**rev. PostRelease**

**Задание ССА межрег Юниоры, Калуга 2025**

итоговый (межрегиональный) этап чемпионатов Всероссийского чемпионатного движения по профессиональному мастерству в 2025 году, компетенция “Сетевое и системное администрирование”, возрастная категория Юниоры 14+

***Авторский состав: Рачеев А.В., Золотарёв А.П.***

***[Примечание автора]***

*Здесь и далее курсивом обозначены примечания авторов, предназначенные, в первую очередь, для экспертов, которые планируют организовывать мероприятия по этому заданию или производным от него а также задействованным в этом технических экспертов.*

* 1. **КОНКУРСНОЕ ЗАДАНИЕ**

Формат участия: индивидуальный

Возрастной ценз: от 14 лет

Общая продолжительность Конкурсного задания: 8 ч.

Количество конкурсных дней: 2 дня.

Вне зависимости от количества модулей, Конкурсное задание должно включать оценку по каждому из разделов требований по компетенции.

Оценка знаний участника должна проводиться через практическое выполнение Конкурсного задания. В дополнение могут учитываться требования работодателей для проверки теоретических знаний/оценки квалификации.

Конкурсное задание состоит из 2 модулей, общее количество баллов конкурсного задания составляет 100.

Оценка каждого дня осуществляется в соответствующий день.

***[Требования к рабочему месту, среде виртуализации и ресурсам]***

*Задание не подразумевает использование множественных физических рабочих мест, а также физических коммутаторов и маршрутизаторов. Рабочее место участника подразумевает только ПК с доступом к интерфейсу среды виртуализации.*

*Для организации лабораторной инфраструктуры подойдет любая среда виртуализации с поддержкой технологий vlan/trunk и возможностью клонирования виртуальных машин или развертывания ВМ из шаблона.*

*Допустимо использовать рабочее место участника как сервер виртуализации при наличии на нем достаточного объема ресурсов, однако такой подход не рекомендован в силу малой надежности и проблем с обслуживанием.*

*Лабораторный стенд для выполнения данного задания при указанных в соответствующем разделе, предустановленных ОС (например развернутых из образа) имеет следующие требования к ресурсам.*

*Минимальные системные требования:*

* *10 гб ОЗУ*
* *4 процессорных ядра*
* *120 гб SSD-пространства (при использовании “тонких” виртуальных дисков)*
* *интернет на скорости не менее 5 мбит/с*
* *Допускается увеличение объема ресурсов в соответствии с возможностями инфраструктуры, в которой проводится чемпионатное мероприятие, с обеспечением равных условий для всех участников*

***[ISP]***

*В сетевой инфраструктуре функционирует недоступная участникам и не указанная явно в задании виртуальная машина ISP, которая имеет следующие роли:*

1. *Представляет функции провайдеров интернета для филиалов и внешних клиентов.*
2. *Является NAT-шлюзом в реальный интернет, что обеспечивает выполнимость задания.*
3. *При необходимости позволяет контролировать и/или ограничивать доступ машин к реальному интернету, однако данная версия задания подразумевает доступ в интернет для его выполнения.*
4. *Является сервером DNS и провайдером DNS для доменов, необходимых для выполнения задания. Провайдер DNS доступен через веб-интерфейс. Может быть реализован как самодельным решением, так и готовым софтом, например SnitchDNS.*
5. *Является сервером времени (chrony).*
6. *При необходимости, на эту машину можно добавлять другие сервисы необходимые для выполнения производных версий от этого задания.*

*При необходимости получить преднастроенную версию ISP или иные комментарии по его функционированию - можете обратиться в чат компетенции, там Вам, скорее всего, помогут.*

**Операционные системы:**

***[Примечание автора]***

*При разработке задания предполагалась возможность реализовывать его на разных операционных системах.*

*Серверные и клиентские устройства без существенных проблем можно заменить на любую другую ОС общего назначения семейства Linux.*

*ОС межсетевых экранов также возможно заменить на другие, однако функционал различного ПО для межсетевого экранирования может иметь существенные отличия, и для некоторых ОС могут потребоваться изменения в задании вплоть до переноса некоторых задач с фаервола на другие сервера и/или исключения из задания протоколов динамической маршрутизации.*

