ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ДОПОЛНИТЕЛЬНОГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«ИНСТИТУТ РАЗВИТИЯ ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ»
(ФГБОУ ДПО ИРПО)

УТВЕРЖДЕНА
приказом ФГБОУ ДПО ИРПО
от 27.08.2026 № 01-09-285/2026

СПЕЦИФИКАЦИЯ КОНТРОЛЬНЫХ ИЗМЕРИТЕЛЬНЫХ МАТЕРИАЛОВ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

Том 1
(инвариантная часть)

Код и наименование профессии (специальности) среднего профессионального образования	09.02.06 Сетевое и системное администрирование
Наименование квалификации (наименование направленности)	Системный администратор (Эксплуатация операционных систем)

Федеральный государственный образовательный стандарт среднего профессионального образования по профессии (специальности) среднего профессионального образования (ФГОС СПО):	ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование, утвержденный приказом Минпросвещения России от 10.07.2023 № 519
Виды аттестации:	Государственная итоговая аттестация
	Промежуточная аттестация
Уровень демонстрационного экзамена:	Базовый
	Профильный (инвариантная часть)
Шифр КИМ:	КИМ 09.02.06-4-2027

Образец задания для ГИА ДЭ БУ

Задание 1. Разработка и настройка инфраструктуры информационно-коммуникационной системы

Необходимо разработать и настроить инфраструктуру информационно-коммуникационной системы согласно предложенной топологии (см. **Рисунок 1**).

Задание включает базовую настройку устройств:

- присвоение имен устройствам;
- расчет IP-адресации;
- настройку коммутации и маршрутизации;

В ходе проектирования и настройки сетевой инфраструктуры следует вести отчет о своих действиях, включая таблицы и схемы, предусмотренные в задании.

По каждому пункту задания, требующего отчёт, составить текстовый документ, название которого должно содержать индекс пункта и краткое описание. Текстовый документ должен содержать текстовую информацию и может включать снимки экрана, кадрированные таким образом, чтобы относящаяся к выполнению задания информация на снимках была читаемой.

Итоговый отчет по окончании работы следует сохранить на диске рабочего места и задать имя файла - ФамилияУчастникаЗадание1 без учёта расширения.

