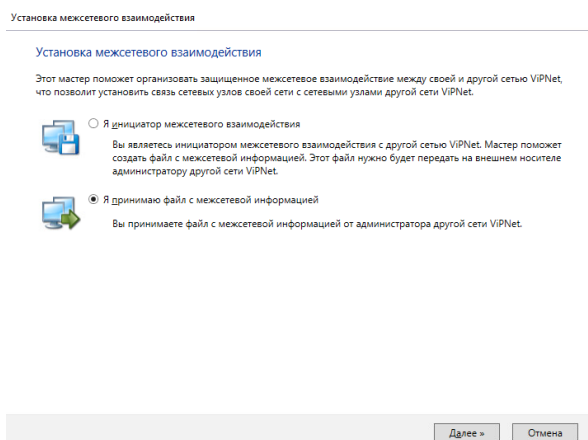


Рисунок 10 – Установка межсетевого взаимодействия

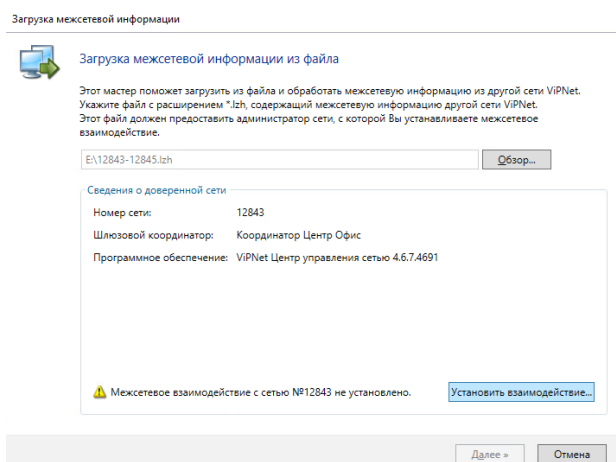


Рисунок 11 – Загрузка межсетевой информации из файла

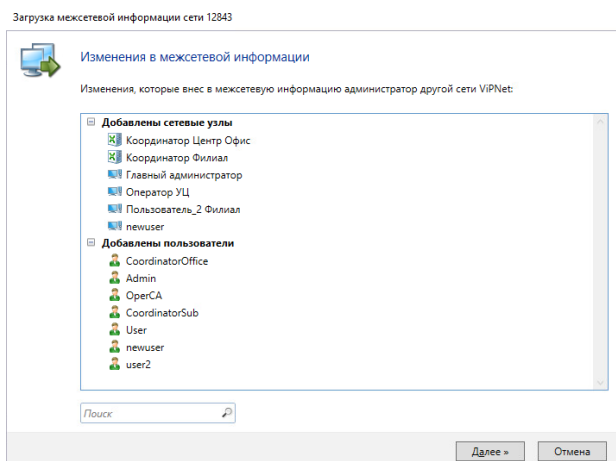


Рисунок 12 – Изменение в межсетевой информации

Заходим в УКЦ, переходим в «Администрирование». Дважды кликаем ЛКМ на сертификат, выбираем его и нажимаем «Импортировать».