*Обновления ОС до более новых версий в рамках ближайших нескольких лет не должны привести к невыполнимости задания, т.к. все используемые технологии продолжают развиваться/поддерживаться и не предполагают вывода из эксплуатации в ближайшее время.*

*Конкретное графическое окружение (GUI) ОС Linux не принципиально для выполнения задания, однако там, где указано, графическое окружение должно быть. Обратите внимание, что графическое окружение может существенно влиять на потребность ВМ в ресурсах.*

*В виртуальные машины с ОС семейства Linux рекомендуется предустановить следующие пакеты: компоненты управления используемой среды виртуализации (qemu-guest-agent / open-vm-tools / hyperv-daemons / …), dnsutils / bind-utils, tcpdump и иные компоненты, обусловленные особенностями Вашей инфраструктуры.*

*На указанных ОС задание выполнимо на 100%.*

*В данной таблице указаны ОС для модуля Б.*

| **ВМ** | **ОС** | **Ресурсы (примерно)** | **GUI** |
| --- | --- | --- | --- |
| ISP | - | 0.5Gb; 1CPU | - |
| FW-KLG | OPNsense 25.1 | 1Gb; 1CPU | - |
| DC-KLG | Alt Server 10.2 | 2Gb; 2CPU | - |
| PC-KLG | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |
| ARM-KLG | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |
| FW-TUL | OPNsense 25.1 | 1Gb; 1CPU | - |
| SRV-TUL | Alt Server 10.2 | 1Gb; 1CPU | - |
| PC-TUL | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |
| CLIENT-EXT | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |

**Стек технологий, знание которых требуется для выполнения задания и возможных изменений в задании в рамках 30% изменений:**

*Вариативная и расширенная вариативная часть стека не подразумевает использование всех технологий в конкретном чемпионатном мероприятии, однако если вы используете задание как основу для своего образовательного процесса или планируете подготовку для мероприятий межрегионального и федерального уровня, то данные разделы могут быть Вам полезны.*

**Инвариативная часть:**

* Настройка IPv4 адресации
* DHCPv4
* NAT, PAT, Проброс портов
* Статическая маршрутизация
* Туннелирование/VPN (Site-to-Site)
* Пользователи и группы
* Работа с дисками (разметка, монтирование)
* Реализация дискреционной модели прав доступа к файловой системе
* Установка программного обеспечения
* DNS (прямой просмотр)
* Веб-сервер
* NTP/Chrony
* SSH
* Контейнеры Docker
	+ Установка и запуск контейнеров;
	+ Проброс портов;
	+ Связь между контейнерами;
	+ Управление контейнерами.

**Вариативная часть:**

* Loopback-интерфейсы
* Динамическая маршрутизация
* Туннелирование/VPN (Site-to-Client)
* DNS (обратный просмотр)
* Доменные инфраструктуры (FreeIPA)
* Базы данных (Postgresql/Mariadb)
* Центр сертификации, SSL
* Передача файлов по сети (FTP, NFS)
* Централизованная система журналирования (syslog, rsyslog и т.п.)
* Работа с дисками (LVM, RAID, квотирование, шифрование)
* Системы мониторинга ресурсов (Zabbix)
* Отказоустойчивость и/или балансировка нагрузки
* Настройка автоматизированного рабочего места
* Работа с юнитами systemd (управление юнитами, создание простого юнита)
* Работа с системным загрузчиком GRUB

**Расширенная вариативная часть:**

* Авторизация пользователей для получения доступа к ЛВС.
* AAA
* Кластеризованные сетевые и серверные системы
* Резервные провайдеры интернет
* Защищенные сетевые сегменты (специализированные VLAN, отдельные провайдеры с ограниченным доступом, VPN-туннель в закрытый сегмент)
* Автоматизации настройки и развертывания программного обеспечения

**ЗАДАНИЕ**

***[примечание автора]***

*Далее идет та часть, предназначенная для выдачи участникам, однако в ее содержании, в основном в преамбуле, есть определенные моменты, которые могут зависеть от преднастроя и реализации машин в конкретной инфраструктуре виртуализации. Сразу отмечу, что преамбула является неотъемлемой частью задания и содержит моменты, непосредственно влияющие на проверку задания и его выполнимость.*

**Преамбула: Техническое описание лабораторной инфраструктуры и общие требования к реализации.**

В случае, если в тексте задания не указано иное, все учетные записи должны иметь пароль P@ssw0rd

Если для выполнения определенного действия вам требуется указать имя пользователя, которое не указано в задании и система не имеет пользователя по умолчанию, или система имеет повышенные требования к паролю и P@ssw0rd использовать невозможно, укажите необходимые данные для входа около соответствующего пункта задания.

