Акционерное общество «Птицефабрика «Северная»
ИНН 4706002688, ОГРН 1024701330741, Россия, 187322, Ленинградская область, Кировский муниципальный район, Синявинское городское поселение, дорога «Подъезд к Синявинским высотам от автодороги «Кола», здание 1А
+7 (812) 339-30-10 info@severnaya.ru www.severnaya.ru
ПТИЦЕФАБРИКА СЕВЕРНАЯ

# Лист согласования регионального чемпионата «Профессионалы» Ленинградской области по компетенции сетевое и системное администрирование

| № | Документ | Рекомендации и внесенные изменения |
|---|---|---|
| 1 | Конкурсное задание | - |
| 2 | Инфраструктурный лист | - |

Руководитель IT отдела Белов Сергей Александрович _____

Акционерное общество "Птицефабрика "Северная" Ленинградская обл. Кировский район АО "Птицефабрика "Северная"

12.02.2024

Разработано главным экспертом по компетенции
«СЕТЕВОЕ И СИСТЕМНОЕ
АДМИНИСТРИРОВАНИЕ»

_____/Щавелкин Константин Германович
(подпись) (ФИО главного эксперта)

СОГЛАСОВАНО
Индустриальный эксперт


_____/Белов Сергей Александрович
(подпись) (ФИО)

Менеджер компетенции

_____/_____
(подпись) (ФИО)

# КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

## для возрастной категории

## Юниоры

2024 г.

*Чемпионат профессионального мастерства 2024 в рамках Регионального этапа Чемпионата по профессиональному мастерству «Профессионалы»*

**Конкурсное задание включает в себя следующие разделы:**

## Оглавление

**СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ**

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице №1:

*Таблица №1*

**Оценка конкурсного задания**

| Критерий | | Методика проверки навыков в критерии |
|---|---|---|
| **Б** | **Настройка технических и программных средств информационно-коммуникационных систем** | Оцениваемые аспекты имеют разный вес в зависимости от их сложности. Схема оценки построена так, чтобы каждый аспект оценивался только один раз. Например, в задании предписывается настроить корректные имена для всех устройств, данный аспект будет оценен в первый день только один раз и повторная оценка данного аспекта проводиться не будет. Одинаковые пункты могут быть проверены и оценены больше, чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств. Процедура оценки результатов выполнения задания будет производиться в конце дня конкретного модуля. |
| **Д** | **Обеспечение отказоустойчивости и автоматизация** | Оцениваемые аспекты имеют разный вес в зависимости от их сложности. Схема оценки построена так, чтобы каждый аспект оценивался только один раз. Например, в задании предписывается настроить корректные имена для всех устройств, данный аспект будет оценен в первый день только один раз и повторная оценка данного аспекта проводиться не будет. Одинаковые пункты могут быть проверены и оценены больше, чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств. Процедура оценки результатов выполнения задания будет производиться в конце дня конкретного модуля. |
| **Х** | **ВАРИАТИВНЫЙ МОДУЛЬ:**<br>**Аудит ИЛИ Миграция ИЛИ Поиск и устранение неисправностей** | Определена регионом в соответствии с используемыми ОС и сетевым оборудованием: используется виртуализация и скрипты.<br>Задание, указанное в этом документе, является примерным конкурсным заданием. Каждый регион определяет состав этого модуля самостоятельно. |

## 1.1. КОНКУРСНОЕ ЗАДАНИЕ

Формат участия: командный, 2 человека в команде

Возрастной ценз: от 14 лет

Общая продолжительность Конкурсного задания[1]: 12 ч.

Количество конкурсных дней: 3 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 3 модулей, общее количество баллов конкурсного задания составляет 100.

Оценка каждого дня осуществляется в соответствующий день.

