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 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 автоматический сбор 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) Букин Д.
2) Мешков А.
3) Фучко М.
4) Дюгуров Д.
5) Уймин А.
6) Лавров Д.
7) Афанасьев М.
8) Добрынин С.

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 1.

Таблица 1 – Время выполнение модуля

№ п/п	Наименование модуля	Время на задание	День
1	Комплексное задание по пуско-наладке инфраструктуры на основе ОС семейства Linux, ОС семейства Windows, телекоммуникационного оборудования»	5 ч.	1
2		5 ч.	2

Технологии, работоспособность которых ожидается в день 1

Версия 1 от 29.02.2020

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**. Виртуальная машина ISP и ISP Router являются преднастроенными, доступ участника к ним не предусмотрен

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. Для всего активного сетевого оборудования настройте доменное имя semifinal.wsr
2. Создайте локального пользователя admin с паролем Pa$$w0rd
    a. Для активного сетевого оборудования:
        i. Пользователь должен обладать максимальным уровнем привилегий.
        ii. Пароль должен храниться в виде результата хэш функции.
        iii. Используйте алгоритм scrypt
        iv. На Cisco ASA используйте шифрование AES
    b. Для всех ВМ Linux
        i. Пользователь должен иметь возможность запуска утилиты sudo без дополнительной аутентификации
    c. Для всех ВМ Windows:
        i. Пользователь должен быть членом группы локальных администраторов
3. Сконфигурируйте нумерацию строк и подсветку синтаксиса цветовой схемой pablo для текстового редактора VIM для всех пользователей, включая вновь созданных
4. Все сетевые устройства должны быть доступны для управления по протоколу SSHv2
5. Зашифруйте все открытые пароли
6. Все виртуальные машины на ОС Linux должны быть доступны для управления по протоколу SSHv2 из под пользователя root на стандартном порту. При подключении должно отображатся приветственное сообщение, “Welcome to SemiFinal 2020”
7. Все виртуальные машины на ОС Windows должны быть доступны для управления по протоколу RDP из под учетной записи admin, а так же из под учетной записи доменного администратора

Конфигурация активного сетевого оборудования

1. Создайте на коммутаторе SW1 следующие VLAN:

   VLAN10:CLIENT

   VLAN20:SERV

   VLAN30:DMZ

   VLAN1000:MANAGE

   VLAN1500:NATIVE

   VLAN1666:SHUTDOWN

2. Сконфигурируйте магистральные каналы
   a. Отключите порт f0/24 на SW1 и g1/5 на FW
   b. Транки между коммутаторами должны быть согласованы с использованием DTP. SW1 должен инициировать согласование, SW2 и SW3 должны быть настроены в пассивном режиме
   c. Транк между SW2 и SW3 должен быть согласован без использования протокола DTP
   d. На портах f0/10 коммутаторов SW2 и SW3 сконфигурируйте магистральные каналы без использования динамического согласования. Отключите протокол DTP явным образом.
   e. На портах f0/10 SW2 и SW3 обеспечьте быструю сходимость, без ожидания протокола 802.1w. Аналогичную настройку произведите на магистральном канале между этими двумя коммутаторами.

3. Сконфигурируйте портовые группы между коммутаторами
   a. Между коммутаторами SW1 и SW2 настройте агрегирование по протоколу LACP. SW1 должен работать в активном режиме, SW2 в пассивном

b. Между коммутаторами SW1 и SW3 настройте агрегирование по протоколу PAgP. SW1 должен работать в активном режиме, SW3 в пассивном

c. На SW2 настройте балансировку нагрузки по MAC адресу источника + назначения, на SW3 настройте балансировку по IP адресу источника + назначения

4. Сконфигурируйте протокол остовного дерева
   a. На всех коммутаторах используйте протокол, совместимый со стандартом 802.1w
   b. Корнем для всех VLAN является SW1. При отказе SW1 корнем должен стать SW2. При отказе SW2 корнем должен стать SW3.
   c. На портах f0//10 на коммутаторах SW2 и SW3 сконфигурируйте защиту от перехвата роли корневого моста.
   d. Необходимо обеспечить передачу трафика, до VLAN20 через Po1
   e. Необходимо обеспечить передачу трафика, до VLAN10 через Po2
   f. Будут пояснения и дополнения
5. Обеспечьте маршрутизацию между сетями VLAN с использованием технологии Router-on-a-Stick
6. Обеспечьте связь между RTR, FW и BRANCH с использованием выделенного провайдером L2 VPN
   a. На межсетевой экране FW сконфигурируйте L2VPN между FW RTR BRANCH используя тегированный трафик,а также для связи с RTR. На BRANCH и RTR произвести соответствующую настройку.

