Конкурсное задание

Компетенция

(Сетевое и системное администрирование 14-16)

Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Задание
4. Критерии оценки

Количество часов на выполнение задания: 12ч.

1. ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Командный конкурс, команда 2 человека.

2. ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания является Создание и настройка сетевой инфраструктуры дома или небольшого офиса. Участники соревнований получают инструкцию и топологию сети. Конкурсное задание сквозное и выполняется в течении 3^{x} дней.

Конкурс включает в себя выполнение пуско-наладочных работ сетевого и пользовательского оборудования.

Окончательные аспекты критериев оценки уточняются оценивающими экспертами. Оценка производится ежедневно по окончании работ. 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 оценивающими экспертами.

Предисловие

Используемые версии ПО

Машины	**ОС**
BR, GW	OPNSense
HQRTR	Linux (VyOS)
LINCLI, REMOTECLI, BRCLI	Debian 10 (MATE), English
LINSRV, WEBSRV, BRSRV, LINRTR	Debian 10 (CLI)
WINSRV	Windows Server 2019 Standard(GUI)
WINCLI	Windows 10 Education, English
WDSCLI	Отсутствует

Исходная настройка

При выполнении задания учитывайте информацию из этого раздела.

В случае, если в тексте задания не указано иное, все пользовательские учетные записи должны иметь пароль **P@ssw0rd**.

На маршрутизаторе HQRTR логин/пароль по умолчанию - **vyos/vyos**

На межсетевых экранах BR и GW логин/пароль по умолчанию - **root/opnsense**

При выполнении настоящего задания всегда нужно руководствоваться **правилом наименьших привилегий**.

На сетевых устройствах сделаны базовые сетевые настройки:

- На маршрутизаторе HQRTR на подынтерфейсе eth1.1 и интерфейсе eth0 настроены IPv4-адреса для сети FLOOR1 и для соединения с межсетевым экраном GW, а также статический маршрут по умолчанию в сторону GW.
- На межсетевом экране GW настроен IPv4-адрес на внутреннем интерфейсе, добавлен статический маршрут до сети FLOOR1 через HQRTR, DHCP выключен, остальные настройки по умолчанию.
- На BR все настройки по умолчанию.

Управление HQRTR осуществляется через локальную консоль.

Управление GW осуществляется через Web-интерфейс с устройств в сети FLOOR1.

Управление BR осуществляется через Web-интерфейс с устройств в сети BRANCH.

На BR и GW дополнительно доступна локальная консоль.

На машине WEBSRV установлены и работают следующие службы:

- FTP

- Адрес: 3.14.15.126
- Логин ftpuser
- Пароль ftppass

- Веб-сервер обслуживает сайты:
  - jun.ru
  - worldskills.ru
- DNS

Консольный доступ к виртуальной машине WEBSRV для участника не предполагается.

На всех Linux машинах существует пользователь **root** с паролем **toor** и пользователь **skill39** с паролем **P@ssw0rd**

В дисководе оптических дисков машины WINSRV установлен диск с дистрибутивом Windows 10 Education.

Задание

Схема IP-адресации.

Сеть	Устройство	Адрес/Маска	Интерфейс
Internet	GW	3.14.15.92/25	em1
	BR	3.14.15.15/25	em1
	LINRTR	3.14.15.75/25	ens192
	Шлюз провайдера	3.14.15.126	
	DNS-серверы	3.3.4.4 3.14.14.3	
Floor1	HQRTR	192.168.1.1/24	eth1.1
	LINCLI	DHCP	
	WINCLI	DHCP	
	WINSRV	192.168.1.10/24	
Floor2	HQRTR	192.168.2.30/27	eth1.2
	WDSCLI	DHCP	
	LINSRV	192.168.2.8/27	
GW-HQRTR	GW	192.168.0.1/30	em0
	HQRTR	192.168.0.2/30	eth0
Branch	BR	192.168.10.1/28	em0
	BRCLI	DHCP	
	BRSRV	192.168.10.10/28	
LINRTR LAN	LINRTR	192.168.20.1/29	ens224
	REMOTECLI	DHCP	ens192

