

ЗАДАНИЕ НА ОЛИМПИАДУ «Информационная безопасность»

ВНИМАНИЕ! ПЕРЕД ВЫПОЛНЕНИЕМ ЗАДАНИЯ РЕКОМЕНДУЕТСЯ ПРОЧИТАТЬ ПОСТАНОВКУ ВОПРОСА ПОЛНОСТЬЮ!

Компания ООО «Олимп ИБ» приняла Вас на стажировку на должность техника по защите информации. Ваша задача организовать базовую систему защиты путем внедрения VPN-решений и средств криптографической защиты информации на базе линейки ViPNet.

При планировании сети ViPNet следует исходить из схемы развертывания VPN в локальной сети компании, представленной на рисунке 1.

ВНИМАНИЕ! ПРИ НАСТРОЙКЕ СЕТЕВЫХ ИНТЕРФЕЙСОВ ОБЯЗАТЕЛЬНО УКАЗЫВАТЬ НАИМЕНОВАНИЕ СЕТИ

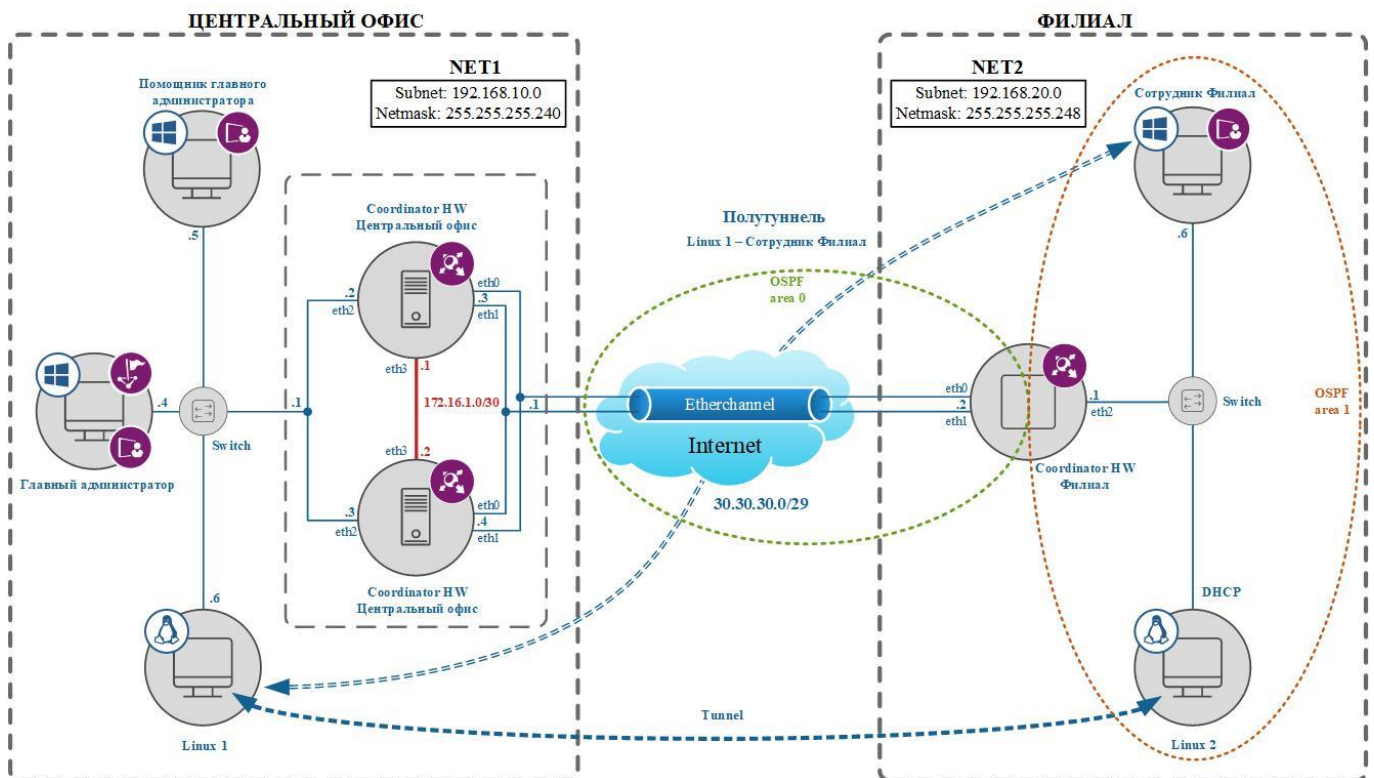


Рисунок 1 – Схема локальной сети ViPNet

Создать сетевые узлы и пользователей согласно таблице 1.

ДЛЯ ВСЕХ СЕТЕВЫХ УЗЛОВ ПРИ ВЫДАЧЕ ПАРОЛЕЙ ОБЯЗАТЕЛЬНО ПРИДЕРЖИВАТЬСЯ СХЕМЫ:

- ПАРОЛЬ НА ПОЛЬЗОВАТЕЛЯ: 11111111 (8 ЕДИНИЦ)

- ПАРОЛЬ НА АДМИНИСТРАТОРА УЗЛА: 55555555 (8 ПЯТЁРОК)

Таблица 1 – Пользователи и сетевые узлы

№	Название сетевого узла	Имя пользователя на сетевом узле
1	Главный администратор	Валеев М.В.
2	Помощник главного администратора	Грибаков С.Л.
3	Сотрудник Филиал	Попов А.В.
4	Coordinator HW Центральный офис	Coordinator HW Центральный офис
5	Coordinator HW Филиал	Coordinator HW Филиал

Связи между пользователями указать согласно таблице 2.