[1] *Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом/командой.*

### 1.2. Структура модулей конкурсного задания

**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:

- 8 гб ОЗУ
- 2-4 процессорных ядра
- 120 гб SSD-пространства
- интернет на скорости не менее 5 мбит/с

Рекомендованные системные требования:

- 12+ гб ОЗУ
- 4-8 процессорных ядра
- 200 гб SSD-пространства
- интернет на скорости не менее 10 мбит/с

**Операционные системы:**

| **VM** | **OS** | **GUI** | **Locale** |
|---|---|---|---|
| FW-KJA | OPNsense 23.1 | - | en_US |
| R0-KJA | Debian 11 | - | en_US |
| SRV-KJA | Debian 11 | - | en_US |
| PC-KJA | Debian 11 | MATE | en_US |
| APP-KJA | Debian 11 | - | en_US |
| FW-VVO | OPNsense 23.1 | - | en_US |
| PC-VVO | RedOS 7.3.2 | MATE | ru_RU, en_US |
| SRV-VVO | RedOS 7.3.2 | - | ru_RU, en_US |

| | | | |
|---|---|---|---|
| GUEST-VVO | RedOS 7.3.2 | MATE | ru_RU, en_US |
| VDS | Debian 11 | - | en_US |
| ClientOMS | Debian 11 | MATE | en_US |
| ClientIKT | RedOS 7.3.2 | MATE | ru_RU, en_US |

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

- Настройка IPv4 адресации
- Loopback-интерфейсы
- DHCPv4
- NAT, PAT, Проброс портов
- Статическая маршрутизация
- Динамическая маршрутизация
- VPN
    - Site-to-site VPN
    - Site-to-client VPN
- LLDP
- Пользователи и группы
- AAA
- Установка программного обеспечения
- DNS (FWD, REV)
- Certificate Authority
- Веб-сервер, SSL
- FTP
- NTP/Chrony
- SSH
- Журналирование, Мониторинг (syslog, rsyslog)
- Домен IPA (FreeIPA)
- Облачные хранилища
- Контейнеры Docker
    - Установка и запуск контейнеров;
    - Проброс портов;
    - Связь между контейнерами;
    - Управление контейнерами.

# ЗАДАНИЕ

**Преамбула:**

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

На межсетевых экранах FW* логин/пароль по умолчанию - root/opnsense

На компьютерах с Debian 10/11 логин/пароль по умолчанию - root/toor и user/P@ssw0rd, пользователь user не имеет sudo-права.

Все проверки работы клиентских технологий (сайтов, клиентских VPN подключений и т.п.) будут выполняться из под пользователя user соответствующих клиентских машин. Сайты будут проверяться через стандартный браузер клиентской ОС (для Windows - Edge, для Debian - Firefox для RedOS - Chromium).

При выполнении настоящего задания всегда нужно руководствоваться правилом наименьших привилегий.

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.

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

**Предыстория:**

Однажды, в одном дальнем-дальнем восточном регионе команда из двух юных, но достаточно компетентных системных администраторов взялась за проект организации сетевой и серверной инфраструктуры для ООО СибИгрСтрой -

небольшой, но перспективной компании по разработке игровых модов и хостингу игровых серверов. На текущий момент в организации имеется два офиса, в городах Красноярск (внутреннее обозначение KJA) и Владивосток (VVO) и виртуальный сервер в интернете с кодовым названием VDS. Все данное оборудование в филиалах только что распаковано, операционные системы предустановлены, дополнительную информацию о предустановленном ПО можно найти в разделах предоставленного вам для работы технического задания. Для широкополосного доступа к сети Интернет нашей компанией заключены договора с провайдерами интернета для обоих филиалов с предоставлением “белых” ip-адресов *(подробнее про сети провайдеров в разделе “Техническое описание лабораторной инфраструктуры и общие требования к реализации”). Также, у нас есть пара постоянных клиентов в городах Омск и Иркутск, которые с радостью предоставят нам свои компьютеры ClientOMS и ClientIKT для тестирования удаленного доступа к великолепным сервисам нашей компании.

