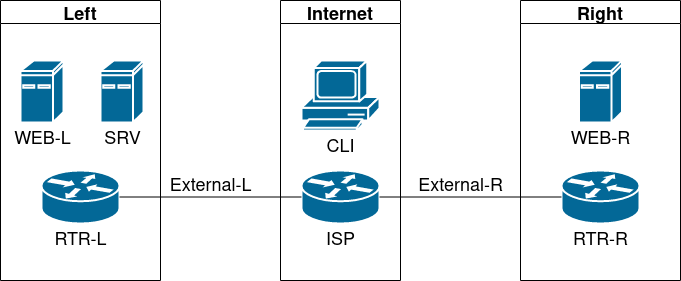
Образец задания для демонстрационного экзамена по комплекту оценочной документации.

# Описание задания Модуль 1

Вариант 1-0 (публичный)



**192.168.100.0/24**

**3.3.3.0/24**

**172.16.100.0/24**

**.100**

**.254**

**.200**

**.10**

**.1**

**.100**

**.254**

**.100**

**4.4.4.0/24**

**.1**

**.1**

**5.5.5.0/24**

**.100**

# Виртуальные машины и коммутация.

Необходимо выполнить создание и базовую конфигурацию виртуальных машин.

* На основе предоставленных ВМ или шаблонов ВМ создайте отсутствующие виртуальные машины в соответствии со схемой.
  + Характеристики ВМ установите в соответствии с **Таблицей 1;**
  + Коммутацию (если таковая не выполнена) выполните в соответствии со схемой сети.
* Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой.
* Адресация должна быть выполнена в соответствии с Таблицей 1;
* Обеспечьте ВМ дополнительными дисками, если таковое необходимо в соответствии с **Таблицей 1;**

регионами работы приложения, а также обеспечить выход ВМ в имитируемую сеть “Интернет”.

* Сети, подключенные к ISP, считаются внешними:
  + Запрещено прямое попадание трафика из внутренних сетей во внешние и наоборот;
* Платформы контроля трафика, установленные на границах регионов, должны выполнять трансляцию трафика, идущего из соответствующих внутренних сетей во внешние сети стенда и в сеть Интернет.
  + Трансляция исходящих адресов производится в адрес платформы, расположенный во внешней сети.
* Между платформами должен быть установлен защищенный туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов.
  + Трафик, проходящий по данному туннелю, должен быть защищен:
    - Платформа ISP не должна иметь возможности просматривать содержимое пакетов, идущих из одной внутренней сети в другую.
  + Туннель должен позволять защищенное взаимодействие между платформами управления трафиком по их внутренним адресам
    - Взаимодействие по внешним адресам должно происходит без применения туннеля и шифрования.
  + Трафик, идущий по туннелю между регионами по внутренним адресам, не должен транслироваться.
* Платформа управления трафиком RTR-L выполняет контроль входящего трафика согласно следующим правилам:
  + Разрешаются подключения к портам DNS, HTTP и HTTPS для всех клиентов;
    - Порты необходимо для работы настраиваемых служб
  + Разрешается работа выбранного протокола организации защищенной связи;
    - Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”
  + Разрешается работа протоколов ICMP;
  + Разрешается работа протокола SSH;
  + Прочие подключения запрещены;
  + Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;
* Платформа управления трафиком RTR-R выполняет контроль входящего трафика согласно следующим правилам:
  + Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;
    - Порты необходимо для работы настраиваемых служб
  + Разрешается работа выбранного протокола организации защищенной связи;
    - Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”
  + Разрешается работа протоколов ICMP;
  + Разрешается работа протокола SSH;
  + Прочие подключения запрещены;
  + Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;
* Обеспечьте настройку служб SSH региона Left:
  + Подключения со стороны внешних сетей по протоколу к платформе управления трафиком RTR-L на порт 2222 должны быть перенаправлены на ВМ Web-L;
  + Подключения со стороны внешних сетей по протоколу к платформе