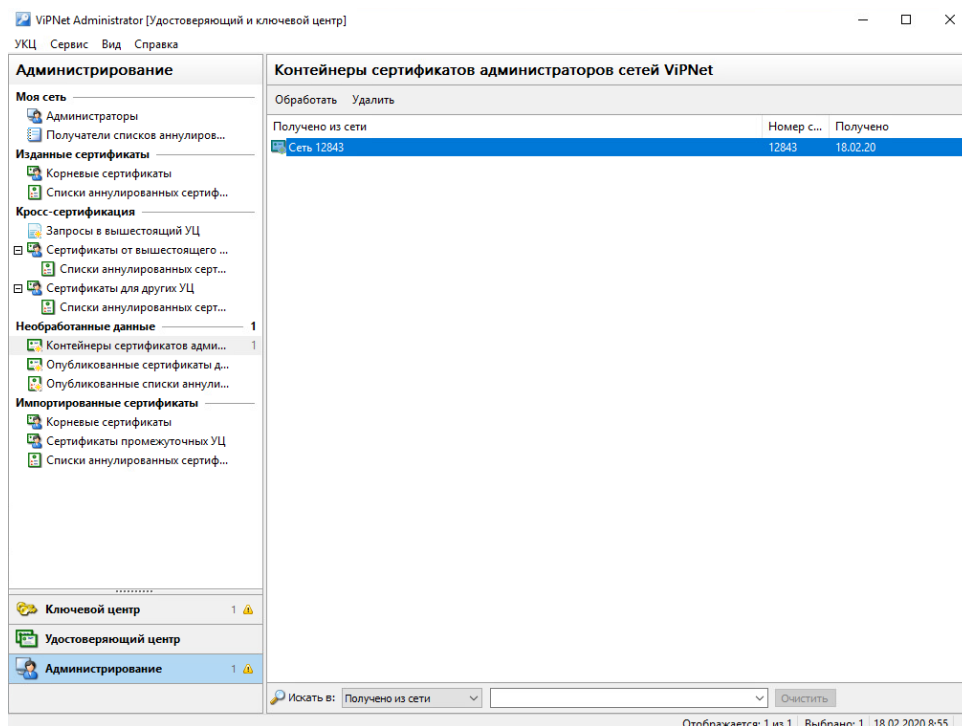


Рисунок 13 – Администрирование

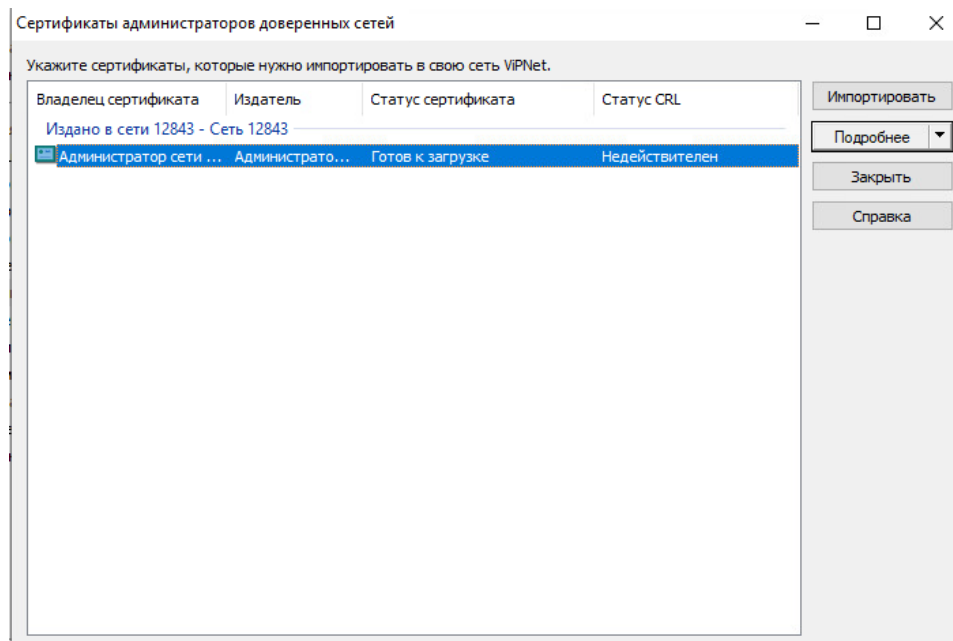


Рисунок 14 – Сертификаты администраторов доверенных сетей

Возвращаемся обратно в УКЦ. В межсетевом взаимодействии выбираем сеть с которой хотим установить связь и нажимаем «Загрузить». Выбираем ранее созданный асимметричный ключ в другой сети.