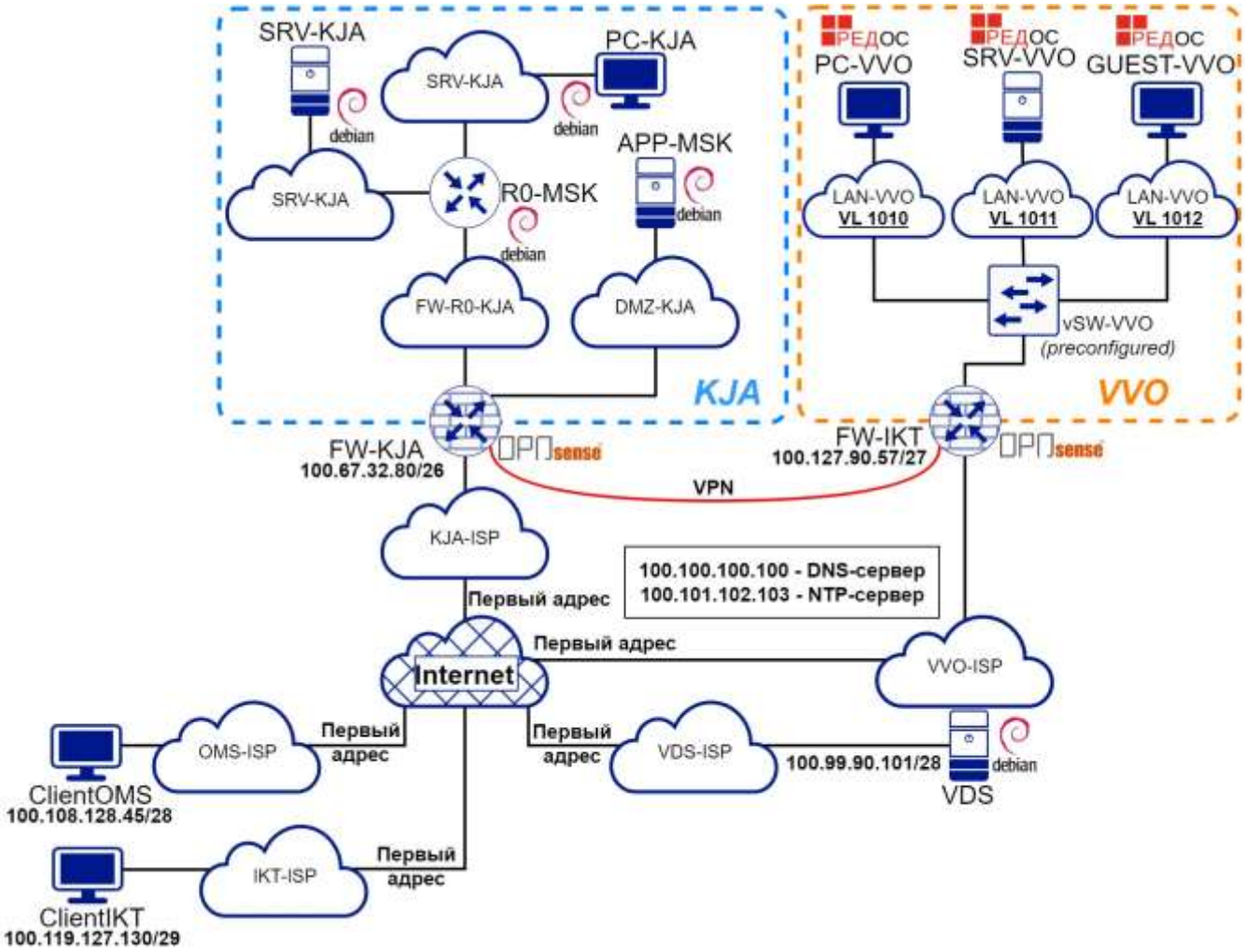
**Схема IP-адресации и схема подключений.**

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 два маршрутизатора, включая сети туннелей site-to-site должны иметь маску сети /30.
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. Все адреса loopback на маршрутизаторах должны иметь индивидуальную маску /32, но при этом быть из одного общего диапазона /24.

