**ЗАДАНИЕ**

**ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА БАЗОВОГО УРОВНЯ**

(2023 год)

|  |  |
| --- | --- |
| **Код и наименование профессии (специальности) среднего профессионального образования**  | 09.02.06 Сетевое и системное администрирование |
| **Наименование квалификации** | Сетевой и системный администратор |

**Вариант № 1**

|  |
| --- |
| **Модуль 1: Выполнение работ по проектированию сетевой инфраструктуры** |
| **Задание модуля 1:**Рисунок 1. Топология1. **Выполнение проектирования кабельной структуры компьютерной сети.**

**Виртуальные машины и коммутация**Необходимо выполнить создание и базовую конфигурацию виртуальных машин.* 1. На основе предоставленных ВМ или шаблонов ВМ создайте отсутствующие виртуальные машины в соответствии со схемой.
	2. Характеристики ВМ установите в соответствии с **Таблицей 1;**
	3. Коммутацию (если таковая не выполнена) выполните в соответствии со схемой сети.
	4. Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой.
	5. Адресация должна быть выполнена в соответствии с Таблицей 1;
	6. Обеспечьте ВМ дополнительными дисками, если таковое необходимо в соответствии с **Таблицей 1.**

Таблица 1. Характеристики ВМ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Имя ВМ | ОС | ОЗУ | Кол- во ядер | IP-адреса | Дополнительно |
| RTR- L | Debian 11 | 2 Гб | 2 | 7.7.7.100/24192.168.100.254/24 |  |
| Cisco CSR |  | 4 |  |  |
| RTR- R | Debian 11 | 2 Гб | 2 | 8.8.8.100/24172.16.100.254/24 |  |
| Cisco CSR |  | 4 |  |  |
| SRV | Debian 11 | 2 Гб | 2 |  |  |
| Windows Server 2019 | 4 Гб | 4 | 192.168.100.200/24 | 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 | 172.16.100.100/24 |  |
| ISP | Debian 11 | 2 Гб | 2 | 7.7.7.1/248.8.8.1/243.3.3.1/24 |  |
| CLI | Windows 10 | 4 | 4 | 3.3.3.10/24 |  |

1. **Осуществление выбора технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности**

**Сетевая связанность*** 1. Настройте статический маршрут по умолчанию на маршрутизаторах **RTR-L** и **RTR-R.**
	2. Настройте динамическую трансляцию портов (PAT):

- На маршрутизаторе **RTR-L** настройте динамическую трансляцию портов (PAT) для сети 192.168.100.0/24 в соответствующие адреса исходящего интерфейса- На маршрутизаторе **RTR-R** настройте динамическую трансляцию портов (PAT) для сети 172.16.100.0/24 в соответствующие адреса исходящего интерфейса.**Конфигурация виртуальных частных сетей*** 1. Между платформами **RTR-L** и **RTR-R** должен быть установлен туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов со следующими параметрами:
1. Используйте в качестве VTI интерфейс Tunnel1
2. Между платформами должен быть установлен туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов

**Настройка маршрутизации*** 1. Настройте динамическую маршрутизацию между платформами **RTR-L** и **RTR-R.**
	2. Трафик, идущий по туннелю между регионами по внутренним адресам, не должен транслироваться.
 |
| **Модуль 2: Организация сетевого администрирования** |
| **Задание модуля 2:**Таблица 2. DNS-записи зон

|  |  |  |  |
| --- | --- | --- | --- |
| Зона | Тип записи | Ключ | Значение |
| demo.wsr | A | ISP | 3.3.3.1 |
| A | www | 7.7.7.100 |
| A | www | 8.8.8.100 |
| 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-L | web-l |
| CNAME | webapp-R | WEB-R |
| CNAME | ntp | SRV |
| CNAME | dns | SRV |

**Администрирование локальных вычислительных сетей и принятие мер по устранению возможных сбоев** **Сетевая связность.**В рамках данного модуля требуется обеспечить сетевую связность между регионами работы приложения, а также обеспечить выход ВМ в имитируемую сеть “Интернет”.**1.1.** Сети, подключенные к **ISP**, считаются внешними:- Запрещено прямое попадание трафика из внутренних сетей во внешние и наоборот;**1.2.** Обеспечьте настройку служб SSH региона Left:* 1. Подключения со стороны внешних сетей по протоколу к платформе управления трафиком **RTR-L** на порт 2222 должны быть перенаправлены на ВМ Web-L;
	2. Подключения со стороны внешних сетей по протоколу к платформе управления трафиком **RTR-R** на порт 2244 должны быть перенаправлены на ВМ **WEB-R**.

