

Санкт – Петербургский Национальный Исследовательский
Университет Информационных Технологий, Механики и Оптики
Кафедра Программных систем

Отчет по лабораторной работе

Построение корпоративной VPN с помощью ПО «Infotecs VipNet»

Выполнил:

Антонов Е.П

Группа: К4120

Проверил: к.т.н. Ананченко И.В.

Санкт – Петербург

2017

Цель работы

Настроить корпоративную VPN при помощи ПО “Infotecs VipNet”.

Ход работы

Построение корпоративной VPN при помощи ПО “Infotecs VipNet” состоит в распределении ролей между участниками такой сети. Наиболее часто использующиеся узлы сети – это администратор, координатор и клиент.

VipNet «Администратор» состоит из двух глобальных частей:

- ЦУС – центр управления сетью
- УКЦ – удостоверяющий и ключевой центр

VipNet «Координатор» – аналог DHCP, DNS, межсетевое взаимодействие с другой сетью

VipNet «Клиент» – это пользователи сети, представляющие рабочее место.

Рабочее место настраивается при помощи следующих конфигурационных файлов:

- КН – ключевой набор
- КД – ключевая дискета
- Справочник
- Infotecs.re – файл сгенерированных специально для данного рабочего места

Настроим три виртуальные машины на основе общего материнского виртуального жёсткого диска. Это позволит ускорить запуск виртуальных машин. Одну виртуальную машину настроим под VipNet «Координатор», а две других будут играть роль VipNet «Клиент».

Начнём с установки приложения координатора.

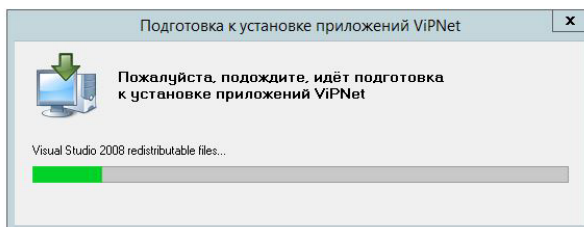


Рисунок 1 – Начало установки координатора

Примем условия лицензионного соглашения.

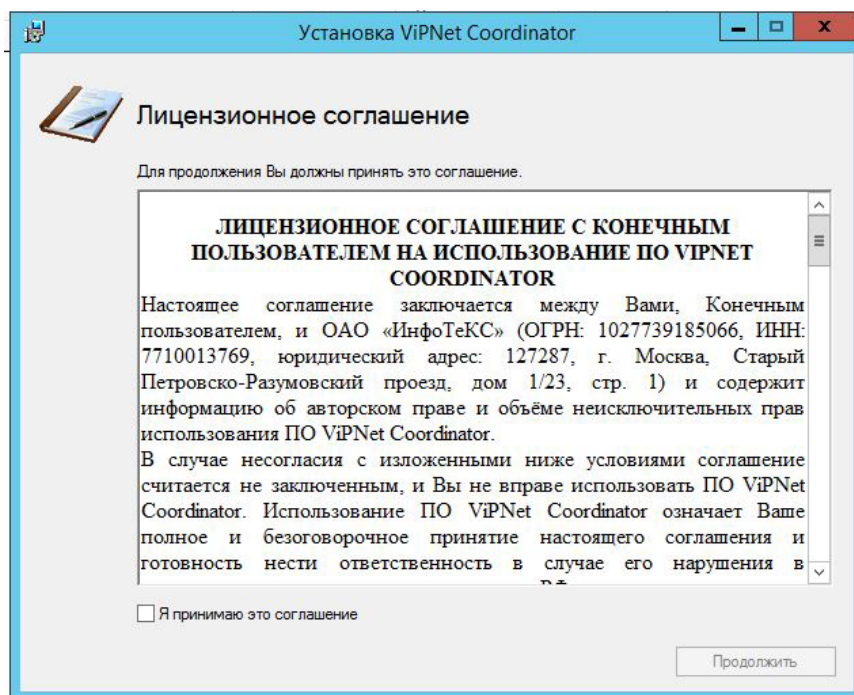


Рисунок 2 – Лицензионное соглашение

Начнём установку программного обеспечения

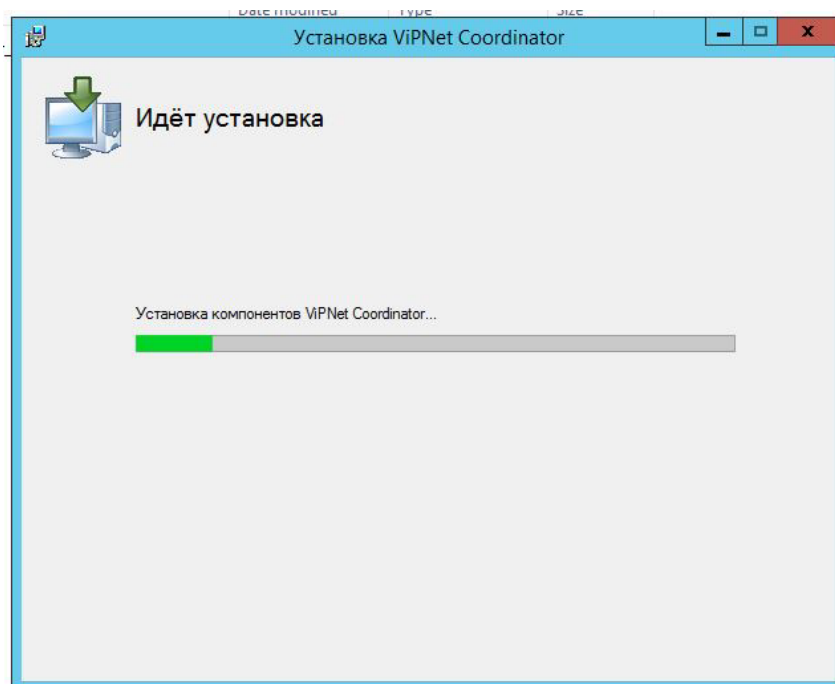


Рисунок 3 – Установка VipNet «Координатор»

Координатор успешно установлен.

