Приложение №3 ****

**Задание для демонстрационного экзамена**

**по стандартам Ворлдскиллс Россия** *(образец)*

**по компетенции «Сетевое и системное администрирование»**

Задание включает в себя следующие разделы:

1. Формы участия
2. Модули задания и необходимое время
3. Критерии оценки
4. Необходимые приложения

Количество часов на выполнение задания: 6ч.

## 1. ФОРМА УЧАСТИЯ

индивидуальная

## 2. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время сведены в таблице 1

Таблица 1.

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование модуля | Максимальный балл | Время на выполнение |
| 1 | Модуль A - Базовая настройка Linux | 15 | 2 часа |
| 2 | Модуль B - Базовая настройка Windows | 15 | 2 часа |
| 3 | Модуль C – Базовые сетевые технологии | 15 | 2 часа |

**Модули с описанием работ**

**Модуль 1:** Модуль A - Базовая настройка Linux

## Конфигурация хостов

1. Настройте имена хостов в соответствии с диаграммой.
2. Установите следующее ПО на ВСЕ виртуальные машины:
   1. Пакет tcpdump
   2. Пакет net-tools
   3. Редактор vim
   4. lynx
   5. bind-utils
   6. mc
   7. nfs-utils
3. На всех хостах сформируйте файл **/etc/hosts** в соответствии с Диаграммой (кроме адреса хоста L-CLI и R-CLI). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет.
   1. В случае корректной работы DNS-сервисов ответы DNS должны иметь более высокий приоритет.

## Конфигурация сетевой инфраструктуры

1. Настройте IP-адресацию на всех хостах в соответствии с диаграммой.
2. Настройте сервер протокола динамической конфигурации хостов для L-CLI.
   1. В качестве DHCP-сервера используйте L-FW.
      1. Используйте пул адресов 172.16.100.60 — 172.16.100.75.
      2. Используете адрес L-SRV в качестве адреса DNS-сервера.
   2. В качестве шлюза по умолчанию используйте соответствующий адрес L-FW.
   3. Используйте DNS-суффикс **skill39.wsr**
   4. DNS-записи типа A и PTR должны обновляться при получении адреса от DHCP-сервера.
3. На L-SRV настройте службу разрешения доменных имен.
   1. Сервер должен обслуживать зону **skill39.wsr**
   2. Сопоставление имен необходимо организовать в соответствии с Таблицей 1.
   3. Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS-серверу ISP. Для проверки используйте доменное имя **worldskills.ru**.
   4. Реализуйте поддержку разрешения обратной зоны в соответствии с Таблицей 1.
   5. Файлы зон необходимо располагать в **/opt/dns/**
4. На DNS сервере ISP приобретена услуга Secondary DNS для зоны **skill39.wsr**
   1. Настройте возможность трансфера зоны **skill39.wsr** в сторону ISP.
   2. Используйте адрес ISP в качестве адреса DNS сервера для R-FW и R-CLI.
   3. Трансфер зоны на другие хосты, кроме ISP, должен быть запрещен.
5. На L-FW и R-FW настройте интернет-шлюз для организации коллективного доступа в Интернет.
   1. Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса соответствующего межсетевого экрана.

## Службы централизованного управления и журналирования

1. Разверните LDAP-сервер для организации централизованного управления учетными записями.
   1. В качестве сервера выступает L-SRV.
   2. Учетные записи создать в соответствии с Таблицей 2.
   3. Группы и пользователей создать в соответствии с Таблицей 2.
   4. Пользователи должны быть расположены в OU Users.
   5. Группы должны быть расположены в OU Groups.
   6. Хосты должны аутентифицироваться через LDAP в соответствии с Таблицей 2.
2. На L-SRV организуйте централизованный сбор журналов с хостов.
   1. Журналы должны храниться в директории **/opt/logs/**
   2. Журналирование должно производиться в соответствии с Таблицей 3.
   3. Сообщения в файлах журналов в директории **/opt/logs** не должны дублироваться.

## Конфигурация служб удаленного доступа

1. Настройте сервер удаленного доступа на основе технологии OpenVPN:
   1. В качестве сервера выступает L-FW.
   2. Параметры туннеля
      1. Устройство TUN
      2. Протокол UDP
      3. Применяется сжатие
      4. Порт сервера 1122
   3. Ключевая информация должна быть сгенерирована на R-FW.
   4. В качестве адресного пространства подключаемых клиентов использовать сеть 5.5.5.0/27.
   5. Хранение всей необходимой (кроме конфигурационных файлов) информации организовать в **/opt/vpn**
2. На OUT-CLI настройте клиент удаленного доступа на основе технологии OpenVPN:
   1. Запуск удаленного подключения должен выполняться скриптом **start\_vpn.sh**
   2. Отключение VPN-туннеля должно выполняться скриптом **stop\_vpn.sh**
   3. Скрипты должны располагаться в **/opt/vpn**
   4. Скрипты должны вызываться из любого каталога без указания пути.
3. Настройте GRE-туннель между L-FW и R-FW:
   1. Используйте следующую адресацию внутри GRE-туннеля:
      1. L-FW: 10.5.5.1/30
      2. R-FW: 10.5.5.2/30
4. На L-FW настройте удаленный доступ по протоколу SSH:
   1. Доступ ограничен пользователями **ssh\_p** и **ssh\_c**
      1. В качестве пароля использовать **ssh\_pass**
   2. SSH-сервер должен работать на порту **1022**.
5. На OUT-CLI настройте клиент удаленного доступа SSH:
   1. Доступ к серверу L-FW должен происходить автоматически по правильному порту, без его явного указания номера порта в команде подключения.
   2. Для других серверов по умолчанию должен использоваться порт **22**.
   3. Доступ к L-FW под учетной записью **ssh\_p** должен происходить с помощью аутентификации на основе открытых ключей.