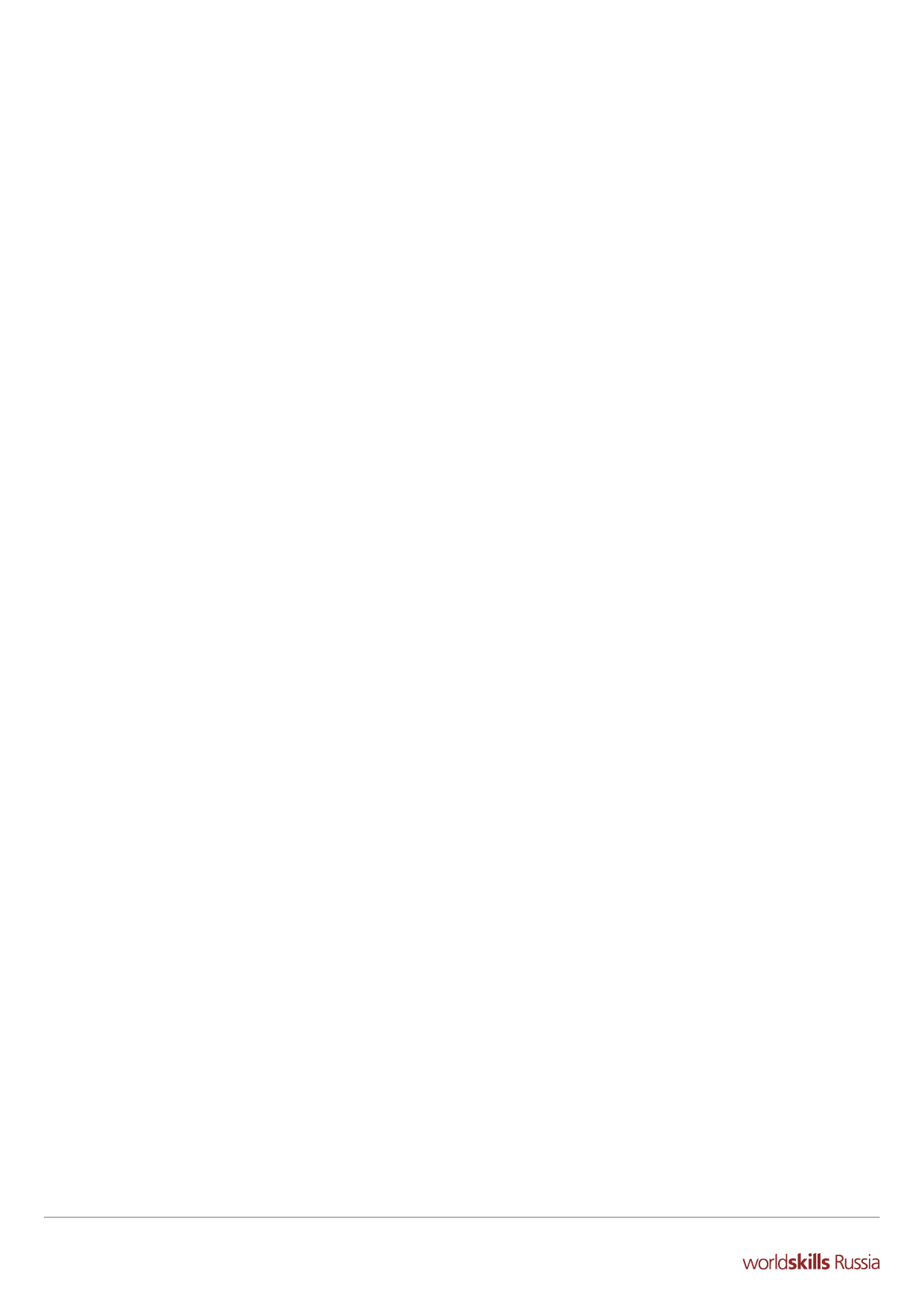
2244

управления трафиком RTR-L перенаправлены на ВМ Web-R;

Rна порт

должны быть

# Инфраструктурные службы.



В рамках данного модуля необходимо настроить основные инфраструктурные службы и настроить представленные ВМ на применение этих служб для всех основных функций.

* Выполните настройку первого уровня DNS-системы стенда:
  + Используется ВМ ISP;
  + Обслуживается зона demo.wsr.
    - Наполнение зоны должно быть реализовано в соответствии с

# Таблицей 2;

* + Сервер делегирует зону int.demo.wsr на SRV;
    - Поскольку SRV находится во внутренней сети западного региона, делегирование происходит на внешний адрес маршрутизатора данного региона.

64

соответствующие порты DNS-службы в порты сервера SRV.

* + Внешний клиент CLI должен использовать DNS-службу, развернутую на ISP, по умолчанию;
* Выполните настройку второго уровня DNS-системы стенда;
  + Используется ВМ SRV;
  + Обслуживается зона int.demo.wsr;
    - Наполнение зоны должно быть реализовано в соответствии с

# Таблицей 2;

* + Обслуживаются обратные зоны для внутренних адресов регионов
    - Имена для разрешения обратных записей следует брать из

# Таблицы 2;

* + Сервер принимает рекурсивные запросы, исходящие от адресов внутренних регионов;
    - Обслуживание клиентов(внешних и внутренних), обращающихся к к зоне int.demo.wsr, должно производится без каких либо ограничений по адресу источника;
  + Внутренние хосты регионов (равно как и платформы управления трафиком) должны использовать данную DNS-службу для разрешения всех запросов имен;
* Выполните настройку первого уровня системы синхронизации времени:
  + Используется сервер ISP.
  + Сервер считает собственный источник времени верным, stratum=4;
  + Сервер допускает подключение только через внешний адрес соответствующей платформы управления трафиком;
    - Подразумевается обращение SRV для синхронизации времени;
  + Клиент CLI должен использовать службу времени ISP;
* Выполните конфигурацию службы второго уровня времени на SRV.
  + Сервер синхронизирует время с хостом ISP;
    - Синхронизация с другими источникам запрещена;
  + Сервер должен допускать обращения внутренних хостов регионов, в том числе и платформ управления трафиком, для синхронизации времени;
  + Все внутренние хосты(в том числе и платформы управления трафиком) должны синхронизировать свое время с SRV;
* Реализуйте файловый SMB-сервер на базе SRV

