Конкурсное задание

КОМПЕТЕНЦИЯ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Модули задания и необходимое время
4. Критерии оценки
5. Необходимые приложения

Количество часов на выполнение задания: 10 ч.

1) ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

2) ЗАДАНИЕ ДЛЯ КОНКУРСА

Данное конкурсное задание разработано с использованием различных технологий, входящих в сертификационные программы LPIC, Red Hat, CCNA, CCNP, MCSA.

Совместное использование этих технологий представляет собой достаточно сложную инфраструктуру. Требования в задании представлены в общем виде, конкретный метод выполнения и технологии, необходимые для его реализации, вы вправе выбрать самостоятельно с учётом указанных в задании требований.

Можно заметить, что многие технологии должны работать в связке или поверх других. Например, динамическая маршрутизация должна выполняться 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 вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа.

Главной задачей является получение работоспособной системы в том или ином виде, а также её ежедневная доработка и улучшение.

Окончательная методика проверки уточняются членами жюри. Оценка производится в отношении работы модулей. Если участник конкурса не выполняет требования техники безопасности, подвергает опасности себя или других конкурсантов, такой участник может быть отстранен от конкурса.

Время и детали конкурсного задания в зависимости от конкурсных условий могут быть изменены членами жюри, по согласованию с менеджером компетенции.

Процедура оценки результатов выполнения задания будет производиться в конце каждого конкурсного дня, причем оцениваться будут именно те технологии, работоспособность которых ожидается по окончании текущего конкурсного дня. Участники могут выполнять задачи «на будущее», но им следует быть уверенными, что при этом не нарушается работоспособность технологий текущего конкурсного дня. Например, в первый день необходимо настроить веб-сервер, работающий по протоколу HTTP, а в третий день включить перенаправление на HTTPS. Если участники включат перенаправление на HTTPS в первый день, то они, скорее всего, могут не получить баллов за работу протокола HTTP в конце первого дня.

Задания разработаны и протестированы группой сертифицированных экспертов:

1) Ф.А. Казаков
2) М.А. Афанасьев
3) М.М. Фучко
4) Д.Н. Новиков
5) Д.С. Лавров
6) А.Г. Уймин

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 2.

Таблица 2 – Время выполнение модуля

№ п/п	Наименование модуля	Время на задание	День
1	Комплексное задание по пуско-наладке инфраструктуры. Модуль А: Пусконаладка сетевой инфраструктуры на базе ОС семейства Linux, Модуль В: Пусконаладка сетевой инфраструктуры на базе ОС семейства Windows, Модуль С: Пусконаладка телекоммуникационного оборудования»	5 ч.	1
2	Комплексное задание по пуско-наладке инфраструктуры. Модуль А: Пусконаладка сетевой инфраструктуры на базе ОС семейства Linux, Модуль В: Пусконаладка сетевой инфраструктуры на базе ОС семейства Windows, Модуль С: Пусконаладка телекоммуникационного оборудования»	5 ч	2

Базовая настройка:

1. Настройте имена всех сетевых устройств, виртуальных машин и серверов в соответствии с диаграммой.
2. Сконфигурируйте доменные имена на сетевом оборудовании, используйте имя домена skill39.msk.
3. На всех серверах Linux и сетевом оборудовании создайте пользователя Admin с паролем PaSsWoRd.
    a. Для сетевого оборудования пароль должен быть регистрочувствительным и хранится в виде результата хэш функции
    b. На Linux серверах обеспечьте возможность использования sudo только для группы Admins, а также локального пользователя Admin. Отключите необходимость дополнительной аутентификации для использования sudo.
    c. Ограничьте локальный вход пользователя root только пятым виртуальным терминалом.
4. В качестве пароля для входа в привилегированный режим используйте WSR
5. Организуйте удаленный доступ до всего сетевого оборудования, а также до серверов и виртуальных машин с ОС Linux по протоколу SSH второй версии. Разрешите доступ всем пользователям, включая пользователя root.
6. Разрешите удаленный доступ по протоколу RDP для машин под управлением ОС Windows Server только группам Workers и администраторам домена.
7. Отключите все неиспользуемые порты на сетевых устройствах

Конфигурация активного сетевого оборудования:

1. Таблица VLAN на сетевых устройствах должна соответствовать:
    a. VLAN 1010 - WIN
    b. VLAN 1011 - LIN
    c. VLAN 50 – Clients
    d. VLAN 999 – Trunk
    e. VLAN 6 – MGMT
    f. VLAN 666 - ISP
2. Настройте передачу тегированного трафика между коммутаторами. В качестве Native VLAN используйте VLAN999.
3. Сконфигурируйте Management адреса на коммутаторах. В качестве подсети используйте 10.0.100.0/24, адреса сконфигурируйте на ваше усмотрение
4. Используйте адресацию основываясь на диаграммах.
5. Настройте магистральные каналы в соответствии с диаграммой L2
    a. Явно отключите протокол DTP.
6. Сконфигурируйте портовые группы в соответствии с диаграммой L2
    a. SW3 должен быть активным для обоих портовых групп. Протокол динамического согласования на ваше усмотрение.
    b. Сконфигурируйте портовую группу между S1 и S2 без использования протоколов согласования
    c. настройте балансировку нагрузки по MAC адресу назначения для каждой из портовых групп
7. Настройте протокол остовного дерева для защиты от петель на канальном уровне
    a. Используйте реализацию протокола 802.1w.
    b. Расставьте приоритеты, чтобы порядок выбора корневого моста был в следующем порядке S3 -> S1 -> S2.

c. Сконфигурируйте порты f0/4 и f0/1 коммутатора S3 таким образом, чтобы порты сразу переходили в состояние forwarding, не дожидаясь пересчета остовного дерева.

8. Настройте протокол LLDP таким образом, чтобы передача сообщений была возможна только на портах между коммутаторами, а прием сообщений - на всех используемых портах.
9. Настройте DHCP сервер:
    a. На R1 и R2 для сетей WIN и LIN соответственно, в качестве адреса шлюза используйте адреса из соответствующей сети, в качестве DNS сервера используйте адреса DC и FS
    b. Исключите из выдачи адреса шлюзов и серверов
10. Для подключения R1 к провайдеру ISP сконфигурируйте PPP
    a. ISP выступает в роли PPP сервера
    b. R1 Выступает в роли PPP клиента
    c. Используйте адреса в соответствии с L3 диаграммой
    d. Настройте двустороннюю аутентификацию по паролю pppass
    e. R1 должен получать адрес автоматически
11. Для подключения R2 к провайдеру ISP настройте L2TP
    a. Используйте адреса в соответствии с L3 диаграммой
    b. В качестве сервера используется ISP, в качестве клиента R2
    c. Сконфигурируйте MTU 1400
    d. Настройте одностороннюю защищенную аутентификацию. Только ISP должен аутентифицировать R2.
        i. В качестве логина используйте l2user
        ii. В качестве пароля используйте l2pass
    e. Транспортные адреса сконфигурируйте на свое усмотрение. Туннельные в соответствии с диаграммой
12. Взаимодействие с ISP осуществляется через VLAN 50
13. Настройте протокол динамической маршрутизации BGP для связи с провайдерами

a. Сконфигурируйте автономные системы в соответствии с таблицей 2.
b. Сконфигурируйте отношения соседства между провайдером и пограничными маршрутизаторами филиалов
c. ISP должен распространять маршрут по умолчанию обоим роутерам
d. Анонсировать сети необходимо только на ISP. На других устройствах требуется анонсировать только Loopback интерфейсы.

14. Для сетей WIN и LIN обеспечьте возможность выхода в Internet
15. Настройте DNS сервер на ISP для разрешения имени vpn.skill39.msk и www.skill39.msk во внешний адрес R2
16. Обеспечьте маршрутизацию между внутренними сетями посредством протокола EIGRP на маршрутизаторах R1 и R2
    a. Анонсируйте все сети, необходимые для достижения полной связанности
    b. Соседство должно устанавливаться только через сеть R1R2, остальные порты необходимо перевести в пассивный режим
17. Сконфигурируйте DHCP для клиентов Student и Teacher
18. Для обеспечения связанности между офисами, сконфигурируйте GRE туннель. Используйте адресацию в соответствии с диаграммой, защита туннеля в текущий день не требуется
19. На маршрутизаторе R1 сконфигурируйте ролевую модель разграничения прав
    a. Создайте пользователей user1, user2 и superuser
    b. Для пользователя user1 создайте контекст, при входе в который пользователю доступны команды ping, traceroute, sh ip interface brief
    c. Для пользователя user2 создайте контекст, при входе в который пользователю доступны все команды debug, команда reload, и настройка интерфейса lo123.
    d. Создайте superview контекст для пользователя superuser, объединяющий эти два контекста.
    e. Каждый пользователь при входе должен попадать в свой контекст.