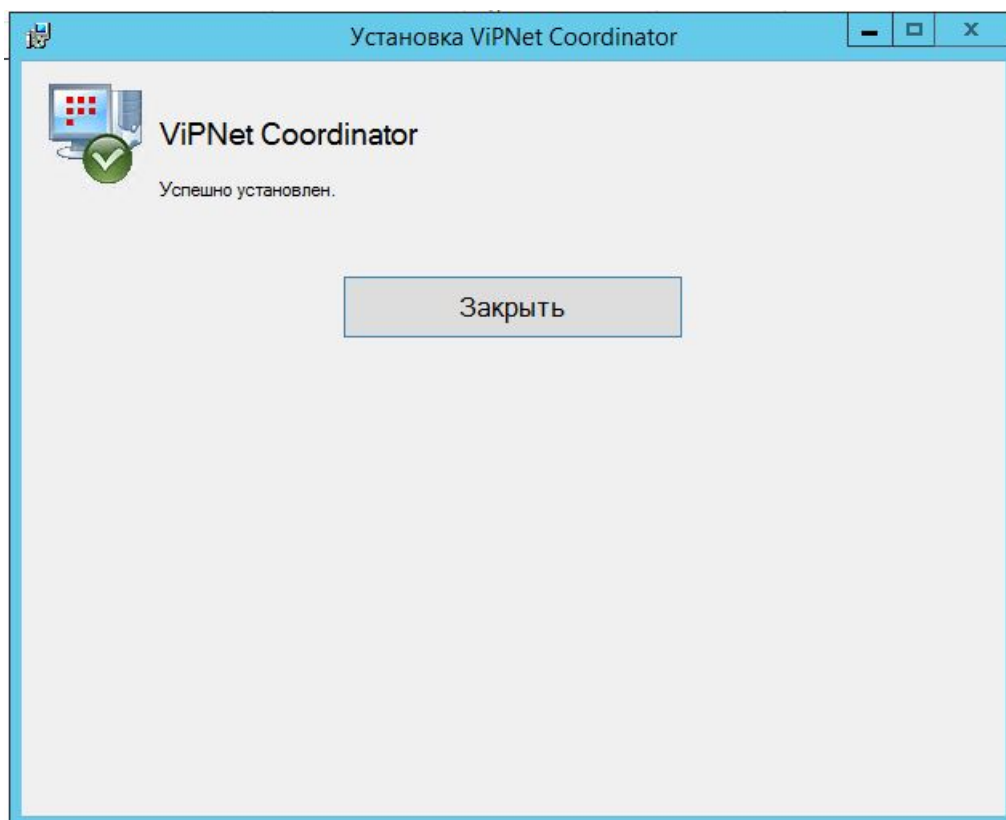


Рисунок 4 – Установка завершена

Установим ключи сети VipNet

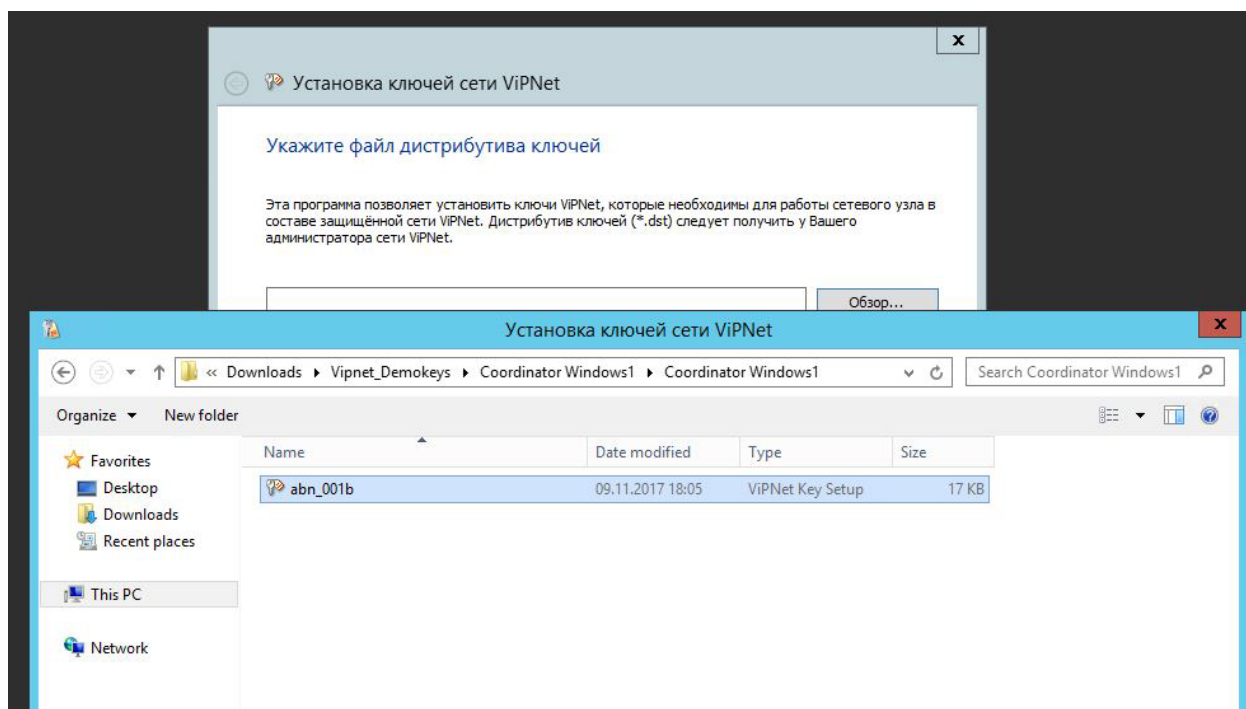


Рисунок 5 – Установка ключей сети для координатора

Ключи успешно установлены.