WEB-L и WEB-R;

* + Сервер, в зависимости от ОС, использует следующие каталоги для хранения файлов:
    - /mnt/storage для система на базе Linux;
    - Диск R:\ для систем на базе Windows;
  + Хранение файлов осуществляется на диске (смонтированном по указанным выше адресам), реализованном по технологии RAID типа “Зеркало”;
* Сервера WEB-L и WEB-R должны использовать службу, настроенную на SRV, для обмена файлами между собой:
  + Служба файлового обмена должна позволять монтирование в виде стандартного каталога Linux;
    - Разделяемый каталог должен быть смонтирован по адресу

/opt/share;

* + Каталог должен позволять удалять и создавать файлы в нем для всех пользователей;
* Выполните настройку центра сертификации на базе SRV:
  + В случае применения решения на базе Linux используется центр сертификации типа OpenSSL и располагается по адресу /var/ca;
  + Выдаваемые сертификаты должны иметь срок жизни не менее 500 дней;
  + Параметры выдаваемых сертификатов:
    - Страна RU;
    - Организация DEMO.WSR;
    - Прочие поля (за исключением CN) должны быть пусты;

# Инфраструктура веб-приложения.

Данный блок подразумевает установку и настройку доступа к веб- приложению, выполненному в формате контейнера Docker.

* Образ Docker (содержащий веб-приложение) расположен на ISO-образе дополнительных материалов;
  + Выполните установку приложения AppDocker0;
* Пакеты для установки Docker расположены на дополнительном ISO-образе;
* Инструкция по работе с приложением расположена на дополнительном ISO-образе;
* Необходимо реализовать следующую инфраструктуру приложения.
  + Хостинг приложения осуществляется на ВМ WEB-L и WEB-R;
  + Доступ к приложению осуществляется по DNS-имени [www](http://www.int.demo/).demo.wsr;
    - Имя должно разрешаться во “внешние” адреса ВМ управления трафиком в обоих регионах;
    - При необходимости, для доступа к к приложению допускается реализовать реверс-прокси или трансляцию портов;
  + Доступ к приложению должен быть защищен с применением технологии TLS;
    - Необходимо обеспечить корректное доверие сертификату сайта, без применения “исключений” и подобных механизмов;
  + Незащищенное соединение должно переводится на защищенный канал автоматически;
* Необходимо обеспечить отказоустойчивость приложения;
  + Сайт должен продолжать обслуживание (с задержкой не более 25 секунд) в следующих сценариях:
    - Отказ одной из ВМ Web
    - Отказ одной из ВМ управления трафиком.

Таблица 1. Характеристики ВМ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Имя ВМ | ОС | ОЗУ | Кол- во ядер | IP-адреса | Дополнительно |
| RTR- L | Debian 11 | 2 Гб | 2 | 4.4.4.100/24  192.168.100.254/  24 |  |
| Cisco CSR |  | 4 |  |
| RTR- R | Debian 11 | 2 Гб | 2 | 5.5.5.100/24  172.16.100.254/2  4 |  |
| Cisco CSR |  | 4 |  |
| SRV | Debian 11 | 2 Гб | 2 | 192.168.100.200/  24 | Дополнительные диски:  2 шт по 2 Гб |
| Windows Server 2019 | 4 Гб | 4 | Дополнительные диски:  2 шт по 2 Гб |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| WEB- L | Debian 11 | 2 Гб | 2 | 192.168.100.100/  24 |  |
| WEB- R | Debian 11 | 2 Гб | 2 | 172.16.100.100/2  4 |  |
| ISP | Debian 11 | 2 Гб | 2 | 4.4.4.1/24  5.5.5.1/24  3.3.3.1/24 |  |
| CLI | Windows 10 | 4 | 4 | 3.3.3.10/24 |  |

Таблица 2. DNS-записи зон

|  |  |  |  |
| --- | --- | --- | --- |
| Зона | Тип записи | Ключ | Значение |
| demo.wsr | A | isp | 3.3.3.1 |
| A | www | 4.4.4.100 |
| A | www | 5.5.5.100 |
| CNAME | internet | isp |
| int.demo.wsr | A | web-l | 192.168.100.100 |
| A | web-r | 172.16.100.100 |
| A | srv | 192.168.100.200 |
| A | rtr-l | 192.168.100.254 |
| A | rtr-r | 172.16.100.254 |
| ~~CNAME~~ | ~~webapp~~ | ~~web-l~~ |
| ~~CNAME~~ | ~~webapp~~ | ~~web-r~~ |
| CNAME | ntp | srv |
| CNAME | dns | srv |

no

no