Настройка серверов под управлением Windows

1. Сконфигурируйте домен skill39.msk
    a. Контроллером домена является DC.
    b. Введите в домен машины FS, RDS и CLI.
    c. Настройте вторым контроллером FS, но без роли глобального каталога.
    d. Контроллер FS должен быть в режиме контроллера домена только для чтения. Разрешите кэширование паролей группы Admins.
2. Сконфигурируйте службу DNS

    a. Создайте необходимые A и CNAME записи. Обеспечьте возможность получения доступа до всех сетевых устройств и виртуальных машин с использованием имен.

    b. Настройте запрет на использование нелатинских символов.

3. Создайте организационные подразделения, группы и пользователей в соответствии с таблицей 3. В качестве пароля для каждого пользователя используйте P@$$w0rd.
    a. Создайте резервную копию пользователей в CSV файле, файл сохраните как users_backup.csv на рабочем столе.
    b. Следует экспортировать все параметры каждого пользователя.
4. Для пользователей группы безопасности Admins сконфигурируйте обязательную минимальную длину пароля: 12 символов.
5. На сервере FS создайте программный RAID 5 из 4 дополнительных дисков емкостью по 1 ГБ, назначьте дисковому массиву букву F
6. Используйте диск F для хранения необходимых общих каталогов
    a. Для пользователей домена группы Admins обеспечьте монтирование домашнего каталога в качестве диска H

    b. Для всех остальных пользователей (кроме группы Admins) обеспечьте монтирование домашнего каталога в качестве диска N

    c. Запретите хранение исполняемых файлов и определите квоту в 1 ГБ для каждого пользователя

    d. Пользователи не должны видеть чужие каталоги через коневую папку и иметь доступа к ним по прямой ссылке.

7. Для всех пользователей группы Workers создайте общую папку
    a. Обеспечьте автоматическое монтирование папки в качестве диска W
    b. Другие пользователи при попытке доступа к каталогу должны получать сообщение “Restricted! Only for office workers!!!”
8. Сконфигурируйте общий каталог для группы Admins
    a. Обеспечьте автоматическое монтирование папки в качестве диска A
    b. Другие пользователи при попытке доступа к каталогу должны получать сообщение “Restricted! Only for Administrators!!!”

9. На сервере FS настройте web-сервер IIS
    a. Сервер должен работать на порту 80 по протоколу http и доступен по имени www.skill39.msk
    b. В качестве стартовой страницы создайте документ index.html с содержимым:

```
<html><body><br><br><br>
        <center><h1><p>Welcome to Moscow!!!</h1></center>
</body></html>
```

Настройка серверов под управлением Linux

1. На сервере MON созданы 5 дополнительных дисков по 1ГБ
    a. Объедините их в RAID 6
    b. Разметьте том как ext4
    c. Обеспечьте автоматическое монтирование тома в директорию /opt Монтирование должно производится автоматически при загрузке системы
2. На MON Сконфигурируйте файловое хранилище по протоколу smb
    a. В качестве корневой директории используйте /opt/samba
    b. В качестве имени общего ресурса используйте имя Samba
    c. Обеспечьте доступ к хранилищу под доменными учетными записями только для пользователей группы Admins
    d. Запретите анонимный доступ
3. Сервера MON и VPN должны быть членами домена skill39.msk
    a. Настройте аутентификацию с использованием доменных реквизитов
    b. Доступ к sudo имеет только группа Admins и локальный пользователь Admin
    c. Обеспечьте возможность доступа по SSH под доменными учетными записями

d. При физическом доступе вход под доменной учетной записью возможен только на 1 виртуальном терминале

