

Один: wqКонкурсное з

**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

ДНСР

Индивидуальный конкурс.

2) ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания являются работы по пусконаладке сетевой инфраструктуры на базе современного сетевого оборудования и операционных систем семейства Windows и Linux. Участники соревнований получают инструкцию, сетевые диаграммы и методические рекомендации по выполнению. Конкурсное задание имеет несколько модулей, выполняемых последовательно.

Задание национального финала является утвержденным. В нем присутствуют 3 из 5 модулей, т.е. возможно набрать максимально 45 из 100 баллов

Конкурс включает в себя “Пусконаладку инфраструктуры на основе ОС семейства Linux”; “Пусконаладку инфраструктуры на основе ОС семейства Windows”; “Пусконаладку телекоммуникационного оборудования”.

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.

Конкурсное задание должно выполняться в формате “один модуль в день”, циклически по модулям А-В-С. Оценка каждого модуля происходит ежедневно.

Задания разработаны и протестированы группой сертифицированных экспертов:

Таблица 1 – Группа сертифицированных экспертов

Модуль конкурсного задания		Роль	ФИО Эксперта
Модуль А: «Пусконаладка инфраструктуры на основе ОС семейства Linux»		Ведущий разработчик	М.М. Фучко
		Группа разработки	А.Г. Уймин
Модуль В: «Пусконаладка инфраструктуры на основе ОС семейства Windows»		Ведущий разработчик	Д.В. Дюгуров
Модуль С: «Пусконаладка телекоммуникационного оборудования»		Ведущий разработчик	С.И. Добрынин
		Группа разработки	А.А. Щербинин
		Группа разработки	А.Г. Уймин.

Ск

ДНСР

3. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице 2.

Таблица 2 – Время выполнение модуля

№ п/п	Наименование модуля	Рабочее	Время на задание
1	Модуль А: «Пусконаладка инфраструктуры на основе ОС семейства Linux»	В	5 ч.
2	Модуль В: «Пусконаладка инфраструктуры на основе ОС семейства Windows»		5 ч.
3	Модуль С: «Пусконаладка телекоммуникационного оборудования»		5 ч.

Ск

DHCP

--	--	--	--

Ск

Модуль А: «Пусконаладка инфраструктуры на основе ОС семейства Linux»

Версия 5 от 31.07.19.

ВВЕДЕНИЕ

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

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

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

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

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна 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, например, вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа.

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. На вас возлагается ответственность за распределение своего рабочего времени. Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

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

Ск

DHCP

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

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

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

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

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

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

В качестве системной ОС в организации LEFT используется Debian

В качестве системной ОС в организации RIGHT используется CentOS

Вам доступен диск CentOS-7-x86_64-Everything-1810.iso

Вам доступен диск debian-10.0.0-amd64-BD-1.iso

Вам доступен диск debian-10.0.0-amd64-BD-2.iso

Вам доступен диск debian-10.0.0-amd64-BD-3.iso

Вам доступен диск debian-10.0.0-amd64-BD-4.iso

Вам доступен диск Additional.iso, на котором располагаются недостающие RPM пакеты

Внимание! Все указанные компоненты предоставляются участникам в виде ISO-файлов на локальном или удаленном хранилище.

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.

ДНСР

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.

Ск

DHCP

Конфигурация хостов

- 1) Настройте имена хостов в соответствии с Диаграммой.
 - a)
- 2) На хостах Установите следующее ПО на ВСЕ виртуальные машины:
 - b) tcpdump
 - c) net-tools
 - d) curl
 - e) vim
 - f) lynx
 - g) dhclient
 - h) bind-utils
 - i) nfs-utils
 - j) cifs-utils
- 3) sshpassопируйте файл /etc/hosts в соответствии с Диаграммой (кроме адреса хоста L-CLI-A). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет.
- 4) В случае корректной работы DNS-сервисов ответы DNS должны иметь более высокий приоритет.
- 5) Все хосты должны быть доступны аккаунту root по SSH на стандартном(22) порту

Конфигурация сетевой инфраструктуры

- 1) Настройте IP-адресацию на ВСЕХ хостах в соответствии с Диаграммой.
- 2) Настройте сервер протокола динамической конфигурации хостов для L-CLI-A и L-CLI-B
 - a) В качестве DHCP-сервера организации LEFT используйте L-RTR-A.
 - i) Используйте пул адресов 172.16.100.65 — 172.16.100.75 для сети L-RTR-A
 - ii) Используйте пул адресов 172.16.200.65 — 172.16.200.75 для сети L-RTR-B
 - iii) Используйте адрес L-SRV в качестве адреса DNS-сервера.