## Конфигурация веб служб

1. На R-FW установите и настройте веб-сервер:
   1. Настройте веб-сайт для внешнего использования **www.skill39.wsr**
      1. Используйте директорию **/var/www/html/out**
      2. Используйте стандартные порты.
      3. Обеспечьте работу сайта по протоколам **http** и **https** (сертификат должен быть сгенерирован на R-FW).
      4. В случае доступности **https** должно происходить автоматическое перенаправление с **http**.
      5. Клиенты должны доверять сертификату сайта.

## Конфигурация служб хранения данных

1. Настройте сервер файлового хранилища на основе технологии NFS:
   1. В качестве сервера должен выступать L-SRV.
   2. В качестве хранилища используется каталог **/opt/nfs**
   3. Доступ организуется для чтения и записи.
2. Настройте автоматическое монтирование NFS хранилища для клиентов L-CLI и R-CLI:
   1. Используйте **/opt/nfs** в качестве пути для монтирования.
   2. Клиенты L-CLI и R-CLI должны монтировать NFS каталог при запуске операционной системы.

## Конфигурация параметров безопасности и служб аутентификации

1. Настройте CA на R-FW, используя OpenSSL.
   1. Используйте **/etc/ca** в качестве корневой директории CA.
   2. Атрибуты CA должны быть следующими:
      1. Страна RU
      2. Организация WorldSkills Russia
      3. CN должен быть установлен как WSR CA
   3. Создайте корневой сертификат CA.
   4. Все клиентские операционные системы должны доверять CA.
2. Настройте межсетевой экран **iptables** на L-FW и R-FW.
   1. Запретите прямое попадание трафика из Интернет во внутренние сети.
   2. Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора L-FW.
   3. Разрешите необходимый трафик для создания GRE туннеля между организациями.
   4. Разрешите SSH подключения на соответствующий порт L-FW и R-FW.
   5. Для VPN-клиентов должен быть предоставлен полный доступ к локальным сетям организаций LEFT и RIGHT.
   6. Разрешите необходимый трафик к серверу L-SRV по транслированным IP-адресам.
   7. Организуйте доступность сервиса DNS на L-SRV по внешнему адресу L-FW.
   8. Разрешите необходимый трафик для работы веб и файловых служб.
   9. Остальные сервисы следует запретить.

**Таблица 1** – DNS-имена

|  |  |
| --- | --- |
| **Хост** | **DNS-имя** |
| L-CLI | A,PTR: l-cli.skill39.wsr |
| L-SRV | A,PTR: l-srv.skill39.wsr  CNAME: dns.skill39.wsr |
| L-FW | A: l-fw.skill39.wsr  CNAME: vpn.skill39.wsr  CNAME: ftp.skill39.wsr |
| R-FW | A: r-fw.skill39.wsr  CNAME: www.skill39.wsr |
| R-CLI | A: r-cli.skill39.wsr |

**Таблица 2** – Учетные записи LDAP

|  |  |  |  |
| --- | --- | --- | --- |
| **Группа** | **CN** | **Пароль** | **Доступ** |
| Administrators | tux | toor | L-CLI  L-FW |
| Users | user1 – user99 | P@ssw0rd | L-CLI |

