Конкурсное задание

Модуль А – Администрирование ОС Linux

Сетевое и системное администрирование

Разработано:

Главный эксперт Лапенко Светлана

СОДЕРЖАНИЕ

Введение **3**

Описание проекта и задач **5**

Задачи конфигурации **7**

Часть 1. Базовая настройка 7

Часть 2. Внутренняя инфраструктура 7

Задача 1. Автоматическая выдача сетевых настроек *7*

Задача 2. Файловый сервер на базе Samba *7*

Задача 3. Внутренний DNS-сервер (BIND9) *7*

Задача 4. Центр сертификации (CA) *8*

Часть 3. DMZ-инфраструктура 8

Задача 5. Веб-сервер *8*

Задача 6. Почтовый сервер *9*

Задача 7. Резервное копирование *9*

Часть 4. Сетевая инфраструктура и безопасность 9

Задача 8. NAT, маршрутизация и файрвол (nftables) *10*

Задача 9. WireGuard VPN *10*

Часть 5. Клиентская рабочая станция и Ansible 10

Задача 10. Браузер и почтовый клиент: *10*

Задача 11. Ansible для автоматизации настройки веб-сервера *10*

Часть 5. Удаленный клиент 11

ВВЕДЕНИЕ

Соревнование имеет фиксированное время начала и окончания. Вы должны решить, как лучше распределить свое время.

Пожалуйста, внимательно прочтите следующие инструкции!

После окончания времени соревнования, пожалуйста, оставьте свою станцию в рабочем состоянии. Оценка будет проводиться в том состоянии, в котором она есть. Перезагрузка не будет инициирована, а выключенные машины не будут включены!

Пожалуйста, используйте информацию ниже для всех серверов и клиентов.

Авторизация

Если в настоящем документе не указано иное, используйте следующую информацию для всех серверов и служб:

Имя пользователя:	root / user
Пароль:	Skill39@Qual

Параметры системы

Регион/часовой пояс:	Asia/Qyzylorda
Локаль:	English US (UTF-8)
Клавиатура:	English US

Важно: Оценка

Большая часть выполненной оценки — это функциональная оценка, вам разрешено выбрать любой пакет, который вы предпочитаете для выполнения задания, например Apache или NGINX. Однако, если указан конкретный пакет, обязательно установите его.

Обратите внимание, что мы не будем изменять ваши конфигурации или перезапускать какие-либо службы или виртуальные машины, если это специально не указано, поэтому убедитесь, что они остаются работоспособными/работающими по окончании конкурса. Службы, которые не работают по окончании конкурса, даже если они почти полностью настроены, не принесут вам баллов.

Может быть несколько способов выполнить определенное задание.

ПРЕДУСТАНОВЛЕННЫЕ РЕСУРСЫ

Каждая система в этой задаче использует Debian 12. Каждая виртуальная машина, которую вы видите в топологической схеме в конце этого документа, предустановлена на физическом хосте, и названа соответствующим образом. Хосты используют VMware Workstation в качестве платформы виртуализации.

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Для целей тестирования все виртуальные машины были установлены со следующими тестовыми инструментами: smbclient, curl, lynx, dnsutils, ldap-utils, ftp, lftp, wget, ssh, nfs-common,

rsync, telnet, traceroute, tcptraceroute, tcpdump. Все виртуальные машины оснащены всеми дисками Debian Blu-ray. Это позволяет устанавливать программное обеспечение с помощью APT.

ОПИСАНИЕ ПРОЕКТА И ЗАДАЧ

Вы новый IT-инженер в компании *KazNet Solutions*. Цель вашего проекта – построение IT-инфраструктуры компании без использования облачных технологий.