Устанавливаем службу DHCP

1) **apt-get install isc-dhcp-server**

2) **vim /etc/default/isc-dhcp-server** - редактируем файл к следующему образу:

```
# Don't use options -cf or -pf here; use DHCPD_CONF/ DHCPD_PID instead
#OPTIONS=""

# On what interfaces should the DHCP server (dhcpd) serve DHCP requests?
#       Separate multiple interfaces with spaces, e.g. "eth0 eth1".
INTERFACESv4="ens224"
INTERFACESv6=""
~
~
```

Где указываем адрес интерфейса, который смотрит в сторону клиента

3) Далее в файле /etc/dhcp/dhcpd.conf - делаем такую запись

Задаем доменное имя (wsr) и доменный сервер (L-SRV)

Ск

DHCP

```
# option definitions common to all supported
option domain-name "skill39.wsr";
option domain-name-servers 172.16.20.10;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls
# attempt to do a DNS update when a lease is
# behavior of the version 2 packages ('none'
# have support for DDNS.)
ddns-update-style interim;
ddns-updates on;
zone skill39.wsr {
    primary 172.16.20.10;
}
zone 16.172.in-addr.arpa{
    primary 172.16.20.10;
}
}
```

- выполнение пункта про DDNS

```
subnet 172.16.100.0 netmask 255.255.255.0 {
    range 172.16.100.65 172.16.100.75;
    option routers 172.16.100.1;
}
subnet 172.16.200.0 netmask 255.255.255.0 {
    range 172.16.200.65 172.16.200.75;
    option routers 172.16.200.1;
}
subnet 172.16.50.0 netmask 255.255.255.252{
}
```

Далее чуть ниже раскомментируем строчки про подсети и настроим их как на скриншоте

Далее добавим, чтобы адрес на L-CLI-B прилетал статично

```
host passacaglia {
    hardware ethernet 00:0C:29:B6:02:E7;
    fixed-address 172.16.200.61;
    option-routers 172.16.200.1;
}
```

4) Перезапускаем службу - `systemctl restart dhcpd`

5) Проверить можно с помощью перезапроса адреса по DHCP с клиентов

На L_RTR_B нужно сделать DHCP Relay

1) Монтируй 2 диск дебиана и качай - `apt install isc-dhcp-relay -y`

Там все визардом протыкай, ставь два интерфейса и ТОЛЬКО один адрес dhcp сервера

2)

TSHOOT:

Ск

DHCP

```
rtt min/avg/max/mdev = 1.321/1.321/1.321/0.000 ms
root@L-RTR-A:~# tcpdump -i ens192 port 67 -vvvvvvv_
```

(полезная команда для дебага DHCP, вводи её на интерфейс, который должен принимать DHCP-запрос)

Команда для статического маршрута - `ip route add 172.16.200.0/24 via 172.16.50.1`
- крути на этом базовую маршрутизацию

`ethtool --offload eth0 rx off tx off` - отключение проверки UDP пакетам и его CRC