Таблица 2 – Матрица связей пользователей

<i>Связи пользователей</i>	Главный администратор	Помощник главного администратора	Сотрудник Филиал	Coordinator HW Центральный офис	Coordinator HW Филиал
Главный администратор		•	•	•	•
Помощник главного администратора	•			•	
Сотрудник Филиал	•				
Coordinator HW Центральный офис	•	•			•
Coordinator HW Филиал	•			•	

Для выполнения задания необходимо будет установить все компоненты ViPNet Administrator 4 на одно виртуальное место. Настроить данное ПО и создать структуру защищенной сети. Развернуть рабочее место помощника главного администратора.

Произвести удаленное обновление программного обеспечения всех клиентов филиала. Установить программное обеспечение для централизованного управления политиками безопасности и создать политику, которая разрешает трафик социальных сетей в обеденный перерыв.

ЗАДАНИЕ 1 Настройка сети

1. Настроить сетевые адаптеры в VirtualBox (как показано на схеме – рисунок 1).
2. Выдать IP-адреса (как показано на схеме – рисунок 1).

ЗАДАНИЕ 2 Главный администратор

1. Установить программное обеспечение «ViPNet Administrator» на машину «Главного Администратора».
2. Создать структуру защищенной сети в соответствии с заданными критериями:
 - Настроить узлы согласно топологии сети;
 - Выдать соответствующие роли для промежуточных узлов;
 - На каждый узел «назначить» пользователей согласно таблице 1;
 - Задать связи между пользователями согласно таблице 2.
3. Выдать пароли пользователям и администраторам согласно требованиям.
4. Установить соответствующее программное обеспечение на машину «Главного Администратора».

ЗАДАНИЕ 3 Помощник главного администратора

1. Установить соответствующее программное обеспечение на машину «Помощник главного админа».
2. Настроить возможность удаленного администрирования ЦУС.

ЗАДАНИЕ 4 Политика безопасности

1. Используя средство централизованного управления политиками безопасности, создать политику, которая разрешает узлу «Сотрудник Филиал» трафик социальных сетей по будням: с часу до двух дня.

Предусмотреть возможность работы двух незащищенных узлов на базе ОС Linux Ubuntu: *Linux 1* и *Linux 2*. Трафик данных узлов защитить на наиболее опасном участке сети и разрешить запросы PING. Linux 2 должен получить IP-адрес и шлюз по протоколу DHCP.

Между двумя координаторами предусмотреть возможность создания агрегированного канала связи. Особое внимание стоит уделить координаторам Центрального офиса. Данные узлы должны быть в кластере горячего резервирования.

Маршруты во всех сетях должны быть анонсированы. Для *Coordinator HW Филиал* предусмотреть настройку маршрутов только по протоколу динамической маршрутизации OSPF.

ЗАДАНИЕ 5 Coordinator HW Центральный офис

1. Произвести инициализацию устройств.
2. Сделать агрегированный канал с балансировкой нагрузки и отказа устойчивости, при котором пакет отправляется последовательно (будет использоваться eth0, eth1).
3. Настроить туннель для Linux 1 и Linux 2.

ЗАДАНИЕ 6 Кластер горячего резервирования

1. Задать адресацию на интерфейс синхронизации согласно схеме.
2. Собрать кластер горячего резервирования.

ЗАДАНИЕ 7 Coordinator HW Филиал

1. Произвести инициализацию устройства.
2. Сделать агрегированный канал с балансировкой нагрузки и отказа устойчивости, при котором пакет отправляется последовательно (будет использоваться eth0, eth1).
3. Настроить протокол динамической маршрутизации OSPF.
4. Настроить DHCP-сервер.
5. Настроить туннель для Linux 1 и Linux 2.

Сотрудник Филиал должен общаться по зашифрованному каналу связи с незащищенными узлами двух сетей.

ЗАДАНИЕ 8 Сотрудник Филиала

1. Установить программное обеспечение «ViPNet Client» на машину «Сотрудник Филиал».
2. Настроить полутуннель для Сотрудника Филиал и Linux 1.
3. Произвести удаленное обновление ПО ViPNet Client с версии 4.5.3.65090 на версию 4.5.3.65117 только для сети филиала.

Версии продуктов:

- ✓ **ViPNet Administrator 4.6.9** (первый вход под учетной записью Administrator, пароль: Administrator)
- ✓ **ViPNet Client 4.5.3**
- ✓ **ViPNet Coordinator HW 4.5.2** (первый вход под учетной записью user, пароль: user)
- ✓ **ViPNet Policy Manager 4.5.5** (первый вход под учетной записью Supervisor, пароль: Supervisor)
- ✓ **Linux Ubuntu 16.04 LTS** (Логин: Student, пароль: 11111 – 6 единиц)
- ✓ **Windows 10** (Логин: Student, пароль: 11111 – 6 единиц)

ВНИМАНИЕ! ВСЯ ПРОВЕРКА ВЫПОЛНЕНИЯ ЗАДАНИЯ ОСУЩЕСТВЛЯЕТСЯ ФУНКЦИОНАЛЬНО!