7. Произведите подключение FW1 к ISP1 и ISP2
   a. Передача данных между FW1 и ISP1 осуществляется тегированным трафиком с использованием VLAN 109.
   b. Передача данных между FW1 и ISP2 осуществляется тегированным трафиком с использованием VLAN 901.

8. Настройте подключение BRANCH к провайдеру ISP1 с помощью протокола PPP.
    a) Настройте Multilink PPP с использованием двух Serial-интерфейсов.
    b) Используйте 1 номер интерфейса.
    c) Не используйте аутентификацию.
    d) BRANCH должен автоматически получать адрес от ISP1.
9. Настройте подключение BRANCH к провайдеру ISP2 с помощью протокола HDLC. Установите адрес статически.
10. На маршрутизаторе BRANCH сконфигурируйте DHCP сервер
    a. Адрес подсети: 172.16.10.0/24
    b. Шлюз по умолчанию: 172.16.10.254
    c. DNS сервер: 172.16.10.20
11. Настройте динамическую трансляцию адресов в адреса петлевых интерфейсов на RTR и BRANCH
    a. Трансляцию следует производить на основе порта источника
12. Для связанности с провайдером настройте BGP
    a. Анонсируйте все сети в соответствии с диаграммой маршрутизации.
    b. FW и RTR связаны по iBGP
13. Сконфигурируйте GRE туннель между RTR и BRANCH.
    a. В качестве адресов источника и назначения используйте адреса соответствующих loopback интерфейсов
14. Обеспечьте полную связанность между офисами через сконфигурированные GRE тунели
    a. Используйте статическую маршрутизацию. Использование протоколов динамической маршрутизации в текущий день не допустимо
15. Сконфигурируйте свободный протокол исследования сети канального уровня таким образом, чтобы можно было идентифицировать сетевые устройства. Только для внутренних сетей
16. RTR синхронизирует время с ISP. Настройте синхронизацию всех серверов, клиентов и активного сетевого оборудования центрального офиса с роутером RTR
    a. Не используйте аутентификацию
    b. Используйте стратум 2

Настройка серверов под управлением Windows

1. На сервере DS-W разверните домен semifinal.wsr
    a. Обеспечьте ввод в домен всех машин центрального офиса
    b. DMZ-W не должен быть членом домена
    c. Обеспечьте возможность трансфера DNS зон на другие DNS сервера домена. Разрешать следует только адреса конкретных серверов
    d. Запретите использование нелатинских символов для DNS
    e. Все запросы выходящие за рамки зоны semifinal.wsr, а также branch.lan должны пересылаться серверу ISP
    f. Будут пояснения и дополнения
2. BRANCH-DC-W синхронизирует время с сервером ISP. Настройте синхронизацию всех серверов, клиентов и активного сетевого оборудования филиала с сервером BRANCH-DC-W
    a. Используйте часовой пояс +2 MSK

3. Сконфигурируйте доменную инфраструктуру
    a. Файл с пользователями размещается на SFTP сервере на ISP и доступен по паролю SecRET_User_F!LE каталога UserBackup
    b. Создайте в домене semifinal.wsr сайты для каждой подсети и задайте их имена в соответствии с именами VLAN для данных подсетей
    c. Создайте организационные подразделения IT, Sales, Workers, Radius.
    d. В организационных подразделениях, кроме подразделения Radius создайте одноименные группы. В подразделении Radius создайте группы MAdmins и SAdmins
    e. Для каждого пользователя создайте автоматически подключаемую домашнюю папку на сервере FS-W: D:\Shares\Users
    f. Ограничьте размер домашней папки в 250МБ, запретите хранение исполняемых.
    g. Смонтируйте домашние папки, в качестве диска U:
    h. При входе на файловый сервер пользователь должен видеть только те домашние папки, к которым ему разрешен доступ

4. На сервере FS-W сконфигурируйте программный RAID1 и назначьте ему букву D

a. Создайте каталог D:\Shares. Внутри этого каталога создайте подкаталоги Projects, Users, Redirected. Внутри каталога Projects создайте подкаталоги ProjectIT, ProjectSales и Temporary
b. Доступ к каталогу Temporary должен даваться только пользователям, у которых в должности указано Auditor.
c. Доступ к каталогу ProjectIT должен даваться только пользователям, состоящим в группе IT.
d. Доступ к каталогу ProjectSales должен даваться только пользователям, состоящим в группе Sales.
e. Смонтируйте каталоги ProjectIT и ProjectSales к соответствующим группам, в качестве диска P:
f. При доступе к каталогу ProjectIT пользователя, у которого нет на него прав, должно выводится сообщение «You do not have permissions to use this path! Do not try it again!»

5. На сервере FS-W сконфигурируйте протокол автоматической конфигурации хоста для выдачи адресов клиентам сети VLAN10. Зарезервируйте адрес в соответствии с топологией L3 клиенту CLI1-W.