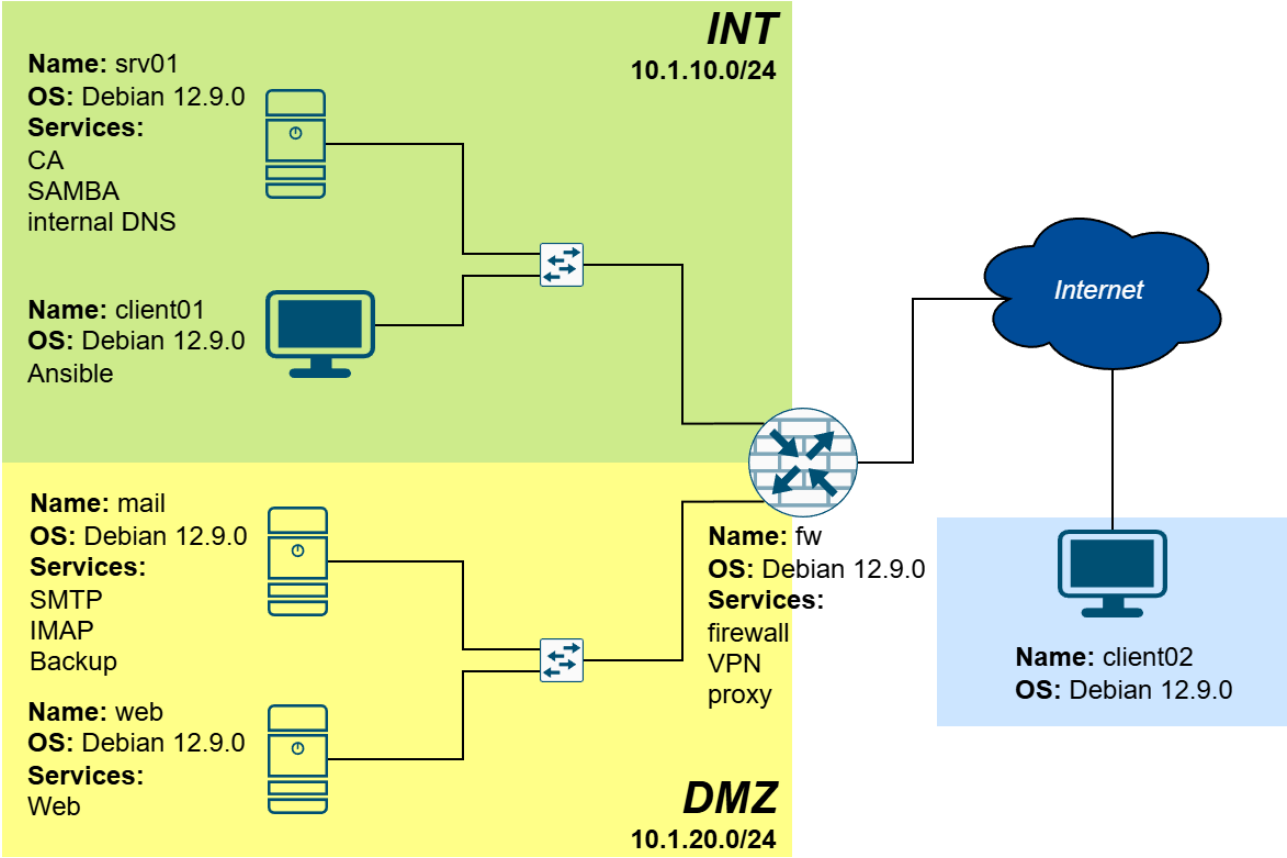
Таблица 1: Сервера и клиенты

FQDN	IPV4	СЛУЖБЫ
fw.kaznet.kz	WAN: 1.1.1.10/24 INT: 10.1.10.1/24 DMZ: 10.1.20.1/24 VPN: 10.1.30.1/24	Firewall (nftables) VPN Server (WireGuard)
srv01.kaznet.kz	INT: 10.1.10.10/24	CA, Samba, DNS Server (BIND9)
mail.kaznet.kz	DMZ: 10.1.20.10/24	Mail server (Dovecot + Postfix)
web.kaznet.kz	DMZ: 10.1.20.31/24	Web server
client01.kaznet.kz	INT: DHCP	Mail Client, Browser, Ansible
client02.kaznet.kz	WAN: 1.1.1.20/24 VPN: 10.1.30.2/24	E-Mail Client, Browser VPN-Client,

Таблица 2: Пользователи Samba

USERNAME	PASSWORD
aliya	Skill39@Astana
erzhan	Skill39@Astana

Топология


INT
10.1.10.0/24
Name: srv01
OS: Debian 12.9.0
Services:
CA
SAMBA
internal DNS
Name: client01
OS: Debian 12.9.0
Ansible
Internet
Name: mail
OS: Debian 12.9.0
Services:
SMTP
IMAP
Backup
Name: web
OS: Debian 12.9.0
Services:
Web
Name: fw
OS: Debian 12.9.0
Services:
firewall
VPN
proxy
Name: client02
OS: Debian 12.9.0
DMZ
10.1.20.0/24

ЗАДАЧИ КОНФИГУРАЦИИ

Часть 1. Базовая настройка

Настройте на всех хостах:

- имя хоста,
- настройка сети,
- часовой пояс,
- настройте доступ по SSH для пользователя root с использованием пароля.

