**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: 15 ч.

1) ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

 Индивидуальный конкурс

2) ЗАДАНИЕ ДЛЯ КОНКУРСА

Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем в сфере интеграции и аутсорсинга корпоративных вычислительных сетей. Если вы можете выполнить задание с высоким результатом, то вы сможете достаточно успешно обслуживать информационную инфраструктуру большого предприятия, ну, или хотя бы делать вид.

### ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

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.

### СХЕМА ОЦЕНКИ

Оцениваемые аспекты имеют разный вес в зависимости от их сложности. Схема оценки построена так, чтобы каждый аспект оценивался только один раз. Например, в задании предписывается настроить корректные имена для всех устройств, данный аспект будет оценен в первый день только один раз и повторная оценка данного аспекта проводится не будет. 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.

Следует также учесть, что для данного задания предусмотрена автоматическая оценка результатов.

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.

Проверка будет производиться с использованием доменных имен. Проверка по IP-адресам выполняться не будет.

Задания разработаны и протестированы группой сертифицированных экспертов:

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

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 1.

Таблица 1 – Время выполнение модуля

|  |  |  |  |
| --- | --- | --- | --- |
| № п/п | Наименование модуля | Рабочее время | Время на задание |
| 1 | День 1 | В соответствии с графиком выполнения | 5 ч. |
| 2 | День 2 | 5 ч. |
| 3 | День 3 |  | 5 ч. |

# Технологии, работоспособность которых ожидается в день 1

Версия 1 от 15.02.2020

## ВВЕДЕНИЕ

Вы устроились администратором в молодую, но быстро развивающуюся компанию, которая занимается разработкой специализированного ПО и включает в себя несколько отделов: разработчики, офисные работники, системные администраторы. Также в компании практикуется удаленная работа, так что часть сотрудников должна иметь удаленный доступ до своего рабочего места в офисе. В компании строго регламентированы корпоративные политики, за нарушение которых предусмотрены штрафы.

На выполнение задания отводится ограниченное время – подумайте, как использовать его максимально эффективно. Составьте план выполнения работ. Вполне возможно, что для полной работоспособности системы в итоге действия нужно выполнять не строго в той последовательности, в которой они описаны в данном конкурсном задании.

Внимательно прочтите задание от начала до конца – оно представляет собой целостную систему. При первом доступе к операционным системам либо следуйте указаниям мастера, либо используйте следующие реквизиты: Windows: ***Administrator/P@ssw0rd*.** Linux:**root:toor**. Машина ISP также настраивается участниками!

Если Вам требуется установить пароль, (и он не указан в задании) используйте: “P@ssw0rd”

Обратите внимание что брандмауэр Windows должен быть включен!

Если предоставленные виртуальные машины начнут самопроизвольно отключаться в процессе работы, попробуйте выполнить на них команду ***slmgr /rearm*** или обратитесь к техническому эксперту.

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.

## НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Конкурсное задание выполнимо в полном объеме с привлечением оборудования и материалов, указанных в Инфраструктурном листе.

Вам доступен диск CentOS-8.1.1911-x86\_64-dvd1.iso

Вам доступен диск WindowsServer2019-XXX.iso

## 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, принимавшими участие в оценке конкурсного задания чемпионата, и вынесено в отдельный документ. Данный документ, как и схема оценки, является объектом внесения 30% изменений.

**Базовая настройка**

1. Настройте имена сетевых устройств и виртуальных машин в соответствии с диаграммой
2. Доменные имена на сетевом оборудовании сконфигурируйте в зависимости от его расположения:
	1. Для основного офиса (Local Office) используйте доменное имя office.local
	2. Для удаленного офиса (Remote Office) используйте доменное имя office.remote
	3. Будут пояснения и дополнения
3. На всех серверах Linux и сетевом оборудовании создайте пользователя Admin с паролем PaSsWoRd
	1. Для сетевого оборудования пароль должен быть регистрочувствительным и хранится в виде результата хэш функции
	2. На Linux серверах обеспечьте возможность использования sudo только для пользователя Admin. Отключите необходимость дополнительной аутентификации для использования sudo
	3. Ограничьте локальный вход пользователя root только пятым виртуальным терминалом.
	4. Будут пояснения и дополнения
4. В качестве пароля для входа в привилегированный режим используйте wsr
5. Обеспечьте доступ по именам ко всем виртуальным машинам и активному сетевому оборудованию с использованием файла hosts. Файл будет использован при проверке, в случае отказа службы DNS
6. Организуйте удаленный доступ до всего сетевого оборудования, а также до всех серверов по протоколам SSH версии 2 и RDP
	1. Доступ разрешен только с ПК администратора
	2. В качестве методов аутентификации для SSH используется только аутентификация на основе открытых ключей. Доступ разрешен только пользователю Admin данного ПК.
	3. Будут пояснения и дополнения

