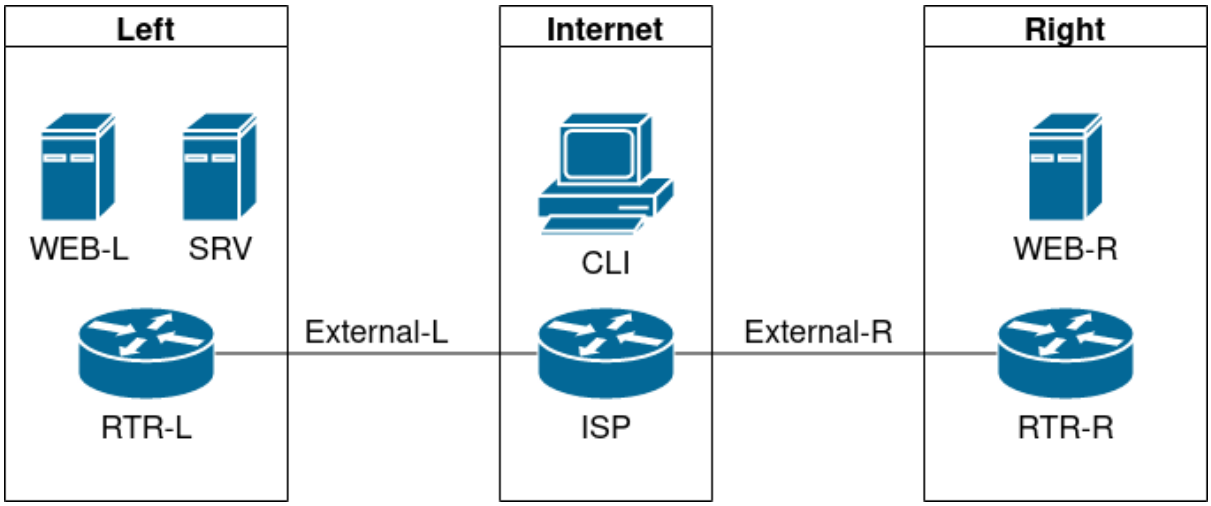
Задание для стажерского квалификационного зачёта на должность «Главный младший эникейщик»

Описание задания

Описание модуля 1



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;**
    - ВМ SRV в планах будет использоваться как гипервизор, убедитесь, что ваша конфигурация ВМ поддерживает аппаратную виртуализацию.
- Имена хостов в созданных ВМ должны быть установлены в соответствии с **Таблицей 1**.
- Адресация должна быть рассчитана самостоятельно, исходя из следующих требований в **Таблице 3**;
- Обеспечьте ВМ дополнительными дисками, если таковое необходимо в соответствии с **Таблицей 1;**

Сетевая связность

В рамках данного модуля требуется обеспечить сетевую связность между 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:
    - Подключения, только со стороны внешних сетей по протоколу к платформе управления трафиком RTR-L на порт 2222 должны быть перенаправлены на ВМ Web-L;
    - Подключения, только со стороны внешних сетей по протоколу к платформе управления трафиком RTR-R на порт 2255 должны быть перенаправлены на ВМ Web-R;
    - Прочие ВМ в ЛВС должны подключаться, используя параметры по умолчанию.
    - Пользователь для подключения - prof

Инфраструктурные службы

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

- Для удобства проверки от вас требуется настроить на SRV выполнение команд от имени администратора без прохождения аутентификации, только при использовании учётной записи prof
- Выполните настройку первого уровня DNS-системы стенда:
    - Используется ВМ ISP;
    - Обслуживается зона audit.prof.

        - Наполнение зоны должно быть реализовано в соответствии с **Таблицей 2;**
    - Сервер делегирует зону int.audit.prof 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.
    - 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.audit.prof;
        - 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 зоне int.audit.prof, должно производиться 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 сервер на базе SRV
    - Сервер должен предоставлять доступ для обмена файлами серверам WEB-L и WEB-R;
    - Сервер, в зависимости от своей ОС, использует следующие каталоги для хранения файлов:
        - /mnt/share для систем на базе Альт;
        - /mnt/exchange для прочих систем;
    - Хранение файлов осуществляется на диске (смонтированном по выбранному выше адресу), реализованном по технологии RAID1;
- 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 Альт используется центр сертификации типа OpenSSL и располагается по адресу /var/root-ca;
    - Выдаваемые сертификаты должны иметь срок жизни не более 300 дней;
    - Параметры выдаваемых сертификатов:
        - Страна RU;
        - Организация AUDIT.PROF;
        - 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;
- Инструкция по работе с приложением расположена на дополнительном ISO-образе;
- Необходимо реализовать следующую инфраструктуру приложения.
    - Клиентом приложения является CLI;
    - Хостинг приложения осуществляется на ВМ WEB-L и WEB-R;
    - Доступ к приложению осуществляется по DNS-имени www.audit.prof;
        - Имя должно разрешаться во “внешние” адреса ВМ управления трафиком в обоих регионах;
        - При необходимости, для доступа 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 переводиться на защищенный канал автоматически;
- Необходимо обеспечить отказоустойчивость сервиса;
    - 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/ системы	Дистрибутив ОС	ОЗУ	Кол-во ядер	IP-адреса	Дополнительно
RTR-L	JeOS	1	1	см. Таблицу 3	
RTR-R	RedOS	1	1	см. Таблицу 3	
SRV	Alt Server	3	2	первый в сети	Дополнительные диски: 2 шт по 2 Гб
WEB-L	Alt Server	2	2	12 адрес для узлов в сети	
WEB-R	RedOS	2	2	12 адрес для узлов в сети	
ISP	JeOS	1	1	см. Таблицу 3	
CLI	Alt Workstation K	2	3	второй адрес, из тех, что не распределены	

Таблица 2. DNS-записи зон

Зона	Тип записи	Ключ	Значение
demo.wsr	A	isp	[IP ISP internet]
	A	www	[IP RTR-R external]
	A	www	[IP RTR-L external]
	CNAME	internet	isp

int.demo.wsr	A	web-l	рассчитать
	A	web-r	рассчитать
	A	srv	рассчитать
	A	rtr-l	рассчитать
	A	rtr-r	рассчитать
	CNAME	time	srv
	CNAME	dns	srv

Таблица 3 – Требования к адресации

Требование	Значение
Базовый блок	10.24.25.0/24
Тип адресации	VLSM
Число подсетей	5
Необходимое число узлов	External-L – 2 External-R – 2 Internet – 3 Left – 25 Right - 45
Дополнительные требования	Шлюзом в локальных сетях выступает последний доступный адрес в сети, а во внешних – первый. Размер подсетей должен быть минимально возможным для требуемого числа узлов. (Запрещено использовать конфигурации, имеющие ограниченную совместимость) Подсети размещаются в базовом блоке адресов от большей к меньшей, с начала адресного пространства (при паритете – по алфавиту) При необходимости, прочие подсети следуют за обязательными, независимо от размеров.