4. На сервере WEB настройте NGINX Reverse Proxy
   a. В качестве бэкэнда используйте веб сайт на FS
   b. Сайт должен быть доступен из внешней сети, по внешнему адресу www.skill39.msk
   c. Реализуйте кэширование. Кэширование успешных запросов должно выполнятся в течении минуты.
5. На сервере WEB настройте web-сервер NGINX
   a. Сервер должен работать на порту 80 по протоколу http
   b. В качестве стартовой страницы создайте документ index.html с содержимым:

```
<html><body><br><br><br>

                    <center><h1><p>Coming soon!<br>
          <a style="color:mediumvioletred">elearn.skill39.msk</h1></center>

</body></html>
```

   c. Сайт должен быть доступен по имени elearn.skill39.msk
   d. При попытке доступа по IP адресу пользователь должен получить ошибку 404
6. На сервере VPN создайте центр сертификации.
   a. Имя центра должно быть Central CA, остальные параметры и атрибуты на ваше усмотрение
   b. Корень CA должен быть в папке /etc/ca/
   c. Все сертификаты необходимые во втором дне должны быть выписаны данным центром сертификации
   d. Все виртуальные машины должны доверять CA

Технологии, работоспособность которых ожидается во второй день:

Конфигурация активного сетевого оборудования

1. Настройте модель AAA на всех сетевых устройствах.
    a. Аутентификация должна производится с использованием доменных реквизитов
    b. Аутентифицироваться могут пользователи групп Netadmins и Workers
    c. После успешной аутентификации Netadmins должны получать максимальный уровень привилегий, а Workers должны иметь доступ только к командам show *
    d. Обеспечьте возможность доступа с использованием локальной базы данных учетных записей при доступе через консоль. При доступе по SSH должны использоваться только доменные реквизиты.
    e. Обеспечьте возможность доступа на ISP с использованием локальный базы данных.
2. На R2 настройте удаленный доступ до веб-сервера
    a. При SSH подключении на внешний адрес и порт 31337 пользователь должен попадать на 22 порт сервера WEB
3. Настройте защиту от атак из внешней сети методом перебора пользователя SSH на R1 и R2
    a. Если произошло 3 неудачных попытки входа по SSH в течении 30 секунд, маршрутизатор должен быть заблокирован на 2 минуты
    b. Настройте задержку в 10 секунд между попытками входа
    c. Настройте логирование всех неудачных попыток подключения
    d. Отключите возможность удаленного подключения по всем протоколам, кроме SSH
4. Все сетевые устройства кроме R1 и R2 должны логировать сообщения уровня Informational и отправлять их на Splunk
5. Сконфигурируйте резервное копирование конфигурации R2 на TFTP сервер MON
    a. Резервное копирование должно производится при каждом сохранении конфигурации
    b. В качестве имени файла используйте <hostname>-<time>.cfg

6. На всех коммутаторах реализуйте защиту от подмены DHCP сервера для подсети VLAN50. Необходимые порты сделайте доверенными. Установите для каждого порта ограничение на 150 пакетов в секунду
7. На всех коммутаторах реализуйте динамическую проверку ARP запросов в сети VLAN50
8. На R1 и R2 настройте IP SLA
    a. Тип ICMP
    b. Адрес 8.8.8.8
    c. Таймаут 3 секунд
    d. Частота 5
    e. При потере соеденения в консоль должно выводится сообщение “Internet is down”
9. Сконфигурируйте проприетарный протокол исследования сети канального уровня таким образом, чтобы прием и передача сообщений были возможны только на магистральных каналах. На всех остальных портах протокол следует отключить
    a. Отключите данный протокол на роутерах в сторону провайдера
10. Сконфигурируйте проброс портов таким образом, чтобы была возможна работа с сервисом openvpn и сайтом www.skill39.msk из внених сетей
11. Обеспечьте защиту GRE тунеля
    a. Используйте ikev2
    b. Аутентификация должна происходить на основе цифровых сертификатов, выпущенных на сервере VPN.
    c. Остальные параметры произвольные.