Рисунок 1. Топология сети

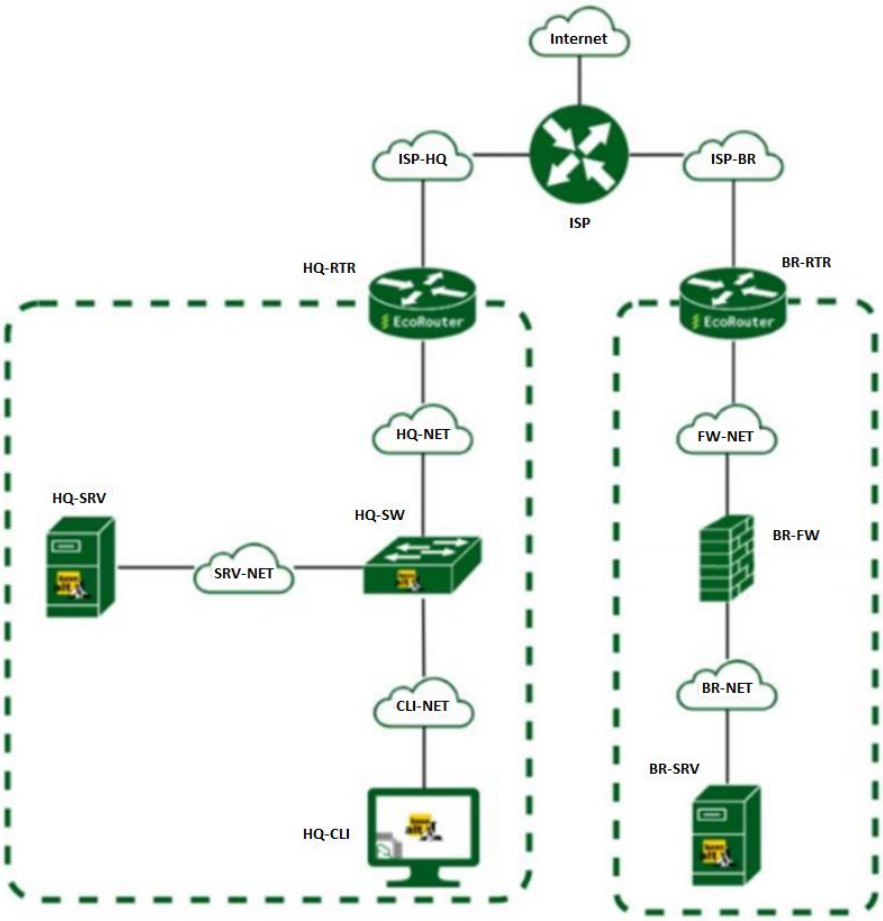


Таблица 1

Имя виртуальной машины	**Оперативная память**	**Центральный процессор, ядер**	**Накопитель**	**Операционная система**
ISP	1 Гб	1 ядро	5 Гб	Серверная операционная система на базе Linux
BR-FW	4 Гб в случае использования Ideco ngfw 1 Гб в случае использования дистрибутива Linux	4 ядра в случае использования Ideco ngfw 1 ядро в случае использования дистрибутива Linux	15 Гб в случае использования Ideco ngfw 5 Гб в случае использования дистрибутива Linux	Ideco ngfw, Vipnet xFirewall, Серверная операционная система на базе Linux
HQ-RTR	4 Гб в случае использования EcoRouter 1 Гб в случае использования	4 ядра в случае использования EcoRouter 1 ядро в случае использования	10 Гб	ОС EcoRouter, в случае невозможности использования EcoRouter

	дистрибутива Linux	дистрибутива Linux		Серверная операционная система на базе Linux
BR-RTR	4 Гб в случае использования EcoRouter 1 Гб в случае использования дистрибутива Linux	4 ядра в случае использования EcoRouter 1 ядро в случае использования дистрибутива Linux	10 Гб	ОС EcoRouter, в случае невозможности использования EcoRouter дистрибутив Серверная операционная система на базе Linux
HQ-SRV	2 Гб	1 ядро	10 Гб	Серверная операционная система на базе Linux
BR-SRV	2 Гб	1 ядро	10 Гб	Серверная операционная система на базе Linux
HQ-CLI	2 Гб	2 ядра	15 Гб	Операционная система на базе Linux с установленной графической оболочкой
Итого	19 (10 в случае использования ОС на базе Linux)	17 (8 в случае использования ОС на базе Linux)	75 Гб	-

Задание 1

1. Произведите базовую настройку устройств:

• настройте имена устройств согласно топологии. Используйте полное доменное имя, используйте **таблицу 3** поле **Запись**

• на всех устройствах необходимо сконфигурировать IPv4:

• ip-адрес должен быть из приватного диапазона;

• локальная сеть в сторону HQ-SRV(VLAN 100) необходимо выделить сеть размером не более 32;

• локальная сеть в сторону HQ-CLI(VLAN 200) необходимо выделить сеть

размером не более 16 адресов;

• локальная сеть для управления (VLAN 999) необходимо выделить сеть размером не более 8;

• между BR-FW и BR-RTR настройте сеть с минимально возможной маской подсети;

• в локальной сети в сторону BR-SRV необходимо выделить сеть из сети размером не более 16 адресов:

• сведения об адресах занесите в **таблицу 2**, в качестве примера используйте Приложение 3;

---

2. Настройте доступ к сети Интернет, на маршрутизаторе ISP:

• настройте адресацию на интерфейсах:

• интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP;

• настройте маршрут по умолчанию, dns сервер, если это необходимо;

• настройте интерфейс, в сторону HQ-RTR, интерфейс подключен к сети 172.16.1.0/28;

• настройте интерфейс, в сторону BR-RTR, интерфейс подключен к сети 172.16.2.0/28;

• на ISP настройте динамическую сетевую трансляцию портов для доступа к сети Интернет HQ-RTR и BR-RTR;

---

3. Создайте локальные учетные записи на серверах HQ-SRV и BR-SRV:

• создайте пользователя sshuser:

• пароль P@ssw0rd;

• идентификатор пользователя 2027;

• пользователь sshuser должен иметь возможность запускать sudo без ввода пароля;

• создайте пользователя net_admin на маршрутизаторах HQ-RTR и BR-RTR:

• пароль P@ssw0rd;

• при настройке ОС на базе Linux, запускать sudo без ввода пароля;

• при настройке ОС отличных от Linux пользователь должен обладать максимальными привилегиями;

---

4. Настройте коммутацию в сегменте HQ следующим образом:

• трафик HQ-SRV должен принадлежать VLAN 100;

• трафик HQ-CLI должен принадлежать VLAN 200;

• предусмотреть возможность передачи трафика управления в VLAN 999;

• реализовать на HQ-RTR маршрутизацию трафика всех указанных VLAN с использованием одного сетевого адаптера ВМ/физического порта;

• сведения о настройке коммутации внесите в отчёт;

---

5. Настройте безопасный удаленный доступ на серверах HQ-SRV и BR-SRV:

• для подключения используйте порт 2027:

• разрешите подключения исключительно пользователю sshuser;

• ограничьте количество попыток входа до двух;

• настройте баннер «Authorized access only»;

---

6. Между офисами HQ и BR, на маршрутизаторах HQ-RTR и BR-RTR необходимо сконфигурировать ip туннель:

• используйте протокол GRE;

• в качестве сетевого диапазона используйте сеть 10.10.10.0/24;

• для туннеля используйте минимально возможную маску подсети;

• сведения о туннеле занесите в отчёт;

---

7. Обеспечьте динамическую маршрутизацию на маршрутизаторах HQ-RTR и BR-RTR и межсетевом экране BR-FW:

• сети одного офиса должны быть доступны из другого офиса и наоборот:

• разрешите выбранный протокол только на интерфейсах туннеля на HQ-RTR и BR-RTR, на BR-FW используйте в OSPF только интерфейс в строну BR-RTR;

• используйте OSPF для маршрутизации;

• используйте аутентификацию в OSPF на маршрутизаторах HQ-RTR и BR-RTR;

• в качестве пароля используйте P@ssw0rd;

• пароль должен передаваться с использованием хешированного ключа MD5;

• сведения о настройке и защите протокола занесите в отчёт;

---

8. Настройка динамической трансляции адресов на маршрутизаторах HQ-RTR и BR-RTR:

• настройте динамическую трансляцию адресов для обоих офисов в сторону ISP, все устройства в офисах должны иметь доступ к сети Интернет

---

9. Настройте протокол динамической конфигурации хостов для сети в сторону HQ-CLI:

• настройте нужную подсеть;

• в качестве сервера DHCP выступает маршрутизатор HQ-RTR;

• клиентом является машина HQ-CLI;

• исключите из выдачи адрес маршрутизатора;

• адрес шлюза по умолчанию — адрес маршрутизатора HQ-RTR;

• адрес DNS-сервера для машины HQ-CLI — адрес сервера HQ-SRV;

• DNS-суффикс — au-team.irpo;

• сведения о настройке протокола занесите в отчёт;

---

10. Настройте инфраструктуру разрешения доменных имён для офисов HQ и BR:

• основной DNS-сервер реализован на HQ-SRV;

• сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с **таблицей 3;**

• в качестве DNS сервера пересылки используйте любой общедоступный DNS сервер (77.88.8.7, 77.88.8.3 или другие);

---

11. Настройте часовой пояс на всех устройствах (за исключением виртуального коммутатора, в случае его использования) согласно месту проведения экзамена

• на всех устройствах (за исключением HQ-SW) выполните настройку часового пояса согласно месту проведения экзамена;

Таблица 2

Имя устройства	IP-адрес	Шлюз по умолчанию
HQ-RTR		
BR-RTR		
HQ-SRV		
HQ-CLI		
BR-SRV		
BR-FW		

