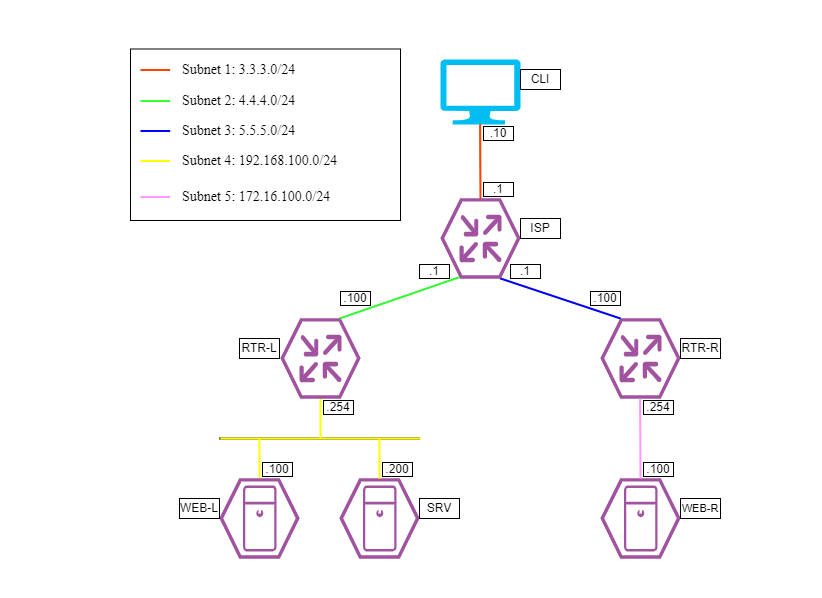
**Модуль 1**

Вариант 1-0 (публичный)

[](https://user-images.githubusercontent.com/79700810/149956179-026c9bba-e6fc-495a-81df-4c6ddb0ec1d6.png)

**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.
   * Характеристики ВМ установите в соответствии с Таблицей 1;
   * Коммутацию (если таковая не выполнена) выполните в соответствии со схемой сети.
2. Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой.
3. Адресация должна быть выполнена в соответствии с Таблицей 1;
4. Обеспечьте ВМ дополнительными дисками, если таковое необходимо в соответствии с Таблицей 1;

**Таблица 1. Характеристики ВМ**

| **Name VM** | **ОС** | **RAM** | **CPU** | **IP** | **Additionally** |
| --- | --- | --- | --- | --- | --- |
| RTR-L | vEltex | 2 GB | 2/4 | 4.4.4.100/24 |  |
|  |  |  |  | 192.168.100.254/24 |  |
| RTR-R | vEltex | 2 GB | 2/4 | 5.5.5.100/24 |  |
|  |  |  |  | 172.16.100.254 /24 |  |
| SRV | RedOS | 2 GB /4 GB | 2/4 | 192.168.100.200/24 | Доп диски 2 шт по 5 GB |
| WEB-L | RedOS | 2 GB | 2 | 192.168.100.100/24 |  |
| WEB-R | RedOS | 2 GB | 2 | 172.16.100.100/24 |  |
| ISP | vEltex | 2 GB | 2 | 4.4.4.1/24 |  |
|  |  |  |  | 5.5.5.1/24 |  |
|  |  |  |  | 3.3.3.1/24 |  |
| CLI | Astra Linux | 4 GB | 4 | 3.3.3.10/24 |  |

**1. На основе предоставленных ВМ или шаблонов ВМ создайте отсутствующие виртуальные машины в соответствии со схемой.**

Убедитесь, что все ВМ созданы в соответствии со схемой

[](https://user-images.githubusercontent.com/79700810/150134013-7ba0f3e5-29cb-4c69-8b6b-3d3c339c99b1.png)

**2. Имена хостов в созданных ВМ должны быть установлены в соответствии со схемой.**

**RTR-L**

en

conf t

hostname RTR-L

do wr

**RTR-R**

en

conf t

hostname RTR-R

do wr

**SRV**

Rename-Computer -NewName SRV

**WEB-L**

hostnamectl set-hostname WEB-L

**WEB-R**

hostnamectl set-hostname WEB-R

**ISP**

hostnamectl set-hostname ISP

**CLI**

Rename-Computer -NewName CLI

**3. Адресация должна быть выполнена в соответствии с Таблицей 1;**

**RTR-L**

int gi 1

ip address 4.4.4.100 255.255.255.0

no sh

int gi 2

ip address 192.168.100.254 255.255.255.0

no sh

end

wr

**RTR-R**

int gi 1

ip address 5.5.5.100 255.255.255.0

no sh

int gi 2

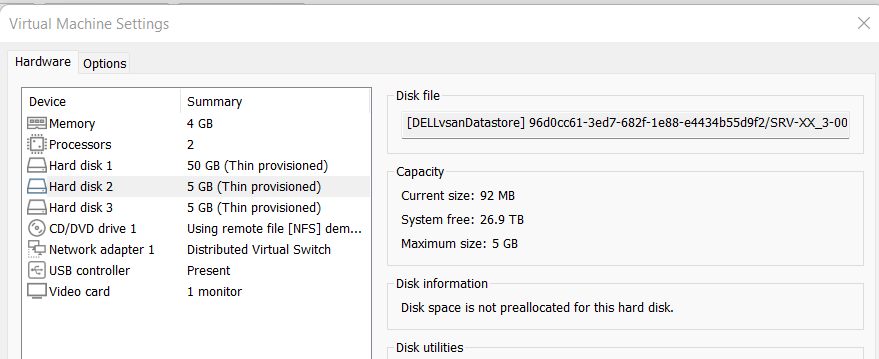
ip address 172.16.100.254 255.255.255.0

no sh

end

wr

**4. Обеспечьте ВМ дополнительными дисками, если таковое необходимо в соответствии с Таблицей 1;**

[](https://user-images.githubusercontent.com/79700810/150127140-0285670d-773e-4d61-8739-29d3455a57b1.png)