Конфигурация серверов под управлением ОС Windows

1. На всех виртуальных машинах, серверах и сетевых устройствах настроить службу NTP
    a. DC должен являться NTP сервером с временной зоной UTC +3 Moscow
2. На сервере RDS:
    a. Установите роль Удаленных рабочих столов (RDS) в режиме сессий
    b. Опубликуйте приложения notepad и Internet Explorer для пользователей группы Workers
    c. Обеспечьте работу веб-интерфейса rds.skill39.msk по протоколу HTTPS без ошибок и предупреждений
    d. Обеспечьте SSO (вход без повторного ввода логина и пароля) как при запуске приложения, так и открытии веб-интерфейса
    e. При подключении к сессии с программой notepad не должно возникать никаких ошибок или предупреждений
    f. Положите ярлык для входа в приложение на рабочий стол всех пользователей группы Workers
3. В случае обычного входа пользователя в систему в качестве стартовой страницы в IE должен открываться сайт https://rds.skill39.msk, а в случае подключения пользователя посредством Remote Desktop Connection в качестве стартовой страницы в IE должен открываться сайт https://www.skill39.msk
4. Настройте роль NPS сервера на контроллере домена для аутентификации и авторизации сетевых устройств по протоколу RADIUS
5. Включите аудит удачных и неудачных попыток входа(Logon), а также при выходе(Logoff)
6. Настройте эмуляцию интернет соединения для всех клиентов windows
7. Настройте перенаправление каталогов Documents и Desktop в директорию FS-W: D:\Shares\Redirected для всех пользователей группы Workers
8. На всех клиентских ПК обоих доменов обеспечьте возможность входа только в рабочее время (9:00-23:00) для группы Workers

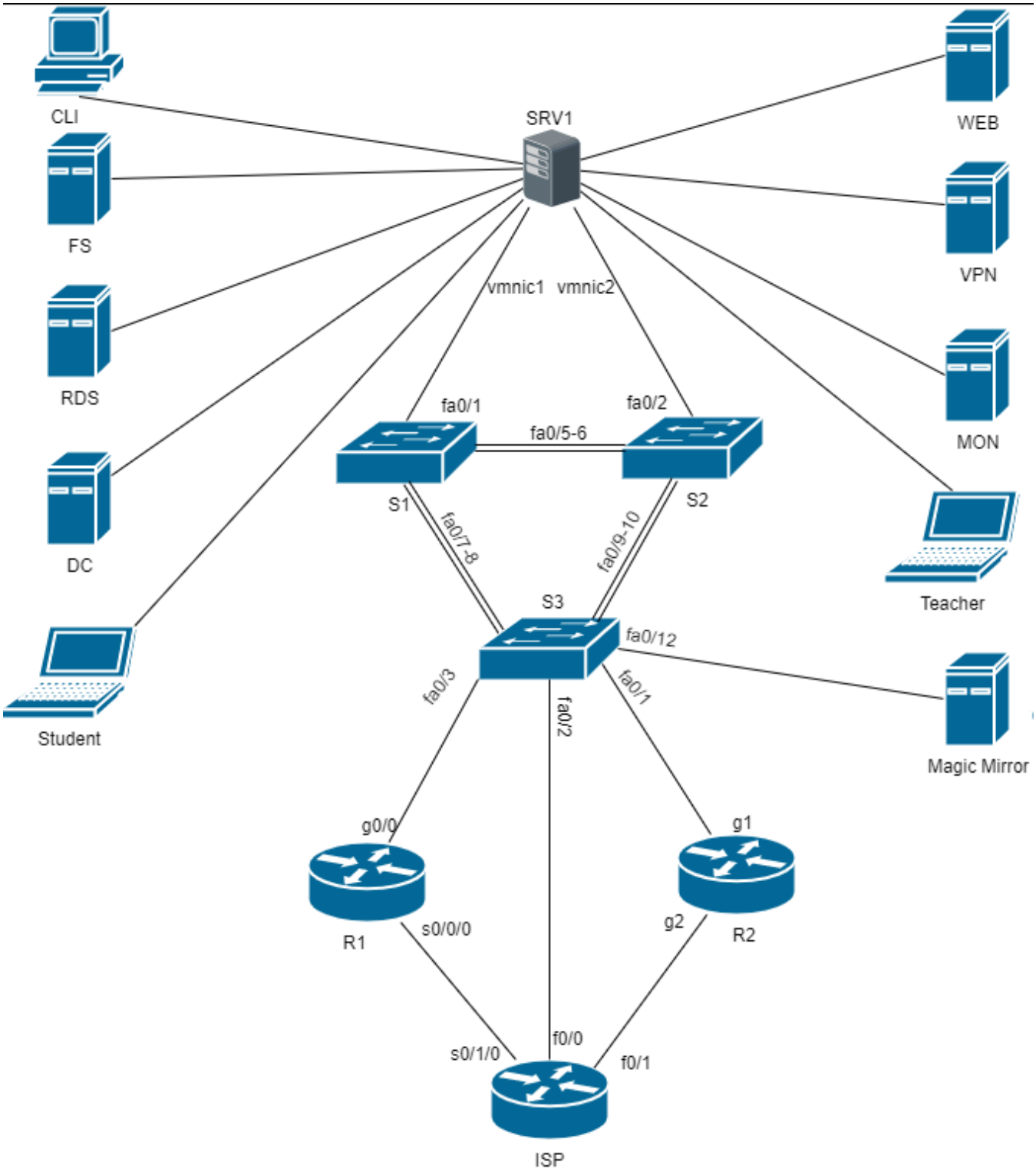
Конфигурация серверов под управлением ОС Linux