6. Сконфигурируйте домен branch.lan на сервере BRANCH-DC-W. Данный домен должен являться частью леса semifinal.wsr.
   a. Все клиенты офиса BRANCH должны быть членами домена branch.lan

7. Сконфигурируйте свободный протокол исследования сети канального уровня таким образом, чтобы можно было идентифицировать сетевые устройства.

8. Сконфигурируйте доменную инфраструктуру branch.lan.
   a. Создайте организационное подразделение IT.
   b. В организационном подразделении создайте соответствующую группу и пользователя IT1 с паролем P@ssw0rd. Включите пользователя в группу IT.

Настройка серверов под управлением Linux

1. Обеспечьте возможность аутентификации с использованием доменных реквизитов на сервер RAD-L и FS-L без указания имени домена.
    a. Только группа IT соответствующего домена должна иметь возможность входа в систему RAD-L и FS-L
    b. Разрешите группе IT использование sudo на RAD-L и FS-L.
        i. Доступ разрешен ко всем командам, кроме passwd и su

2. Реализуйте синхронизацию времени по протоколу NTP на основе сервера Chrony.
    a. Часовой пояс всех хостов: MSK.
    b. Хост LIN-RTR синхронизирует время напрямую с ISP. Так же хост выступает сервером времени для CLI1-L.
        i. Разрешается синхронизация только для клиентов сети CLI1-L.
        ii. Собственный источник времени является резервом синхронизации со стратумом 9.
    c. Все прочие хосты на базе Linux синхронизируют время с ответственным сервером в своей сети.
        i. Машины выполняют синхронизацию аппаратных часов.
        ii. В случае, если отклонение от сервер составляет более двух тысяч секунд - машина выполняет жесткую синхронизацию времени. машины допускают ручное выставление времени средствами Chrony.
3. На сервере RAD-L настройте веб сайты для внутренних и внешних пользователей
    a. Сайт для внутреннего пользования доступен только из внутренней сети офиса HQ по имени www.semifinal.wsr
    b. Исключите возможность доступа на сайт по IP адресу
        i. Достаточно выдачикода ошибки и демонстрации страницы-заглушки.
    c. Для внешних пользователей обеспечьте работу сайта www.semifinal.ru
    d. Настройте сетевое оборудование для обеспечения возможности входа на сайт внешних клиентов. Для этого произведите проброс портов на правильном устройстве.

4. Сконфигурируйте DNS сервер на сервере RAD-L
    a. Сервер должен нести реплику зоны semifinal.wsr без возможности ее изменения.

b. Все запросы выходящие за рамки зоны semifinal.wsr, а также branch.lan должны пересылаться серверу ISP. Запросы к зоне branch.lan должны пересылаться серверу DS-W.
c. Внешние клиенты не должны иметь возможности просмотра внутренней зоны
d. Сконфигурируйте зону semifinal.ru. Данная зона должна быть доступна для просмотра только для внешних клиентов

5. На сервере FS-L сконфигурируйте LVM
   a. Преобразуйте в физические тома LVM все свободные носители.
   b. Создайте группу логических томов SEMIFINAL
   c. Создайте следующие логические тома.
      i. Backup, 200 Мб.
      ii. Storage, 40% от оставшегося свободного места.
   d. Обеспечьте создание снапшотов тома Backup раз в час.
      i. Снапшоты создаются в формате SNAP-XX, где XX - номер снапшота, (01, 02 и т.д.)
      ii. Снапшоту выделяется 5% от общего объема группы томов.
   e. Создайте снапшот чистого тома Backup с названием CLEAR
      i. Снимок должен позволять полное хранение изменений указанного логического тома.
   f. Обеспечьте монтирование тома Storage в каталог /opt/Storage
   g. Обеспечьте монтирование тома Backup в каталог /opt/Backup
   h. Монтирование должно происходить во время загрузки системы.

6. Сконфигурируйте VPN на основе WireGuard на сервере FS-L
   a. В качестве адресного пространства используйте подсеть 10.6.6.0/24.
   b. Клиенты должны иметь полный доступ к офису Branch, при этом анонсировать сеть в процесс маршрутизации запрещено
   c. В качестве клиентов выступают CLI2-L и CLI1-L. Для CLI2-L сконфигурируйте адрес 10.6.6.10, для CLI1-L 10.6.6.20
   d. Запуск соединения осуществляется скриптом wg_connect, остановка wg_disconnect. Скрипты должны вызываться из любого каталога без указания полного пути
   e. Будут пояснения и дополнения