**Конфигурация активного сетевого оборудования**

1. Таблица VLAN для Local Office должна соответствовать:
	1. VLAN 100 - LDMZ
	2. VLAN 200 - LOFFICE
	3. VLAN 300 - LDEV
	4. VLAN 400 - ADMINS
	5. VLAN666 - LNATIVE
2. Таблица VLAN для Remote Office должна соответствовать:
	1. VLAN 210 - RDMZ
	2. VLAN 220 - ROFFICE
	3. VLAN 230 - RDEV
	4. VLAN 240 - RNATIVE
	5. VLAN 400 - ADMINS
3. Адресацию для каждого VLAN разработайте самостоятельно. Для Remote Office выделена подсеть 172.16.0.0/16, для Local Office 192.168.0.0/16. Адреса сетей для VLAN Впишите ниже:
	1. Remote Office:
		1. LDMZ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
		2. LOFFICE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
		3. LDEV \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
		4. ADMINS \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
	2. Local Office:
		1. LDMZ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
		2. LOFFICE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
		3. LDEV \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
		4. ADMINS \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. Настройте магистральные каналы в соответствии с диаграммой L2
	1. Не используйте протоколов динамического согласования
	2. В качестве Native vlan назначьте vlan 666 и vlan 240 в зависимости от офиса
	3. Будут пояснения и дополнения
5. Сконфигурируйте портовые группы в соответствии с диаграммой L2
	1. настройте балансировку нагрузки по MAC адресу назначения для каждой из портовых групп
	2. Будут пояснения и дополнения
6. Настройте протокол 802.1D
	1. Будут пояснения и дополнения
7. Настройте протокол 802.1AB таким образом, чтобы передача сообщений была возможна только на портах между коммутаторами, а прием сообщений - на всех используемых портах.
8. Сконфигурируйте подключение к глобальной сети каждого из офисов
	1. Для подключения Local Office использовать адреса из подсети 10.0.17.16/30; для Remote Office использовать адреса из подсети 10.1.1.24/30
	2. Будут пояснения и дополнения
9. Настройте протокол динамической маршрутизации BGP для связи с провайдерами
	1. Будут пояснения и дополнения
	2. Средствами BGP обеспечьте распределение нагрузки между провайдерами:
		1. Для исходящего трафика приоритетным считать провайдера ISP1
		2. Для входящего трафика приоритетным считать провайдера ISP2
10. Обеспечьте маршрутизацию между VLAN на Core router каждого из офисов
11. Для каждого из офисов обеспечьте возможность выхода в Internet
12. Для обеспечьте связанность между офисами посредством технологии виртуальных частных сетей канального уровня. Защита соединения в текущий день не требуется
13. Настройте протокол маршрутизации OSPF для связи между офисами
	1. Анонсируйте все сети, необходимые для достижения полной связанности
	2. Соседство должно устанавливаться только через GRE туннель. Используйте для этого магистральную зону.
	3. Магистральная зона используется только для передачи маршрутов, анонсировать другие сети в эту зону запрещено
	4. Будут пояснения и дополнения