День 1

Настройка сети

1. Настройте имена устройств согласно топологии.
2. Настройте доменное имя JunWin.wsr на GW и HQRTR.
3. Настройте учётные записи на сетевых устройствах GW, BR и HQRTR.
    1. Используйте логин js и пароль JSfinals2020
    2. Пользователь с логином js должен иметь максимальные полномочия на сетевых устройствах.
4. Настройте IPv4-адреса и шлюз по умолчанию на внешних интерфейсах GW, BR, LINRTR согласно схеме адресации.
5. Настройте IPv4-адреса на устройствах в сети первого этажа (FLOOR1).
6. Настройте IPv4-адреса для сети второго этажа (FLOOR2) согласно следующим требованиям:
    1. Используйте на HQRTR подынтерфейс с номером VLAN 2.
    2. Настройте описание подынтерфейса 'FLOOR2'.
    3. Используйте маску подсети /27.
7. Настройте DHCP Relay на маршрутизаторе HQRTR таким образом, чтобы клиентам в сети FLOOR2 адреса выдавал сервер WINSRV.
8. Обеспечьте выход в интернет для всех устройств центрального офиса.
    1. Настройте дополнительную маршрутизацию там, где это требуется.
    2. Настройте межсетевой экран и NAT на GW.
    3. Сделайте другие необходимые настройки, чтобы устройства центрального офиса могли выйти в интернет и зайти на сайты jun.ru и worldskills.ru
9. Настройте сетевое обнаружение по протоколам CDP и LLDP на всех сетевых устройствах (GW, HQRTR, LINRTR, BR) и на серверах LINSRV и BRSRV.
10. Настройте корректное время и часовой пояс Europe/Moscow на сетевых устройствах.
11. Настройте NTP.
    1. В качестве сервера должен выступать HQRTR
        1. Настройте в качестве клиентов LINCLI и WINSRV

Настройка Linux

1. Настройте имена устройств согласно топологии.
2. Настройте IP адреса на серверах LINSRV, BRSRV согласно схеме адресации.
3. Настройте общий доступ к файлам на LINSRV по протоколу NFS.
    1. Каталог для хранения файлов **/opt/nfs/rw** должен быть доступен для чтения и записи.

2. Каталог для хранения файлов **/opt/nfs/ro** должен быть доступен только для чтения.
3. NFS должен быть доступен для клиентов в сети FLOOR1.

4. Настройте клиент NFS на LINCLI.
    1. В качестве сервера используйте LINSRV.
    2. Путь **/opt/nfs/rw** на LINSRV должен быть смонтирован в каталог **/home/skill39/Desktop/nfs_rw** на LINCLI.
    3. Путь **/opt/nfs/ro** на LINSRV должен быть смонтирован в каталог **/home/skill39/Desktop/nfs_ro** на LINCLI.
5. Каталог **/home/skill39/Desktop/nfs_rw** на LINCLI должен быть доступен для чтения и записи для пользователя **skill39**.
    1. Каталог **/home/skill39/Desktop/nfs_ro** на LINCLI должен быть доступен только для чтения для пользователя **skill39**.
    2. Монтирование должно восстанавливаться при перезагрузке виртуальной машины.
6. Настройте централизованный сбор журналов syslog на LINSRV.
    1. Журналы должны храниться в файле **/opt/logs/errors.log**
    2. LINCLI должен записывать сообщения **error и более важные**.
    3. GW должен записывать системные сообщения (**System Events**).
7. Установите пакет **sudo** на LINSRV.
8. Создайте пользователя **admin** с паролем **P@ssw0rd** на LINSRV.
    1. Добавьте пользователя **admin** в группу **sudo**.
9. Настройте права доступа для каталога **/opt/nfs/**.
    1. Пользователь **admin** должен иметь права на чтение и запись в каталог **/opt/nfs** и все его подкаталоги.
10. Настройте LINRTR для обеспечения доступа в интернет для клиентов локальной сети.
    1. Настройте DHCP для локальной сети.
    2. Используете адрес LINRTR в качестве адреса DNS сервера для клиентов сети.
    3. Настройте NAT для адресов в локальной сети.