7. Обеспечьте доступ к интернету для CLI1-L

a. Настройте динамическое преобразование порта источника для каждого проходящего пакета на LIN-RTR
b. CLI1-L должен получать адрес автоматически от LIN-RTR.
c. LIN-RTR подключается к провайдеру при помощи PPPoE. Настройте PPPoE клиент.
    i. Имя пользователя XXX Пароль YYYY
d. Выполните зонирование трафика на LIN-RTR.
    i. Все пакеты, попадающие из внешней сети считаются зоной external
    ii. Все пакеты, приходящие из внутренней сети, считаются зоной work.
    iii. Все пакеты, приходящие из GRE-туннеля считаются зоной internal
    iv. Любые пакеты, приходящие от CLI-1L считаются trusted.
e. Реализуйте следующие правила работы с трафиком
    i. Зона internal должна допускать работу служб, использующих связность, обеспеченную GRE-туннелем.
        1. Прочий трафик следует запретить
    ii. Зона external должна позволять работу служб IPSEC и GRE.
    iii. Исходящий трафик, покидающий внутреннюю сеть по любому каналу связи, проходит маскарадинг
    iv. Зона work позволяет работу средств автоконфигурации клиентов.
    v. Зона work разрешает работу средств DNS.

8. Между LIN-RTR и RTR настройте GRE туннель для обеспечения связанности с офисом HQ
    a. Используйте адресацию 10.10.10.1/30 и 10.10.10.2/30
    b. Будут пояснения и дополнения
9. Сконфигурируйте статическую маршрутизацию между LIN-RTR и RTR для достижения связности офисов и BRANCH
10. Сконфигурируйте свободный протокол исследования сети канального уровня таким образом, чтобы можно было идентифицировать сетевые устройства.

Технологии, работоспособность которых ожидается в день 2

Конфигурация активного сетевого оборудования

1. Обеспечьте возможность входа на RTR с использованием доменных реквизитов
    a. Группа MAdmins должна получать максимальный уровень привилегий при входе
    b. Группа SAdmins должна получать при входе уровень привилегий 5.
2. Для 5 уровня привилегий сконфигурируйте расширенный набор команд
    a. Добавьте возможность использования команд reload, debug и sh ip int br
3. Все неиспользуемые порты на всех коммутаторах отключите и переведите во VLAN1666
4. На портах f0/10 коммутаторов SW1 и SW2 реализуйте защиту от переполнения таблицы MAC адресов. Максимальное количество адресов 10, адреса должны автоматически сохраняются в конфигурации, при нарушениях политики, порт должен быть отключен
5. На всех коммутаторах центрального офиса реализуйте защиту от подмены DHCP сервера для подсети VLAN10. Необходимые порты сделайте доверенными. Установите для каждого порта ограничение на 150 пакетов в секунду
6. На всех коммутаторах центрального офиса реализуйте защиту от перехвата трафика между двумя узлами в одном широковещательном домене для подсети VLAN10.
7. На коммутаторах SW2 и SW3 реализуйте защиту от подмены MAC адреса
    a. Будут пояснения и дополнения
8. 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
9. Обеспечьте передачу нетегированного трафика через VLAN1500
10. На магистральных каналах обеспечьте передачу данных только сконфигурированных VLAN. Передача данных по VLAN 1 на магистральных каналах должна быть запрещена
11. Защитите при помощи IPSEC GRE туннели между RTR и BRANCH и между LIN-RTR и RTR
    a. Используйте произвольные параметры во всех фазах.
    b. Защиту туннелей обеспечьте средствами IPSEC (ikev2, для аутентификации используйте цифровые сертификаты выданные DomSubCA)

12. Сконфигурируйте маршрутизацию между BRANCH и RTR с использованием протокола EIGRP, не забыв избавиться от статических маршрутов
    a. Соседство устанавливается через GRE туннель
    b. Анонсируйте все сети, необходимые для достижения полной связанности в соответствии со схемой маршрутизации
    c. Настройте аутентификацию
    d. При отказе защищенного туннеля соседство должно устанавливаться через L2 VPN
13. Настройте маршрутизацию между LINRTR и RTR через защищенный туннель с использованием протокола OSPF, не забыв избавиться от статических машрутов
    a. Будут пояснения и дополнения
14. Настройте AnyConnect SSL-VPN средствами FW
    a. в качестве центра сертификации используйте DomSubCA
    b. Подключаться может только доменная группа MAdmins
    c. Анонсирована должна быть только сеть VLAN20
    d. Возможность подключения должна быть со всех внешних клиентских ПК
    e. Для подключения необходимо использовать только имя vpn.semifinal.ru
    f. Подключение необходимо произвести скриптом. Скрип должен отрабатывать как команда и быть доступен в консоли. подключение connect_vpn Отключение disconnect_VPN
15. Для обеспечения отказоустойчивости доступа в глобальную сеть настройте IP SLA с использованием протокола icmp для офиса BRANCH
    a. Параметры SLA произвольные
    b. Реализуйте автоматический переход на доступ в глобальную сеть через L2VPN и офис HQ при недоступности провайдеров ISP1 и ISP2
16. Необходимо обеспечить отказоустойчивость всех филиалов , без использования статических маршрутов