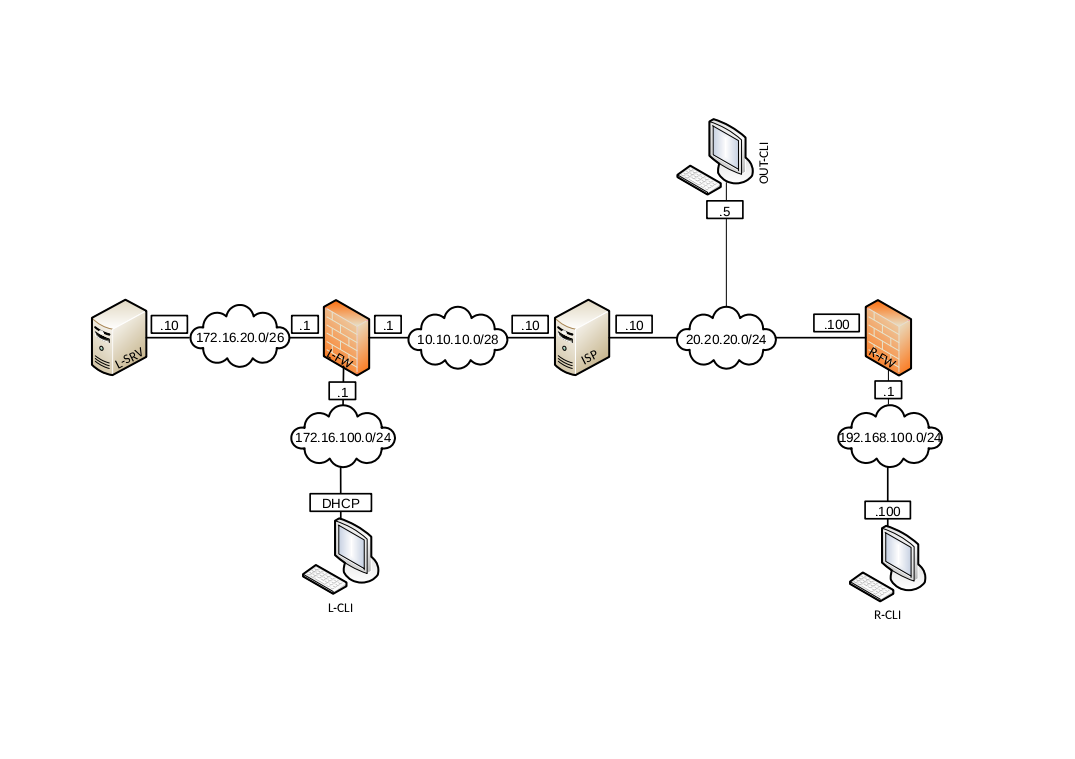
**Таблица 3** – Правила журналирования

|  |  |  |
| --- | --- | --- |
| **Источник** | **Уровень журнала** | **Файл** |
| L-SRV  L-FW | critical | /opt/logs/<HOSTNAME>/crit.log |
| L-SRV | auth.\* | /opt/logs/<HOSTNAME>/auth.log |
| L-FW | \*.err | /opt/logs/<HOSTNAME>/error.log |
| L-CLI  R-CLI | \*.err | /opt/logs/err.log |

\*<HOSTNAME> - название директории для журналируемого хоста

\*\*В директории /opt/logs/ не должно быть файлов, кроме тех, которые указаны в таблице

## ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



**Модуль 2:** Модуль B - Базовая настройка Windows

**Настройка DC1**

**Базовая настройка**

* переименуйте компьютер в DC1;
* перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «10.10.18.х/?». Длину маски рассчитайте исходя из того, чтобы в каждой образовавшейся подсети можно было разместить ровно 14 клиентов. Для адресации в домене Pest.com используйте третью по счету подсеть; в качестве адреса DC1 используйте первый возможный адрес из этой подсети;
* обеспечьте работоспособность протокола ICMP (для использования команды ping).

**Active Directory**

* сделайте сервер контроллером домена Pest.com.

**DHCP**

* настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все не занятые серверами адреса в подсети;
* настройте failover: mode – Load balancer, partner server – SRV1, state switchover – 10 min;
* настройте дополнительные свойства области (адреса DNS-серверов и основного шлюза).

**DNS**

* настройте необходимые зоны прямого и обратного просмотра;
* создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов.

**GPO**

* запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
* в браузерах IE Explorer и Microsoft Edge (установите и используйте windows10.admx) должна быть настроена стартовая страница – www.Pest.com;

**Элементы доменной инфраструктуры**

* создайте подразделения: Experts, Competitors, Managers, Visitors и IT;
* в соответствующих подразделениях создайте доменные группы: Experts, Competitors, Managers, Visitors, IT;

**Внимание! Указанные выше подразделения и группы должны быть созданы в домене обязательно. Если Вы считаете, что для выполнения задания необходимы дополнительные элементы доменной инфраструктуры, Вы можете создать их.**

* создайте пользователей, используя прилагаемый excel-файл (вся имеющаяся в файле информация о пользователях должна быть внесена в Active Directory); поместите пользователей в соответствующие подразделения и группы; все созданные учетные записи должны быть включены и доступны;
* для каждого пользователя создайте автоматически подключаемую в качестве диска U:\ домашнюю папку по адресу SRV1→d:\shares\users;

**Настройка SRV1**

**Базовая настройка**

* переименуйте компьютер в SRV1;
* перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «10.10.18.х/?». Длину маски рассчитайте исходя из того, чтобы в каждой образовавшейся подсети можно было разместить ровно 14 клиентов. Для адресации в домене Pest.com используйте третью по счету подсеть; в качестве адреса SRV1 используйте второй возможный адрес из этой подсети;
* обеспечьте работоспособность протокола ICMP (для использования команды ping);
* присоедините компьютер к домену Pest.com;
* с помощью дополнительных жестких дисков создайте зеркальный массив; назначьте ему букву D:\.

**Active Directory**

* сделайте сервер дополнительным контроллером домена Pest.com.

**DHCP**

* настройте протокол DHCP для автоконфигурации клиентов;
* настройте failover: mode – Load balancer, partner server – DC1, state switchover – 10 min;

**DNS**

* сделайте сервер дополнительным DNS-сервером в домене Pest.com;
* загрузите c DC1 все зоны прямого и обратного просмотра.

**Общие папки**

* создайте общие папки для подразделений (Competitors, Experts and Managers) по адресу SRV1→d:\shares\departments;
* обеспечьте привязку общей папки подразделения к соответствующей группе в качестве диска G:\.