**Администрирование сетевых ресурсов в информационных системах** **Инфраструктурные службы.**В рамках данного модуля необходимо настроить основные инфраструктурные службы и настроить представленные ВМ на применение этих служб для всех основных функций.* 1. Выполните настройку первого уровня DNS-системы стенда:

a. Используется ВМ **ISP**;* 1. Обслуживается зона demo.wsr.
		+ - Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;
	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.
			- Маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера **SRV**.
	3. Внешний клиент **CLI** должен использовать DNS-службу, развернутую на **ISP**, по умолчанию;

**2.2.** Выполните настройку второго уровня DNS-системы стенда;a. Используется ВМ **SRV**;b. Обслуживается зона int.demo.wsr;* + - * Наполнение зоны должно быть реализовано в соответствии с Таблицей 2;
	1. Обслуживаются обратные зоны для внутренних адресов регионов
		+ - Имена для разрешения обратных записей следует брать из Таблицы 2;
	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;
	3. Внутренние хосты регионов (равно как и платформы управления трафиком) должны использовать данную DNS-службу для разрешения всех запросов имен;

**2.3.** Выполните настройку первого уровня системы синхронизации времени:a. Используется сервер **ISP**.b. Сервер считает собственный источник времени верным, stratum=4;* 1. Сервер допускает подключение только через внешний адрес соответствующей платформы управления трафиком;
* Подразумевается обращение **SRV** для синхронизации времени;
	1. Клиент **CLI** должен использовать службу времени **ISP**;
	2. Выполните конфигурацию службы второго уровня времени на **SRV**.

a. Сервер синхронизирует время с хостом **ISP**;- Синхронизация с другими источникам запрещена;b. Сервер должен допускать обращения внутренних хостов регионов, в том числе и платформ управления трафиком, для синхронизации времени;1. Все внутренние хосты(в том числе и платформы управления трафиком) должны синхронизировать свое время с **SRV**;

**2.5.** Реализуйте файловый SMB-сервер на базе **SRV*** 1. Сервер должен предоставлять доступ для обмена файлами серверам **WEB-L** и **WEB-R**;
	2. 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;
	3. Хранение файлов осуществляется на диске (смонтированном по указанным выше адресам), реализованном по технологии RAID типа “Зеркало”;

**2.6.** Сервера **WEB-L** и **WEB-R** должны использовать службу, настроенную на **SRV**, для обмена файлами между собой:* + - * 1. Служба файлового обмена должна позволять монтирование в виде стандартного каталога Linux;
			* Разделяемый каталог должен быть смонтирован по адресу /opt/share;
	1. Каталог должен позволять удалять и создавать файлы в нем для всех пользователей;

**2.7.** Выполните настройку центра сертификации на базе **SRV**:* + - * 1. В случае применения решения на базе Linux используется центр сертификации типа OpenSSL и располагается по адресу /var/ca;
				2. Выдаваемые сертификаты должны иметь срок жизни не менее 500 дней;
				3. Параметры выдаваемых сертификатов:
			* Страна RU;
			* Организация DEMO.WSR;
			* Прочие поля (за исключением CN) должны быть пусты;

**Взаимодействие со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности****Инфраструктура веб-приложения.**Данный блок подразумевает установку и настройку доступа к веб- приложению, выполненному в формате контейнера Docker.* 1. Образ Docker (содержащий веб-приложение) расположен на ISO-образе дополнительных материалов;
	2. Выполните установку приложения AppDocker0;
	3. Пакеты для установки Docker расположены на дополнительном ISO-образе;
	4. Инструкция по работе с приложением расположена на дополнительном ISO-образе;
	5. Необходимо реализовать следующую инфраструктуру приложения.
1. Клиентом приложения является **CLI** (браузер Edge);
2. Хостинг приложения осуществляется на ВМ **WEB-L** и **WEB-R**;
3. 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;1. Доступ к приложению должен быть защищен с применением технологии TLS;

- Необходимо обеспечить корректное доверие сертификату сайта, без применения “исключений” и подобных механизмов;1. Незащищенное соединение должно переводится на защищенный канал автоматически;
	1. Необходимо обеспечить отказоустойчивость приложения;
		* + 1. Сайт должен продолжать обслуживание (с задержкой не более 25 секунд) в следующих сценариях:

- Отказ одной из ВМ Web- Отказ одной из ВМ управления трафиком. |

|  |
| --- |
| **Модуль 3: Эксплуатация объектов сетевой инфраструктуры** |
| **Задание модуля 3:****Установка, настройка, эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей** **Конфигурация виртуальных частных сетей*** 1. Защита туннеля должна обеспечиваться с помощью **IPsec** между платформами **RTR-L** и **RTR-R**.
1. Используйте аутентификацию по общему ключу.
2. Параметры **IPsec** произвольные.

**Установка, настройка, эксплуатация и обслуживание сетевых конфигураций.****Настройка списков контроля доступа****2.1.** Платформа управления трафиком **RTR-R** выполняет контроль входящего трафика согласно следующим правилам:* 1. Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;
	2. Разрешаются подключения к портам HTTP и HTTPS для всех клиентов;

- Порты необходимо для работы настраиваемых служб* 1. Разрешается работа выбранного протокола организации защищенной связи;

- Разрешение портов должно быть выполнено по принципу “необходимо и достаточно”* 1. Разрешается работа протоколов ICMP;
	2. Разрешается работа протокола SSH;
	3. Прочие подключения запрещены;
	4. Для обращений в платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно;

**2.2.** 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 службРазрешается 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 к платформам со стороны хостов, находящихся внутри регионов, ограничений быть не должно. |