Конфигурация серверов под управлением ОС Windows

1. Для всех компьютеров в ip сети офиса BRANCH, под управлением ОС WINDOWS должно выводиться сообщение при входе “Welcome to Branch office!”.Для всех компьютеров в ip сети офиса HQ, под управлением ОС WINDOWS должно выводиться сообщение при входе “Welcome to main

office!” В домене branch.lan не должно присутствовать политик, обеспечивающих выполнение данного пункта, все они должны располагаться на сервере DS-W.

2. На сервере DMZ-W сконфигурируйте корневой центр сертификации. Переустанавливать ОС или добавлять сервер в домен запрещено.
    a. Имя центра сертификации RootCA
    b. Срок действия: 8 лет
    c. Тип центра сертификации Standalone Root CA
    d. Произведите настройку точек публикации CRT:
        1). Пути по-умолчанию
        2).На диске RootCA по пути:
        C:\Certs\<CertificateName>.crt
        3).FS-W: \InetPub\wwwroot\PKIData\<CertificateName>.crt
    e. Произведите настройку точки распространения CRT:
        http://cdp.semifinal.wsr/pki/<CertificateName>.crt
    f. Произведите настройку точек публикации CRL:
        1). Пути по-умолчанию
        2).На диске RootCA по пути:
        C:\Certs\<CrlNameSuffix>.crl
        3).FS-W: \InetPub\wwwroot\PKIData\<CrlNameSuffix>.crl
    g. Произведите настройку точки распространения CRL:
        http://cdp.semifinal.wsr/pki/<CrlNameSuffix>.crl

3. На сервере CS сконфигурируйте подчиненный центр сертификации
    a. Имя центра сертификации DomSubCA
    b. Срок действия: 4 года
    c. Тип центра сертификации Enterprise Subordinate CA
    d. Сертификат для данного центра должен быть выдан центром RootCA
    e. Произведите настройку точки распространения CRT:
        http://cdp.semifinal.wsr/pki/<CertificateName>.crt
    f. Произведите настройку точки распространения CRL:
        http://cdp.semifinal.wsr/pki/<CrlNameSuffix><DeltaCRLAllowed>.crl
    g. Обеспечьте защищенное подключение к хостовому серверу с хостовой машины. Ошибок, связанных с сертификатами возникать не должно. Сертификаты должны быть выданы DomSubCA.

4. На сервере DS-W разверните RDS
    a. Настройте SSO для автоматического доступа к порталу и опубликованным приложениям

b. У всех пользователей на рабочем столе должен присутствовать ярлык приложения wordpad
c. Web доступ к сайту должен осуществляться по протоколу https. Сертификат должен быть выписан центром DomSubCA, и восприниматься доверенным со всех устройств домена semifinal.wsr и branch.lan.

5. В обоих офисах сконфигурируйте стартовую страницу в браузере Internet explorer. Для офиса HQ www.semifinal.wsr, для офиса BRANCH rds.semifinal.wsr.
6. Настройте перенаправление каталогов Documents и Desktop в директорию FS-W: D:\Shares\Redirected для всех пользователей группы Workers
7. На всех клиентских ПК обоих доменов обеспечьте возможность входа только в рабочее время (9:00-18:00) для группы Workers
8. Отключите использование спящего режима на клиентских ПК, включая Linux клиентов
9. С серверов FS-W, DMZ-W и BRANCH-DC-W настройте перенаправление логов на сервер DS-W
    a. Должна осуществляться пересылка только системных журналов, а также журналов безопасности
    b. Обеспечьте сбор сообщений всех уровней
10. Будут пояснения и дополнения