Настройка Windows

1. Настройте имена устройств на первом этаже согласно топологии.
2. WINSRV, WINCLI и WDSCLI должны отвечать на запросы по протоколу ICMP.

Настройка WINSRV

1. Настройте сетевой интерфейс на WINSRV согласно схеме адресации.

2. Установите основной контроллер домена JunWin.wsr и основной DNS-сервер, полномочный для зоны JunWin.wsr.

3. Создайте доменные группы Engineers и Workers.

4. В группе Workers создайте пользователей Denis и AlexS. В группе Engineers создайте пользователей NikS и AlexT. Все пользователи в домене должны менять пароль на новый не позже, чем через 10 дней.

5. Разрешите членам группы Engineers локальный вход на контроллер домена.

6. Настройте DNS-зоны прямого и обратного просмотра, необходимые для клиентских компьютеров, расположенных на первом и втором этажах.

7. Настройте пересылку неизвестных DNS-запросов на серверы 3.3.4.4 и 3.14.14.3.

8. Настройте DHCP-сервер, способный выдавать адреса всем клиентским компьютерам, находящимся на первом и втором этажах.

9. Настройте WDS-сервер. Используйте дистрибутив ОС, находящийся в дисководе оптических дисков. Для хранения установочных файлов используйте дополнительный жесткий диск, системный жесткий диск для этих целей использовать запрещается! Право устанавливать ОС по сети должны иметь члены группы доменных администраторов и члены группы Workers. Обеспечьте согласованную работу сервиса со службой DHCP. После установки ОС компьютеры должны автоматически входить в домен с именами WDSCLI1, WDSCLI2 и т.д.

10. Для всех клиентских компьютеров домена должна быть отключена приветственная анимация.

Настройка WINCLI

1. Сделайте компьютер членом домена JunWin.wsr.

2. На компьютере должна быть только одна локальная учетная запись пользователя - Administrator.

Настройка WDSCLI

1. Установите на компьютер ОС Microsoft Windows 10 Education.

2. Обеспечьте членство компьютера в домене JunWin.wsr.

3. На компьютере должна быть только одна локальная учетная запись пользователя - Administrator.

День 2

Настройка сети

1. Настройте сеть филиала BRANCH
    1. На межсетевом экране BR поменяйте адрес внутренней сети, чтобы он соответствовал схеме IP-адресации.
    2. Настройте DHCP-сервер на BR, чтобы он выдавал следующие настройки:
        1. Сеть и маска согласно схеме адресации
        2. Шлюз - BR
        3. Адреса DNS-серверов - 3.3.4.4 и 3.14.14.3
        4. Домен - branch
        5. Диапазон адресов - с .3 по .8 включительно.
    3. Настройте NAT и межсетевой экран таким образом, чтобы был обеспечен выход в интернет для всех устройств филиала.
    4. Настройте IPsec между GW и BR для связи филиала и домашнего офиса со следующими параметрами:
        1. Протокол IKEv2.
        2. Параметры согласования IKEv2 - AES128, SHA256, DH15, аутентификация по общему ключу.
        3. Параметры IPsec - Режим Tunnel, защита ESP AES128, SHA256
        4. Туннель должен обеспечивать связь через защищённый канал между филиалом BRANCH и сетью FLOOR1 центрального офиса.
2. Настройте OSPFv2 между HQRTR и GW
    1. Используйте область 0.
    2. GW должен узнавать о сетях FLOOR1 и FLOOR2 через OSPF. Не используйте на GW статические маршруты до этих сетей.
    3. HQRTR должен получать маршрут по умолчанию и другие необходимые маршруты от GW через OSPF. Не используйте статические маршруты на HQRTR.
    4. Интерфейсы в сторону сетей FLOOR1 и FLOOR2 на HQRTR должны быть настроены как пассивные.