1. На сервере WEB для сайтов www.skill39.msk и elearn.skill39.msk сконфигурируйте SSL и автоматическое перенаправление на HTTPS
2. Установите и настройте Splunk Enterprise на сервере MON
    a. Обеспечьте доступ по доменным учетных записям. Пользователи групп Admins и Netadmins должны иметь полный доступ
    b. Все сетевые устройства и машины должны отправлять логи на Splunk, кроме ISP, Student и Teacher
    c. Обеспечьте доступ к Splunk по адресу splunk.skill39.msk, по протоколу https.
    d. Создайте Dashboard для просмотра логов, внутри которого создайте три панели:
        i. Для устройств под управление Windows из сети WIN, назовите панель WIN
        ii. Для устройств под управление Linux из сети LIN, назовите панель LIN
        iii. Для сетевых устройств, назовите панель NET
3. Сконфигурируйте SSH на сервере MON
    a. Запретите использование пустых паролей
    b. Разрешите открытие не более 5 SSH подключений в течении 120 секунд
    c. Если подключение не активно в течении 5 минут, оно должно быть разорвано
    d. Обеспечьте аутентификацию с использованием ключей для пользователя root на машине Teacher
        i. Защитите ключи для пользователя root при помощи пароля P@ssw0rd_t00r
4. На сервере WEB настройте FTP сервер
    a. В качестве корневой директории используйте директорию с веб сайтом
    b. В качестве пользователя используйте wwwuser с паролем wwwpass
    c. Доступ должен производится для чтения и записи
    d. Произведите необходимые настройки на R2 для доступа к FTP из внешней сети.
5. На сервере MON сконфигурируйте tftp сервер
    a. В качестве корневой директории используйте /opt/backup
6. На сервере VPN установите и настройте OpenVPN
    a. Используйте сеть 10.0.10.0/24 для клиентов