**Сетевая связность.**

В рамках данного модуля требуется обеспечить сетевую связность между регионами работы приложения, а также обеспечить выход ВМ в имитируемую сеть “Интернет”

1. Сети, подключенные к ISP, считаются внешними:
   * Запрещено прямое попадание трафика из внутренних сетей во внешние и наоборот;
2. 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.
3. 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.
4. 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;
5. 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;
6. Обеспечьте настройку служб SSH региона Left и Right:
   * 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 управления трафиком RTR-R на порт 2244 должны быть перенаправлены на ВМ Web-R;

**1. Сети, подключенные к ISP, считаются внешними:**

**RTR-L Gitw**

ip route 0.0.0.0 0.0.0.0 4.4.4.1

**RTR-R gitw**

ip route 0.0.0.0 0.0.0.0 5.5.5.1

**2. Платформы контроля трафика, установленные на границах регионов, должны выполнять трансляцию трафика, идущего из соответствующих внутренних сетей во внешние сети стенда и в сеть Интернет.**

**3. Между платформами должен быть установлен защищенный туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов.**

**4. Платформа управления трафиком RTR-L выполняет контроль входящего трафика согласно следующим правилам:**

**RTR-L ACL**

ip access-list extended Lnew

permit tcp any any established

permit udp host 4.4.4.100 eq 53 any

permit udp host 5.5.5.1 eq 123 any

permit tcp any host 4.4.4.100 eq 80

permit tcp any host 4.4.4.100 eq 443

permit tcp any host 4.4.4.100 eq 2222

permit udp host 5.5.5.100 host 4.4.4.100 eq 500

permit esp any any

permit icmp any any

int gi 1

ip access-group Lnew in

**5. Платформа управления трафиком RTR-R выполняет контроль входящего трафика согласно следующим правилам:**

**RTR-R ACL**

ip access-list extended Rnew

permit tcp any any established

permit tcp any host 5.5.5.100 eq 80

permit tcp any host 5.5.5.100 eq 443

permit tcp any host 5.5.5.100 eq 2244

permit udp host 4.4.4.100 host 5.5.5.100 eq 500

permit esp any any

permit icmp any any

int gi 1

ip access-group Rnew in

**6. Обеспечьте настройку служб SSH региона Left:**

**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:
   * 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.
     + Маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера SRV
   * Внешний клиент CLI должен использовать DNS-службу, развернутую на ISP, по умолчанию;
2. 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;
3. 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;
4. 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;
5. Реализуйте файловый SMB-сервер на базе SRV
   * Сервер должен предоставлять доступ для обмена файлами серверам 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”;
6. 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;
7. 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;

**Таблица 2. DNS-записи зон**

| **Zone** | **Type** | **Key** | **Meaning** |
| --- | --- | --- | --- |
| demo.wsr | A | isp | 3.3.3.1 |
|  | A | www | 4.4.4.100 |
|  | A | www | 5.5.5.100 |
|  | CNAME | internet | isp |
|  | NS | int | rtr-l.demo.wsr |
|  | A | rtr-l | 4.4.4.100 |

**1. Выполните настройку первого уровня DNS-системы стенда:**

**RTR-L**

b. Маршрутизатор региона должен транслировать соответствующие порты DNS-службы в порты сервера SRV.

ip nat inside source static tcp 192.168.100.200 53 4.4.4.100 53

!

ip nat inside source static udp 192.168.100.200 53 4.4.4.100 53

**2. Выполните настройку второго уровня DNS-системы стенда;**

**SRV**

| **Zone** | **Type** | **Key** | **Meaning** |
| --- | --- | --- | --- |
| 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 | webapp1 | web-l |
|  | CNAME | webapp2 | web-r |
|  | CNAME | ntp | srv |
|  | CNAME | dns | srv |

**3. Выполните настройку первого уровня системы синхронизации времени:**

**ISP NTP**

**4. Выполните конфигурацию службы второго уровня времени на SRV**

**5. Реализуйте файловый SMB-сервер на базе SRV**

**SRV RAID1**

**SRV SMB**

**6. Сервера WEB-L и WEB-R должны использовать службу, настроенную на SRV, для обмена файлами между собой:**

**WEB-L SMB**

**WEB-R SMB**

**7. Выполните настройку центра сертификации на базе SRV:**

**SRV ADCS**

**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;
   * Выполните установку приложения AppDocker0;
2. Пакеты для установки Docker расположены на дополнительном ISO-образе;
3. Инструкция по работе с приложением расположена на дополнительном ISO-образе;
4. Необходимо реализовать следующую инфраструктуру приложения.
   * Клиентом приложения является CLI (браузер Edge);
   * Хостинг приложения осуществляется на ВМ WEB-L и WEB-R;
   * Доступ к приложению осуществляется по DNS-имени [www.demo.wsr](http://www.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;
5. 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.