| Сеть | Устройство | Адрес/Маска | Шлюз |
|---|---|---|---|
| INTERNET | FW-KJA | 100.67.32.80/26 | ISP – первый адрес в сети |
| | FW-VVO | 100.127.90.57/27 | ISP – первый адрес в сети |
| | VDS | 100.99.90.101/28 | ISP – первый адрес в сети |
| | ClientOMS | 100.108.128.45/28 | ISP – первый адрес в сети |
| | ClientIKT | 100.119.127.130/29 | ISP – первый адрес в сети |
| | DNS-сервер | 100.100.100.100 | |
| | NTP-сервер | 100.101.102.103 | |
| FW-R0-KJA | FW-KJA | STATIC | |
| | R0-KJA | STATIC | FW-KJA (OSPF) |
| LAN-KJA | FW-KJA | STATIC | |

| | | | |
|---|---|---|---|
| | PC-KJA | DHCP | R0-KJA |
| SRV-KJA | R0-KJA | STATIC | |
| | SRV-KJA | STATIC | R0-KJA |
| DMZ-KJA | FW-KJA | STATIC | |
| | APP-KJA | STATIC | FW-KJA |
| LAN-VVO | FW-VVO | STATIC | |
| | PC-VVO | DHCP | FW-VVO |
| SRV-VVO | FW-VVO | STATIC | |
| | SRV-VVO | STATIC | FW-VVO |
| GUEST-VVO | FW-VVO | STATIC | |
| | GUEST-VVO | DHCP | FW-VVO |




## Модуль Б: Настройка технических и программных средств информационно-коммуникационных систем (4 часа)

1. Настройте IPv4-адреса согласно схеме адресации:
   1.1. Настройте адреса шлюза по умолчанию, где это требуется;
   1.2. На FW* и R* настройте описания интерфейсов, согласно схеме сети

1.3. Обеспечьте отсутствие IPv6 адресации на FW* на всех интерфейсах, исключение допускается только для loopback-интерфейсов.

2. Настройте интерфейсы loopback на всех FW* и R*.
3. Настройте имена всех устройств согласно топологии.
4. Все устройства должны иметь доступ в интернет, если в задании явно не указано иного.
5. Настройте OSPFv2 между R0-KJA и FW-KJA
   5.1. FW-KJA должен узнавать о сети SRV-KJA через OSPF.
   5.2. R0 должен получать маршрут по умолчанию и другие необходимые маршруты от FW-KJA через OSPF.
   5.3. Не используйте статические маршруты до этих сетей. Статические маршруты применимы только в качестве временной меры.
   5.4. Маршруты до loopback интерфейсов также должны распространяться по OSPF.
   5.5. R0-KJA должен быть защищен от вброса маршрутов с интерфейсов смотрящих в сторону сети SRV-KJA.
   5.6. FW-KJA должен быть защищен от вброса маршрутов с интерфейса смотрящего в сторону сетей LAN-KJA, DMZ-KJA.
6. В филиале VVO разверните домен vvo.jun.profi на базе FreeIPA с контроллером домена на сервере SRV-VVO. При развертывании учтите, что это устройство также будет выполнять функции DNS и DHCP сервера в филиале VVO. Также, выполните следующие действия в развернутом домене:
   6.1. Создайте пользователей den и alex, поместите их в группу jun-users
   6.2. Введите компьютер PC-VVO в домен, обеспечьте возможность входа под всеми доменными учетными записями на данный ПК.
   6.3. Создайте правило, разрешающее доменному пользователю admin использовать sudo на всех компьютерах в домене без ограничения.
   6.4. Обеспечьте доменному пользователю admin, после успешной авторизации на компьютере PC-VVO, возможность заходить в интерфейс FreeIPA без использования пароля. Для аутентификации и авторизации используйте Kerberos.
7. Настройте инфраструктуру разрешения имен в филиалах следующим образом:
   7.1. DNS-сервер в филиале KJA располагается на FW-KJA.
   7.2. DNS-сервер в филиале VVO располагается на SRV-VVO и интегрирован с доменом FreeIPA.
   7.3. Все устройства в локальных сетях должны обращаться с DNS запросами к DNS-серверам соответствующих филиалов

7.4. Указанные DNS-сервера должны выполнять пересылку DNS запросов от локальных клиентов на DNS сервер провайдера, указанный в Схеме IP-адресации.