Таблица 3

Устройство	Запись	Тип
HQ-RTR	hq-rtr.au-team.irpo	A
BR-RTR	br-rtr.au-team.irpo	A
BR-FW	br-fw.au-team.irpo	A
HQ-SRV	hq-srv.au-team.irpo	A,PTR
HQ-CLI	hq-cli.au-team.irpo	A
BR-SRV	br-srv.au-team.irpo	A,PTR

ISP (интерфейс направленный в сторону HQ-RTR)	docker.au-team.irpo	A
ISP (интерфейс направленный в сторону BR-RTR)	web.au-team.irpo	A

Необходимые приложения:

Прил_1_ОЗ_КИМ_09.02.06-4-2027.docx

Прил_2_ОЗ_КИМ_09.02.06-4-2027.docx

Прил_3_ОЗ_КИМ_09.02.06-4-2027.docx

Прил_4_ОЗ_КИМ_09.02.06-4-2027.docx

Инструкции для администратора центра проведения экзамена: Инструкция по настройке оборудования для проведения ДЭ будет представлена отдельным файлом в варианте.

Задание 2. Разработка и настройка инфраструктуры информационно-коммуникационной системы

Необходимо разработать и настроить инфраструктуру информационно-коммуникационной системы согласно предложенной топологии (см. **Рисунок 2**).

Для задания 2 используется отдельный стенд. Инструкция по настройке стенда для технических администраторов площадки в отдельном файле.

В стенде преднастроены:

• контроллер домена samba-dc на сервере BR-SRV. Контроллер домена установлен и функционирует, учётных записей компьютеров, подразделений, пользователей нет;

• IP-адреса, маски подсетей и шлюзы по умолчанию;

• сетевая трансляция адресов;

• IP туннель;

• динамическая маршрутизация;

• созданы пользователи sshuser на серверах и net_admin на маршрутизаторах, им предоставлены административные привилегии;

• порты ssh на серверах;

• DHCP-сервер;

• DNS-сервер;

• сервер HQ-SRV имеет два дополнительных накопителя размером 1ГБ;

По каждому пункту задания, требующего отчёт, составить текстовый документ, название которого должно содержать индекс пункта и краткое описание. Текстовый документ должен содержать текстовую информацию и может включать снимки экрана, кадрированные таким образом, чтобы относящаяся к выполнению задания информация на снимках была читаемой.

Итоговый отчет по окончании работы следует сохранить на диске рабочего места и задать имя файла - **ФамилияУчастникаЗадание2** без учёта расширения.

