**кОмпетенция**

**«Сетевое и системное администрирование»**

**Конкурсное задание**

**модуль A:**

**Пуско-наладка инфраструктуры   
на основе ОС   
семейства Linux**

**Разработано:**

**Сертифицированным экспертом WSR: Фучко М.М.**

**Сертифицированным экспертом WSR: Силаевым Н.О.**

**Мухаметовым Р.А**

**Дата: 20.06.18**

**Версия: 3**

## Содержание

Данное конкурсное задание состоит из следующих документов\файлов:

1. NC18\_TP39\_Module-A\_RU.docx

## ВВЕДЕНИЕ

Умение работать с системами на основе открытого исходного кода становится все более важным навыком для тех, кто желает построить успешную карьеру в ИТ. Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном, интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

## Описание конкурсного задания

Данное конкурсное задание разработано с использованием различных открытых технологий, с которыми вы должны быть знакомы по сертификационным курсам LPIC и Red Hat. Задания поделены на следующие секции:

* Базовая конфигурация
* Конфигурация сетевой инфраструктуры
* Службы централизованного управления и журналирования
* Конфигурация служб удаленного доступа
* Конфигурация веб- и почтовых служб
* Конфигурация служб хранения данных
* Конфигурация параметров безопасности и служб аутентификации

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна выполнять поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает что работа не будет оценена. Например, для удаленного доступа необходимо настроить IPsec-туннель, внутри которого организовать GRE-туннель. Если, например, вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа.

## Инструкции для участника

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. Например, задание 6 в секции «Базовая конфигурация» предписывает автоматизировать удаленный доступ, который, разумеется, не будет работать без предварительной конфигурации, изложенной в секции «Маршрутизация и удаленный доступ». На вас возлагается ответственность за распределение своего рабочего времени. Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

**Доступ ко всем виртуальным машинам настроен по аккаунту root:toor**.

**Виртуальная машина ISP преднастроена. Управляющий доступ участника к данной виртуальной машине для выполнения задания не предусмотрен. При попытке его сброса возникнут проблемы.**

Организация LEFT включает виртуальные машины: L-SRV, L-FW, L-RTR-A, L-RTR-B, L-CLI-A, L-CLI-B.

Организация RIGHT включает виртуальные машины: R-DMZ, R-FW, R-RTR, R-CLI.

## Необходимое Оборудование, приборы, ПО и материалы

Ожидается, что конкурсное задание выполнимо Участником с привлечением оборудования и материалов, указанных в Инфраструктурном Листе.

В качестве Системной ОС используется **CentOS 17.08**

Вам доступен диск CentOS-7-x86\_64-Everything-1708.iso

Вам доступен диск AdditionalPackages.iso на котором располагаются недостающие RPM пакеты

## Схема оценки

Каждый субкритерий имеет приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в субкритерии.

Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в секции «Базовая конфигурация» предписывается настроить имена для всех устройств, однако этот пункт будет проверен только на одном устройстве и оценен только 1 раз. 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.

Подробное описание методики проверки должно быть разработано экспертами, принимающими участие в оценке конкурсного задания чемпионата, и вынесено в отдельный документ. Данный документ, как и схема оценки, является объектом внесения 30% изменений.