Настройка Linux

1. Настройте службу DNS на LINRTR.
    1. LINRTR должен выполнять трансляцию DNS запросов (DNS Proxy) от локальных клиентов.
    2. Используйте для проверки адрес jun.ru.
2. На BRSRV настройте веб-сервер.
    1. Файлы веб-сайта должны располагаться в каталоге **/var/www/**

2. Сайт должен быть доступен по локальному IP адресу для клиентов сети BRANCH.
3. Сайт должен быть доступен по IP адресу BR для клиентов сети Internet.
4. Веб-сайт должен работать по протоколу HTTPS.
    1. Настройте автоматическую переадресацию протокола HTTP на HTTPS.
    2. Используйте самоподписанные сертификаты. Доверие сертификатам со стороны клиентов не требуется.

Настройка Windows

Настройка WINSRV

1. Установите и настройте доменный корневой центр сертификации с именем ROOTCA и сроком действия основного сертификата 6 лет.
2. Установите и настройте web-сервер.
3. Установите и настройте ftp-сервер.
4. Создайте сайт, доступный клиентам, находящимся на первом и втором этаже, по имени home.junwin.wsr. Тело сайта, файл c:\Site\index.htm:

```
<html>
<body>


 <center>Hello, World!!!</center>

 </body>
</html>
```

Сайт должен быть доступен только по протоколу HTTPS. Сертификат безопасности должен быть выдан ROOTCA. При обращении к сайту по протоколу HTTP должно включаться автоматическое перенаправление на протокол HTTPS.

5. На контроллере домена в браузере IE в качестве домашней страницы должно использоваться содержимое папки, содержащей актуальный список отзыва сертификатов для ROOTCA. Список отзыва сертификатов должен быть доступен для скачивания по нажатию на ссылку.
6. На клиентах домена в браузере IE в качестве домашней страницы должен использоваться сайт home.junwin.wsr.

День 3

Настройка сети

1. Настройте проброс портов на BR. Веб-сервер на BRSRV должен быть доступен из интернета по адресу внешнего интерфейса BR и портам 80 и 443.
2. Настройте OpenVPN
    1. OpenVPN-сервером должен быть GW.
    2. Используйте хеширование SHA-256 и шифрование AES.
    3. Клиентом будет REMOTECLI
    4. Используйте аутентификацию по логину **jsremote** и паролю **JSopenvpn**

5. У клиента должна быть связь с сетью FLOOR1

6. Используйте WINSRV в качестве DNS-сервера

Настройка Linux

1. По протоколу FTP получите файлы сайта на сервере провайдера WEBSRV и поместите полученное в каталог **/var/www/**

2. Настройте удаленный доступ по протоколу SSH для LINRTR.

    1. SSH сервер должен принимать подключения только из локальной сети.

    2. REMOTECLI должен выступать клиентом удаленного доступа по протоколу SSH.

    3. Доступ к LINRTR для пользователя **skill39** должен происходить с помощью аутентификации на основе открытых ключей (без ввода логина и пароля).

Настройка Windows

Настройка WINSRV

1. Члены группы Engineers должны иметь возможность скачивать и загружать файлы в папку C:\Site по протоколу FTP.