**Квоты/Файловые экраны**

* установите максимальный размер в 1Gb для каждой домашней папки пользователя (U:\);
* запретите хранение в домашних папках пользователей файлов с расширениями .mp3 и .wav; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

**IIS**

* создайте сайт для менеджеров компании (используйте предоставленный htm-файл в качестве документа по умолчанию);
* сайт должен быть доступен по имени managers.pest.com только по протоколу https исключительно для членов группы Managers по их пользовательским сертификатам;

**Настройка DCA**

**Базовая настройка**

* переименуйте компьютер в DCA;
* перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «10.10.18.х/?». Длину маски рассчитайте исходя из того, чтобы в каждой образовавшейся подсети можно было разместить ровно 14 клиентов. Для адресации в домене Pest.com используйте третью по счету подсеть; в качестве адреса DCA используйте третий возможный адрес из этой подсети;
* обеспечьте работоспособность протокола ICMP (для использования команды ping);
* присоедините компьютер к домену Pest.com.

**Службы сертификации**

* установите службы сертификации;
* настройте основной доменный центр сертификации;
* имя центра сертификации – Pest CA;
* срок действия сертификата – 10 лет;
* настройте шаблон выдаваемого сертификата для клиентских компьютеров *ClientComps*: *subject name=common name*, автозапрос для компьютера BRIDGE1;
* настройте шаблон выдаваемого сертификата для группы Managers *ManUsers*: *subject name=common name*, автозапрос только для пользователей – членов группы Managers.

**Настройка CLI1**

**Базовая настройка**

* переименуйте компьютер в CLI1;
* обеспечьте работоспособность протокола ICMP (для использования команды ping);
* присоедините компьютер к домену Pest.com;
* установите набор компонентов удаленного администрирования RSAT;
* запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
* используйте компьютер для тестирования настроек в домене Pest.com: пользователей, общих папок, групповых политик, в том числе – тестирования удаленных подключений через Direct Access (временно переключая компьютер в сеть Internet).

**Настройка DC2**

**Базовая настройка**

* переименуйте компьютер в DC2;
* перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «192.168.19.y/?». Длину маски рассчитайте исходя из того, чтобы в данном пространстве имелось ровно 8 подсетей. Для адресации в поддомене Buda.Pest.com используйте вторую по счету подсеть; в качестве адреса DC2 используйте первый возможный адрес из этой подсети;
* обеспечьте работоспособность протокола ICMP (для использования команды ping).

**Active Directory**

* сделайте сервер контроллером поддомена Buda.Pest.com.

**DHCP**

* настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все не занятые серверами адреса в подсети.

**DNS**

* настройте необходимые зоны прямого и обратного просмотра;
* создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
* обеспечьте разрешение имен сайтов www.pest.com и www.buda.pest.com (оба сайта должны быть доступны со всех клиентских компьютеров сети предприятия).

**GPO**

* настройте необходимые политики, обеспечивающие использование сервера DCA.Pest.com в качестве доверенного центра сертификации.

**Настройка SRV2**

**Базовая настройка**

* переименуйте компьютер в SRV2;
* перед установкой сетевых настроек решите задачу: вам дано адресное пространство следующего вида – «192.168.19.y/?». Длину маски рассчитайте исходя из того, чтобы в данном пространстве имелось ровно 8 подсетей. Для адресации в поддомене Buda.Pest.com
* используйте вторую по счету подсеть; в качестве адреса SRV2 используйте второй возможный адрес из этой подсети;
* обеспечьте работоспособность протокола ICMP (для использования команды ping).

**IIS**

* создайте сайт www.pest.com (используйте предоставленный htm-файл в качестве документа по умолчанию);
* создайте сайт www.buda.pest.com (используйте предоставленный htm-файл в качестве документа по умолчанию);
* оба сайта должны быть доступны по протоколу https с использованием сертификатов, выданных DCA.

**Настройка CLI2**

**Базовая настройка**

* переименуйте компьютер в CLI2;
* обеспечьте работоспособность протокола ICMP (для использования команды ping);
* присоедините компьютер к поддомену Buda.Pest.com;
* запретите использование «спящего режима» таким образом, чтобы пользователи поддомена не могли изменить эту настройку без участия администратора поддомена;
* используйте компьютер для тестирования настроек в поддомене Buda.Pest.com.

**Настройка BRIDGE2**

**Базовая настройка**

* переименуйте компьютер в BRIDGE2;
* задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к inet используйте адрес 200.100.100.1/24; для сетевого адреса в подсети buda.pest.com используйте последний возможный адрес из рассчитанной ранее подсети;
* обеспечьте работоспособность протокола ICMP (для использования команды ping);
* присоедините компьютер к поддомену Buda.Pest.com.

**Настройка RRAS**

* установите службу RRAS;
* настройте VPN-соединение с доменом Pest.com по протоколу PPTP; весь трафик между доменами должен передаваться через это соединение.