Часть 2. Внутренняя инфраструктура

Сервер: `srv01.kaznet.kz`

IP-адреса:

- IPv4: 10.1.10.10/24

Задача 1. Автоматическая выдача сетевых настроек

1. **Установка и настройка службы DHCP:**
    - Установите службу DHCP.
    - Определите параметры сервера в соответствии с требованиями:
        - Клиентами являются рабочие станции домена INT
        - Исключите из раздачи первые 100 адресов.

Задача 2. Файловый сервер на базе Samba

2. **Установка и настройка:**
    - Установите Samba на сервер.
    - Создайте локальных пользователей для доступа к файловым ресурсам (например, пользователей `aliya` и `erzhan` с паролем `Skill39@Astana`).
3. **Настройка расшаренных директорий:**
    - **/public:**

      Доступ: чтение для всех (включая гостей), запись разрешена только аутентифицированным пользователям.
    - **/internal:**

      Доступ: только для аутентифицированных пользователей (чтение и запись).

Задача 3. Внутренний DNS-сервер (BIND9)

1. **Установка и настройка BIND9:**
    - Установите BIND9.
    - Создайте зону `kaznet.kz` и соответствующие обратные зоны для внутренней сети.

2. **DNS-записи:**
   - Добавьте записи для основных серверов внутренней сети
3. **Алиасы для служб**
   - Создайте алиас для web-сервера **www.kaznet.kz** к серверу **web.kaznet.kz**.
   - Важно: не создавайте A-запись для этой службы
4. **Рекурсия:**
   - Отключите рекурсивное разрешение запросов для клиентов сети.

Задача 4. Центр сертификации (CA)

1. **Создание Root CA:**
   - С помощью OpenSSL создайте корневой центр сертификации с именем «KazNet Root CA».
   - Используйте подходящие значения для полей сертификата (CN, Country и т.д.).
2. **Генерация сертификатов для сервисов:**
   - На основе Root CA создайте и подпишите сертификаты для следующих сервисов:
     - **Веб-сервер:** для домена `www.kaznet.kz`
     - **Почтовый сервер:** для домена `mail.kaznet.kz`
3. **Размещение сертификатов:**
   - Сохраните корневой сертификат как `ca.pem` и подписанные сертификаты как `web.pem` и `mail.pem` в каталоге `/opt/ssl`, чтобы эксперты могли их проверить.

Часть 3. DMZ-инфраструктура

1. **Общая сеть DMZ:**
   - Домен: kaznet.kz
   - IPv4: 10.1.20.0/24

Задача 5. Веб-сервер

Сервер: `web.kaznet.kz`

1. **Установка веб-сервера:**
   - Установите и настройте Apache или NGINX.
2. **Стартовая страница:**
   - Стартовая страница должна выдавать текст «Welcome to KazNet!»
   - Ниже должна располагаться гиперссылка на страницу /whoami.
3. **Настройка сайта:**
   - Сайт обслуживает домен `www.kaznet.kz`.
   - Файлы сайта должны располагаться в каталоге `/var/www/html/` с файлом `index.html` по умолчанию.

4. **TLS:**
    - Настройте веб-сервер на использование сертификата `web.pem` (а также корневого сертификата `ca.pem` для цепочки доверия).
5. **Функциональное требование:**
    - При обращении к URL `/whoami` веб-сервер должен возвращать имя хоста сервера (например, `web.kaznet.kz`).

Задача 6. Почтовый сервер

Сервер: `mail.kaznet.kz`

1. **Установка почтовых сервисов:**
    - Установите Postfix и Dovecot для обслуживания домена `dmz.kaznet.kz`.
2. **TLS:**
    - Настройте TLS для всех почтовых соединений, используя сертификат `mail.pem` (с цепочкой, включающей `ca.pem`), сгенерированный на предыдущем шаге.
3. **Локальная аутентификация:**
    - Настройте локальных пользователей для доступа к почтовой системе (например, используйте пользователя `aliya` с паролем `Skill39@Astana`).