Все проверки работы клиентских технологий (сайтов, клиентских VPN подключений и т.п.), если в задании не указано иного, будут выполняться из под пользователя user соответствующих клиентских машин.

При выполнении настоящего задания всегда нужно руководствоваться правилом наименьших привилегий, в особенности при настройке внешних интерфейсов пограничных шлюзов.

Консольный доступ к виртуальной машине провайдера ISP для участника не предполагается. Следите за тем, чтобы виртуальная машина ISP была включена в течение всего времени выполнения задания.

Обратите внимание, что провайдерская адресация 100.64.0.0/10 относится к серому (частотному) диапазону адресов, что может потребовать дополнительных настроек на граничных сетевых устройствах межсетевого экранирования. Однако, в терминологии задания, сеть 100.64.0.0/10 относится к внешним (“белым”) сетям, наряду с “белыми” сетями из реального интернета.

Знак \* (звёздочка, астериск) в задании является подстановочным знаком заменяет произвольную последовательность символов от начала строки или пробельного символа до другого пробельного символа или конца строки. К примеру, при указании на устройство FW\* имеются ввиду все устройства в задании, название которых начинается с FW, например FW1, FW-MSK, FWabc и т.п., а при указании сетей \*MSK имеются в виду все сети в задании, название которых заканчивается на MSK, например LAN1-MSK, SRV-MSK, dmzMSK и т.п.

Операционная система OPNsense в интерфейсе при названии некоторых объектов не допускает использование символа “-”, в таком случае его можно заменять на знак “\_”, но только там, где указать “-” невозможно.

В инфраструктуре функционирует DNS-провайдер (расположенный на ВМ ISP), его интерфейс доступен по адресу https://ns.ext/. Учетная запись: jun

При настройке FreeIPA FQDN в обязательном порядке требуется указывать в нижнем регистре.

vSW на схеме не является отдельным устройством или виртуальной машиной. Данный функционал обеспечивается сетевой подсистемой используемой среды виртуализации.

Согласно политике Организации, все службы и технологии, необходимые для выполнения задания, должны запускаться автоматически и функционировать в соответствии с заданием при запуске операционных систем, если в задании явно не указано иного.

**Предыстория:**

Доброго времени суток, коллеги! Сообщаем Вам, что по результатам успешного запуска нашей инфраструктуры, руководство “Destination Reachable” решило заняться аутсорсингом IT-услуг и отправляет Вас налаживать работу IT-инфраструктуры одному из наших постоянных логистических клиентов НПО “КаТуль”. Как можно догадаться из названия, организация исторически работает в двух городах - Калуга (внутреннее наименование KLG) и Тула (TUL), где и расположены ее основные филиалы. При решении поставленной перед Вами задачи, естественно, стоит использовать Ваш опыт реализации предыдущих проектов, однако стоит также уделить внимание потребностям НПО “КаТуль”, которые подробно описаны в представленном Техническом задании. У Вас, вероятно, возник вопрос, а как же НПО “КаТуль” работало до этого? Ваши старшие коллеги уже произвели аудит инфраструктуры организации, и пришли к выводу, что лучше начать все с чистого листа, как Вы умеете. Все оборудование только что распаковано, операционные системы предустановлены, в соответствии с техническим заданием. Для доступа к сети Интернет заключены договора с провайдерами интернета для обоих филиалов с предоставлением “белых” ip-адресов \*(подробнее в разделе “Техническое описание лабораторной инфраструктуры и общие требования к реализации”).