**Настройка BRIDGE1**

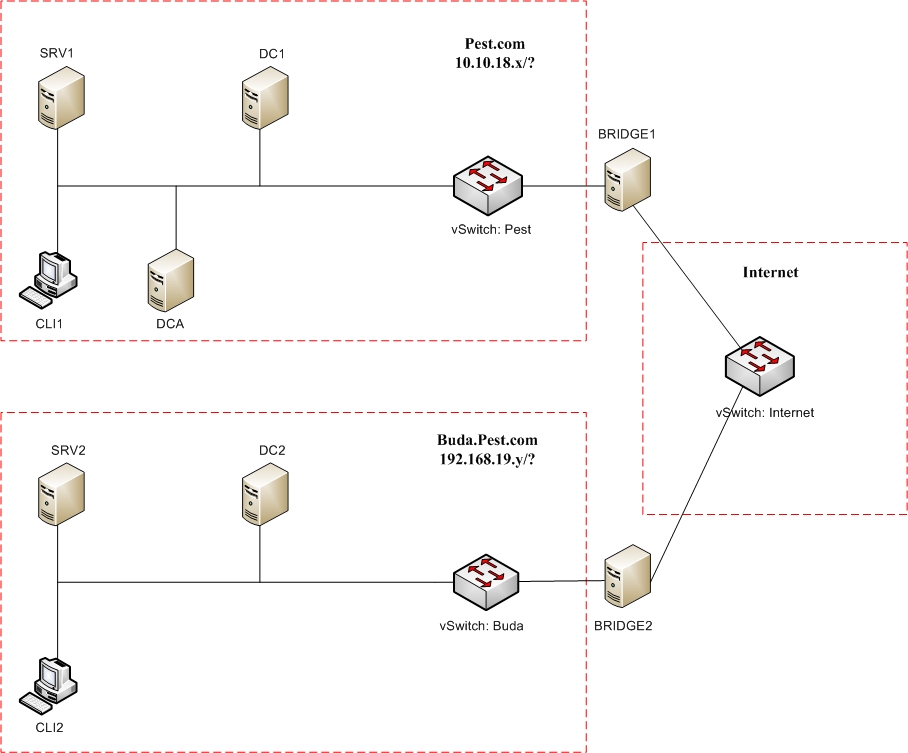
**Базовая настройка**

* переименуйте компьютер в BRIDGE1;
* задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к inet используйте адрес 200.100.50.1/24; для сетевого адреса в подсети pest.com используйте последний возможный адрес из рассчитанной ранее подсети;
* обеспечьте работоспособность протокола ICMP (для использования команды ping);
* присоедините компьютер к домену Pest.com.

**Настройка RRAS**

* установите службу RRAS;
* настройте защищенное VPN-соединение с поддоменом buda.pest.com по протоколу PPTP; весь трафик между доменами должен передаваться через это соединение.

## ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



**Модуль 3:** Модуль C – Базовые сетевые технологии

## Базовая настройка

1. Задайте имя всех устройств в соответствии с топологией.
2. Назначьте для всех устройств доменное имя **wsr2018.ru**.
3. Создайте на всех устройствах пользователей **wsr2018** с паролем **cisco**
   1. Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.
   2. Пользователь должен обладать максимальным уровнем привилегий.
4. На всех устройствах установите пароль **wsr** на вход в привилегированный режим.
   1. Пароль должен храниться в конфигурации НЕ в виде результата хэш-функции.
   2. Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде.
5. Для всех устройств реализуйте модель AAA.
   1. Аутентификация на линиях виртуальных терминалов с 0 по 15 должна производиться с использованием локальной базы учётных записей. (кроме маршрутизатора HQ1)
   2. После успешной аутентификации при удалённом подключении пользователи сразу должен получать права, соответствующие их уровню привилегий или роли (кроме межсетевого экрана FW1).
   3. Настройте необходимость аутентификации на локальной консоли.
   4. При успешной аутентификации на локальной консоли пользователи должны сразу должен получать права, соответствующие их уровню привилегий или роли.
6. На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, подинтерфейсы и интерфейсы типа петля, назначьте IP-адреса.
7. На маршрутизаторе HQ1 на виртуальных терминальных линиях с 0 по 15 настройте аутентификацию с использованием RADIUS-сервера.
   1. Используйте на линиях vty с 0 по 4 отдельный список методов с названием method\_man
   2. Порядок аутентификации:
      1. По протоколу RADIUS
      2. Локальная
   3. Используйте общий ключ **cisco**
   4. Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно
   5. Адрес RADIUS-сервера 172.16.20.2
   6. Настройте авторизацию при успешной аутентификации
   7. Проверьте аутентификацию по протоколу RADIUS при удаленном подключении к маршрутизатору HQ1, используя учетную запись **radius** с паролем **cisco**
8. Все устройства должны быть доступны для управления по протоколу SSH версии **2**.

## Настройка коммутации

1. Для централизованного конфигурирования VLAN в коммутируемой сети предприятия используйте протокол VTP версии **3**.
   1. В качестве основного сервера VTP настройте SW1.
   2. Коммутаторы SW2 и SW3 настройте в качестве VTP клиента.
   3. В качестве домена используйте **wsr2018.ru**
   4. Используйте пароль **VTPPass** для защиты VTP.
   5. Таблица VLAN должна содержать следующие сети:
      1. VLAN100 с именем MGT.
      2. VLAN200 с именем DATA.
      3. VLAN300 с именем OFFICE.
      4. VLAN 400
2. Между всеми коммутаторами настройте транки с использованием протокола IEEE 802.1q.
   1. Порты F0/10 коммутаторов SW1 и SW3, а также порт F0/24 коммутатора SW2 должны быть работать в режиме доступа без использования согласования. Отключите протокол DTP явным образом.
   2. Транк между коммутаторами SW2 и SW3 должен быть настроен без использования согласования. Отключите протокол DTP явным образом.
   3. Транки между коммутаторами SW1 и SW2, а также между SW1 и SW3, должны быть согласованы по DTP, коммутатор SW1 должен инициировать создание транка, а коммутаторы SW2 и SW3 должны ожидать начала согласования параметров от соседа, но сами не инициировать согласование.
3. Настройте агрегирование каналов связи между коммутаторами.
   1. Номера портовых групп:

1 – между коммутаторами SW1 (F0/1-3) и SW2 (F0/1-3);

2– между коммутаторами SW2 (F0/6-7) и SW3 (F0/6-7);

* 1. Агрегированный канал между SW1 и SW2 должен быть организован с использованием протокола согласования LACP. SW1 должен быть настроен в активном режиме, SW2 в пассивном.
  2. Агрегированный канал между SW2 и SW3 должен быть организован с использованием протокола согласования PAgP. SW2 должен быть настроен в предпочтительном, SW3 в автоматическом.