**Настройка серверов под управлением Windows**

1. В офисе Local Office сконфигурируйте домен company.local
	1. Контроллером домена является WLSRV1;
	2. Сконфигурируйте службу DNS;
		1. Создайте необходимые А и CNAME записи;
		2. Настройте запрет на использование нелатинских символов;
		3. Настройте необходимую переадресацию для разрешения имен во внешней сети и в сети филиала.
		4. Будут пояснения и дополнения
2. Создайте организационные подразделения Office, Admins, Dev, Servers, Temporary. Добавьте в подразделения соответствующие группы безопасности
3. На сервер WLSRV1 установите службы PKI.
	1. Имя центра: CompanyCA;
	2. Срок действия сертификата: 9 лет;
	3. Сконфигурируйте доступ к CRL по адресу <http://company.local/crl>.
	4. Будут пояснения и дополнения
4. На сервере WRSRV1 сконфигурируйте поддомен remote.company.local
	1. Будут пояснения и дополнения
5. Сконфигурируйте DHCP сервер на WRSRV1
	1. Клиенты сетей Office и Dev должны получать IP адреса автоматически
	2. ПК администратора должен получать фиксированный IP адрес
	3. Настройте DHCP FailOver в режиме HotStandby с сервером WRSRV2.
	4. Будут пояснения и дополнения
6. Для выдачи адресов клиентам в Remote Office сконфигурируйте DHCP сервер на LLSRV1 и обеспечьте отказоустойчивость с использованием LLSRV2
7. Для пользователей группы безопасности Admins сконфигурируйте обязательную минимальную длину пароля: 12 символов.
8. К серверам WRSRV2 и WLSRV1 примонтируйте по 1 дополнительному HDD емкостью 5 Гб. Отформатируйте томы и назначьте им букву D
9. Используйте дополнительные диски для хранения всех необходимых общих каталогов
	1. Обеспечьте синхронизацию данных между серверами средствами DFS
	2. Будут пояснения и дополнения
10. Для каждого пользователя домена обеспечьте монтирование домашнего каталога в качестве диска H:. Запретите хранение исполняемых файлов и определите квоту в 1ГБ для каждого пользователя.
11. Для всех пользователей группы Dev создайте общую папку
	1. Обеспечьте автоматическое монтирование папки в качестве диска G:
	2. Доступ для чтения и записи только для администраторов
	3. Другие пользователи при попытке доступа к каталогу должны получать сообщение “Only for Developers!!!”
	4. Будут пояснения и дополнения
12. Аналогично сконфигурируйте общий каталог для группы Office
	1. В качестве сообщения об ошибке доступа сконфигурируйте “Only for office!!”
	2. Разрешите хранение только офисных документов
	3. Будут пояснения и дополнения

**Настройка серверов под управлением Linux**

1. На HQLinSRV сконфигурируйте вторичный DNS сервер на базе BIND
	* 1. В качестве master сервера используйте WLSRV1
		2. Настройте перенаправление всех неизвестных запросов на сервер ISP. Для проверки используйте имя ya.ru
		3. Делегируйте поддомен ext.company.ru серверу ISPSRV
			1. Для тестирования используйте test.ext.company.local
			2. Будут пояснения и дополнения
2. Создайте 4 дополнительных жестких диска по 1гб и сконфигурируйте LVM на LLSRV1
	* 1. Разметьте том как ext4
		2. Обеспечьте автоматическое монтирование тома в директорию /opt. Монтирование должно производится автоматически, при загрузке системы
		3. Метка тома должна соответствовать optroot
		4. Будут пояснения и дополнения
3. На LLSRV1 Обеспечьте шифрование раздела /opt средствами dm-crypt/LUKS
	* 1. Алгоритм шифрования: AES-XTS-plain64
		2. Алгоритм хэширования: SHA-512
		3. Длина ключа: 512 бит
		4. Используйте пароль LeTsEnCrYpT!
		5. Будут пояснения и дополнения
4. На LRSRV2 Сконфигурируйте файловое хранилище по протоколу smb
	* 1. В качестве корневой директории используйте /opt/samba
		2. Обеспечьте доступ к хранилищу под учетной записью smbuser с паролем smbpass
		3. Смонтируйте хранилище на АРМ Администратора как сетевой диск. В качестве буквы диска используйте N:
		4. Будут пояснения и дополнения
5. Для LLSRV1 и LLSRV2 должны быть членами домена Company.local. Настройте аутентификацию с использованием доменных реквизитор. Доступ к sudo имеет только группа Admins
6. На LRSRV2 сконфигурируйте централизованный сбор журналов с активного сетевого оборудования
	* 1. Сбор журналов должен производится в /var/log/network
		2. Собирать следует все уровни сообщений
		3. Обеспечьте защиту от переполнения базы данных
			1. Очистка базы данных должна производится автоматически, каждый день в полночь
			2. Обеспечьте возможность выполнения очистки базы в ручном режиме при помощи команды clear\_syslog\_db
		4. Сконфигурируйте активное сетевое оборудование соответствующим образом
		5. Будут пояснения и дополнения
7. На LRSRV1 настройте Reverse proxy на базе NGINX
	* 1. В качестве бэкэнда используйте веб сайт на LRSRV1
		2. Сайт должен быть доступен из внешней сети, по внешнему адресу www.company.ru.
		3. Сконфигурируйте SSL и автоматическое перенаправление на HTTPS
		4. Реализуйте пассивную проверку работоспособности бэкэнда
			1. Проверка должна производится раз в 30 секунд
			2. Сервер считается нерабочим после 3 ошибок
			3. Сервер считается снова рабочим после 2 удачных проверок
			4. Будут пояснения и дополнения
8. На LRSRV2 разверните Web сервер Apache
	1. Сервер должен работать на порту 8088
	2. В качестве стартовой страницы создайте документ /var/www/html/index.php с содержимым “phpinfo()”
	3. Будут пояснения и дополнения