- b) Настройте DHCP-сервер таким образом, чтобы L-CLI-B всегда получал фиксированный IP-адрес в соответствии с Диаграммой.
 - c) В качестве шлюза по умолчанию используйте адрес интерфейса соответствующего маршрутизатора в локальной сети.
 - d) Используйте DNS-суффикс `skill39.wsr`.
 - e) DNS-записи типа A и PTR соответствующего хоста должны обновляться при получении им адреса от DHCP-сервера.
- 3) На L-SRV настройте службу разрешения доменных имен
- a) Сервер должен обслуживать зону `skill39.wsr`.
 - b) Сопоставление имен организовать в соответствии с Таблицей 1.
 - c) Настройте на R-SRV роль вторичного DNS сервера для зоны `skill39.wsr`.
 - i) Используйте адрес R-SRV в качестве адреса DNS-сервера для R-CLI.
 - d) Запросы, которые выходят за рамки зоны `skill39.wsr` должны пересылаться DNS-серверу ISP. Для проверки используйте доменное имя `ya.ru`.
 - e) Реализуйте поддержку разрешения обратной зоны.
 - f) Файлы зон располагать в `/opt/dns/`
`apt install bind9`
 Далее отредактируйте файл `/etc/bind/named.conf.options` - `vim /etc/bind/named.conf.options`

Ск

DHCP

```

options {
    directory "/var/cache/bind";

    // If there is a firewall between you and nameservers you want
    // to talk to, you may need to fix the firewall to allow multiple
    // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

    // If your ISP provided one or more IP addresses for stable
    // nameservers, you probably want to use them as forwarders.
    // Uncomment the following block, and insert the addresses replacing
    // the all-0's placeholder.

    forwarders {
        10.10.10.10;
    };

    //=====
    // If BIND logs error messages about the root key being expired,
    // you will need to update your keys.  See https://www.isc.org/bind-keys
    //=====
    dnssec-validation no;
    recursion yes;
    allow-query {any};

    listen-on { any; };
};

```

- отредактируйте файл следующим образом

Далее перейдите в редактирование файла `/etc/bind/named.conf.default-zones` - `vim /etc/bind/named.conf.default-zones`

$$C_K$$

DHCP

```
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "skill139.wsr" {
    type master;
    file "/opt/dns/skill139";
    allow-update {any;};
    allow-transfer {any;};
};

zone "16.172.in-addr.arpa" {
    type master;
    file "/opt/dns/172";
    allow-update {any;};
};

zone "168.192.in-addr.arpa" {
    type master;
    file "/opt/dns/192";
};
```

Создаем папку /opt/dns - mkdir /opt/dns

Скопировали пример прямой зоны -

g) cp /etc/bind/db.local /opt/dns/skill139.wsr

Скопировали пример обратной зоны - cp /etc/bind/db.127 /opt/dns/твоя подсеть

h)

vim /opt/dns/skill139.wsr

```
;
; BIND data file for local loopback interface
;
$TTL      604800
@         IN      SOA      skill139.wsr. root.skill139.wsr. (
                        2      ; Serial
                        604800 ; Refresh
                        86400  ; Retry
                        2419200 ; Expire
                        604800 ) ; Negative Cache TTL
;
@         IN      NS       skill139.wsr.
@         IN      A        172.16.20.10
l-cli-b   A       172.16.200.61
l-cli-a   A
l-srv     A       172.16.20.10
server    CNAME   l-srv
l-fw      A       172.16.20.1
r-fw      A       20.20.20.100
www        CNAME   r-fw
r-srv     A       192.168.20.10_
~
~
```

Ск

DHCP

LDAPьшпф

```
;
; BIND reverse data file for local loopback interface
;
$TTL      604800
@         IN      SOA      skill139.wsr. root.skill139.wsr. (
                        201926453      ; Serial
                        604800         ; Refresh
                        86400          ; Retry
                        2419200        ; Expire
                        604800 )       ; Negative Cache TTL
;
@         IN      NS       skill139.wsr.
10.20     IN      PTR      1-srv.skill139.wsr.
@         IN      A        172.16.20.10
2.50      IN      PTR      1-rtr-a.skill139.wsr.
2.55      IN      PTR      1-rtr-b.skill139.wsr.
61.200    IN      PTR      1-cli-b.skill139.wsr.
1.20      IN      PTR      1-fw.skill139.wsr.
```

На R-SRV - создай установи - yum install bind -y

Далее в файле vim /etc/named.conf -

```
one "skill139.wsr" IN {
    type slave;
    file "/opt/dns/skill139.wsr";
    masters { 172.16.20.10; };
};

include "/etc/named.rfc1912.zones";
```

Отключи все проверки и радуйся!