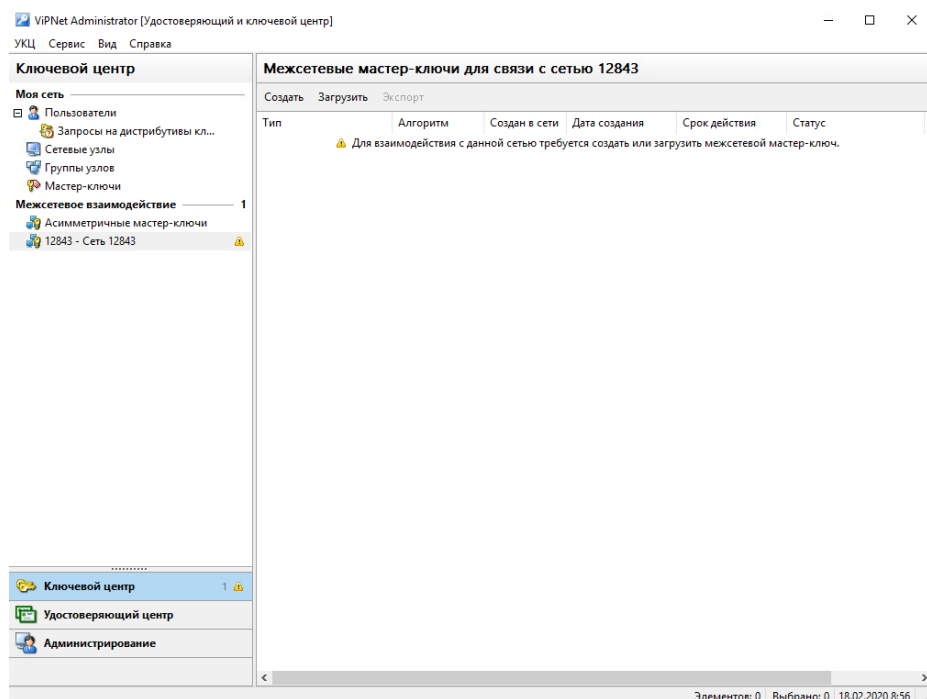


Рисунок 15 – Межсетевые мастер-ключи

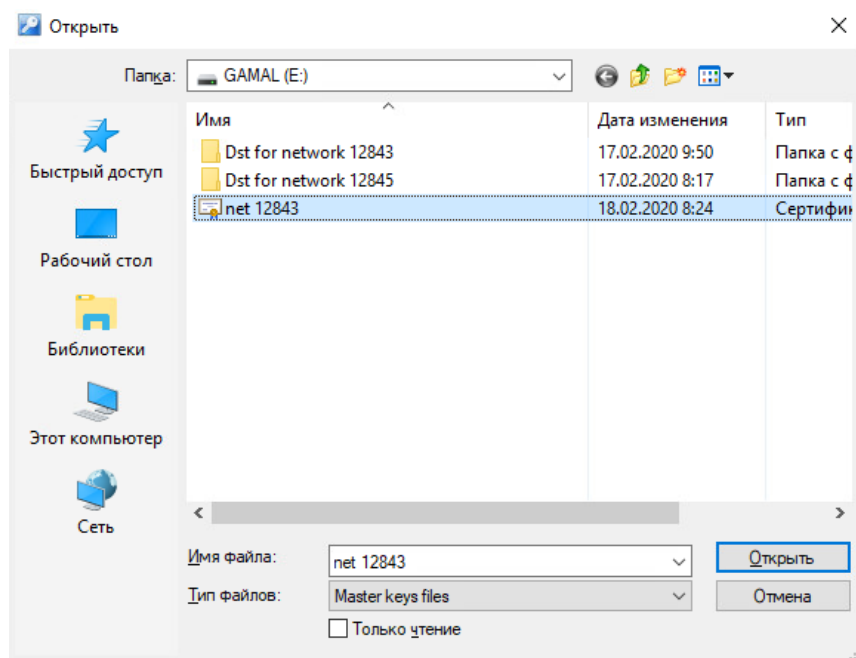


Рисунок 16 – Выбор ключа

Нажимаем ПКМ по загруженному ключу «Использовать» → «Да».

