*Приложение 4*

**Чертежи, технологические карты, алгоритмы, схемы и т.д.**

**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
* интернет на скорости не менее 5 мбит/с

Рекомендованные системные требования:

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

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.

**Операционные системы:**

|  |  |  |  |
| --- | --- | --- | --- |
| **ВМ** | **ОС** | **Ресурсы (примерно)** | **GUI** |
| FW-KLG | OPNsense 24.1 | 1Gb; 1CPU | - |
| R2-KLG | Alt Server 10.2 | 0.5Gb; 1CPU | - |
| R3-KLG | Alt Server 10.2 | 0.5Gb; 1CPU | - |
| SRV-KLG | Alt Server 10.2 | 2Gb; 2CPU | - |
| APP-KLG | Alt Server 10.2 | 1Gb; 1CPU | - |
| ARM-KLG | Alt Workstation 10.2 | 1Gb; 1CPU | MATE |
| PC-KLG | Alt Workstation 10.2 | 1Gb; 1CPU | MATE |
| FW-RZN | OPNsense 24.1 | 1Gb; 1CPU | - |
| SRV-RZN | Debian 12 | 1Gb; 1CPU | - |
| PC-RZN | Debian 12 | 1Gb; 1CPU | MATE |
| NB-RZN | Debian 12 | 1Gb; 1CPU | MATE |
| VDS | Alt Server 10.2 | 2Gb; 2CPU | - |
| ClientTVR | Alt Workstation 10.2 | 1Gb; 1CPU | MATE |

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

**Инвариативная часть:**

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

**Вариативная часть:**

* Loopback-интерфейсы
* Динамическая маршрутизация
* Доменные инфраструктуры (FreeIPA)
* Центр сертификации, SSL
* FTP
* Журналирование, Мониторинг (syslog, rsyslog и т.п.)
* Работа с дисками (LVM, RAID, квотирование, шифрование, монтирование)
* Системы мониторинга ресурсов (Zabbix)
* Настройка централизованной системы журналирования
* Настройка автоматизированного рабочего места
* Работа с юнитами systemd (управление юнитами, создание простого юнита)
* Работа с системным загрузчиком GRUB
* Авторизация пользователей для получения доступа к ЛВС.

**Расширенная вариативная часть:**

* 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

**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.

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. Web-сервисы и сайты, согласно политике Организации, будут проверяться через Яндекс-браузер, который должен запускаться через ярлык на рабочем столе или через основное меню.

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.

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.

Обратите внимание, что для получения доступа к веб-интерфейсу FW-KLG вам потребуется средствами локальной командной строки создать на нем временный маршрут до сети рабочего места, с которого будет производиться настройка, а также предпринять другие шаги, необходимые для обеспечения IP-связности между указанными устройствами.

**Предыстория**

Добро пожаловать в славный город Калугу, колыбель космонавтики, край промышленности и торговли. С сегодняшнего дня Вы с напарником устроены в ЗАО “СетСервТрансМаш” (далее Организация) на должность сетевых и системных администраторов. Наша организация занимается разработкой, обслуживанием и поддержанием вычислительной и коммуникационной инфраструктуры организаций в городе и окрестностях, с акцентом на производственные комплексы, связанные с транспортным машиностроением. Следуя запросам наших клиентов, Организация старается достичь максимально возможного уровня использования отечественных аппаратных и программных решений. Головной офис Организации находится в Калуге (внутреннее обозначение KLG) а также имеется небольшой филиал в Рязани (RZN) и виртуальный сервер в интернете с кодовым названием VDS. Все оборудование в филиалах только что распаковано, операционные системы предустановлены, в соответствии с техническим заданием. Для доступа к сети Интернет нашей компанией 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”). Также, у нас есть удаленный сотрудник, работающий из Твери.

**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. Все адреса loopback на маршрутизаторах должны иметь индивидуальную маску /32, но при этом быть из одного общего диапазона /24 для каждого из филиалов.
5. 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-RZN | 100.127.90.57/27 | ISP – первый адрес в сети |
|  | VDS | 100.99.90.101/28 | ISP – первый адрес в сети |
|  | ClientTVR | 100.108.128.45/28 | ISP – первый адрес в сети |
|  | DNS-сервер | 100.100.100.100 |  |
|  | NTP-сервер | 100.101.102.103 |  |
| FW-R1-KLG | FW-KLG | STATIC |  |
|  | R1-KLG | STATIC |  |
| SRV-KLG (vl2005) | R1-KLG | STATIC |  |
|  | SRV-KLG | STATIC | R1-KLG |
| DMZ-KLG (vl2008) | R1-KLG | STATIC |  |
|  | APP-KLG | STATIC | R1-KLG |
| LAN-KLG (vl2010) | R1-KLG | STATIC |  |
|  | PC-KLG | DHC | R1-KLG |
| SEC-KLG (vl2011) | R1-KLG | STATIC |  |
|  | PC-KLG | DHCP | R1-KLG |
| SRV-RZN | FW-RZN | STATIC |  |
|  | SRV-RZN | STATIC | FW-RZN |
| LAN-RZN | FW-RZN | STATIC |  |
|  | PC-RZN | DHCP | FW-RZN |
| GST-RZN | FW-RZN | STATIC |  |
|  | NB-RZN | DHCP | FW-RZN |
| Loopback | FW-KLG | STATIC |  |
|  | R2-KLG | STATIC |  |
|  | R3-KLG | STATIC |  |
|  | FW-RZN | STATIC |  |