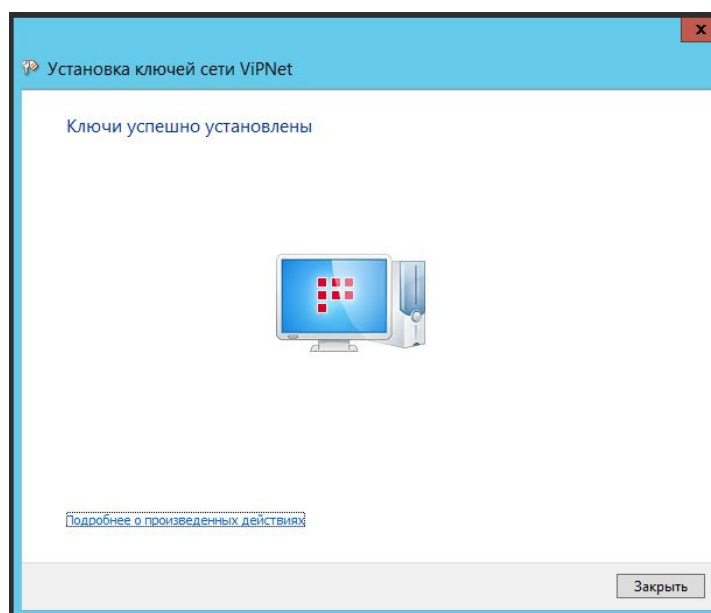


Рисунок 6 – Установка ключей завершена

Войдём в установленное приложение с учетными данными демо-версии.

- Имя пользователя: Coordinator Windows1
- Пароль: 11111111

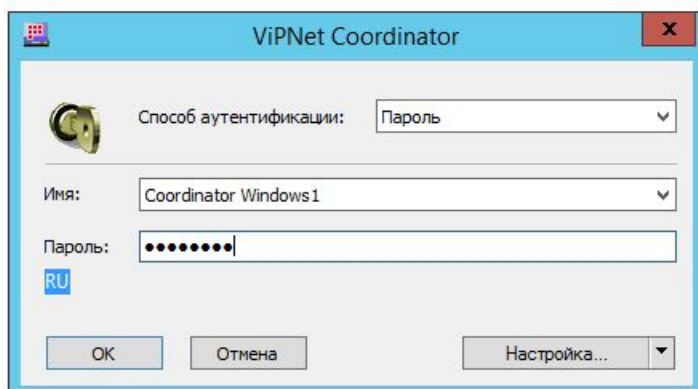


Рисунок 7 – Вход в VipNet Coordinator

Интерфейс приложения выглядит следующим образом:

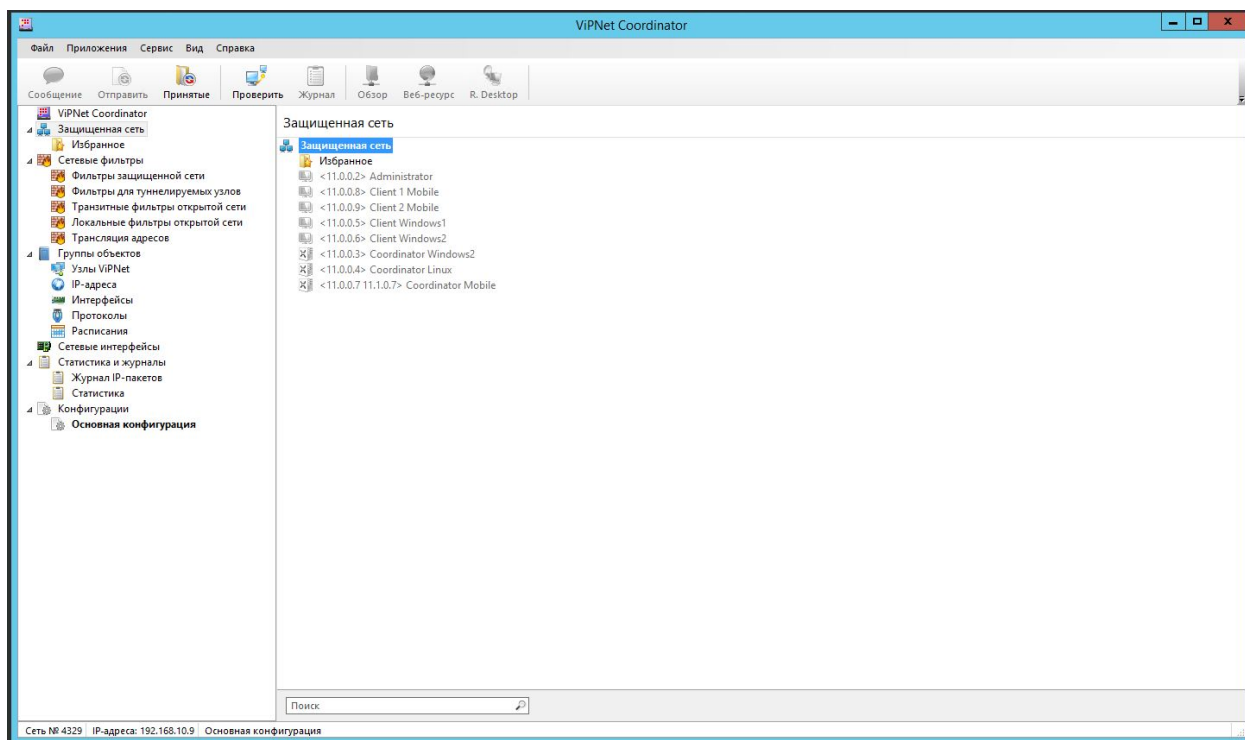


Рисунок 8 – Интерфейс координатора

Можно заметить, что сеть VipNet пока пустая, т.к. не было установлено ни одного клиента.

Установим два клиента на ранее подготовленные виртуальные машины.