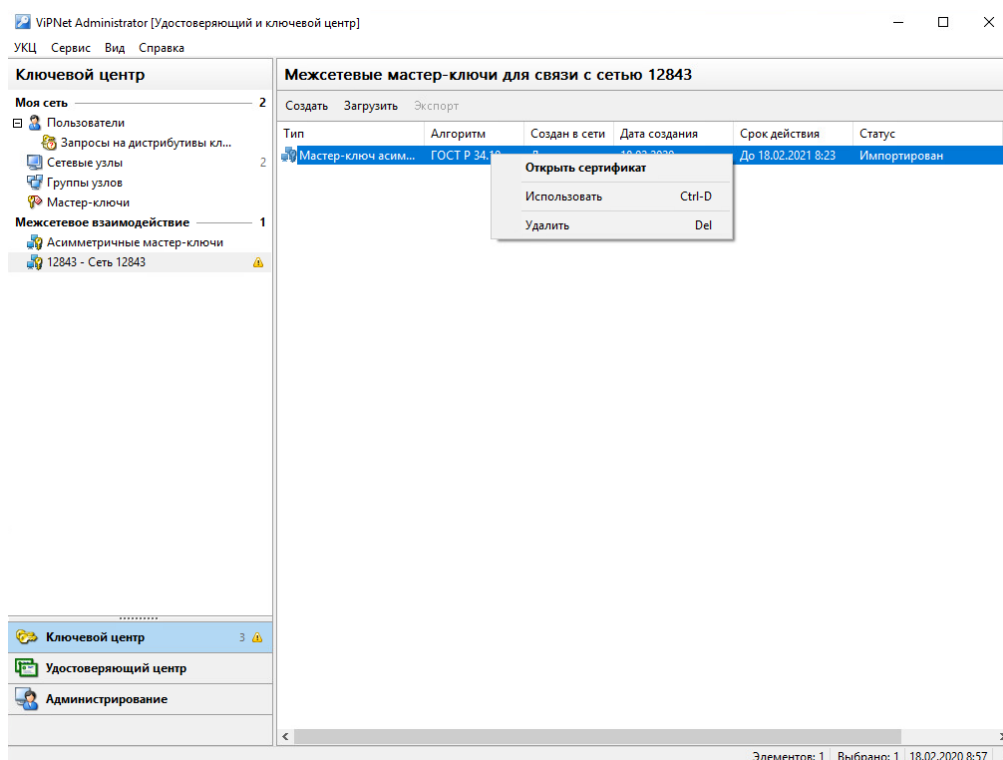


Рисунок 17 – Межсетевые мастер ключи ч.2

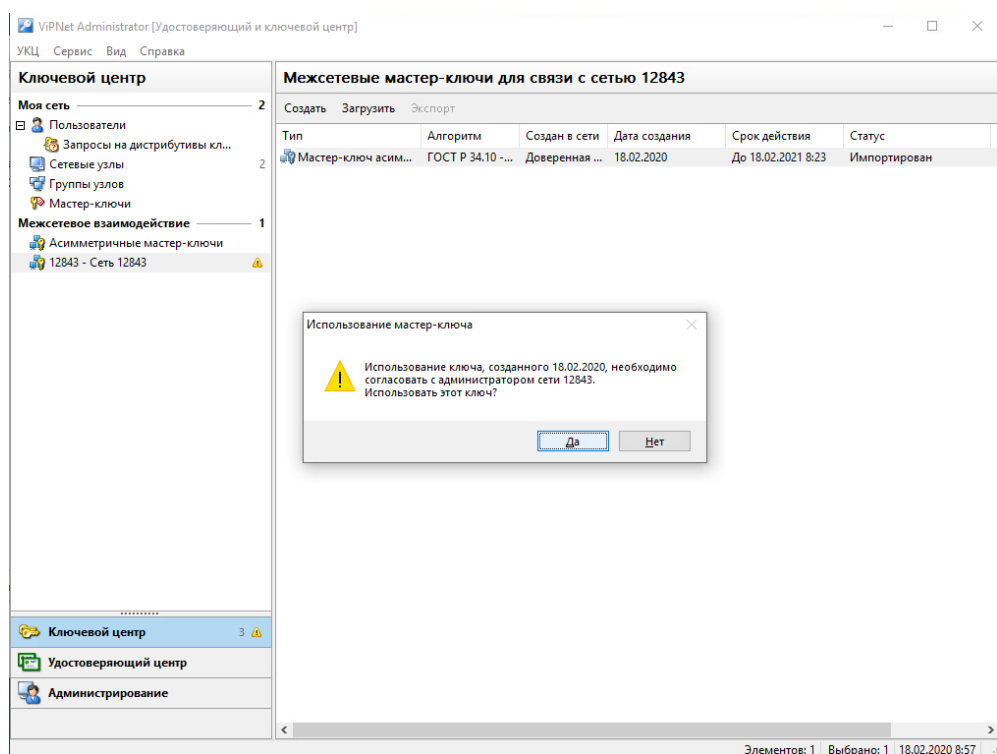


Рисунок 18 - Межсетевые мастер ключи ч.3

Делаем точно те же самые действия, только для другой сети, а именно:

1. Создание и загрузка межсетевой информации для другой сети.
2. Обработка сертификата после загрузки межсетевой информации.
3. Создание и загрузка асимметричного ключа для другой сети.

Теперь, когда у обеих сетей установлены сертификаты и ключи, мы можем отправлять межсетевую информацию. Для проверки нам нужно отправить сообщение деловой почты, но для начала нужно установить связь с пользователем из доверенной сети.

В меню «Свойства пользователя» → «Связи с пользователями» нажимаем «Добавить». В отображении объектов ставим на пункт «Доверенных сетей (1 из 1)», выбираем нашего пользователя из второй сети и нажимаем «Добавить». Создаем и отправляем межсетевую информацию, обрабатываем в другой сети и

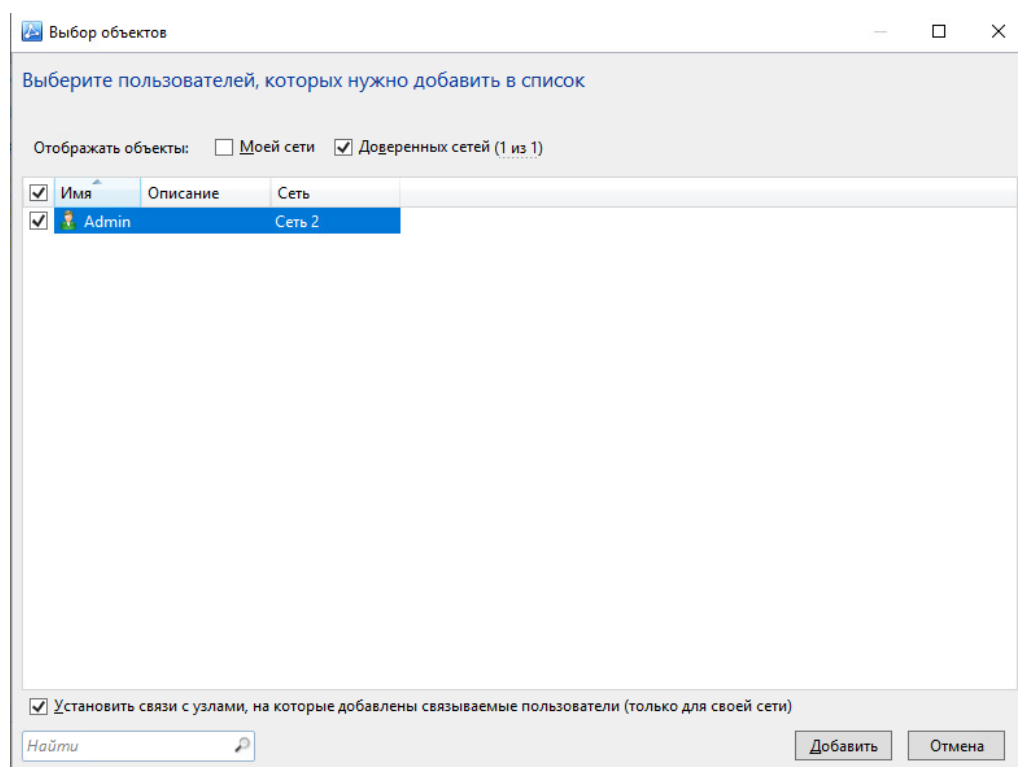


Рисунок 19 – Добавление пользователя из доверенной сети

Создаем и отправляем межсетевую информацию, обрабатываем в другой сети.