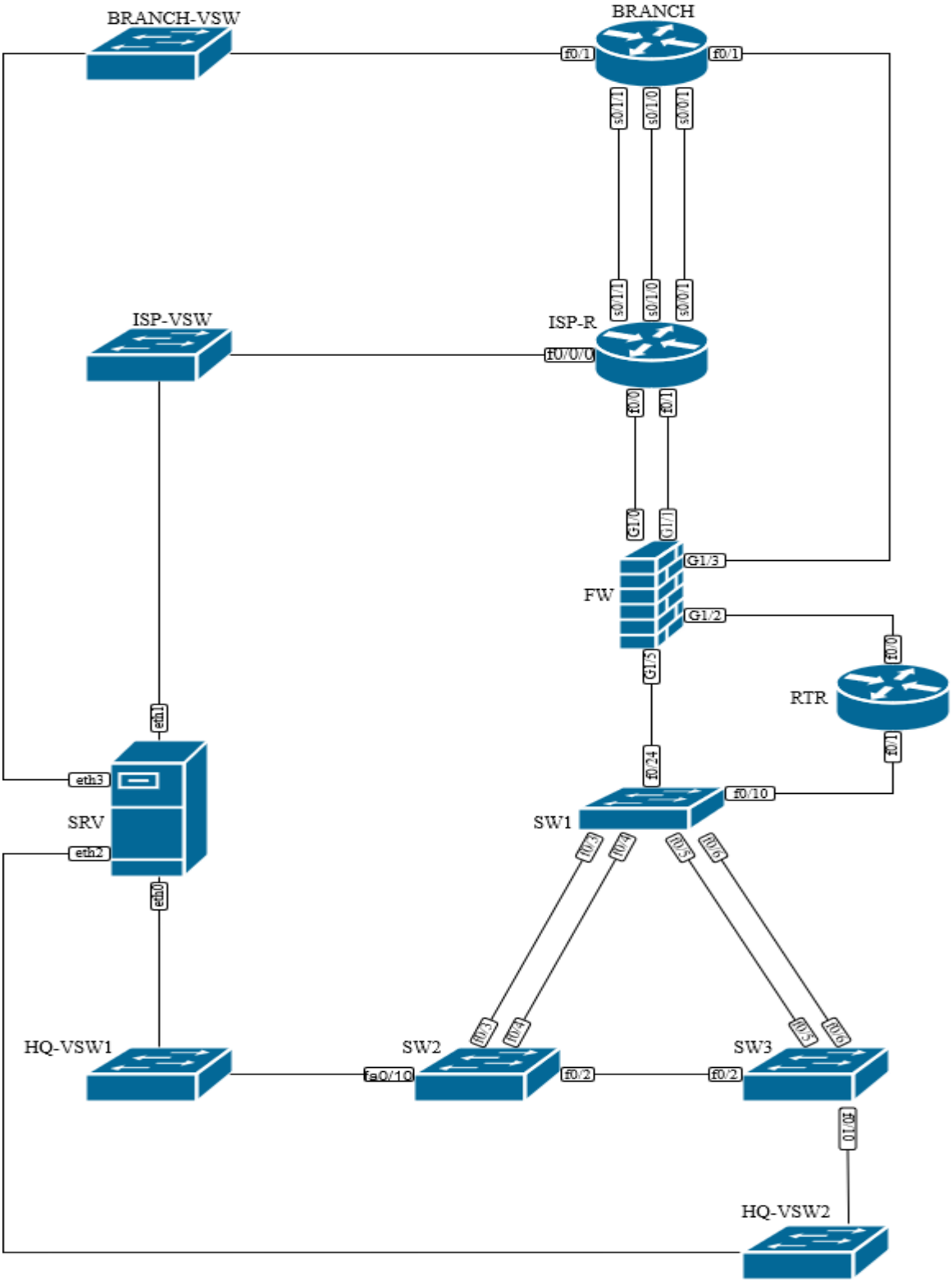
Конфигурация серверов под управлением ОС Linux

1. На хосте FS-L реализуйте TFTP-сервер.
    a. Создайте директорию /opt/Backup/tftp.
    b. Сделайте директорию корневой для tftp сервера
    c. Обеспечьте доступ для всех пользователей на чтение и запись
    d. Обеспечьте резервное копирование конфигурации маршрутизатора BRANCH в данную директорию. Резервное копирование должно производиться при каждом сохранении конфигурации. Файл должен называться BRRTR-<timestamp>.cfg
    e. Обеспечьте резервное копирование файлов nsswitch.conf и hosts и resolv.conf всех Linux серверов в данную директорию. Резервное копирование выполняется каждые 30 минут. Форматом имени считать <Хостнейм>-<ИмяФайла>.
2. Сконфигурируйте SSHv2 сервер на FS-L
    a. Сервер должен работать на стандартном порту
    b. Доступ ограничен пользователями root, sshuser
    c. Запретите использование пустых паролей

d. Разрешите открытие не более 5 SSH подключений в течении 120 секунд
e. Если подключение не активно в течении 5 минут, оно должно быть разорвано
f. При подключении клиентов на внешний адрес BRANCH порт 2222, должно происходить подключение к FS-L на стандартный порт