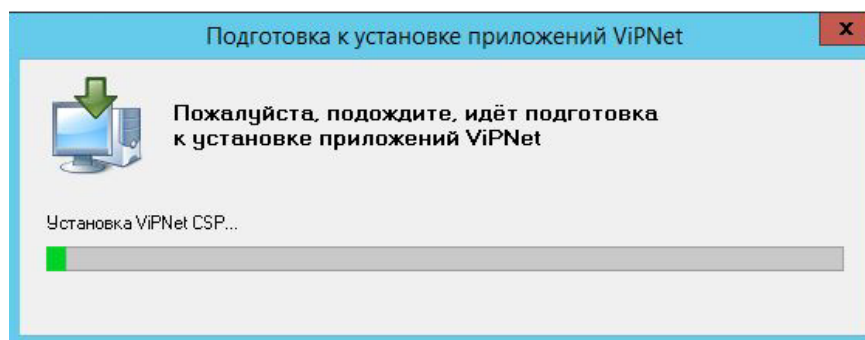


Рисунок 9 – Подготовка к установке клиента

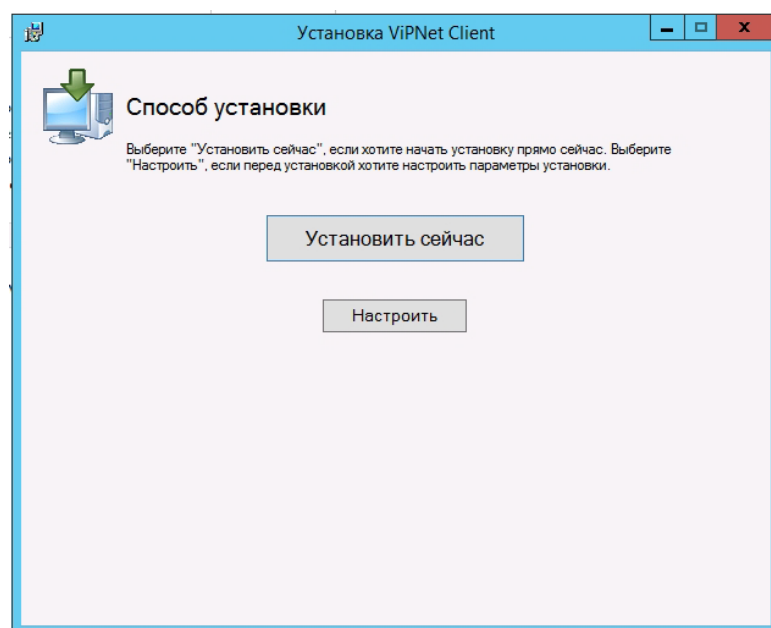


Рисунок 10 – Выбор настроек установки

Установка обоих клиентов практически идентична, за исключением установки ключей для каждого из клиентов