Ваше время крайне ограничено, поэтому настоятельно рекомендуем вам хорошо подготовиться и спланировать свои задачи. И не забывайте девиз нашей организации:

“ Destination Reachable – Доставку обеспечат Профессионалы! ”

**Схема IP-адресации и схема подключений.**

Схема адресации локальных сетей в задании разрабатывается участниками, однако требуется придерживаться следующих условий:

1. Для локальных сетей используется только приватная адресация из стандартных приватных диапазонов.
2. Все сети, соединяющие маршрутизаторы между собой, включая сети туннелей site-to-site должны иметь маску сети /30 или /29 (там где необходимо).
3. Все остальные локальные сети, включая клиентские VPN-сети, должны иметь адресацию с маской /24. При этом шлюзом по умолчанию в таких сетях должен быть первый или последний адрес в сети, после принятия решения по адресации шлюзов по умолчанию, используйте аналогичные (только первые или только последние) адреса для шлюзов во всей инфраструктуре.
4. При выполнении задания впишите адреса выданные устройствам в столбец “Адрес/Маска” рядом со словом “STATIC”

| Сеть  | Устройство  | Адрес/Маска  | Шлюз |
| --- | --- | --- | --- |
| INTERNET | FW-KLG | 100.67.32.80/26 | ISP – первый адрес в сети |
|  | FW-TUL | 100.127.90.57/27 | ISP – первый адрес в сети |
|   | Client-EXT | 100.108.128.45/28 | ISP – первый адрес в сети |
|  | DNS-сервер  | 100.100.100.100 |  |
|  | NTP-сервер | 100.101.102.103 |  |
| SRV-KLG (vl2000) | FW-KLG | STATIC |   |
|   | DC-KLG | STATIC | FW-KLG |
| LAN-KLG (vl2010) | FW-KLG | STATIC |   |
|   | PC-KLG | DHCP | FW-KLG |
| SEC-KLG (vl2020) | FW-KLG | STATIC |   |
|   | ARM-KLG | DHCP | FW-KLG |
| SRV-TUL | FW-TUL | STATIC |   |
|   | SRV-TUL | STATIC | FW-TUL |
| LAN-TUL | FW-TUL | STATIC |   |
|   | PC-TUL | DHCP | FW-TUL |