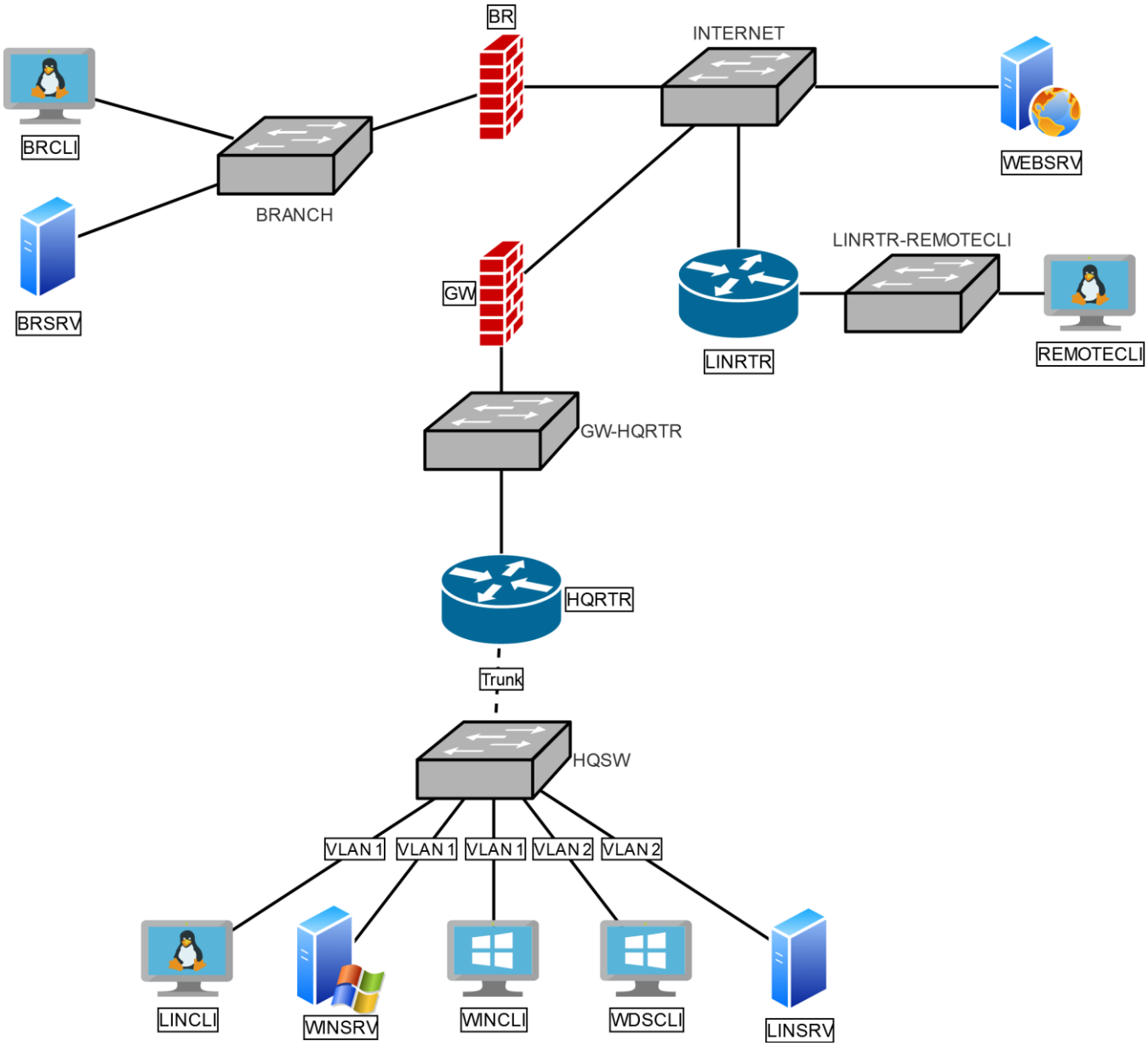
Настройка WINCLI

1. Запретите запуск любого исполняемого кода из корневого каталога диска C:. Учтите, что хранение исполняемых файлов в этом каталоге должно оставаться возможным для членов групп локальных и доменных администраторов. Указанный запрет не должен распространяться на WDSCLI.