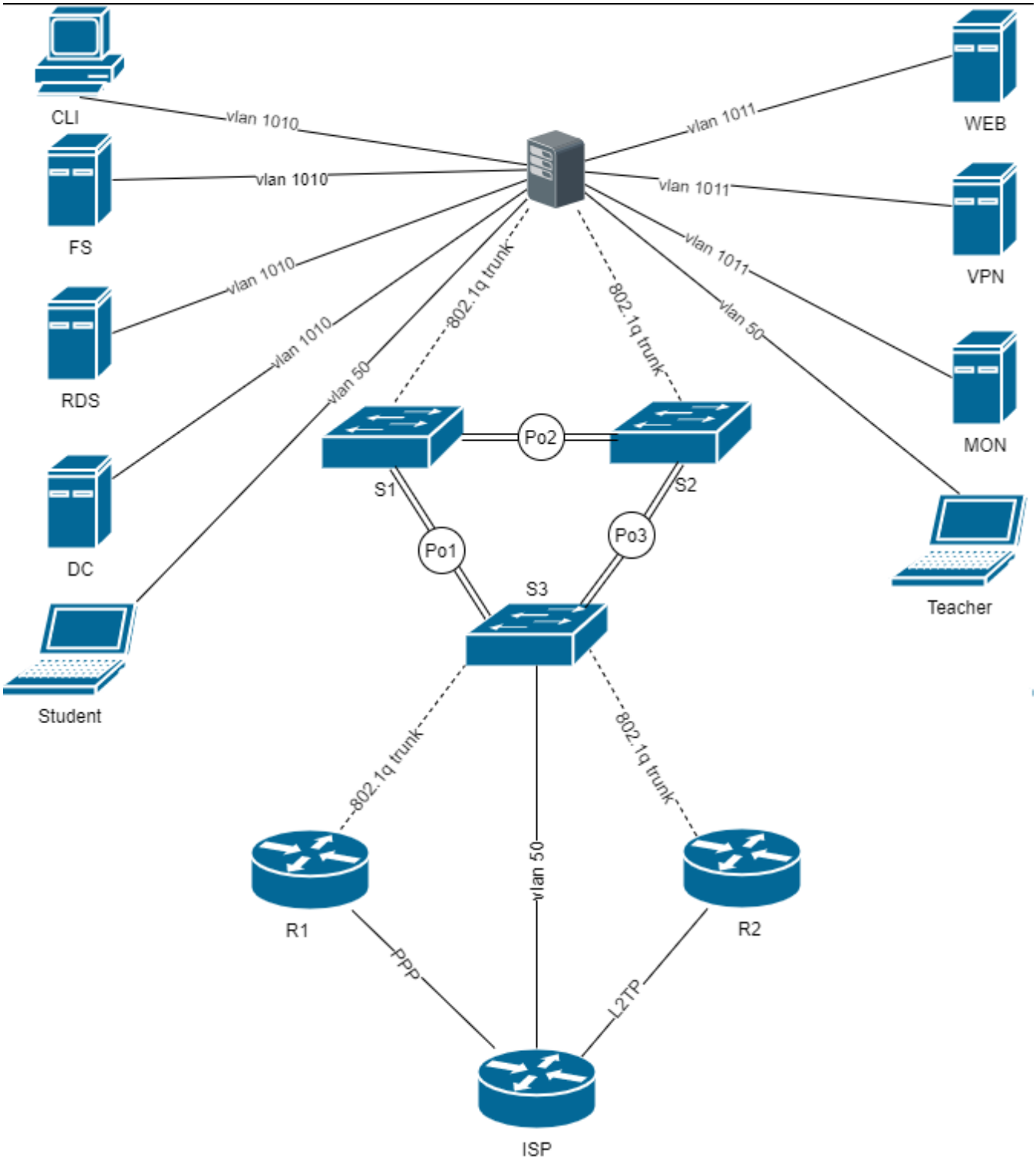
b. Используйте сертификаты, выданные центром сертификации на сервере VPN
c. Создайте ярлыки на рабочем столе рабочих станций Student и Teacher для автоматического подключения и отключения VPN соединения. Назовите их Start_VPN и Stop_VPN, расширение ярлыков на ваше усмотрение. Данные ярлыки должны быть доступны для всех существующих и новых пользователей.
d. После подключения пользователи должны иметь доступ к внутренним ресурсам
e. Клиенты должны быть автоматически настроены на использование внутренних DNS серверов компании

7. Сконфигурируйте на всех LINUX серверах межсетевой экран при помощи nftables
    a. Обеспечьте доступ только к необходимым для работы сервисов портам
    b. Все остальные соединения должны отбрасываться
    c. На ICMP сообщения все LINUX хосты должны отвечать icmp-host-prohibited