1. Конфигурация протокола остовного дерева:
   1. Используйте протокол Rapid STP.
   2. Коммутатор SW1 должен являться корнем связующего дерева в сетях VLAN 100, 200 и 300, в случае отказа SW1, корнем должен стать коммутатор SW2.
   3. Настройте используемые порты коммутаторов SW1 и SW2 так, чтобы во всех VLAN корнем связующего дерева могли стать только SW1 или SW2, а при получении BPDU пакета с лучшим приоритетом корня, порт должен перейти в состояние root-inconsistent.
   4. Настройте порт F0/10 коммутатора SW2, таким образом, что при включении они сразу переходили в состояние forwarding не дожидаясь пересчета остовного дерева. При получении BPDU пакета данные порты должны переходить в состояние error-disabled.
2. Настройте порты F0/10 коммутаторов SW1, SW2 и порт F0/24 коммутатора SW3, в соответствии с L2 диаграммой. Порты должны быть настроены в режиме доступа.
3. Отключите протокол CDP на маршрутизаторах HQ1 и BR1, только на портах в сторону провайдера ISP1.

## Настройка подключений к глобальным сетям

1. Настройте подключение PPPoE между ISP1 и маршрутизатором BR1.
   1. Настройте PPPoE клиент на BR1.
   2. Используйте имя пользователя **cisco** и пароль **cisco**
   3. Устройства походят **одностороннюю** аутентификацию по протоколу **CHAP**, только ISP1 проверяет имя пользователя и пароль.
   4. BR1 должен автоматически получать адрес от ISP1.
2. Настройте подключение HQ1 к провайдеру ISP1 с помощью протокола PPP.
   1. Настройте Multilink PPP с использованием двух Serial-интерфейсов.
   2. Используйте 1 номер интерфейса.
   3. Не используйте аутентификацию.
   4. HQ1 должен автоматически получать адрес от ISP2.
3. FW1 подключена к провайдеру ISP1 с помощью IPoE и имеет статический адрес.

## Настройка маршрутизации

1. В офисе HQ, на устройствах HQ1 и FW1 настройте протокол динамической маршрутизации OSPF.
   1. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   2. Используйте область с номером 51 для всех сетей центрального офиса.
   3. HQ1 и FW1 должны устанавливать соседство только в сети 172.16.0.12/30.
   4. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
2. Настройте протокол динамической маршрутизации OSPF в офисе BR1 с главным офисом HQ.
   1. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   2. Используйте магистральную область для GRE туннеля.
   3. Соседства между офисами HQ и BR1 должны устанавливаться через защищенный туннель.
   4. В офисе BR1 используйте область с номером 1.
   5. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
3. ISP1 предоставляет подсеть PA (Provider Aggregatable) адресов (11.11.11.11/32) для офиса BR1. На маршрутизаторе BR1 настройте протокол динамической маршрутизации EIGRP с номером автономной системы **2018**.
   1. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   2. Используйте аутентификацию MD5 с помощью связки ключей EIGRP c ключом **WSR** и номером ключа **2**.
   3. Провайдер ISP1 выполняет редистрибуцию маршрута 11.11.11.11/32 в сеть BGP, убедитесь в том, что вы корректно анонсируете данный маршрут провайдеру.
4. Офис HQ имеет подсети PI (Provider Independent) адресов и автономную систему 65000. На маршрутизаторе и межсетевом экране настройте протокол динамической маршрутизации BGP в соответствии с таблицей

|  |  |
| --- | --- |
| Устройство | AS |
| HQ1 | 65000 |
| FW1 | 65000 |
| ISP1 | 65001 |

* 1. Настройте автономные системы в соответствии с Routing-диаграммой.
  2. Маршрутизатор HQ1 и FW1 должны быть связаны с помощью iBGP. Используйте для этого соседства, интерфейсы, которые находятся в подсети 172.16.0.12/30.
  3. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

1. Настройте прокол динамической маршрутизации OSPFv3 поверх защищенного туннеля. На маршрутизаторах HQ1 и BR1 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.
   1. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
   2. Используйте зону с номером **0**.