Рисунок 2. Топология сети

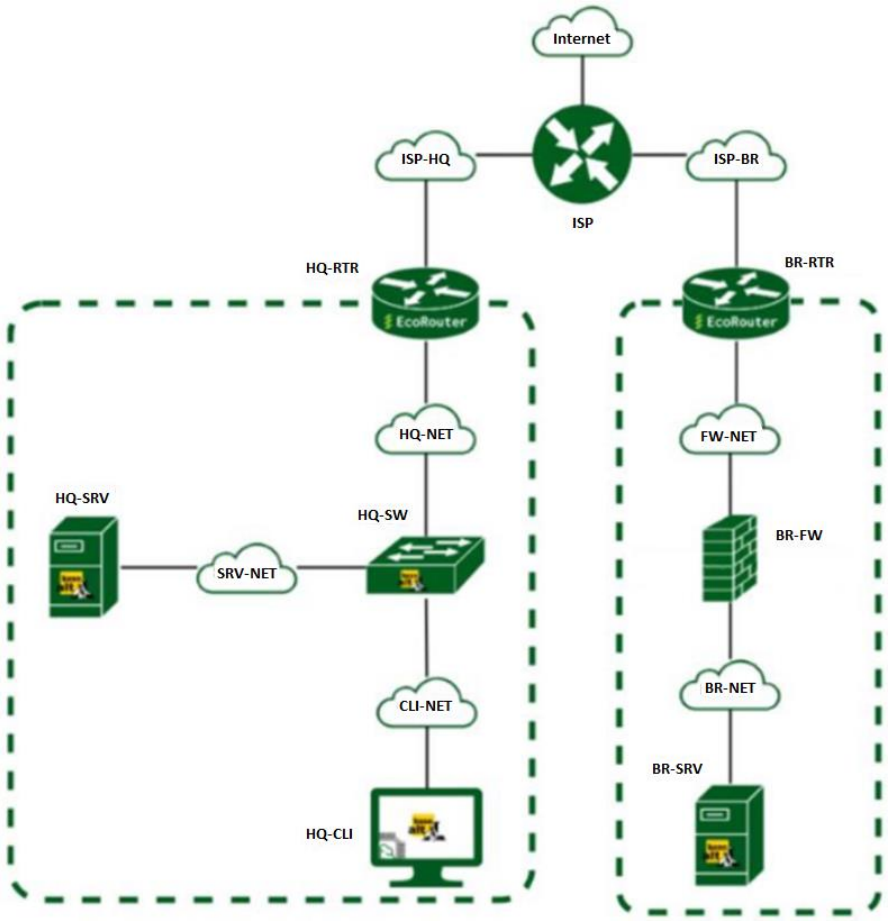


Таблица 4

Имя виртуальной машины	**Оперативная память**	**Центральный процессор, ядер**	**Накопитель**	**Операционная система**
ISP	1 Гб	1 ядро	5 Гб	Серверная операционная система на базе Linux
BR-FW	4 Гб в случае использования Ideco ngfw 1 Гб в случае использования дистрибутива Linux	4 ядра в случае использования Ideco ngfw 1 ядро в случае использования дистрибутива Linux	15 Гб в случае использования Ideco ngfw 5 Гб в случае использования дистрибутива Linux	Ideco ngfw, Vipnet xFirewall, Серверная операционная система на базе Linux
HQ-RTR	4 Гб в случае использования EcoRouter 1 Гб в случае использования	4 ядра в случае использования EcoRouter 1 ядро в случае использования	10 Гб	ОС EcoRouter, в случае невозможности использования EcoRouter

	дистрибутива Linux	дистрибутива Linux		Серверная операционная система на базе Linux
BR-RTR	4 Гб в случае использования EcoRouter 1 Гб в случае использования дистрибутива Linux	4 ядра в случае использования EcoRouter 1 ядро в случае использования дистрибутива Linux	10 Гб	ОС EcoRouter, в случае невозможности использования EcoRouter дистрибутив Серверная операционная система на базе Linux
HQ-SRV	2 Гб	1 ядро	10 Гб	Серверная операционная система на базе Linux
BR-SRV	2 Гб	1 ядро	10 Гб	Серверная операционная система на базе Linux
HQ-CLI	2 Гб	2 ядра	15 Гб	Операционная система на базе Linux с установленной графической оболочкой
Итого	19 (10 в случае использования ОС на базе Linux)	17 (8 в случае использования ОС на базе Linux)	75 Гб	-

Задание 2

1. Настройте установленный контроллер домена Samba DC на сервере BR-SRV:

• введите в созданный домен машину HQ-CLI;

• создайте 5 пользователей для офиса HQ: имена пользователей формата hquser№ (например hquser1, hquser2 и т.д.), политика паролей:

• Минимальная длина пароля 8 символов;

• Блокировка учётной записи после 5 неудачных попыток входа;

• создайте группу hq, введите в группу созданных пользователей;

• убедитесь, что пользователи группы hq имеют право аутентифицироваться на HQ-CLI;

• пользователи группы hq должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id. Запускать другие команды с повышенными привилегиями пользователи группы права не имеют;

---

2. Сконфигурируйте файловое хранилище на сервере HQ-SRV:

• при помощи двух подключенных к серверу дополнительных дисков размером 1 Гб сконфигурируйте дисковый массив уровня 0;

• имя устройства — md0, при необходимости конфигурация массива размещается в файле /etc/mdadm.conf;

• создайте и отформатируйте раздел, в качестве файловой системы используйте ext4;

• обеспечьте автоматическое монтирование в папку /raid;

---

3. Настройте сервер сетевой файловой системы (nfs) на HQ-SRV:

• в качестве папки общего доступа выберите /raid/nfs, доступ для чтения и записи исключительно для сети в сторону HQ-CLI;

• на HQ-CLI настройте автомонтирование в папку /mnt/nfs;