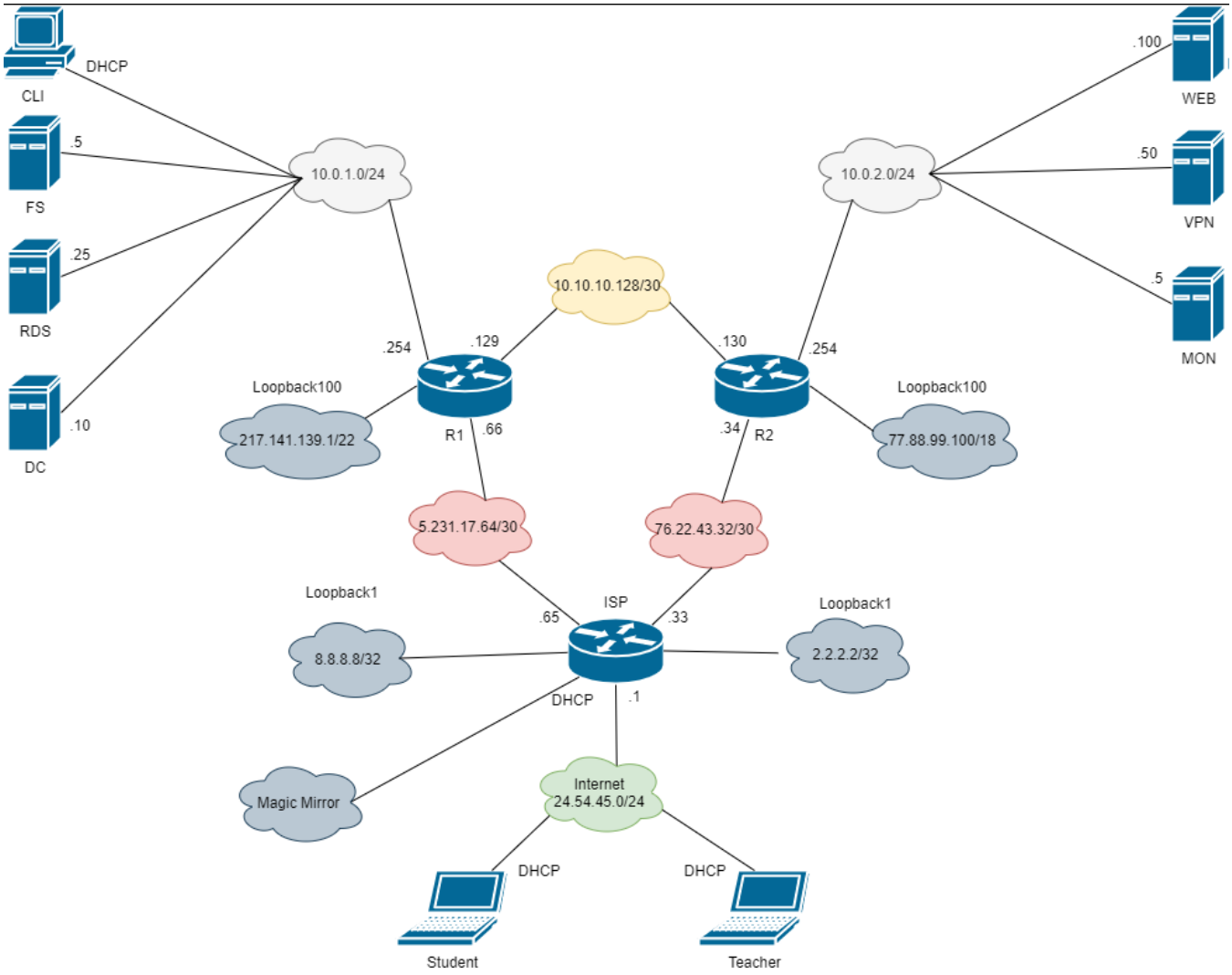
Топология L1



Топология L2



Топология L3



Приложение

Таблица 1 – Требования к виртуальным машинам

Имя	**CLI/GUI**	**Операционная система**
DC	GUI	Windows Server 2019
RDS	GUI	Windows Server 2019
FS	CLI	Windows Server 2019
Student	GUI	Windows 10 Enterprise
CLI	GUI	Windows 10 Enterprise
WEB	CLI	Debian 10.6.0
VPN	CLI	Debian 10.6.0
MON	CLI	Debian 10.6.0
Teacher	GUI	Debian 10.6.0

Устройство	**AS**
R1	65010
R2	65020
ISP	65000

Таблица 2 – Автономные системы BGP

Таблица 3 – Подразделения, группы и пользователи

Подразделение	**Группа**	**Пользователи**
Admins	Admins	Admin1, Admin2, Admin3
Education	Students	Student1, Student2, Student3
Education	Teachers	Teacher1, Teacher2, Teacher3
Office	Workers	Worker1, Worker2, Worker3
Admins	Netadmins	Netadmin1