**Технологии, работоспособность которых ожидается в день 2**

**Конфигурация активного сетевого оборудования**

1. На всех сетевых устройствах настройте модель AAA
	1. Аутентификация на всех терминальных линиях должна производится с использованием локальный базы данных
		1. Для устройств центрального офиса аутентификация с использованием локальной базы данных должна производится только в случае недоступности RADIUS сервера
	2. При успешной аутентификации пользователи должны получать права, соответствующие их уровню привилегий
	3. Настройте необходимость аутентификации и авторизации на локальной консоли
	4. Будут пояснения и дополнения
2. На всех устройствах центрального офиса сконфигурируйте аутентификацию с использованием доменных реквизитов
	1. Только группа Admins имеет возможность аутентификации
	2. Используйте общий ключ cisco
	3. Пользователи должны получать максимальный уровень привилегий при входе
	4. Будут пояснения и дополнения
3. На Core router обоих офисов сконфигурируйте политику удаленного доступа
	1. При ssh подключении на порт 2222 пользователь должен попадать на 10 VTY линию
	2. Независимо от активности пользователя разрыв соединения должен производится через 10 минут после начала сессии
	3. Обеспечьте предупреждение за 1 минуту до разрыва сессии
	4. Максимальное число ssh сессий: 2
	5. Если пользователь неактивен в течении 3 минут, сессия должна быть разорвана
	6. Включите журналирование событий при подключении по SSH
	7. Будут пояснения и дополнения
4. Настройте защиту от атак методом перебора на Core router обоих офисов
	1. Если произошло 3 неудачных попытки входа в течении 30 секунд, маршрутизатор должен быть заблокирован на 2 минуты
	2. Настройте задержку в 10 секунд между попытками входа
	3. Настройте логирование всех неудачных попыток подключения
	4. Доступ из подсети для администрирования блокироваться не должен
	5. Будут пояснения и дополнения

**Конфигурация серверов под управлением ОС Windows**

1. На всех серверах в центральном офисе и филиале настроить службу NTP на получение времени с ISP и временной зоны +3 Moscow.
2. На всех серверах и клиентских машинах в центральном офисе и филиале настроить эмуляцию нахождения в Интернет.
3. На сервере WRSRV1 создать ресурс для публикации CRL CompanyCA по адресу http://company.local/crl. Обеспечить синхронизацию содержимого ресурса с центральным офисом, чтобы при внесении изменений в центральном офисе, они автоматически применялись в филиале.
4. На сервере WRSRV2:
	1. Установите роль Удаленных рабочих столов (RDS);
	2. Опубликуйте приложение notepad для пользователей группы rdsusers;
	3. Обеспечьте работу веб-интерфейса rds.company.local по протоколу HTTPS без ошибок и предупреждений;
	4. Обеспечьте SSO (вход без повторного ввода логина и пароля) как при запуске приложения, так и открытии веб-интерфейса;
	5. При подключении к сессии notepad не должно возникать никаких ошибок или предупреждений;
	6. Положите ярлык для входа в приложение на рабочий стол всех пользователей группы rdsusers;
	7. Доступ к web-форме удаленных рабочих столов должен быть доступен только для пользователей группы rdsusers по их пользовательским сертификатам;
	8. Для пользователей группы rdsusers подключить сетевой диск \\HQWinSRV2\RDS\ при использовании notepad в терминальной сессии, причем, при обычном входе в систему, данная папка подключаться не должна;
	9. Будут пояснения и дополнения

При подключении к сессии notepad через RDS пользователь не должен иметь возможность «видеть» другие подключенные диски (кроме подключенного в пункте h), локальные диски сервера и клиента.