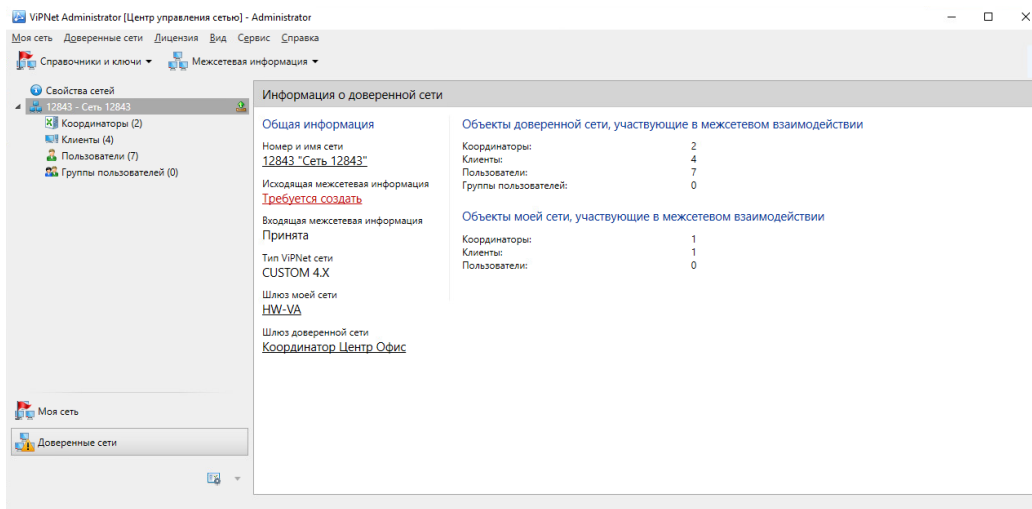


Рисунок 20 – Создание межсетевой информации ч.1

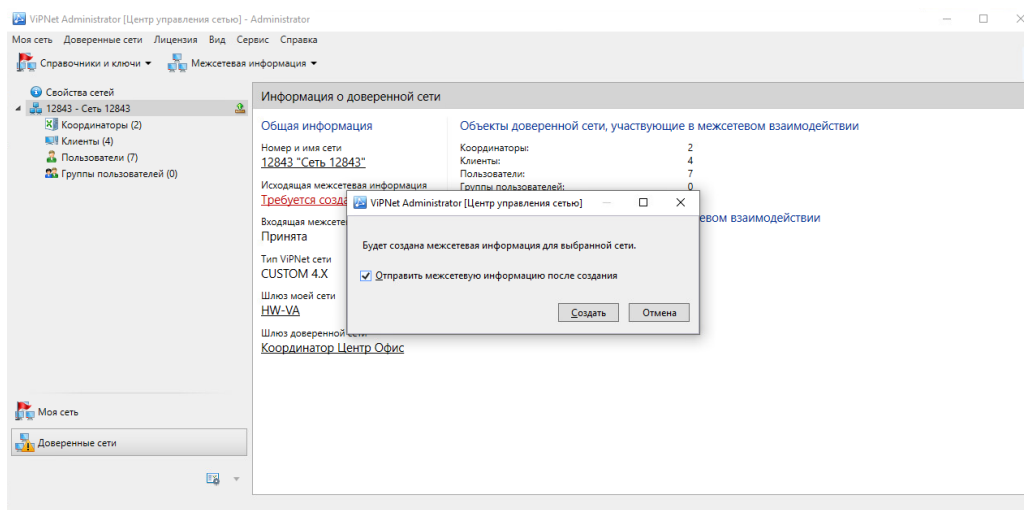


Рисунок 21 - Создание межсетевой информации ч.2

Не забываем создавать справочники и ключи для узлов, потерпевшие изменения.

После чего проверяем:

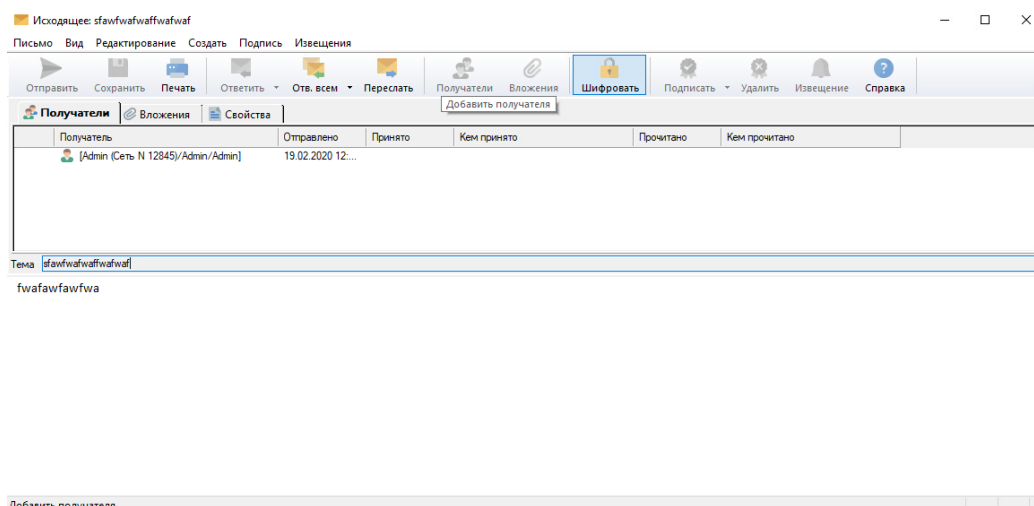


Рисунок 22 – Проверка межсетевого взаимодействия ч.1

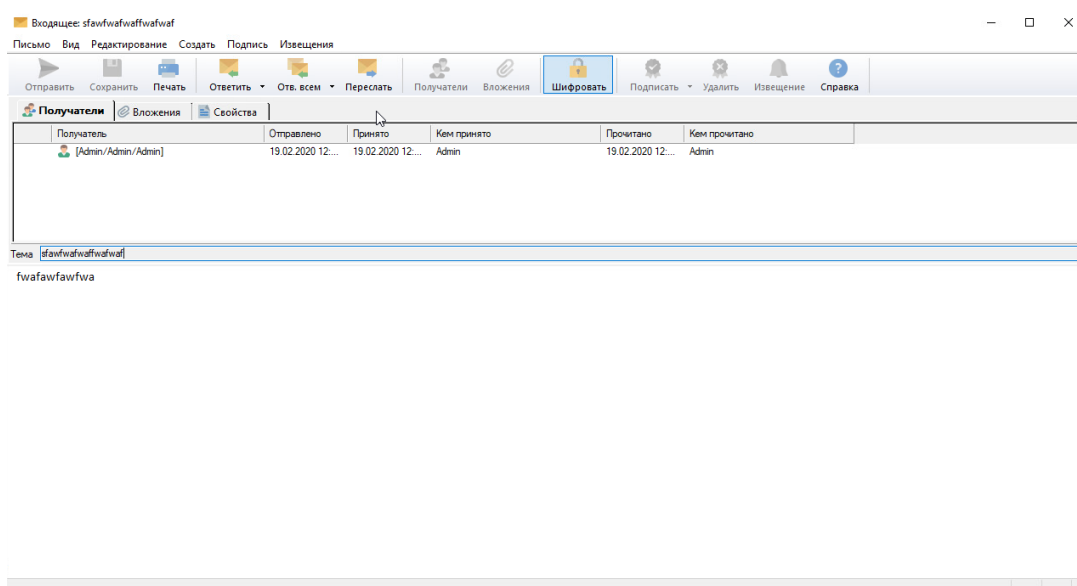


Рисунок 23 – Проверка межсетевого взаимодействия ч.2

Проверить через журнал IP-пакетов можно при помощи веб-интерфейса, написать ссылку в браузере или же в самом координаторе прописать команду. Для просмотра журнала IP-пакетов, вы должны находиться в режиме администратора.

<http://<ip-адрес координатора>:8080> – ссылка на веб интерфейс

`iplir view` – команда для просмотра журнала IP-пакетов

Задача 2.3. Туннелирование в рамках межсетевого взаимодействия

Подключить незащищенную машину в сети 3.

Настроить туннелирование таким образом, чтобы взаимодействие между открытыми узлами из разных сетей осуществлялось по зашифрованному каналу. Проверить доступность незащищённых машин друг другу любым другим протоколом; проанализировать журналы IP-пакетов на координаторах.

Скриншоты:

- Настройка максимального количества туннелей на координаторах
- Скриншоты прохождения ICMP пакетов (ping) и любого другого трафика с незащищенного узла
- Скриншоты журнала IP-пакетов координатора с установленным фильтром «Туннелирование» для проверки прохождения ICMP-пакетов и любого другого трафика с помощью туннелирования

Задача 2.2: Решение

Для создания туннеля между незащищенными машинами мы должны настроить туннелирование у координаторов первой и второй сети.

Заходим в свойства координатора первой сети. Переходим в «Туннелирование» → «Добавить» и указываем IP-адрес нашего незащищенного узла. По заданию указываем максимальное число: 30.