7.5. Client* и VDS должны обращаться с DNS запросами на сервер провайдера, указанный в Схеме IP-адресации.

7.6. Настройте для всех устройств филиалов в Красноярске и Владивостоке доменные имена в зонах kja.jun.profi и vvo.jun.profi соответственно.

7.7. Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией в доменах соответствующих филиалов. К примеру srv-kja.kja.jun.profi или pc-vvo.vvo.jun.profi

7.8. В рамках каждого филиала короткие имена должны автоматически дополняться доменным именем соответствующего филиала

7.9. Создайте обратную зону(ы) DNS в доменном DNS-сервере SRV-VVO, чтобы все ip-адреса в филиале VVO, кроме сети GUEST-VVO, расшифровывались в соответствующие им DNS-имена.

8. Настройте DHCP-сервер на FW-KJA для клиентов сети LAN-KJA, а также на SRV-VVO для клиентов сетей LAN-VVO и GUEST-VVO. DHCP-сервер должен передавать клиентам все необходимые опции для работы в сети и взаимодействия с другими устройствами и сетями по IP и DNS именам.

8.1. Выдаваемый диапазон адресов должен оставлять свободными ровно 10 адресов в начале сети, зарезервированных для дальнейшего использования, все остальные адреса должны предназначаться для выдачи клиентам по DHCP.

9. Настройте необходимые параметры на устройстве FW-VVO таким образом, чтобы клиентам в сети LAN-VVO и GUEST-VVO адреса выдавал сервер SRV-VVO.

10. Настройте синхронизацию времени

10.1. Сервер точного времени в филиале KJA располагается на SRV-KJA.

10.2. Сервер точного времени в филиале VVO располагается на FW-VVO.

10.3. Все устройства в локальных сетях должны использовать указанные сервера.

10.4. Все сервера и клиенты, которые поддерживают Chrony должны использовать данную реализацию протокола. На устройствах, которые не поддерживают Chrony допускается использовать стандартный NTP.

10.5. Указанные сервера времени, а также сервера и клиенты во внешних сетях должны синхронизировать свое время с NTP сервером по адресу 100.101.102.103.

10.6. Настройте часовой пояс на всех устройствах в соответствии с их географическим расположением. Для машины VDS используйте часовой пояс Красноярска.

11. Установите пользователю PC-VVO Яндекс Браузер. Для удобства работы создайте для него ярлык на рабочем столе.

12. Настройте правила межсетевого экранирования для сети DMZ-KJA:

12.1. Устройства в сетях DMZ-* не должны иметь возможности инициировать соединения к клиентам в приватных сетях организации, при этом входящие соединения из всех остальных локальных сетей в сети DMZ-* должны быть разрешены.

12.2. Устройства в сетях DMZ-* не должны иметь доступа к интернету, за исключением подключенных репозиториев ОС для установки и обновления пакетов и полного IPv4 доступа к серверу VDS.

12.3. При необходимости, допускается возможность открывать конкретные дополнительные порты, необходимые для выполнения задания.

13. Настройте защищенный VPN-туннель FW-KJA<=>FW-VVO со следующими параметрами:

13.1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.

13.2. Используйте современные надежные протоколы шифрования AES, SHA-2 или ChaCha20.

13.3. Не допускается использование протоколов шифрования и аутентификации с длиной ключа/хеша менее 256 бит.

13.4. Настройте маршрутизацию, NAT и межсетевой экран таким образом, чтобы трафик для другого офиса не натировался и не блокировался

14. Настройте работу OSPF между R* и FW*, чтобы все маршрутизаторы имели полную информацию о маршрутов во все локальные сети всех филиалов.

15. Настройте централизованный сбор журналов syslog на SRV-KJA.

15.1. Журналы должны храниться в файлах /opt/logs/[hostname]/[program].log, где

[hostname] - это короткое или полное доменное имя машины, предоставившей соответствующие сообщения,
[program] - имя программы по определению BSD syslogd.