**Конфигурация хостов**

1. Настройте имена хостов в соответствии с **диаграммой.**
2. Установите следующее ПО на **ВСЕ** виртуальные машины:
   1. Пакет tcpdump
   2. Клиент ftp
   3. Клиент lftp
   4. Пакет net-tools
   5. Редактор vim
   6. lynx
   7. dhclient
   8. bind-utils
   9. nfs-utils
3. На хостах сформируйте файл **/etc/hosts** в соответствии с **диаграммой** (кроме адреса хоста L-CLI-A). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет.
4. 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-A и L-CLI-B
   1. В качестве DHCP-сервера организации LEFT используйте L-RTR-A
      1. Используйте пул адресов 172.16.100.60 — 172.16.100.75 для сети L-RTR-A
      2. Используйте пул адресов 172.16.200.60 — 172.16.200.75 для сети L-RTR-B
      3. Используете адрес L-SRV в качестве адреса DNS-сервера
   2. Настройте DHCP-сервер таким образом, чтобы L-CLI-B всегда получал фиксированный IP-адрес в соответствии с **диаграммой.**
   3. В качестве шлюза по умолчанию используйте адрес интерфейса соответствующего маршрутизатора в локальной сети
   4. Используйте DNS-суффикс **skill39.wsr**
   5. DNS-записи типа A соответствующего хоста должны обновляться при получении им адреса от DHCP-сервера.
3. На L-SRV настройте службу разрешения доменных имен
   1. Сервер должен обслуживать зону **skill39.wsr**
   2. Сопоставление имен организовать в соответствии с **Таблицей 1**
   3. Настройте на R-DMZ роль вторичного DNS сервера для зоны **skill39.wsr**
      1. Используете адрес R-DMZ в качестве адреса DNS-сервера для R-CLI
   4. Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS-серверу ISP
   5. Реализуйте поддержку разрешения обратной зоны.
   6. Файлы зон располагать в **/opt/dns/**
   7. Сервер L-FW должен перенаправлять внешние DNS запросы от OUT-CLI на L-SRV.
      1. Важно преобразовывать только [www.skill39.wsr](http://www.skill39.wsr/) во внешний адрес R-FW
   8. Делегируйте поддомен ext.skill39.wsr серверу ISP.
4. На L-FW настройте интернет-шлюз для организации коллективного доступа в интернет. Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса.
   1. Организуйте доступность сервиса DNS на L-SRV по внешнему адресу L-FW.

**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. OU создать в соответствии с **Таблицей 2**
   4. L-CLI-A и L-CLI-B должны аутентифицироваться через LDAP
   5. Только OU «Admin» и «Guest» могут аутентифицироваться на клиентах
2. Реализуйте централизованное хранение домашних каталогов пользователей LDAP
   1. Сервером домашних каталогов выступает L-SRV
   2. Хранение домашних каталогов выполнять в /opt/homes/
   3. Определите квоту на хранение в 10 MB
   4. Доступ к каталогам осуществлять по протоколу NFS
3. На L-SRV организуйте централизованный сбор журналов с хостов L-CLI-A, L-CLI-B, L-FW и L-SRV
   1. Журналы должны храниться в директории **/opt/logs/**
   2. Журналирование должно производится в соответствии с **Таблицей 3.**
   3. Размеры файлов логов не должны превышать **10Кб**.
   4. Должна быть настроена циклическая запись журналов

**Конфигурация служб удаленного доступа**

1. На L-FW 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 L-FW
   4. Должна быть реализована аутентификация средствами LDAP-сервера, развернутого на L-SRV
      1. Только LDAP-пользователи в OU «VPN» должны получать доступ к VPN-службе
   5. В качестве адресного пространства подключаемых клиентов использовать сеть 5.5.5.0/24
      1. Обеспечить присвоение закрепленных адресов в соответствии с **диаграммой.**
   6. 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**
      1. Скрипт принимает на вход следующие параметры(последовательно):
         1. Имя пользователя OpenVPN
         2. Пароль в открытом виде
      2. Автоматизация отключения VPN-туннеля не требуется
      3. Скрипт должен располагаться в **/opt/vpn**.
      4. Скрипт должен вызываться из любого каталога без указания пути
      5. Используйте следующий путь для расположения файла скрипта **/opt/vpn/start\_vpn.sh**
3. Настройте защищенный канал передачи данных между L-FW и R-FW с помощью технологии IPSEC:
   1. Параметры политики первой фазы IPSec:
      1. Проверка целостности SHA-1
      2. Шифрование 3DES
      3. Группа Диффи-Хелмана — 7
      4. Аутентификация по общему ключу WSR-2018
   2. Параметры преобразования трафика для второй фазы IPSec:
      1. Протокол ESP
      2. Шифрование DES
      3. Проверка целостности SHA-1
   3. В качестве трафика, разрешенного к передаче через IPsec-туннель, должен быть указан только GRE-трафик между L-FW и R-FW
4. 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
5. Настройте динамическую маршрутизацию по протоколу OSPF с использованием пакета Quagga:
   1. Анонсируйте все сети, необходимые для достижения полной связности
   2. Используйте зону с номером 0
   3. Применение статических маршрутов не допускается
   4. В обмене маршрутной информацией участвуют L-RTR-A, L-RTR-B, R-RTR, L-FW и R-FW
   5. Соседство и обмен маршрутной информацией между L-FW и R-FW должно осуществляться исключительно через настроенный GRE-туннель
   6. Анонсируйте сети локальных интерфейсов L-RTR-A и L-RTR-B.
6. 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**
7. 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- и почтовых служб**