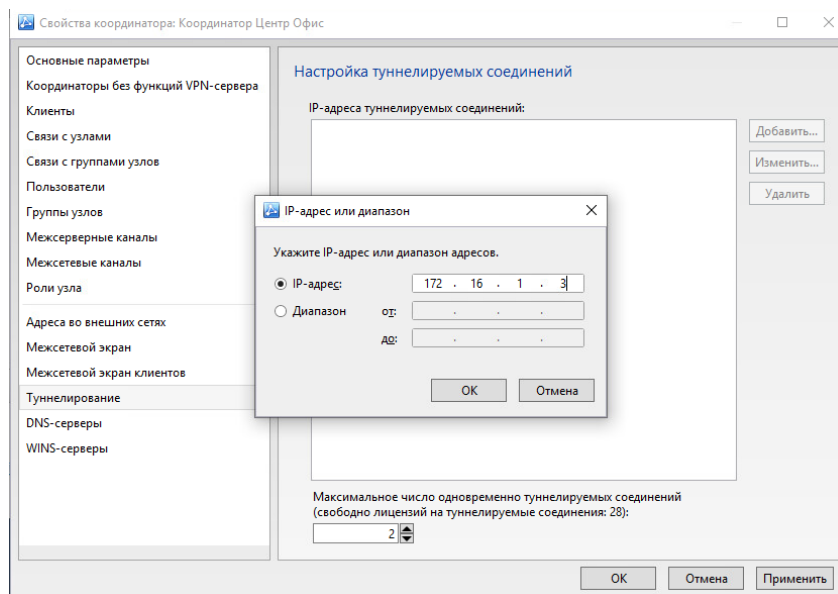


Рисунок 24 – Настройка туннелируемых соединений ч.1

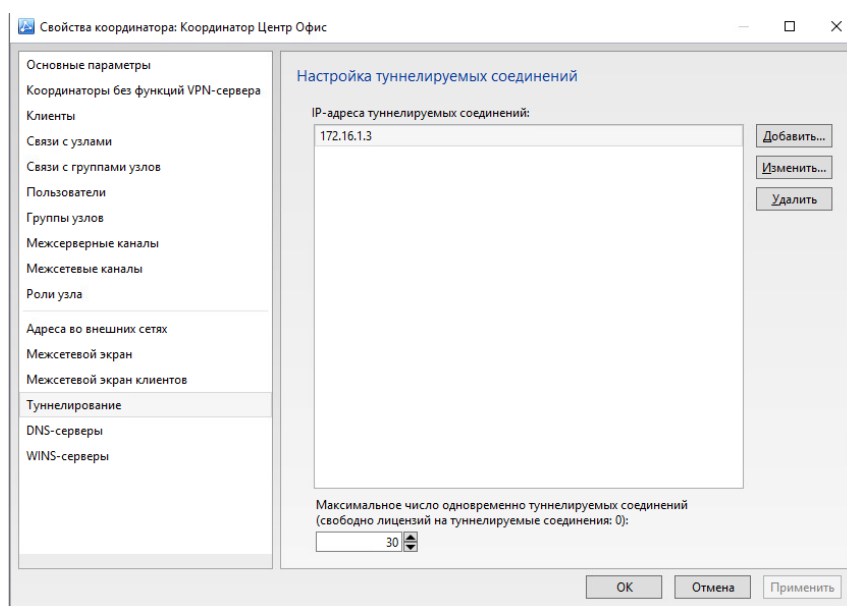


Рисунок 25 – Настройка туннелируемых соединений ч.2

У второй сети:

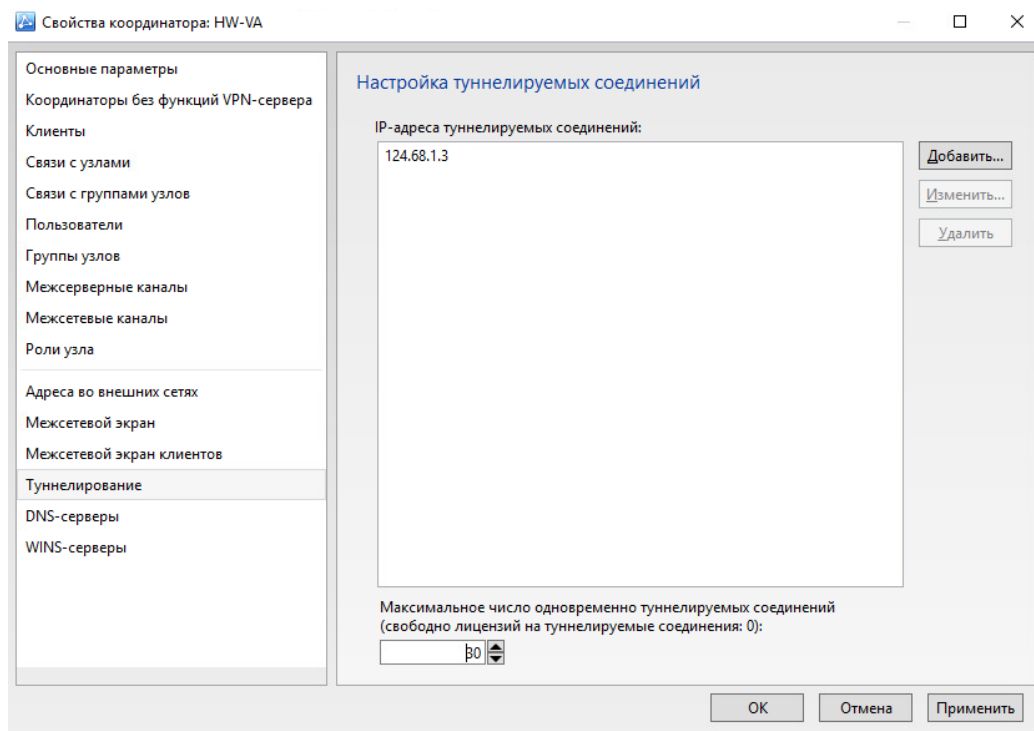
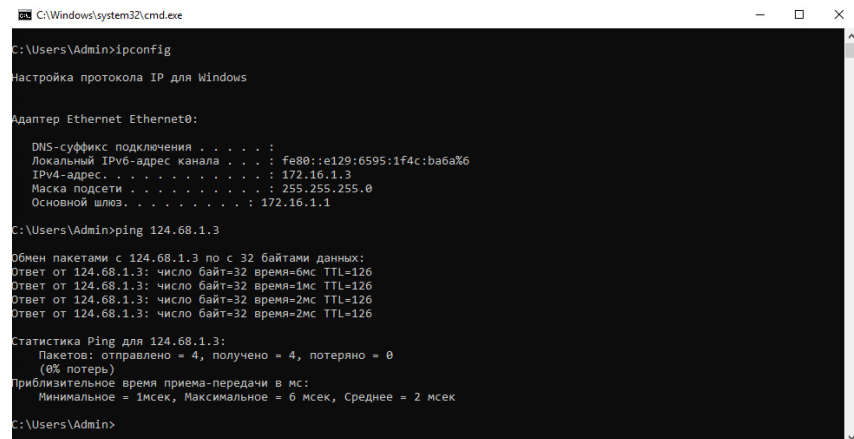