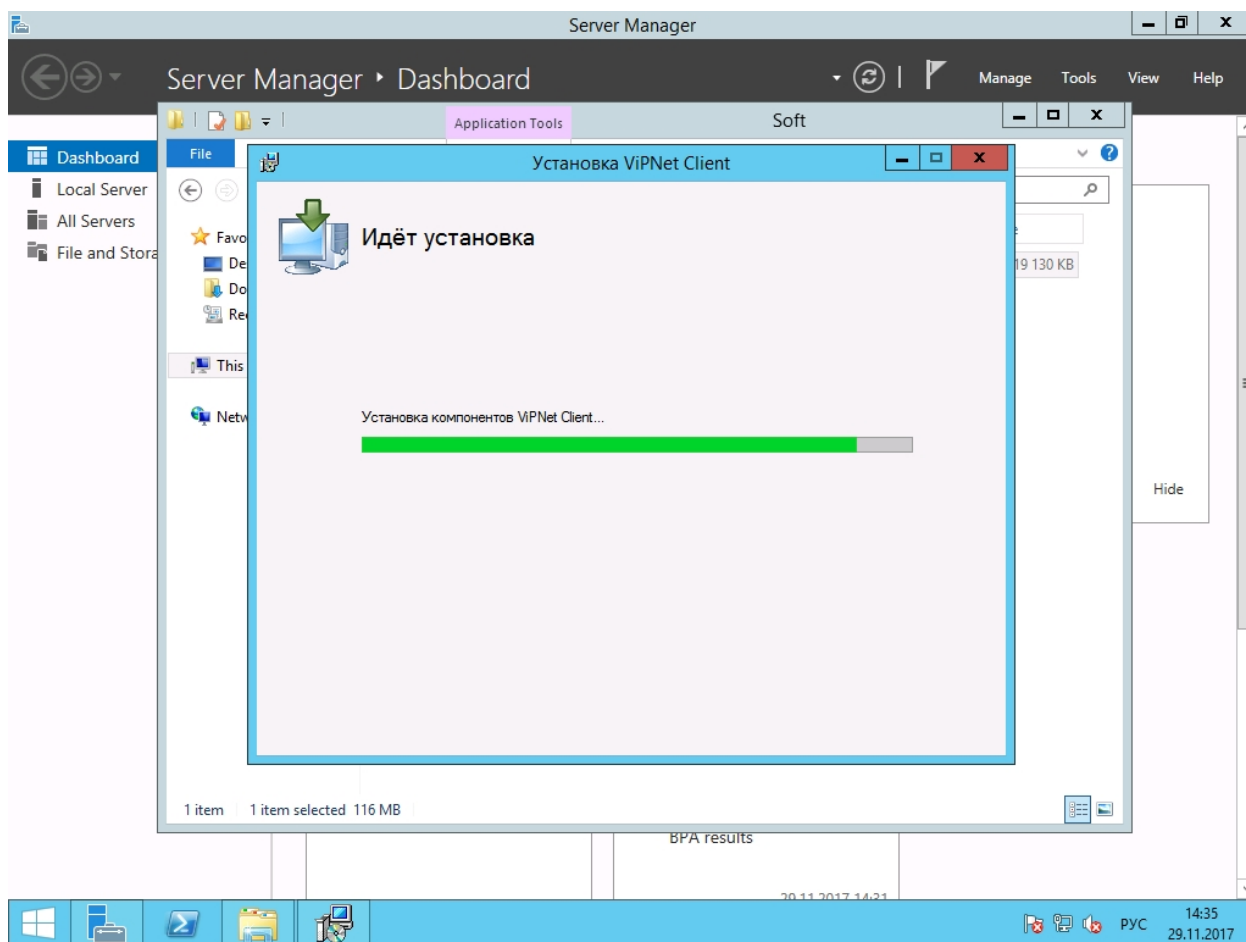


Рисунок 11 – Установка компонентов VipNet Client

Клиент успешно установлен

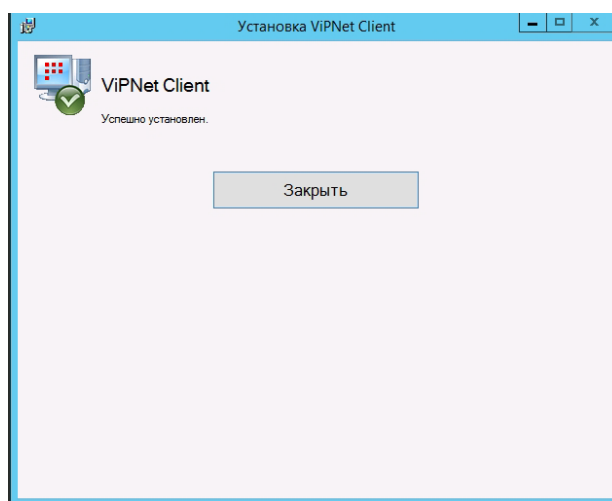


Рисунок 12 – VipNet клиент установлен

Установим ключи для каждого из клиентов.

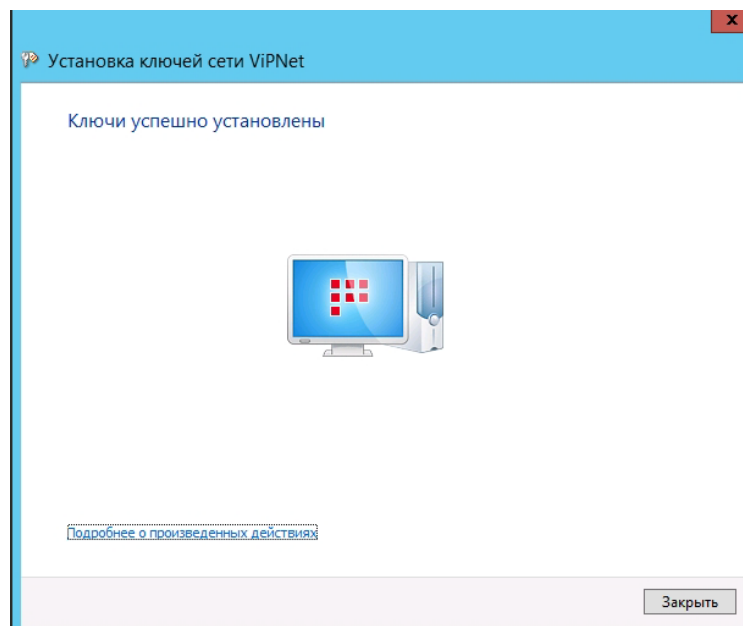


Рисунок 13 – Ключи успешно установлены

Теперь в защищенной сети для каждого из клиентов можно увидеть остальные узлы сети

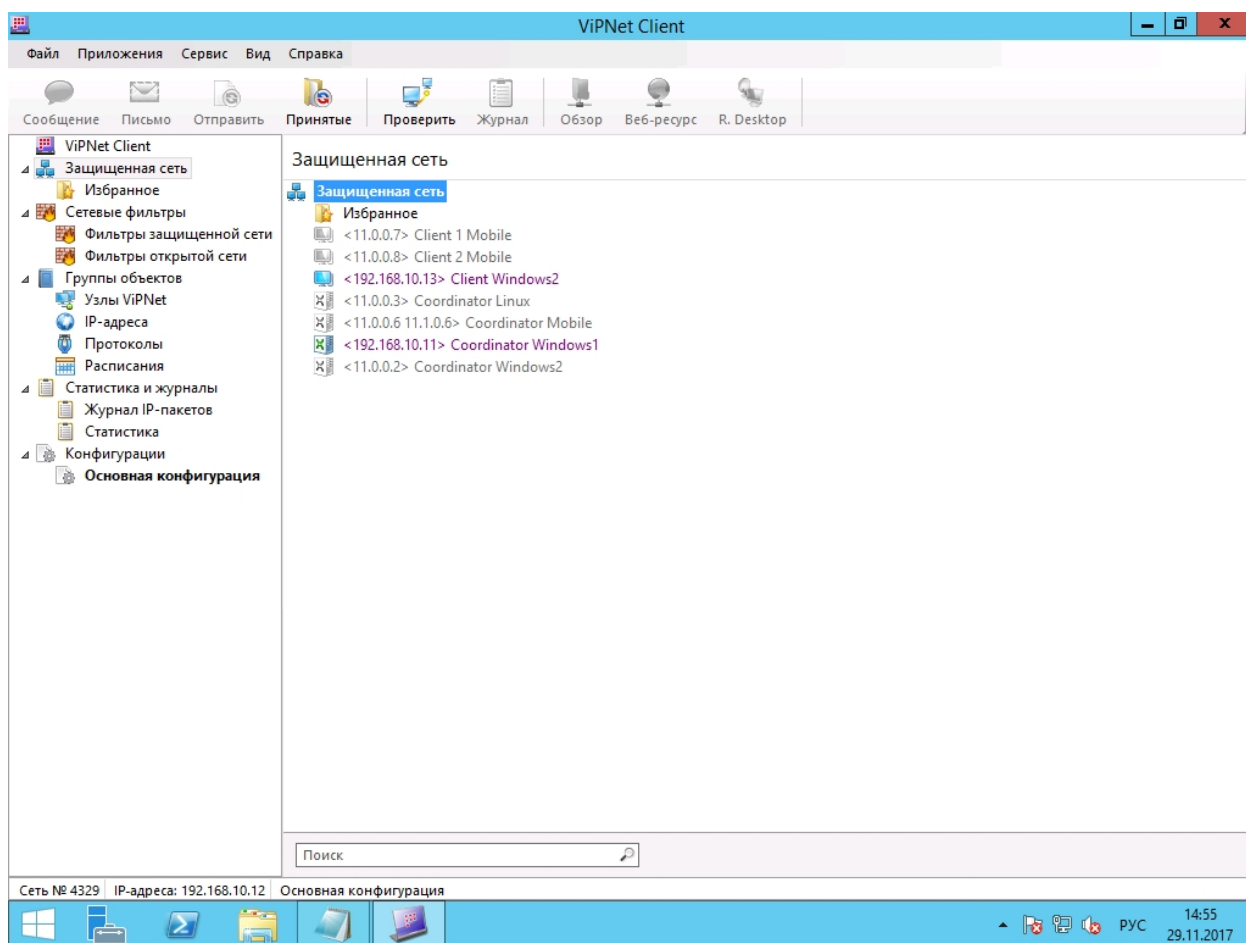


Рисунок 14 – Интерфейс «клиента 1»