• основные параметры сервера отметьте в отчёте;

---

4. Настройте службу сетевого времени на базе сервиса chrony на маршрутизаторе ISP:

• вышестоящий сервер ntp на маршрутизаторе ISP - на выбор участника;

• стратум сервера - 5;

• в качестве клиентов ntp настройте: HQ-SRV, HQ-CLI, BR-RTR, BR-SRV;

---

5. Сконфигурируйте ansible на сервере BR-SRV:

• сформируйте файл инвентаря, в инвентарь должны входить HQ-SRV, HQ-CLI, HQ-RTR и BR-RTR;

• рабочий каталог ansible должен располагаться в /etc/ansible;

• все указанные машины должны без предупреждений и ошибок отвечать pong на команду ping в ansible посланную с BR-SRV;

---

6. Разверните веб-приложение в docker на сервере BR-SRV:

• средствами docker должен создаваться стек контейнеров с веб приложением и базой данных;

• используйте образы site_latest и mariadb_latest располагающиеся в директории docker в образе Additional.iso;

• в качестве docker файла используйте файл compose.yaml, который располагается в образе Additional.iso;

• приложение testapp, развёрнутое через docker, доступно для внешних подключений через порт 8080;

---

7. Разверните веб-приложение на сервере HQ-SRV:

• используйте веб-сервер apache;

• в качестве системы управления базами данных используйте mariadb;

• файлы веб приложения и дамп базы данных находятся в директории web образа Additional.iso;

• выполните импорт схемы и данных из файла dump.sql в базу данных webdb;

• создайте пользователя web с паролем P@ssw0rd и предоставьте ему права доступа к этой базе данных;

• файлы index.php и файл logo.png скопируйте в корневой каталог сайта;

• в файле index.php укажите правильные учётные данные для подключения к БД;

• запустите веб сервер и убедитесь в работоспособности приложения;

• основные параметры отметьте в отчёте;

---

8. На маршрутизаторах сконфигурируйте статическую трансляцию портов:

• пробросьте порт 8080 в порт приложения testapp BR-SRV на маршрутизаторе BR-RTR, для обеспечения работы приложения testapp извне;

• пробросьте порт 8080 в порт веб приложения на HQ-SRV на маршрутизаторе HQ-RTR, для обеспечения работы веб приложения извне;

• пробросьте порт 2027 на маршрутизаторе HQ-RTR в порт 2027 сервера HQ-SRV, для подключения к серверу по протоколу ssh из внешних сетей;

• пробросьте порт 2027 на маршрутизаторе BR-RTR в порт 2027 сервера BR-SRV, для подключения к серверу по протоколу ssh из внешних сетей;

---

9. Удобным способом установите приложение Яндекс Браузер на HQ-CLI

• установку браузера отметьте в отчёте

Необходимые приложения:
Прил_5_ОЗ_КИМ_09.02.06-4-2027.txt

Инструкции для администратора центра проведения экзамена: Инструкция и список чекпойнтов по настройке оборудования для проведения ДЭ, а также файл users.csv будут представлены в варианте.

Задание 3. Разработка и настройка инфраструктуры информационно-коммуникационной системы

Необходимо разработать и настроить инфраструктуру информационно-коммуникационной системы согласно предложенной топологии (см. **Рисунок 3**).

Задание 3 содержит создание пользователей с помощью сценария, развёртывание и настройку центра сертификации, выдачу сертификатов веб серверам для шифрования трафика, принт-сервера, сервера логирования и мониторинга, автоматизации на основе инфраструктуры открытых ключей, настройку защиты протокола ssh от перебора, настройку программного обеспечения для создания архивных копий.

В ходе проектирования и настройки сетевой инфраструктуры следует заносить записи в отчет о своих действиях, когда это требуется в задании. Отчет по окончании работы следует сохранить на диске рабочего места и задать имя файла без учёта расширения - ФамилияУчастникаЗадание3.