Задача 7. Резервное копирование

1. **Монтирование внешнего диска:**
    - На сервере `mail.kaznet.kz` создайте точку монтирования `/opt/backup` и смонтируйте диск, имитируемый устройством `/dev/sdb`.
    - Обеспечьте автоматическое монтирование через настройку файла `/etc/fstab`.
2. **Скрипт резервного копирования:**
    - Напишите скрипт `/opt/backup.sh`, который будет копировать данные почтовых ящиков и важные конфигурационные файлы почтового сервера в `/opt/backup`.
    - Скрипт должен позволять восстановить систему в случае сбоя.

Часть 4. Сетевая инфраструктура и безопасность

Сервер: `fw.kaznet.kz`

Роль: маршрутизатор, файрвол и VPN-сервер

IP-адреса:

- IPv4:
    - WAN: 1.1.1.10/24
    - INT: 10.1.10.1/24
    - DMZ: 10.1.20.1/24
    - VPN: 10.1.30.1/24

Задача 8. NAT, маршрутизация и файрвол (nftables)

1. **IP-пересылка:**
   - Включите пересылку пакетов для IPv4 и IPv6.
2. **Настройка NAT:**
   - Организуйте маскарадинг для исходящего трафика на внешнем интерфейсе.
3. **Порт-форвардинг:**
   - Настройте переадресацию портов:
     - HTTP (80/tcp) и HTTPS (443/tcp) – на веб-сервер в DMZ.
     - DNS (53/tcp и 53/udp) – на DNS-сервер в DMZ.
4. **Фильтрация трафика:**
   - Разрешите трафик между внутренней сетью (включая VPN) и DMZ.
   - Все прочие подключения – по умолчанию запрещены.

Задача 9. WireGuard VPN

1. **Установка и настройка:**
   - Установите WireGuard и настройте VPN-сервер на `fw.kaznet.kz`.
2. **Конфигурация туннеля:**
   - Используйте сеть VPN 10.1.30.0/24 для клиентов.
   - Настройте маршрутизацию всего трафика клиентов через VPN.
   - Примените пред-общий ключ (pre-shared key) для повышения безопасности.
3. **DNS:**
   - Клиенты VPN должны использовать внутренний DNS-сервер для разрешения имён.

Часть 5. Клиентская рабочая станция и Ansible

Сервер/рабочая станция: `client01.kaznet.kz`

Роль: тестирование инфраструктуры и автоматизация

Задача 10. Браузер и почтовый клиент:

- Установите Firefox (домашняя страница – `https://www.kaznet.kz`)
- Установите Thunderbird (настройте почтовую учётную запись для пользователя `aliya@kaznet.kz` с использованием TLS).

Задача 11. Ansible для автоматизации настройки веб-сервера

1. **Подготовка Ansible playbook:**
   - На сервере `client01.kaznet.kz` создайте Ansible playbook, который будет настраивать веб-сервер `web.dmz.kaznet.kz`.
2. **Содержимое playbook должно включать:**
   - Установку выбранного веб-сервера (Apache или NGINX).

- Развёртывание конфигурационного файла для обслуживания домена `www.kaznet.kz` с корневой директорией `/var/www/html/` и файлом `index.html` по умолчанию.
- Перезапуск сервиса веб-сервера для применения изменений.

3. **Проверка:**
   - Эксперты запустят команду:
     `ansible-playbook /opt/ansible/configure-web.yml`
   - Убедитесь, что изменения применены корректно.

Часть 5. Удаленный клиент

Сервер/рабочая станция: `client02.kaznet.kz`

Роль: тестирование внешнего доступа к инфраструктуре

Установка GNOME и создание пользователя:

- Установите графическую среду GNOME.
- Создайте локального пользователя `testuser` с паролем `Skill39@Astana`.

Настройка VPN-клиента:

- Настройте подключение WireGuard через NetworkManager и подключитесь к VPN.

Браузер и почтовый клиент:

- Установите Firefox (домашняя страница – `https://www.kaznet.kz`) и Thunderbird (настройте почтовую учётную запись для пользователя `aliya@kaznet.kz` с использованием TLS).