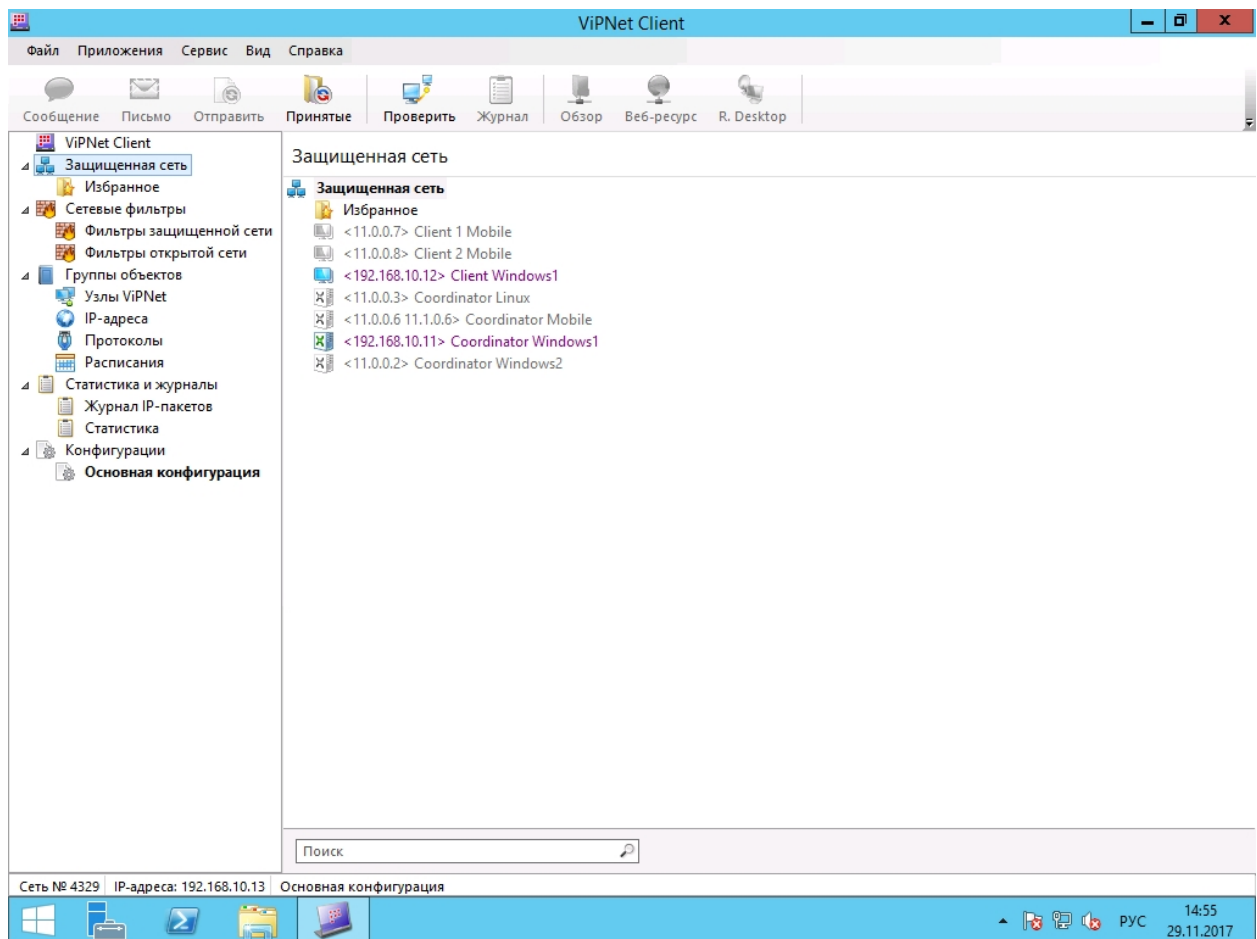


Рисунок 15 – Интерфейс «клиента 2»

VipNet обеспечивает полный контроль над сетевыми настройками компьютера.

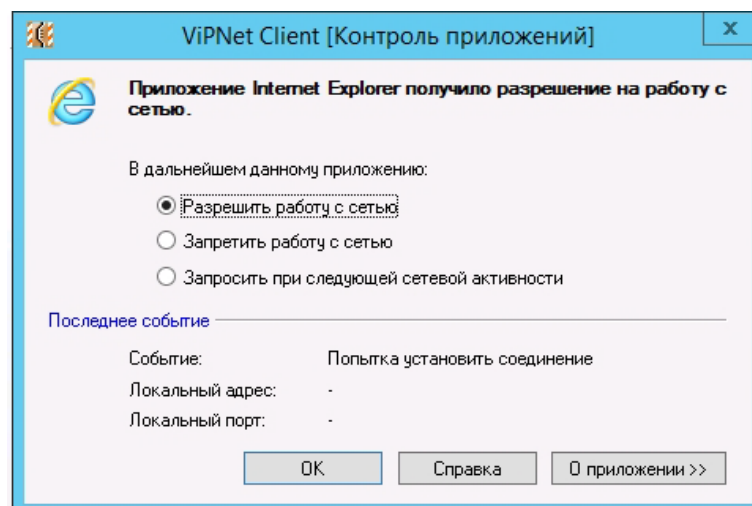


Рисунок 16 – Контроль приложений

Обращение клиента к координатору

1-Журнал регистрации IP-пакетов

Журнал Сервис Вид Справка

Обновить Имя Найти Свойства Справка

Время регистрации IP-пакетов - Последний час: с 29.11.2017 14:05:45, не более 100 записей