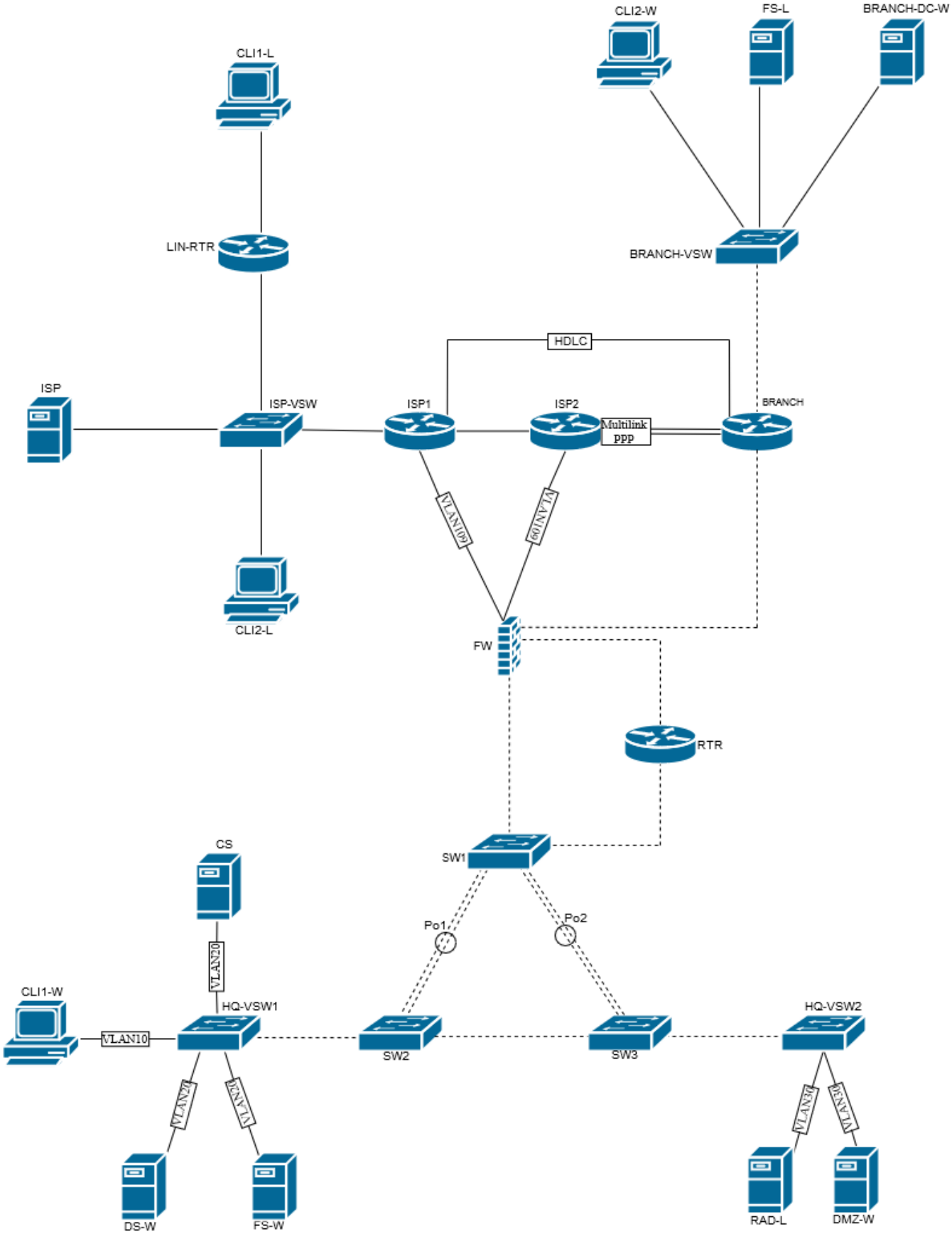
3. На CLI-2L сконфигурируйте SSH клиент. Создайте алиас FS-L со следующими параметрами
   a. Автоматическое подключение к порту 2222
   b. Сконфигурируйте аутентификацию при помощи ключей для пользователя sshuser
4. Настройте мониторинг LIN-RTR по протоколу SNMP v3
   a. Доступ происходит из под пользователя snmpuser с паролем snmpPa$$
   b. Шифрование AES. Хэш-функция SHA.
   c. Доступ аутентифицирован, передача данных зашифрована.
5. Сконфигурируйте скрипт для SNMP мониторинга на CLI1-L
   a. Хранение скрипта организовать в /opt/scripts
   b. Скрипт принимает на вход следующие параметры
      i. Тип аутентификации
      ii. Тип шифрования
      iii. Имя пользователя
      iv. Пароль
   c. Следует соблюдать порядок передачи параметров
   d. Скрипт должен вызываться из любого каталога без явного указания пути при помощи команды snmp_check
6. Реализуйте кэширующий DNS-сервер на LIN-RTR.
   a. Запросы, не попадающие в кэш, перенаправляются на RAD-L.
   b. Запросы к серверу принимаются исключительно от сети CLI-1L
   c. Обеспечьте фильтрацию запросов.
      i. Будут пояснения и дополнения.
7. Зашифруйте LVM-том при помощи VeraCrypt
   a. Будут пояснения и дополнения