Рисунок 26 – Настройка туннелируемых соединений ч.3

Не забываем нажать «Применить».

Проверяем УКЦ с ЦУСом и отправляем межсетевую информацию с двух сетей для обработки.

После принятия межсетевой информации проверяем, пингуя с одного незащищенного узла другой:



```
C:\Windows\system32\cmd.exe
C:\Users\Admin>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet0:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::e129:6595:1f4c:ba6a%6
    IPv4-адрес. . . . . : 172.16.1.3
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 172.16.1.1

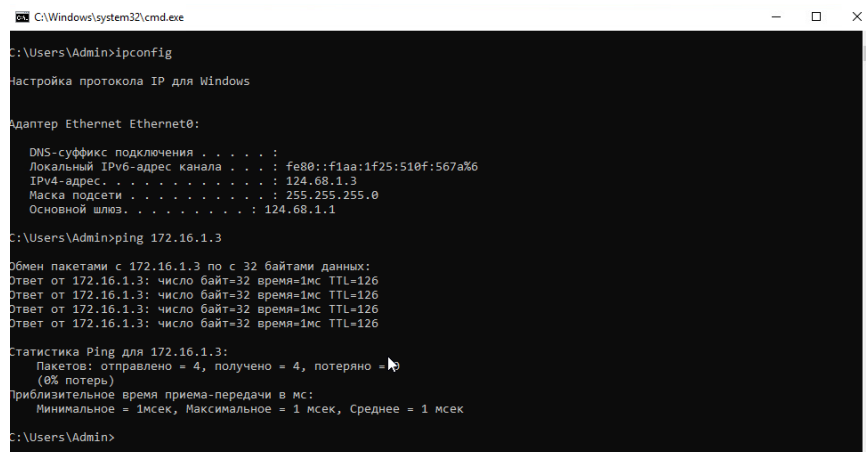
C:\Users\Admin>ping 124.68.1.3

Обмен пакетами с 124.68.1.3 по 32 байтами данных:
Ответ от 124.68.1.3: число байт=32 время=0мс TTL=126
Ответ от 124.68.1.3: число байт=32 время=1мс TTL=126
Ответ от 124.68.1.3: число байт=32 время=2мс TTL=126
Ответ от 124.68.1.3: число байт=32 время=2мс TTL=126

Статистика Ping для 124.68.1.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потеря)
    Приблизительное время приема-передачи в мс:
        Минимальное = 1мсек, Максимальное = 6 мсек, Среднее = 2 мсек

C:\Users\Admin>
```

Рисунок 27 – Проверка туннелирования узлов



```
C:\Windows\system32\cmd.exe
C:\Users\Admin>ipconfig

Настройка протокола IP для Windows

Адаптер Ethernet Ethernet0:

    DNS-суффикс подключения . . . . . :
    Локальный IPv6-адрес канала . . . : fe80::f1aa:1f25:510f:567a%6
    IPv4-адрес. . . . . : 124.68.1.3
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз. . . . . : 124.68.1.1

C:\Users\Admin>ping 172.16.1.3

Обмен пакетами с 172.16.1.3 по 32 байтами данных:
Ответ от 172.16.1.3: число байт=32 время=1мс TTL=126
Ответ от 172.16.1.3: число байт=32 время=1мс TTL=126
Ответ от 172.16.1.3: число байт=32 время=1мс TTL=126
Ответ от 172.16.1.3: число байт=32 время=1мс TTL=126

Статистика Ping для 172.16.1.3:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потеря)
    Приблизительное время приема-передачи в мс:
        Минимальное = 1мсек, Максимальное = 1 мсек, Среднее = 1 мсек

C:\Users\Admin>
```

Рисунок 28 – Проверка туннелируемых узлов