**Лабораторная работа № 6. Знакомство с работой продуктов ViPNet. Соединение Site to Site. Распределенная система сетевых экранов. Мобильная безопасность.**

***Задание***

Сконфигурировать стенды, согласно приведенному описанию. Выполнить проверку работоспособности полученной компьютерной сети.

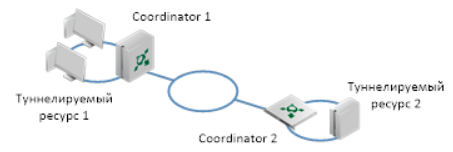
**Соединение Site to Site**

Используемые ключи:

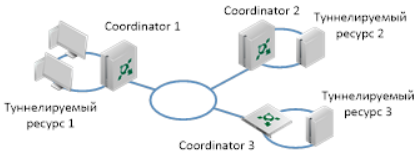
Client Windows1

Coordinator Windows2 и/или Coordinator Linux1

**Схема стенда 4:**



**Схема стенда 5:**



Для работы схемы необходимо настроить маршрутизацию пакетов во всех сегментах. На узлах туннелируемых ресурсов шлюзами по умолчанию следует указывать интерфейсы «собственных» координаторов. Предполагается, что между сегментами подсетей отсутствует широковещательный трафик. На узлах Coordinator 2 и Coordinator 3 шлюзом по умолчанию рекомендуется выбрать Coordinator 1.

Данный стенд позволяет:

1. Промоделировать взаимодействие узлов в сегментах распределенной сети по защищенным каналам
2. Опробовать способ решения проблемы совпадения IP-адресов в сегментах сети.

**Распределенная система сетевых экранов**

Используемые ключи:

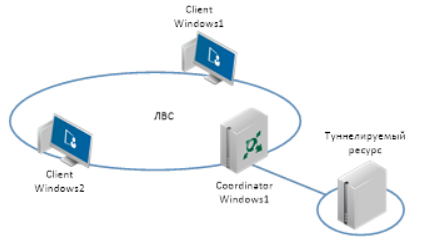
Coordinator Windows1

Client Windows1

Client Windows2

Для демонстрации этого сценария подходит рекомендуемая схема:

**Схема стенда 6**



Для работы схемы необходимо настроить маршрутизацию пакетов во всех сегментах. На узлах туннелируемых ресурсов шлюзами по умолчанию следует указывать интерфейсы «собственных» координаторов. Предполагается, что между сегментами подсетей отсутствует широковещательный трафик. На узлах Coordinator 2 и Coordinator 3 шлюзом по умолчанию рекомендуется выбрать Coordinator 1.

Данный сценарий позволяет:

* Настроить и проверить работу сетевых экранов ПО ViPNet на каждом из узлов.
* Исследовать способы разрешения и запрещения трафика путем задания правил экранирования.
* Опробовать работу раздельной фильтрации защищенного, открытого, транзитного, туннелируемого трафика.
* Посмотреть результаты работы файрволла во встроенном сниффере (журнале регистрации IP-пакетов)

**Мобильная безопасность**

a. Защита трафика мобильного устройства

b. ViPNet Connect — защищенные коммуникации

Используемые ключи:

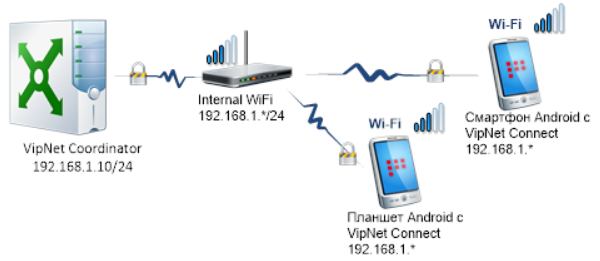
Coordinator Mobile

Client Android1

Client Android2

Для демонстрации этого сценария рекомендуемая схема:

**Схема стенда 6:**



Для развертывания стенда и первичной настройки необходимо выполнить требование подключения устройств к Координатору по WiFi с указанными IP=-адресами. Шлюзом по умолчанию на узде Coordinator необходимо указать точку доступа. В дальнейшем, если WiFi роутер подключен к Интернет, то возможно подключение мобильных устройств к Координатору извне (используя любые способы подключения устройств к Интернет).

В данной схеме можно:

* Познакомиться с интерфейсом ViPNet Client и ViPNet Connect для мобильных устройств под управлением ОС Android;
* Протестировать телефонную связь и передачу сообщений (чат) между мобильными устройствами в режиме peer-to-peer,
* Если дополнить схему туннелируемым ресурсом, то можно продемонстрировать доступ с мобильных устройств к ресурсам корпоративной сети, например, к почтовому серверу организации.

***Варианты индивидуальных заданий***

Каждый обучающийся самостоятельно конфигурирует стенд для выполнения лабораторной работы. Информация по используемым именам: если имя компьютера и имя рабочей группы (или домена) не задано явной для ОС, используемой в конфигурируемом стенде, то используются следующие правила именования – имя рабочей группы (или домена) соответствует фамилии обучающегося, набранной латинскими буквами, а имена компьютеров – имени обучающегося, набранного латинскими буквами, и порядковому номеру. Например, обучающийся Иван Иванов, в сети два компьютера, входящие в одну рабочую группу. Тогда имя группы – ivanov, имя первого компьютера – ivan1, второго – ivan2.