1. На R-DMZ установите и настройте веб-сервер apache:
   1. Настройте веб-сайт для внешнего пользования www.skill39.wsr
      1. Используйте директорию **/var/www/html/out**
      2. Используйте порт 8088
   2. Настройте веб-сайт для внутреннего пользования intra.skill39.wsr
      1. Используйте директорию **/var/www/html/intra**
      2. Доступ разрешен только для OU “webusers”
2. На R-FW настройте пакет HAProxy
   1. Сайт www.skill39.wsr должен быть доступен из внешней сети по внешнему адресу R-FW
   2. Настройте SSL

**Конфигурация служб хранения данных**

1. Создайте LVM-том на R-RTR и разместите на нём каталог **/opt/lvm**
   1. Виртуальные диски для размещения LVM-тома создайте самостоятельно
   2. Обеспечьте создание снапшотов по расписанию раз в час с именем <Date>.<Time>
      1. Убедитесь, что на время проверки хотя бы один снапшот создан
2. Реализуйте распределенное DFS-хранилище
   1. DFS-корень расположить на L-SRV, каталог **/opt/dfs/**
   2. Клиентские разделяемые ресурсы смонтировать в **/opt/dfs**
      1. В качестве имени разделяемого ресурса использовать hostname клиента.
   3. Использовать real linking
   4. Клиенты организуют общий доступ к каталогу **/opt/smb**
   5. Аутентификацию пользователей проводить по протоколу LDAP
      1. Доступ разрешен только OU «Guest»

**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 сетей в **Internal**
   2. Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора L-FW
   3. Разрешите необходимый трафик для создания IPSec и GRE туннелей между организациями
   4. Разрешите SSH подключения на соответствующий порт
   5. Для VPN-клиентов должен быть предоставлен полный доступ к сети **Internal**
   6. Разрешите необходимый трафик к серверам L-SRV и R-DMZ по транслированным IP-адресам
   7. Настройте ограничение доступа к сайту www.skill39.wsr при подключении по Remote-Access VPN. Разрешите доступ только к intra.wsr.right
   8. Остальные сервисы следует запретить.
      1. В отношении входящих (из внешней сети) ICMP запросов поступать по своему усмотрению

**Таблица 1** – DNS-имена

|  |  |
| --- | --- |
| **Хост** | **DNS-имя** |
| L-CLI-A | A: l-cli-a.skill39.wsr |
| L-CLI-B | A: l-cli-b.skill39.wsr |
| L-RTR-A | A: l-rtr-a.skill39.wsr |
| L-RTR-B | A: l-rtr-b.skill39.wsr |
| L-SRV | A: l-srv.skill39.wsr  CNAME: server.skill39.wsr  CNAME: center.skill39.wsr |
| L-FW | A: l-fw.skill39.wsr  CNAME: vpn.skill39.wsr |
| R-FW | A: r-fw.skill39.wsr  CNAME: www.skill39.wsr |
| R-DMZ | A: r-dmz.skill39.wsr  CNAME: intra.skill39.wsr |
| R-RTR | A: r-rtr.skill39.wsr |
| R-CLI | A: r-cli.skill39.wsr |

**Таблица 2** – Учетные записи LDAP

|  |  |  |  |
| --- | --- | --- | --- |
| **OU** | **CN** | **Пароль** | **Доступ** |
| Admin | tux | toor | На все хосты полный |
| Guest | user1 – user99 | P@ssw0rd | только на клиентские хосты |
| VPN | vpn1 – vpn99 | Passw0rd | только для VPN |
| webuser | webuser1 – webuser99 | P@ssword | только для доступа к сайту intra.skill39.wsr |

**Таблица 3** – Правила журналирования

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