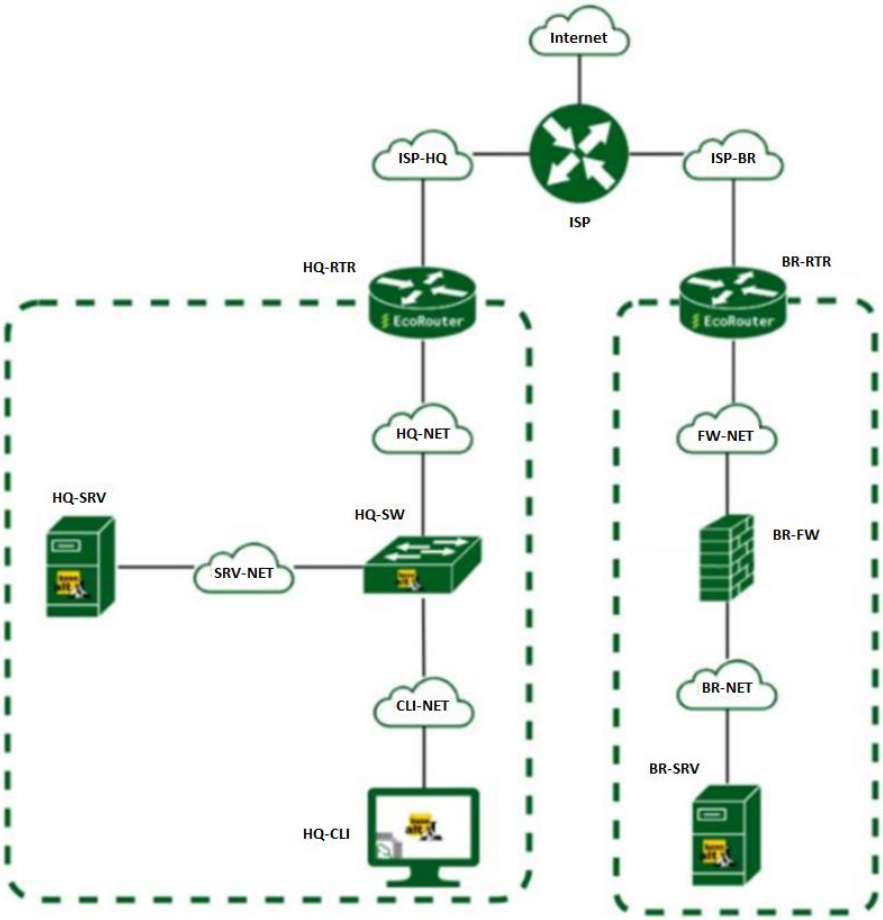


Рисунок 3. Топология сети

Таблица 5

Имя виртуальной машины	Оперативная память	Центральный процессор, ядер	Накопитель	Операционная система
ISP	1 Гб	1 ядро	5 Гб	Серверная операционная система на базе Linux
BR-FW	4 Гб в случае использования Ideco ngfw 1 Гб в случае использования дистрибутива Linux	4 ядра в случае использования Ideco ngfw 1 ядро в случае использования дистрибутива Linux	15 Гб в случае использования Ideco ngfw 5 Гб в случае использования дистрибутива Linux	Ideco ngfw, Vipnet xFirewall, Серверная операционная система на базе Linux
HQ-RTR	4 Гб в случае использования EcoRouter 1 Гб в случае использования дистрибутива Linux	4 ядра в случае использования EcoRouter 1 ядро в случае использования дистрибутива Linux	10 Гб	ОС EcoRouter, в случае невозможности использования EcoRouter Серверная операционная система на базе Linux
BR-RTR	4 Гб в случае использования EcoRouter 1 Гб в случае использования дистрибутива Linux	4 ядра в случае использования EcoRouter 1 ядро в случае использования дистрибутива Linux	10 Гб	ОС EcoRouter, в случае невозможности использования EcoRouter дистрибутив Серверная операционная система на базе Linux
HQ-SRV	2 Гб	1 ядро	10 Гб	Серверная операционная система на базе Linux
BR-SRV	2 Гб	1 ядро	10 Гб	Серверная операционная система на базе Linux
HQ-CLI	2 Гб	2 ядра	15 Гб	Операционная система на базе