Конец интерв...	Источник	Назначение	Протокол	По...	По...	Кол...	Размер	Событие
29.11.2017 15:0...	Client Windows2	Coordinator Windo...	UDP	2046	2046	34	6611	40 - пропущен зашифрованный IP-пакет
29.11.2017 15:0...	192.168.10.1	224.0.0.1	IGMP	0	0	84	2352	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	204.2.255.224	192.168.10.13 (WIN...	TCP	443	493...	8	4394	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	13.33.76.4	192.168.10.13 (WIN...	TCP	443	493...	15	10064	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	88.221.73.188	192.168.10.13 (WIN...	TCP	443	493...	13	8359	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	62.67.193.85	192.168.10.13 (WIN...	TCP	443	493...	15	5119	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	62.67.193.85	192.168.10.13 (WIN...	TCP	443	493...	11	3671	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	23.35.100.252	192.168.10.13 (WIN...	TCP	443	493...	12	7111	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	173.194.73.94	192.168.10.13 (WIN...	TCP	443	493...	9	4823	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	173.194.73.106	192.168.10.13 (WIN...	TCP	443	493...	8	4804	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	151.101.38.49	192.168.10.13 (WIN...	TCP	443	493...	12	7433	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	151.101.38.49	192.168.10.13 (WIN...	TCP	443	493...	10	6532	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	108.177.14.154	192.168.10.13 (WIN...	TCP	443	493...	14	9796	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	108.177.14.154	192.168.10.13 (WIN...	TCP	443	493...	14	9601	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	108.177.14.154	192.168.10.13 (WIN...	TCP	443	493...	11	7588	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	108.177.14.154	192.168.10.13 (WIN...	TCP	443	493...	12	7442	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	173.194.222.154	192.168.10.13 (WIN...	TCP	443	493...	7	3967	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	173.194.222.154	192.168.10.13 (WIN...	TCP	443	493...	9	5201	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	23.193.43.16	192.168.10.13 (WIN...	TCP	443	493...	12	7790	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	107.178.240.89	192.168.10.13 (WIN...	TCP	443	493...	9	4416	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	107.178.240.89	192.168.10.13 (WIN...	TCP	443	493...	7	3787	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	66.117.28.68	192.168.10.13 (WIN...	TCP	443	492...	9	4350	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	2.18.77.65	192.168.10.13 (WIN...	TCP	443	492...	11	6732	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	63.251.88.56	192.168.10.13 (WIN...	TCP	443	492...	10	4738	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	185.29.135.234	192.168.10.13 (WIN...	TCP	443	492...	9	5113	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	104.244.42.131	192.168.10.13 (WIN...	TCP	443	492...	10	4885	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	108.177.14.154	192.168.10.13 (WIN...	TCP	443	492...	11	7524	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	108.177.14.154	192.168.10.13 (WIN...	TCP	443	492...	10	7308	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	95.100.9.163	192.168.10.13 (WIN...	TCP	443	492...	12	4641	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	95.100.9.163	192.168.10.13 (WIN...	TCP	443	492...	34	42072	60 - пропущен незашифрованный локаль...
29.11.2017 15:0...	40.77.226.250	192.168.10.13 (WIN...	TCP	443	492...	19	8138	60 - пропущен незашифрованный локаль...

15:06 29.11.2017

Рисунок 17 – Обращение клиента к координатору

С координатора можно посмотреть на работоспособность клиентов и последнюю активность на компьютере.

Administrator... - Проверка соединения

Файл Действия Вид Справка

Узел	Статус	Активность на компьютере	Имя компьютера	Версия ПО	Версия ОС
Administrator	Доступен				
Client 1 Mobile	Доступен				
Client 2 Mobile	Доступен				
Client Windows1	Доступен	29 ноября 2017 г. 14:55:19	WIN-6ID9I737OHU	4.3(3.47224) RUS	Microsoft Windows Server 2012 R2
Client Windows2	Доступен	29 ноября 2017 г. 14:56:15	WIN-6ID9I737OHU	4.3(3.47224) RUS	Microsoft Windows Server 2012 R2
Coordinator Linux	Недоступен				
Coordinator Mobile	Недоступен				
Coordinator Windows2	Недоступен				