**Схема сети приведена в отдельном файле!**

**Модуль Б. (Настройка технических и программных средств информационно-коммуникационных систем) (инвариант)**

Время на выполнение модуля: 4 часа

1. Настройте IPv4-адреса согласно схеме адресации:
	1. Настройте адреса шлюза по умолчанию, где это требуется;
	2. На FW\* настройте описания интерфейсов, согласно схеме сети
2. Настройте имена всех устройств согласно топологии.
3. Все устройства должны иметь доступ в интернет, если в задании явно не указано иного.
4. Подготовьте PC-KLG к работе пользователя:
	1. Установите офисный пакет (МойОфис / Р7 Офис) и создайте на него ярлык на рабочем столе.
	2. Установите Яндекс-браузер и создайте на него ярлык на рабочем столе.
5. В филиале KLG разверните домен klg.jun.profi на базе FreeIPA с контроллером домена на DC-KLG. При развертывании учтите, что это устройство будет выполнять функции DNS и DHCP сервера в филиале KLG.
	1. Создайте пользователей и группы в домене:
		1. группу jun-users, добавьте в нее пользователей: max и andrey
		2. группу jun-sec, добавьте в нее пользователей: max, andrey и admin
		3. группу jun-net, добавьте в нее пользователей: max и admin
	2. Введите компьютер PC-KLG в домен, обеспечьте возможность входа под всеми доменными учетными записями на данный ПК.
	3. Создайте правило, разрешающее доменному пользователю admin использовать sudo на всех компьютерах в домене без ограничения.
	4. Обеспечьте доменному пользователю admin, после успешной авторизации на компьютере PC-KLG, возможность заходить в интерфейс FreeIPA без использования пароля. Для аутентификации и авторизации используйте Kerberos.
6. Настройте инфраструктуру разрешения имен в филиалах следующим образом:
	1. DNS-сервер в филиале KLG располагается на DC-KLG и интегрирован с доменом FreeIPA.
	2. DNS-сервер в филиале TUL располагается на FW-TUL.
	3. Все устройства в локальных сетях должны обращаться с DNS запросами к DNS-серверам соответствующих филиалов. Исключение допустимо только для гостевых и защищенных сетей, при наличии технической необходимости.
	4. Указанные DNS-сервера должны выполнять пересылку “внешних” DNS запросов от локальных клиентов на DNS сервер провайдера, указанный в Схеме IP-адресации.
	5. CLIENT-EXT должен обращаться с DNS запросами на сервер провайдера, указанный в Схеме IP-адресации.
	6. Настройте для всех устройств филиалов доменные имена в зонах klg.jun.profi и tul.jun.profi в соответствии с их расположением.
	7. Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией в доменах соответствующих филиалов. К примеру srv-tul.tul.jun.profi или pc-klg.klg.jun.profi
	8. В рамках каждого филиала короткие имена должны автоматически дополняться доменным именем соответствующего филиала.
	9. Создайте обратную зону(ы) DNS в доменном DNS-сервере DC-KLG, чтобы все ip-адреса в филиале KLG расшифровывались в соответствующие им DNS-имена.
7. Настройте DHCP-сервера:
	1. на FW-TUL для клиентов сети LAN-TUL
	2. на DC-KLG для клиентов сетей LAN-KLG и SEC-KLG
	3. DHCP-сервера должны передавать клиентам все необходимые опции для работы в сети и взаимодействия с другими устройствами и сетями по IP и DNS именам.
	4. Выдаваемые по DHCP адреса не должны пересекаться с зарезервированными, служебными и прочими “занятыми” адресами, необходимыми для выполнения задания.
	5. DHCP-сервера должны работать на основе ПО “Kea DHCP server”
8. Настройте синхронизацию времени:
	1. Сервер точного времени в филиале KLG располагается на DC-KLG.
	2. Сервер точного времени в филиале TUL располагается на FW-TUL.
	3. Все устройства в локальных сетях должны использовать указанные сервера.
	4. Все сервера и клиенты, которые поддерживают Chrony должны использовать данную реализацию протокола. На устройствах, которые не поддерживают Chrony допускается использовать стандартный NTP.
	5. Указанные сервера времени, а также сервера и клиенты во внешних сетях должны синхронизировать свое время с NTP сервером, указанным в схеме IP-адресации.
	6. Настройте часовой пояс на всех устройствах в соответствии с их географическим расположением. Для машины CLIENT-EXT используйте часовой пояс Норильска.
	7. ⚠ Устройства в сетях повышенной безопасности должны синхронизироваться после авторизации в сети.
9. Настройте защищенный VPN-туннель FW-KLG<=>FW-TUL со следующими параметрами:
	1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.
	2. Используйте современные надежные протоколы шифрования AES, SHA-2 или ChaCha20.
	3. Не допускается использование протоколов шифрования и аутентификации с длиной ключа/хеша менее 256 бит.
	4. Настройте маршрутизацию, NAT и межсетевой экран таким образом, чтобы трафик для другого офиса не подвергался трансляции адресов и не блокировался. На текущем этапе все устройства в локальных сетях филиалов должны иметь возможность взаимодействовать между собой без ограничений, кроме сегментов и устройств, для которых в задании явно указано иное.
10. Настройте OSPFv2 по защищенному туннелю между FW-KLG и FW-TUL так, чтобы FW\* имели полную информацию о маршрутах во все локальные сети всех филиалов.
	1. FW\* должны быть защищены от вброса маршрутов с любых интерфейсов, кроме тех, на которых обмен маршрутами явно требуется.
	2. ⚠ В таблицах маршрутизации могут содержаться дополнительные резервные маршруты, но именно OSPF-маршруты должны быть “выбраны” системой маршрутизации.
11. Обеспечьте авторизацию пользователей в защищенной сети SEC-KLG через captive portal.
	1. Для авторизации используйте локального пользователя FW-KLG с именем sec.
	2. Доступ к сетевым ресурсам должен появляться только после авторизации.
	3. Пользователи данной сети должны иметь доступ только к локальным ресурсам, и не иметь доступа в сеть интернет, кроме официального сайта с документацией ОС семейства Альт (docs.altlinux.org)
	4. Для удобства пользователя создайте на рабочем столе ярлык на открытие страницы captive portal.
12. Для хранения важных данных в сервер SRV-TUL установлено два дополнительных диска. Объедините их в зеркальный отказоустойчивый массив используя встроенные возможности файловой системы ZFS и подключите раздел по пути /opt/data/ для дальнейшего использования.
13. Настройте права доступа для каталога /opt/data на SRV-TUL следующим образом:
	1. пользователь webdev (его требуется создать) должен иметь полные права на чтение и запись в указанный каталог и все его подкаталоги;
	2. обычные пользователи не должны иметь доступа в данный каталог;
	3. серверным службам, использующим данный каталог, должны быть предоставлены необходимые права для их работы;
	4. ⚠ При назначении прав учитывайте, что для папки задача обеспечить “чтение” подразумевает также возможность перечисления содержимого папки и возможность зайти в эту директорию с помощью команды cd.
14. Обеспечьте возможность подключения к FW-KLG под доменными пользователями:
	1. посредством веб-интерфейса с полным доступом к настройкам;
	2. посредством протокола SSH с доступом к выполнению команд через sudo;
	3. доступ должен быть только у пользователей доменной группы jun-net.
15. Настроить удаленный доступ к SRV-TUL по SSH
	1. На сервере SRV-TUL сервис SSH должен функционировать на порте 2502.
	2. Устройство PC-TUL при входе под пользователем user должно иметь доступ к SRV-TUL под пользователем user c использованием SSH ключей, без необходимости ввода пароля.
	3. Пользователь user на SRV-TUL должен иметь возможность выполнять команды через sudo без ввода пароля.
	4. Пользователю user при использовании sudo должна быть доступна только команда su.
	5. Подключение к SRV-TUL с PC-TUL из под пользователя user должно осуществляться командой “ssh SRV” без дополнительных параметров.
16. На сервере SRV-TUL разверните сервер мониторинга и настройте его следующим образом:
	1. При развертывании не используйте технологии контейнеризации
	2. Сервер: Zabbix LTS
	3. База данных: PostgreSQL
	4. Веб-интерфейс: на основе Nginx
	5. Основной адрес: mon.jun.profi
	6. Порт веб-интерфейса: 80(HTTP)\*
	7. Подключите к серверу мониторинга все устройства организации
	8. Обеспечьте сбор показателей со всех подключенных устройств с помощью стандартных шаблонов используемых ОС
	9. Обеспечьте хранение файлов базы данных внутри отказоустойчивого хранилища /opt/data/
	10. ⚠ Подключение устройств в сетях повышенной защищенности и внешних сетях не требуется