1. На время командировки сотрудников центрального офиса в филиал стартовая страница пользователя должна автоматически меняться на [https://rds.company.local](http://rds.company.local), а при возвращении на <https://portal.company.local>.
2. Будут пояснения и дополнения

**Конфигурация серверов под управлением ОС Linux**

1. C LLSRV1 должен быть доступен мониторинг устройств по протоколу SNMPv3
	1. Скрипт должен располагаться по пути /opt/utils/snmp\_test.sh
	2. При запуске скрипта без параметров должен выводится пример использования скрипта
	3. Скрипт должен вызываться из любого каталога без указания полного пути и расширения.
	4. Команда принимает на вход последовательно следующие аргументы: имя устройства; алгоритм шифрования; алгоритм аутентификации; логин; пароль
	5. При передаче скрипту ключа --help или -h должен выводится пример использования

**Пример использования скрипта при проверке: snmp\_test HQ\_GW1 AES128 SHA1 snmpv3user snmpv3pass**

* + 1. Будут пояснения и дополнения
1. На сервере LRSRV1 и LRSRV2 сконфигурируйте сервер WireGuard
2. Клиентам должен быть обеспечен доступ до внутренней сети обоих офисов
3. Сервер должен работать на порту 1122
	1. В качестве адресного пространства для VPN используйте 10.8.0.0/24
	2. Сервер должен иметь адрес 10.8.0.1/24
	3. Сконфигурируйте активное сетевое оборудование для нормальной работы WireGuard
	4. Настройте WireGuard клиент на HomeOfiice. Клиент должен запускатся автоматически при запуске системы
	5. Будут пояснения и дополнения
4. Обеспечьте резервное копирование каталога /opt/homes на сервере XXX в /opt/backup на сервере XXX средствами lsyncd
5. Будут пояснения и дополнения

*ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ*

Тология L1



Топология L2



Топология L3



# Приложение 1

#  Дополнительные настройки модуля

## ВВЕДЕНИЕ

Настоящие дополнения содержат описание вида предустановок, описание используемых операционных систем, рекомендации по выделению ресурсов для виртуальных машин.

##

|  |  |  |
| --- | --- | --- |
| ***Название Ресурса*** | ***CLI/GUI*** | ***Примечания*** |
| ***DMZ Office*** | ***CLI*** | ***Возможно использование OVS*** |
| ***RASW*** | ***CLI*** | ***Возможно использование OVS*** |
| ***Office Core Router*** | ***CLI*** | ***Linux Router*** |
| ***ISP1*** | ***CLI*** | ***Возможно использование CSR с заменой Serial линков на Ethernet*** |
| ***ISP2*** | ***CLI*** | ***Возможно использование CSR с заменой Serial линков на Ethernet*** |
| ***BR1*** | ***CLI*** | ***Возможно использование CSR*** |
| ***BR2*** | ***CLI*** | ***Возможно использование CSR*** |
| ***Remote Core Router*** | ***CLI*** | ***Linux Router*** |
| ***LASW*** | ***CLI*** | ***Возможно использование OVS*** |
| ***DMZ Local*** | ***CLI*** | ***Возможно использование OVS*** |
| ***WRSRV1*** | ***GUI*** | ***Windows server 2019*** |
| ***WRSRV2*** | ***CLI*** | ***Windows Server 2019*** |
| ***LRSRV1*** | ***CLI*** | ***Centos 8*** |
| ***LRSRV2*** | ***CLI*** | ***Centos 8*** |
| ***WS Office*** | ***GUI*** | ***Windows 10 Enterprise*** |
| ***WS Developers*** | ***GUI*** | ***Centos 8*** |
| ***WS Admin*** | ***GUI*** | ***Windows 10 Enterprise*** |
| ***HomeOffice*** | ***GUI*** | ***Windows 10 Enterprise*** |
| ***WS Local Office*** | ***GUI*** | ***Windows 10 Enterprise*** |
| ***WS Developers Local*** | ***GUI*** | ***Centos 8*** |
| ***WLSRV1*** | ***GUI*** | ***Windows Server 2019*** |
| ***LLSRV1*** | ***CLI*** | ***Centos 8*** |
| ***LLSRV2*** | ***CLI*** | ***Centos 8*** |

##