				Linux с установленной графической оболочкой
Итого	19 (10 в случае использования ОС на базе Linux)	17 (8 в случае использования ОС на базе Linux)	75 Гб	-

Задание 3

1. Выполните импорт пользователей в домен au-team.irpo:

• скрипт import.sh располагается в корневой директории в образе Additional.iso;

• в качестве файла источника выберите файл users.csv располагающийся в образе Additional.iso;

• пользователи должны быть импортированы со своими паролями и другими атрибутами;

• убедитесь, что импортированные пользователи могут войти на машину HQ-CLI;

---

2. Настройте обратный прокси-сервер на маршрутизаторе ISP:

• при обращении по доменному имени web.au-team.irpo у клиента должно открываться веб приложение на HQ-SRV;

• при обращении по доменному имени docker.au-team.irpo клиента должно открываться веб приложение testapp;

---

3. На маршрутизаторе ISP настройте web-based аутентификацию:

• при обращении к сайту web.au-team.irpo клиенту должно быть предложено ввести аутентификационные данные:

• в качестве логина для аутентификации выберите WEB с паролем P@ssw0rd;

• при успешной аутентификации клиент должен перейти на веб сайт;

---

4. Выполните настройку центра сертификации на базе HQ-SRV:

• рекомендуется использовать отечественные алгоритмы шифрования;

• сертификаты выдаются на 30 дней;

• обеспечьте доверие сертификату для HQ-CLI;

• выдайте сертификаты веб серверам;

• перенастройте ранее настроенный реверсивный прокси на протокол https;

• при обращении к веб серверам https://web.au-team.irpo и https://docker.au-team.irpo у браузера клиента не должно возникать предупреждений;

---

5. На сервере HQ-SRV необходимо настроить утилиту atop для сбора информации о состоянии сервера:

• установите и настройте утилиту atop;

• сервис должен иметь возможность вести непрерывный мониторинг состояния сервера (процессор, оперативная память, дисковые операции, сетевые подключения) с интервалом сбора данных 7 минут;

---

6. Настройте принт-сервер cups на сервере HQ-SRV:

• опубликуйте виртуальный pdf-принтер;

• на клиенте HQ-CLI подключите виртуальный принтер как принтер по умолчанию;

---

7. Реализуйте механизм инвентаризации машин HQ-SRV и HQ-CLI через Ansible на BR-SRV:

• плейбук должен собирать информацию о рабочих местах:

  • имя компьютера;

  • IP-адрес компьютера;

• плейбук должен быть размещен в директории /etc/ansible, отчёты в поддиректории PC-INFO, в формате .yml. Файлы должны называется именем компьютера, который был инвентаризирован;

• файл плейбука располагается в образе Additional.iso в директории playbook;

---

8. На HQ-SRV настройте программное обеспечение fail2ban для защиты ssh:

• укажите порт ssh;

• при 3 неуспешных авторизациях адрес атакующего попадает в бан;

• бан производится на 1 минуту;

---

9. Настройка резервного копирования директории сервера HQ-SRV:

• на HQ-SRV развернуть программное обеспечение для резервного копирования и восстановления данных с защитой от вирусов-шифровальщиков;

• в качестве решения рекомендуется использовать программное обеспечение Кибер Бэкап версии 18 или аналог, совпадающий по функционалу;

• настройте подразделение irpo;

• настройте пользователя с правами администратора, имя пользователя irpoadmin, пароль P@ssw0rd;

• установите на HQ-CLI агент с функциями узла хранилища и подключите его к серверу управления;

• на узле хранилища HQ-CLI создайте директорию /backup и выберите её в качестве устройства хранения;

• создайте план резервного копирования для сервера HQ-SRV:

• план для резервного копирования директории /etc и всех её поддиректорий;

• выполните резервное копирование директории /etc и всех её поддиректорий сервера HQ-SRV на узел хранения HQ-CLI;

Необходимые приложения:

Прил_6_ОЗ_КИМ_09.02.06-4-2027.txt

Инструкции для администратора центра проведения экзамена: Инструкция по настройке стенда для проведения ДЭ будет представлена отдельным файлом в варианте.