**Модуль Г: Обеспечение отказоустойчивости (2-й день, 4 часа)**

Для бесперебойного функционирования корпоративной инфраструктуры, а также качественного предоставления сервиса внешним клиентам, руководство приняло решение организовать отказоустойчивый кластер высокой доступности. Кроме того, штатный специалист по ИБ требует, чтобы все рабочие скрипты и документация были размещены на self-hosted системе контроля версий, которую Вам и требуется развернуть в отказоустойчивом кластере.

Оборудование уже подключено, операционные системы установлены.

⚠ Компьютер CLIENT-EXT не подразумевает внесения дополнительных настроек, помимо IP-адресации, DNS-параметров и обеспечения доверия сертификатам, и используется только для проверки доступности сервисов Компании из внешних сетей.

**Операционные системы:**

| **ВМ** | **ОС** | **Ресурсы (примерно)** | **GUI** |
| --- | --- | --- | --- |
| ISP | - | 0.5Gb; 1CPU | - |
| CL-GW1 | OPNsense 25.1 | 1Gb; 1CPU | - |
| CL-GW2 | OPNsense 25.1 | 1Gb; 1CPU | - |
| CL-FRONT1 | Alt Server 10.4 | 1Gb; 1CPU | - |
| CL-FRONT2 | Alt Server 10.4 | 1Gb; 1CPU | - |
| CL-BACK1 | Alt Server 10.4 | 1Gb; 1CPU | - |
| CL-BACK2 | Alt Server 10.4 | 1Gb; 1CPU | - |
| MGMT-PC | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |
| CLIENT-EXT | Alt Workstation 10.4 | 1Gb; 1CPU | MATE |

**Схема IP-адресации и схема подключений.**

Схема адресации локальных сетей в задании разрабатывается участниками, однако требуется придерживаться следующих условий:

1. Для локальных сетей используется только приватная адресация из стандартных приватных диапазонов.
2. Все сети, соединяющие маршрутизаторы между собой, включая сети туннелей site-to-site должны иметь маску сети /30 или /29 (там где необходимо).
3. Все остальные локальные сети, включая клиентские VPN-сети, должны иметь адресацию с маской /24. При этом шлюзом по умолчанию в таких сетях должен быть первый или последний адрес в сети, после принятия решения по адресации шлюзов по умолчанию, используйте аналогичные (только первые или только последние) адреса для шлюзов во всей инфраструктуре.
4. При выполнении задания впишите адреса выданные устройствам в столбец “Адрес/Маска” рядом со словом “STATIC”

| Сеть  | Устройство  | Адрес/Маска  | Шлюз |
| --- | --- | --- | --- |
| INTERNET | Client-EXT | 100.108.128.45/28 | ISP – первый адрес в сети |
|  | DNS-сервер  | 100.100.100.100 |  |
|  | NTP-сервер | 100.101.102.103 |  |
| CL-WAN | <СЕТЬ> | 100.99.90.96/28 |  |
|  | ISP | первый адрес в сети |  |
|  | CL-GW1 | STATIC | ISP |
|  | CL-GW2 | STATIC | ISP |
|   | CL-GW(VIP) | STATIC | ISP |
| CL-LAN | CL-CL-GW1 | STATIC |   |
|   | CL-GW2 | STATIC |  |
|  | CL-GW(VIP) | STATIC |  |
|  | CL-FRONT1 | STATIC | CL-GW |
|  | CL-FRONT2 | STATIC | CL-GW |
|  | CL-FRONT(VIP) | STATIC | CL-GW |
|  | CL-BACK1 | STATIC | CL-GW |
|  | CL-BACK2 | STATIC | CL-GW |
|  | MGMT-PC | DHCP | CL-GW |
| SYNC | CL-GW1 | STATIC |  |
|  | CL-GW2 | STATIC |  |

**Схема сети приведена в отдельном файле!**

1. Настройка DNS в соответствии с таблицей
	1. Настройте DNS-сервер на межсетевых экранах CL-GW1 и CL-GW2
	2. Для работоспособности портала из внешнего мира, внесите необходимые данные через веб-интерфейс DNS-провайдера.

| Устройства | тип | имя | адрес |
| --- | --- | --- | --- |
| CL-GW(CL-GW1 и CL-GW2) | А | git.jun.profi | CL-FRONT(VIP) |
| DNS-провайдер ns.ext | A | git.jun.profi | CL-GW (WAN VIP) |