## Настройка служб

1. В сетевой инфраструктуре сервером синхронизации времени является SRV1. Все остальные сетевые устройства должны использовать в качестве сервера времени HQ1.
   1. Передача данных между HQ1 и SRV1 осуществляется без аутентификации.
   2. Настройте временную зону с названием MSK, укажите разницу с **UTC +3** часов.
   3. Настройте сервер синхронизации времени. Используйте стратум **2**.
   4. Используйте для синхронизации клиентов с HQ1 аутентификацию MD5 с ключом **WSR**.
2. Настройте динамическую трансляцию портов (PAT):
   1. На маршрутизаторе BR1 настройте динамическую трансляцию портов (PAT) для сети 192.168.1.0/24 в адрес петлевого интерфейса 11.11.11.11.
3. Настройте протокол динамической конфигурации хостов со следующими характеристиками
   1. На маршрутизаторе HQ1 для подсети OFFICE:
   2. Адрес сети – 30.30.30.0/24.
   3. Адрес шлюза по умолчанию интерфейс роутера HQ1.
   4. Адрес TFTP-сервера 172.16.20.2.
   5. Компьютер PC1 должен получать адрес 30.30.30.30.

## Настройка механизмов безопасности

1. На маршрутизаторе BR1 настройте пользователей с ограниченными правами.
   1. Создайте пользователя **user1** с паролем **cisco**
   2. Назначьте пользователю **user1** уровень привилегий **5**. Пользователь должен иметь возможность выполнять все команды пользовательского режима, а также выполнять перезагрузку и отладку с помощью команд debug.
2. На коммутаторе SW3 включите DHCP Snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных.
3. На коммутаторе SW3 включите динамическую проверку ARP-запросов в сети OFFICE. Сделайте порт Fa0/11 доверенным.

## Настройка параметров мониторинга и резервного копирования

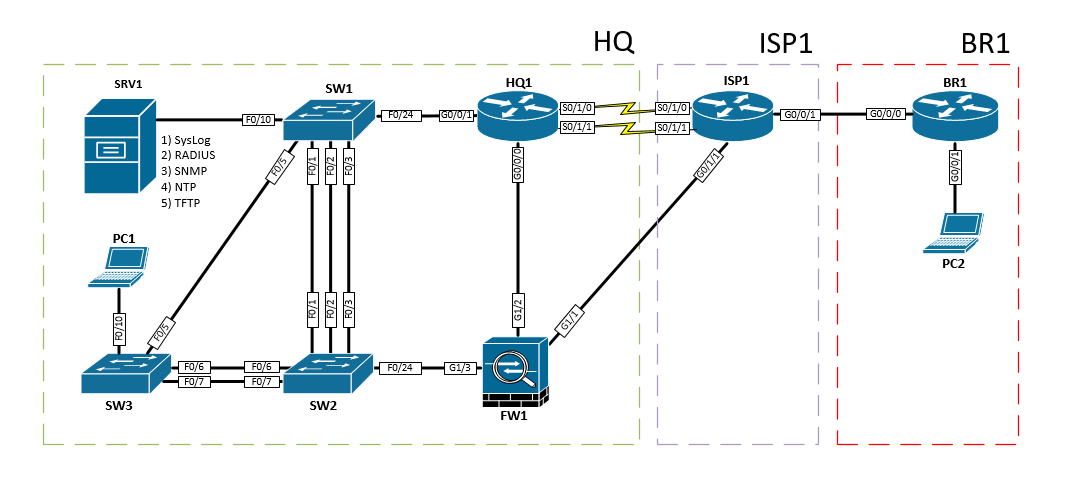
1. На маршрутизаторе HQ1 и межсетевом экране FW1 настройте возможность удаленного мониторинга по протоколу SNMP v3.
   1. Задайте местоположение устройств EKB, Russia
   2. Задайте контакт [admin@wsr.ru](mailto:admin@hitech.ru)
   3. Используйте имя группы WSR.
   4. Создайте профиль только для чтения с именем RO.
   5. Используйте для защиты SNMP шифрование AES128 и аутентификацию SHA1.
   6. Используйте имя пользователя: **snmpuser** и пароль: **snmppass**
   7. Для проверки вы можете использовать команду snmp\_test\_HQ и snmp\_test\_FW на SRV1.

## Конфигурация виртуальных частных сетей

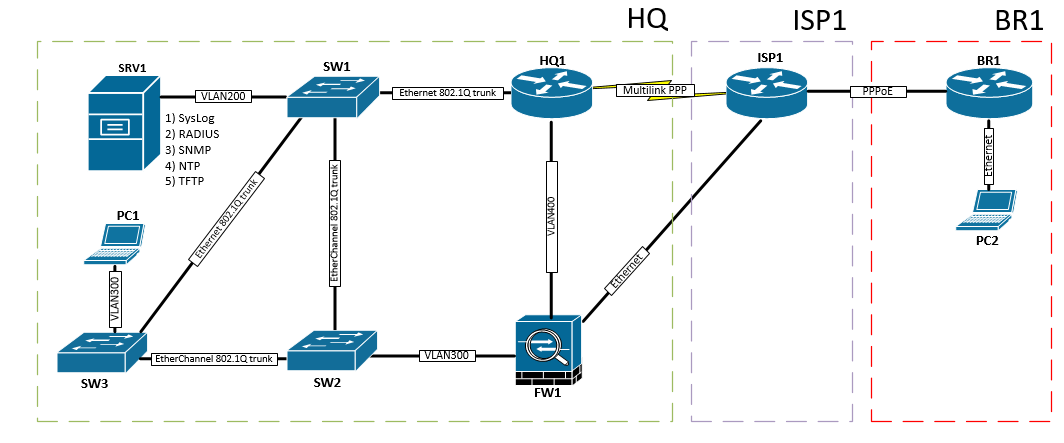
1. На маршрутизаторах HQ1 и BR1 настройте DMVPN:
   1. Используйте в качестве VTI интерфейс Tunnel1
   2. Используйте адресацию в соответствии с L3-диаграммой
   3. Режим — GRE multipoint
   4. Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.
   5. Идентификатор сети – 100.