15:06 29.11.2017

Рисунок 18 – Администрирование и контроль

Зашифрованные пакеты внутри VPN можно увидеть в журнале регистрации IP-пакетов

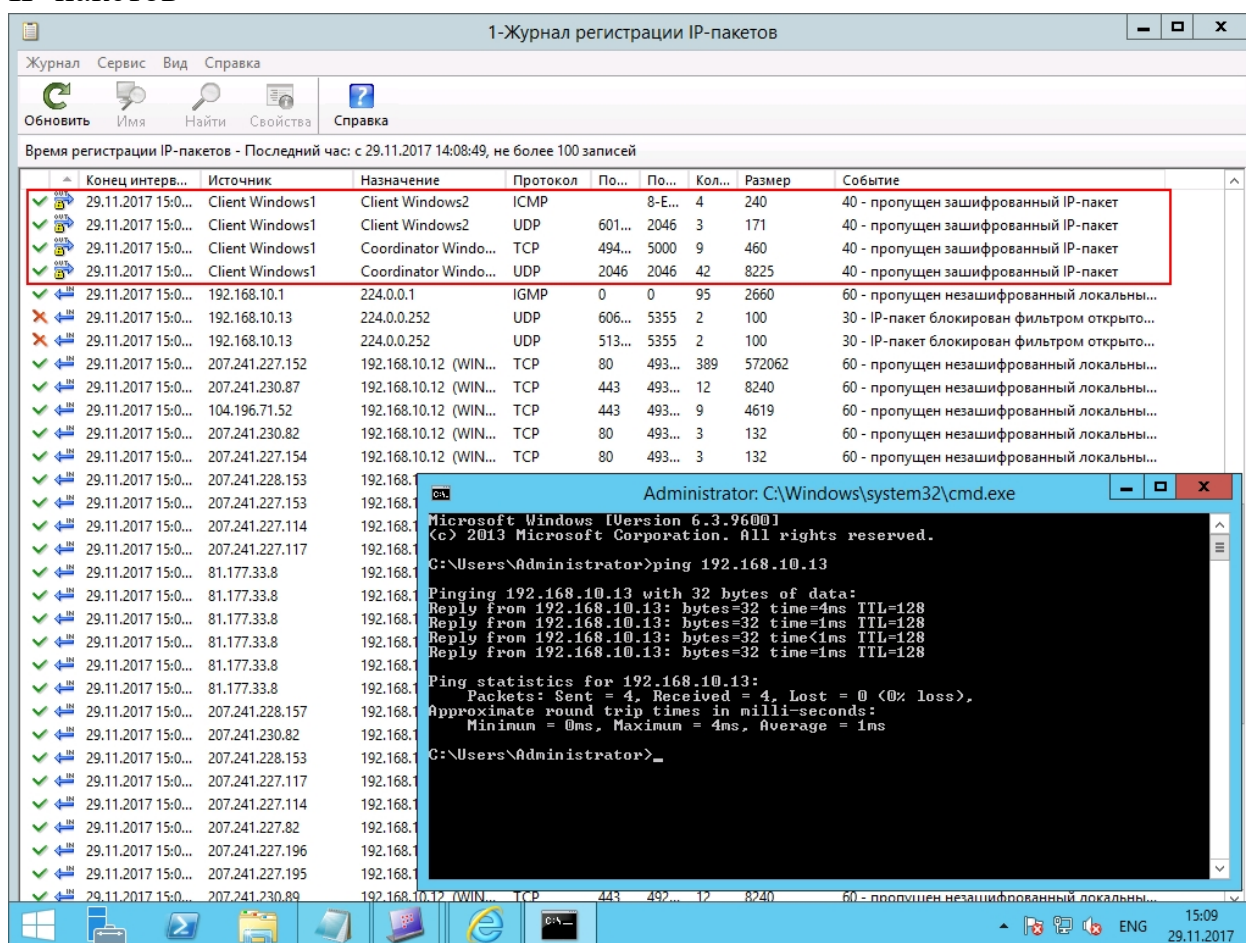


Рисунок 19 – Просмотр журнала пакетов

Отправим файл от одного компьютера к другому при помощи интерфейса приложения.

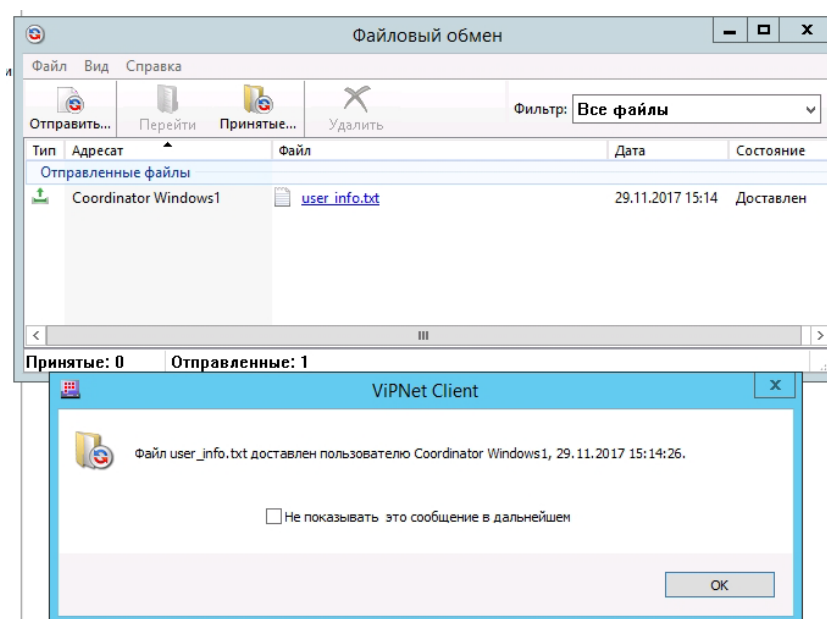


Рисунок 20 – Файл отправлен

Получим этот файл на другом компьютере

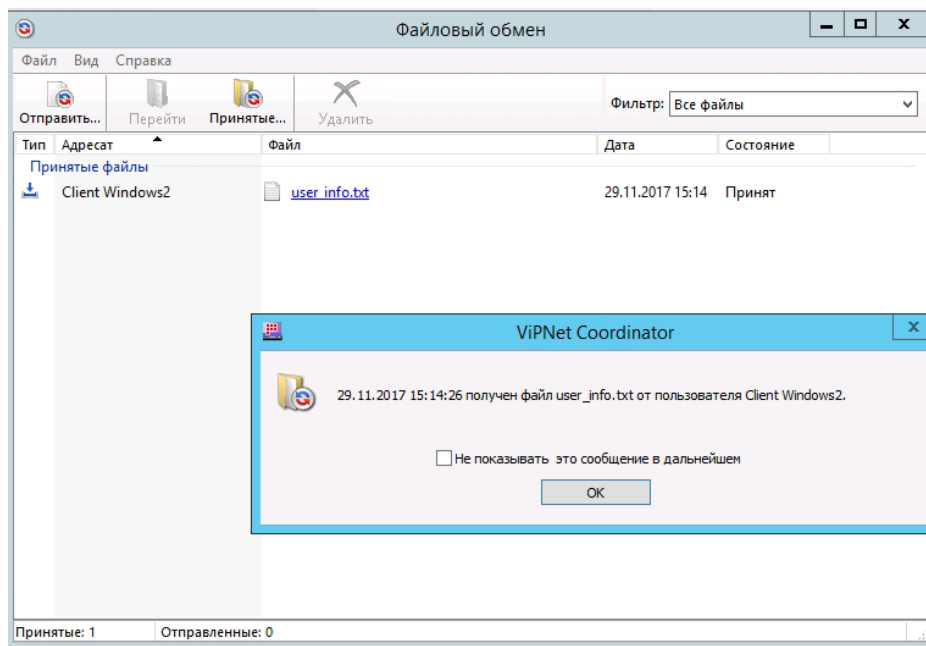


Рисунок 21 – Файл получен

Вывод:

В ходе лабораторной работы была настроена корпоративная VPN при помощи ПО “Infotecs VipNet”. Выбранная архитектура сети состоит из следующих узлов: два клиента и один координатор. Для них были установлены ключи регистрации в сети и настроены параметры взаимодействия.