1. Настройка отказоустойчивого кластера маршрутизации
	1. Обеспечьте наличие доступа в интернет со всех устройств в сети CL-LAN
	2. Настройте CARP на CL-GW1 как основной сервер и GW2 как подчинённый сервер
	3. Назначьте номер группы 10 для внешнего интерфейса и номер группы 20 для внутреннего
	4. Проверьте, что при отключении CL-GW1 доступ в интернет (по IP и DNS) сохраняется через CL-GW2
	5. Убедитесь, что внешний и внутренний адреса переключаются на CL-GW2 при сбое
	6. Проверьте, что при включении CL-GW1 он восстанавливает свои адреса и повторно становится основным
	7. Обеспечьте автоматизированную репликацию конфигурации и состояний CL-GW1 на CL-GW2 посредством pfSync и XMLRPC-sync
	8. Настройте дополнительные параметры для обеспечения корректной работы кластера маршрутизации
2. Настройка кластера DHCP
	1. Настройте DHCP-сервер на CL-GW1 как основной
	2. Настройте DHCP-сервер на CL-GW2 как запасной
	3. Настройте механизм DHCP failover между CL-GW1 и CL-GW2
	4. Обеспечьте синхронизацию данных между основным и запасным серверами
	5. Настройте CL-GW2 для выдачи IP-адресов в случае сбоя CL-GW1
	6. Проверьте работоспособность кластера при отключении CL-GW1
	7. Убедитесь в корректной работе DHCP на обоих шлюзах после перезагрузки
	8. В качестве DHCP-сервера используйте программную реализацию Kea
3. Перенаправление внешнего порта на внешних интерфейсах CL-GW
	1. Настройте перенаправление трафика из внешнего мира при обращении на стандартные порты протоколов HTTP и HTTPS на общий ip-адрес CL-FRONT\*
	2. Убедитесь, что все запросы корректно обрабатываются на целевом адресе
4. Установка и настройка отказоустойчивого клиентского приложения на серверах CL-BACK\*
	1. ⚠ Допускается разворачивать сервер приложения как с использованием контейнеров, так и без них.
	2. На серверах CL-BACK\* разверните сервер Gitea. Необходимые файлы содержимого приложения разместите в директории /opt/app/
	3. файлы управления системой контейнеризации (при наличии) а также иные файлы, необходимые для запуска и управления приложением разместите в директории /opt/ (при необходимости, допустимо создавать вложенные директории)
	4. Используйте версию приложения не менее 1.21.0
	5. Порт приложения: 3000
	6. ⚠ настройка порта SSH не требуется
	7. База данных - PostgreSQL > 15.0 / MySQL > 8.0 / MariaDB > 11.4
	8. Обеспечьте работу приложения в отказоустойчивом режиме, для этого:
		1. Обеспечьте проверку доступности приложения на CL-BACK\* со стороны CL-FRONT\*
		2. Обеспечьте репликацию базы данных между CL-BACK\*
		3. Обеспечьте репликацию директории /opt/app между CL-BACK\*, для этого реализуйте сценарий репликации директории /opt/app на сервере CL-BACK1
		4. При вызове сценария CL-BACK1 синхронизирует содержимое директории /opt/app с CL-BACK2
		5. Назовите сценарий sync-web, расположите его в директории /opt/ и укажите пользователя, из под которого работает скрипт: \_\_\_\_\_\_\_\_\_\_\_
		6. Реализуйте планировщик сценария sync-web с помощью systemd таймера с именем sync-web, синхронизация происходит автоматически каждые 2 минуты
		7. При необходимости выполните дополнительные действия для обеспечения отказоустойчивости приложения.
		8. Проверьте, что при отключении любого из хостов CL-BACK\* работоспособность приложения сохраняется
	9. Обеспечьте автоматический запуск приложения при старте сервера.
	10. Обеспечьте работоспособность сервера приложения и возможность входа в панель администрирования под пользователем gitadm
	11. Создайте в системе под пользователем gitadm репозиторий scripts и загрузите в него скрипт sync-web
5. Настройка веб служб на серверах CL-FRONT\*
	1. Настройте программное обеспечение nginx на CL-FRONT\* как обратный прокси для приложения на CL-BACK\*
	2. Сайт должен функционировать по протоколу HTTPS. При обращении по протоколу HTTP должен происходить автоматический редирект на HTTPS.
	3. Требуется обеспечить доверие сертификату сайта, используя корректную цепочку доверия (центр сертификации + сертификат ресурса).
		1. Для корневого сертификата используйте CN “Jun Profi CA”
	4. Сайт должен открываться с MGMT-PC и CLIENT-EXT без ошибок и предупреждений.
	5. При обращении по доменному имени git.jun.profi из внешних или локальных сетей происходит обратное проксирование на CL-BACK\* в порт приложения
	6. При обращении по ip загружается локальная страница-заглушка с идентификацией сервера, на странице размером <h3> написано имя хоста, отдавшего страницу
6. Настройка отказоустойчивости веб служб
	1. Создайте группу серверов keepalived со следующими параметрами:
	2. Иерархия группы - CL-FRONT1 -> CL-FRONT2
	3. Идентификатор группы – 173
	4. Приоритет - 220 и 200 соответственно
	5. Виртуальный адрес группы - CL-FRONT(VIP)
	6. Интервал рассылки сообщений - 3 секунды
	7. Время, после которого сервер с более высоким приоритетом заберет обратно себе роль мастера – 20 секунд
	8. Настройте keepalived таким образом, чтобы при отключении службы nginx на CL-FRONT1 общий ip адрес передавался CL-FRONT2, при включении общий ip адрес снова возвращался CL-FRONT1
7. Настройка доступа к приложению на серверах CL-BACK\*
	1. Настройте межсетевой экран для ограничения доступа к порту приложения только для серверов CL-FRONT1 и CL-FRONT2
	2. Убедитесь, что другие источники не могут подключаться к указанным портам