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ

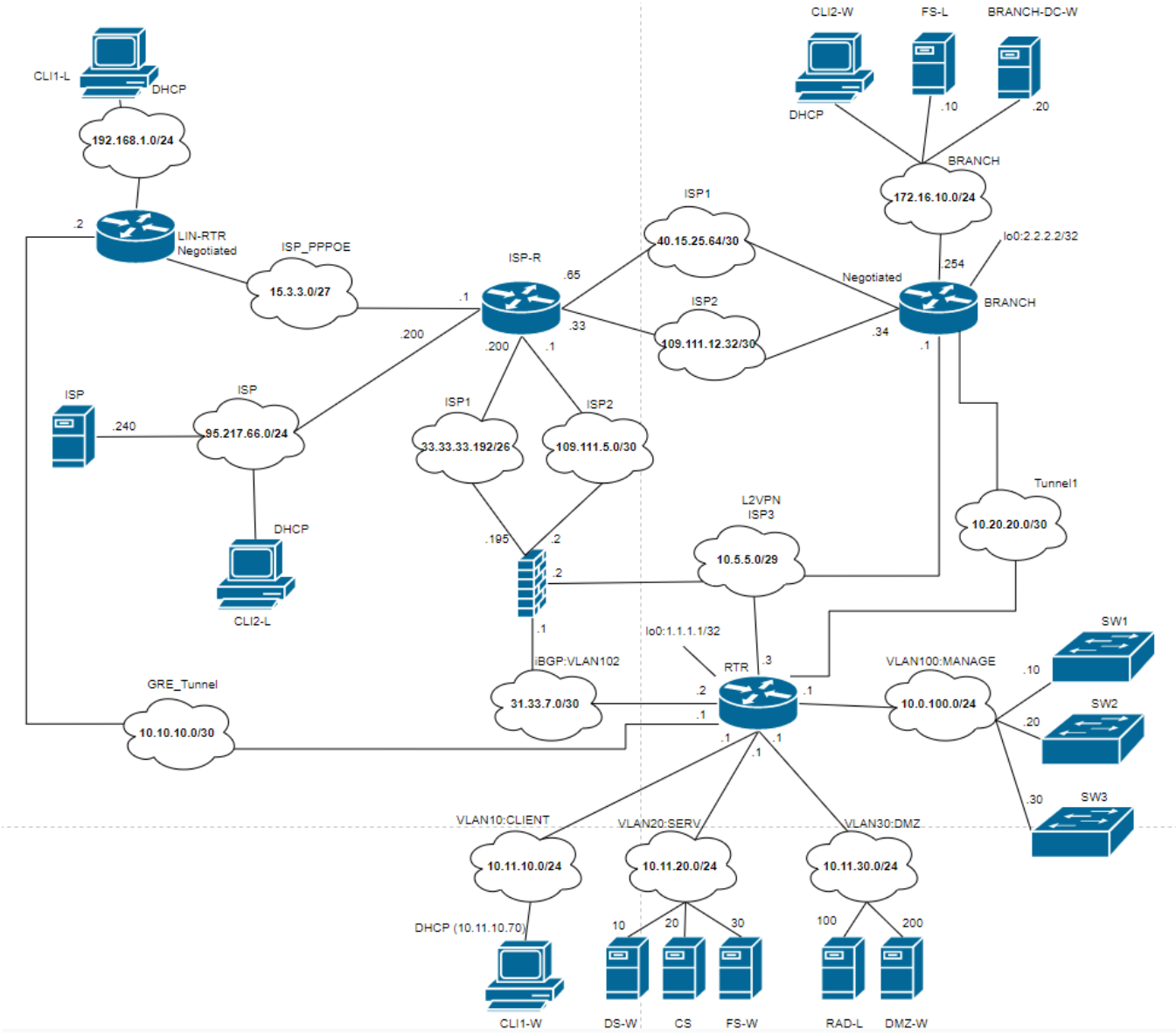


Тология L1

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***
FW	***ASDM/Telnet/SSH***	***5506***
All network devices	***Telnet/SSH***	***-***
CLI1-W	***GUI***	***Windows 10 Enterprise***
DS-W	***GUI***	***Windows Server 2019***
CS	***GUI***	***Windows Server 2019***
FS-W	***CLI***	***Windows Server 2019***
RAD-L	***CLI***	***Centos 8***
DMZ-W	***GUI***	***Windows Server 2019***
CLI2-W	***GUI***	***Windows 10 Enterprise***
FS-L	***CLI***	***Centos 8***
BRANCH-DC-W	***GUI***	***Windows Server 2019***
LINRTR	***CLI***	***Centos 8***
CLI1-L	***GUI***	***Centos 8***
CLI2-L	***GUI***	***Centos 8***
ISP	***CLI***	***Centos 8***