15.2. R0-KJA и APP-KJA должны записывать только сообщения warning и более важные.

15.3. SRV-KJA должен записывать только сообщения error и никакие другие.

15.4. FW-KJA должен записывать сообщения от служб ospf уровня не менее notice; а также сообщения от любых служб уровня не менее error.

16. Обеспечьте авторизацию пользователей сети GUEST-VVO через captive portal.

16.1. Для авторизации используйте локального пользователя FW-VVO с именем guest.
16.2. Доступ к сетевым ресурсам должен появляться только после авторизации.
16.3. Пользователи данной сети должны иметь доступ в интернет и не иметь доступа к локальным ресурсам, кроме необходимых для выполнения задания.

## Модуль Д: Обеспечение отказоустойчивости и автоматизация (4 часа)

1. Обеспечьте подключение клиента ClientIKT к серверу VPN на FW-KJA.
    1.1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.
    1.2. Клиент должен иметь доступ к серверам в сети SRV-KJA и DMZ-KJA.
    1.3. Соединение должно автоматически устанавливаться при включении компьютера или входе под пользователем user.
2. Настройте CA на SRV-KJA со следующими параметрами
    2.1. Используйте /opt/ca в качестве корневой директории CA.
    2.2. Страна: RU;
    2.3. Организация: JUN PROFI
    2.4. CN должен быть установлен как JUN PROFI CA.
    2.5. Создайте корневой сертификат CA.
    2.6. SRV-KJA и PC-KJA должны доверять CA.
3. На сервере APP-KJA должен быть развернут WEB-сервер корпоративного портала организации:
    3.1. Файлы сайта должны располагаться в директории /var/www/portal
    3.2. Сайт должен открываться по адресу corp.jun.profi
    3.3. Обращение к сайту из внутренних сетей организации должно происходить только по внутренним каналам связи, однако сайт должен также быть доступен и внешним клиентам по тому же адресу.
    3.4. Для работоспособности портала из внешнего мира, передайте необходимые настройки хостинг-провайдеру.
    3.5. Сайт должен содержать следующий текст “Welcome to secure corporate portal jun.profi”
    3.6. Сайт должен функционировать по протоколу HTTPS. При обращении по протоколу HTTP должен происходить автоматический редирект на HTTPS.
    3.7. WEB-сервер должен иметь сертификат, подписанный корпоративным центром сертификации

3.8. Сайт должен открываться с PC-KJA и PC-VVO без ошибок и предупреждений.
3.9. При обращении к серверу по ip-адресу или любому другому DNS-имени, кроме адреса корп.портала, сервер должен выдавать ошибку 404.

4. Обеспечьте подключение удаленного сотрудника с компьютера ClientIKT к корпоративному порталу https://corp.jun.profi следующим образом:
   4.1. посредством VPN-подключения, когда оно активно.
   4.2. посредством доступа по внешнему адресу, когда vpn-соединение неактивно.
   4.3. Открытие портала не должно вызывать ошибок и предупреждений безопасности.
5. Создайте пользователя admin на APP-KJA, и добавьте его в группу ftpusers.
6. Настройте права доступа для каталога /var/www на APP-KJA следующим образом:
   6.1. пользователь admin должен иметь полные права на чтение и запись в указанный каталог и все его подкаталоги.
   6.2. обычные пользователи не должны иметь прав на запись в данный каталог
   6.3. службы настроенного ранее веб-сервера должны иметь необходимые права для работы сайта.
7. Настройте общий доступ к файлам на APP-KJA по протоколу FTP.
   7.1. Доступ должен быть только у пользователей группы ftpusers.
   7.2. FTP-сервер должен предоставлять доступ только к содержимому папки /var/www/ и вложенных в нее папок.
   7.3. Доступ к FTP-серверу должен быть только у клиентов сети LAN-KJA
8. Настройте клиент FTP на PC-KJA.
   8.1. Установите ПО Filezilla актуальной стабильной версии и проверьте возможность подключения к корпоративному FTP-серверу. Для удобства, создайте ярлык Filezilla на рабочем столе
   8.2. Обеспечьте монтирование корпоративного FTP-хранилища на PC-KJA в папку /opt/ftp/
   8.3. Монтирование должно восстанавливаться при перезагрузке виртуальной машины.
9. Обеспечьте веб-интерфейс FW-KJA сертификатом HTTPS, подписанным корпоративным центром сертификации, обеспечивающим доверенное соединение при обращении к FW-KJA по полному и сокращенному DNS-имени и IP-адресу с PC-KJA.
10. Обеспечьте возможность подключения к FW-KJA под пользователем admin:

10.1. посредством веб-интерфейса с полным доступом к настройкам;
10.2. посредством протокола SSH с доступом к выполнению команд через sudo;
10.3. при подключении с компьютера PC-KJA авторизация SSH должна осуществляться по ключу без необходимости ввода пароля.

11. Настроить удаленный доступ к VDS и R0-KJA по SSH
    11.1. На сервере VDS сервис SSH должен функционировать на порте 2202
    11.2. Устройство PC-KJA при входе под пользователем user должно иметь доступ к VDS под пользователем user с использованием SSH ключей, без необходимости ввода пароля.
    11.3. Пользователь user на VDS должен иметь возможность выполнять команды через sudo без ввода пароля.
    11.4. Подключение к VDS с PC-KJA должно осуществляться по имени “VDS”
    11.5. Устройство PC-KJA при входе под пользователем user должно иметь доступ к R0-KJA под пользователем user с использованием SSH ключей, без необходимости ввода пароля.
12. Для хранения важных данных в сервер VDS установлено два дополнительных диска. Объедините их в RAID1 используя технологию md raid. На полученном резервированном носителе создайте файловую систему XFS и подключите раздел по пути /opt/mc/data/ для дальнейшего использования.
13. На VDS разверните сервер Minecraft со следующими параметрами:
    13.1. Имя сервера: Jun Profi
    13.2. Ограничение кол-ва игроков: 12
    13.3. Порт: по умолчанию
    13.4. Проверка аккаунтов пользователей: отключена
    13.5. Сервер должен быть запущен в виде контейнера Docker
    13.6. Данные сервера должны храниться по пути /opt/mc/data/
    13.7. Контейнер должен автоматически запускаться после перезагрузки компьютера.
14. Помогите постоянному клиенту из Омска подготовить рабочее место ClientOMS:
    14.1. Установите tlauncher. Обязательно создайте ярлык установленного tlauncher на рабочем столе пользователя, чтобы ему было удобнее подключаться к Вашему серверу.
    14.2. Установите OBS последней стабильной версии посредством системы управления пакетами Flatpak. Обязательно создайте ярлык

установленного OBS на рабочем столе пользователя, чтобы ему было удобнее запускать стрим игры на Вашем сервере.

15. На сервере SRV-KJA разверните сервер облачного хранения данных со следующими параметрами:
    15.1. Файловый сервер: NextCloud
    15.2. База данных: PostgreSQL
    15.3. Веб интерфейс БД: PgAdmin
        i. Подключите PgAdmin к созданному серверу БД с полным административным доступом под пользователем pgadm@jun.profi
    15.4. Порт NextCloud: 80
    15.5. Порт PgAdmin: 8888
    15.6. Все сервисы должны быть запущены в виде контейнеров Docker
    15.7. Все контейнеры должны автоматически запускаться после перезагрузки компьютера
    15.8. Обеспечьте работоспособность сервера NextCloud и возможность входа под пользователем user с паролем "jun.profi_pass".
16. Обеспечьте возможность сохранения конфигурации FW-KJA на развернутое хранилище NextCloud в директорию opns-backup, под пользователем user посредством веб-интерфейса FW-KJA.
    16.1. Настройте автоматическое сохранение конфигурации в указанное расположение каждые 12 минут.
17. Обеспечьте возможность удаленным сотрудникам, подключенным к корпоративному VPN-сервису, использовать корпоративное облачное хранилище.

## Модуль X: Поиск и устранение неисправностей

## Секретное задание