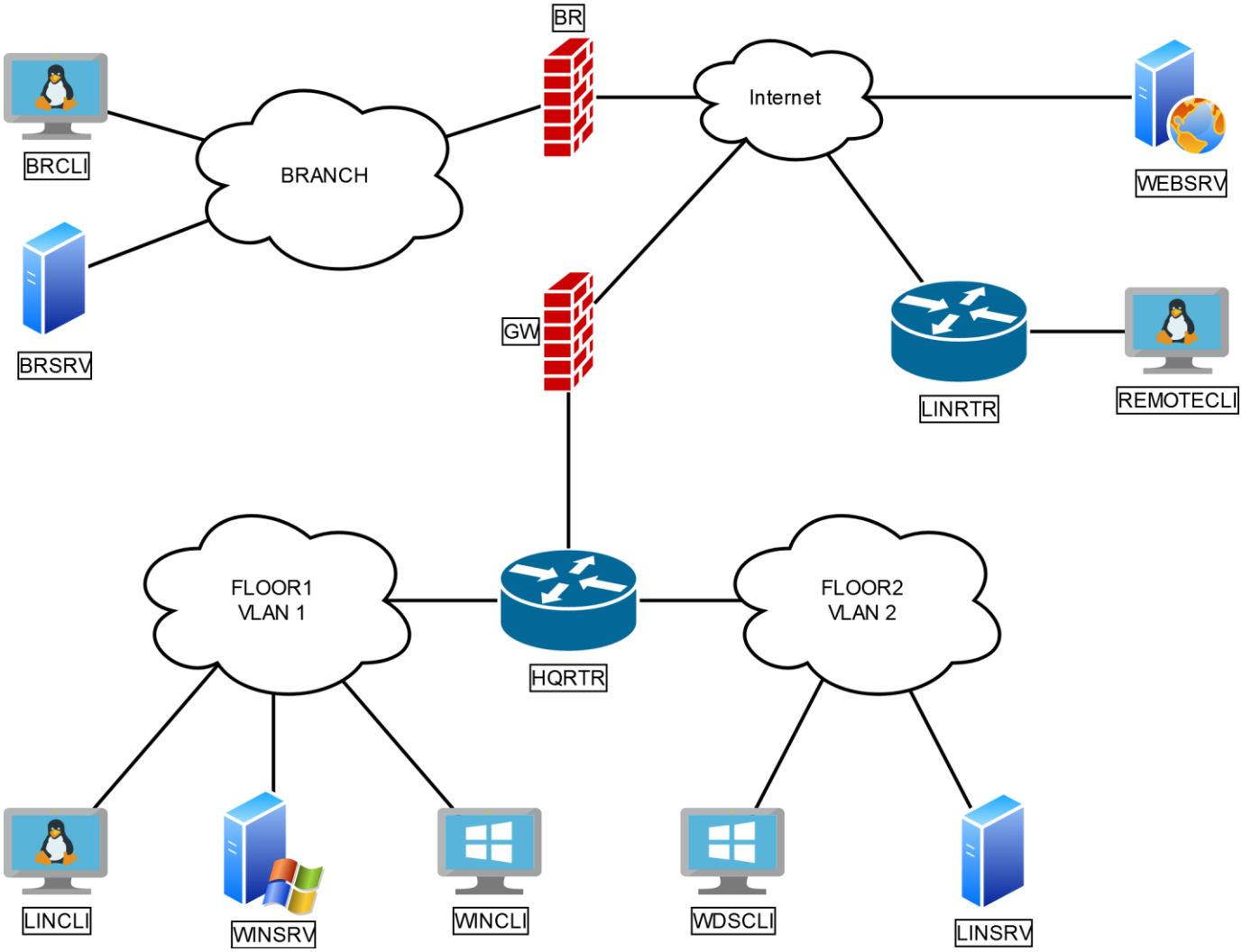
2. Запросите у ROOTCA сертификат для пользователя Denis и поместите его в хранилище личных сертификатов.

Топология

L1-L2



L3


BR
Internet
BRCLI
BRANCH
WEBSRV
BRSRV
GW
LINRTR
REMOTECLI
FLOOR1
VLAN 1
HQRTR
FLOOR2
VLAN 2
LINCLI
WINSRV
WINCLI
WDSCLI
LINSRV