Аутентификация по ключу cysco

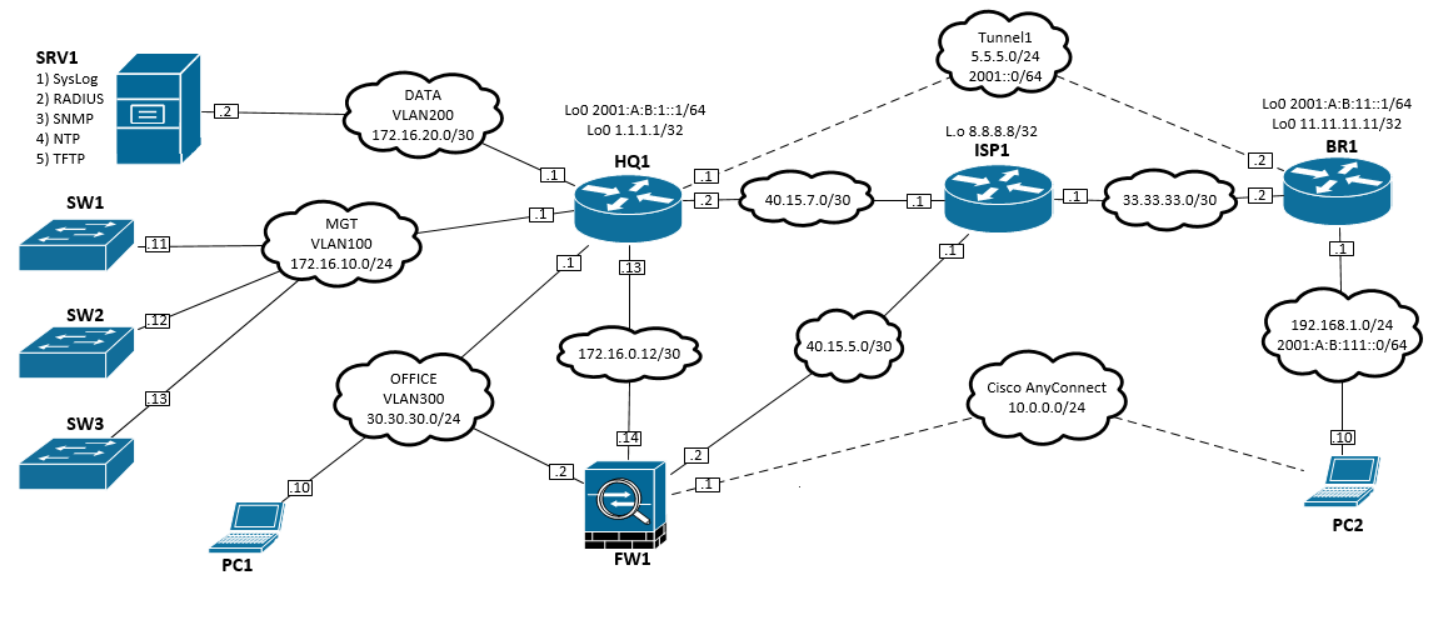
***Топология L1***



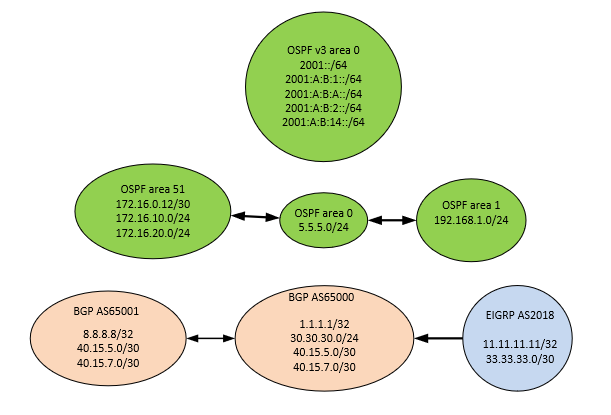
***Топология L2***



***Топология L3***



***Routing-диаграмма***



## 3. Критерии оценки

В данном разделе определены критерии оценки и количество начисляемых баллов (субъективные и объективные) в Таблице 2.

Общее количество баллов задания/модуля по всем критериям оценки составляет \_\_\_.

Таблица 2.

| **Раздел** | **Критерий** | **Оценки** |
| --- | --- | --- |
| **Судейство** | **Объективная** | **Общая** |
| WSSS Sec.6 | Базовая настройка ОС Linux | 0 | 13 | 13 |
| WSSS Sec.6 | Базовая настройка ОС Windows | 0 | 13 | 13 |
| WSSS Sec. 7 | Базовые сетевые технологии | 0 | 13 | 13 |
| WSSS Sec 3, 4 | Базовая настройка ОС Linux  Базовая настройка ОС Windows  Базовые сетевые технологии | 0 | 6 | 6 |
| Итого = | | 0 | 45 | 45 |

**Субъективные оценки -**0.

## 4. НЕОБХОДИМЫЕ ПРИЛОЖЕНИЯ

Нет.