Пример для обратной и прямой зоны, дай максимальные права на эти файлы

4) На L-FW и R-FW настройте интернет-шлюзы для организации коллективного доступа в Интернет.

- Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса.
- Организируйте доступность сервиса DNS на L-SRV по внешнему адресу L-FW.
- Сервер L-FW должен перенаправлять внешние DNS запросы от OUT-CLI на L-SRV. www.skill139.wsr должен преобразовываться во внешний адрес R-FW.

Правило пиши вот такого типа:

```
iptables -t nat -A POSTROUTING -s 172.16.0.0/16 -o ens192 -j MASQUERADE
```

-t - идем по цепочке NAT

-A - при ПОСТроутинге

-s - подсеть внутри

-o - исходящий интерфейс

-j - выполняемое действие

В Debian пользуйся пост-апом (после loopback interface), а в CentOS качай

iptables-services и успешно конфигурируй все в файл /etc/sysconfig/iptables

Также, удобнее сначала ввести команду в CLI, а затем iptables-save >

Ск

DHCP

/etc/sysconfig/iptables.config - так точно взлетит!

```
iptables -t nat -A POSTROUTING -s 172.16.0.0/16 -o ens192 -j MASQUERADE
iptables -t nat -A PREROUTING -p udp --dport 53 -i ens192 -j DNAT --to-destination 172.16.20.10
~
~
```

На дебиан скачай пакет iptables-persistence и конфигурь файл /etc/iptables/rules.v4

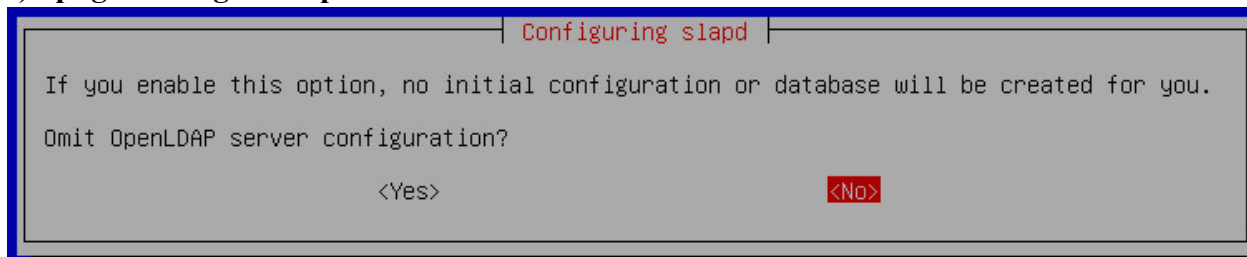
NAT на R-FW:

- 1) `firewall-cmd --zone=public --list-all` - данной командой ты увидишь, какие сетевые интерфейсы отнесены к зоне public, и где ICMP(и прочая туфта) запросы наглухо блочаться
- 2) `firewall-cmd --permanent --zone=trusted --add-interface=<NAME>` - данной командой добавляешь навсегда интерфейс в доверенную зону, где все запросы разрешены и все хорошо
- 3) `firewall-cmd --permanent --zone=public --add-masquerade` - включаешь нат на нем
- 4) Далее ребутай `firewalld` и должно все быть хорошо!

Для ya.ru

Службы централизованного управления и журналирования

- 1) Разверните LDAP-сервер для организации централизованного управления учетными записями
 - a) В качестве сервера выступает L-SRV.
 - b) Учетные записи создать в соответствии с Таблицей 2.
 - c) Группы(LDAP) и пользователей создать в соответствии с Таблицей 2.
 - d) Пользователи должны быть расположены в OU Users.
 - e) Группы должны быть расположены в OU Groups.
 - f) L-CLI-A, L-SRV и L-CLI-B должны аутентифицироваться через LDAP.
- 2) На L-SRV организуйте централизованный сбор журналов с хостов L-FW, L-SRV.
 - a) Журналы должны храниться в директории /opt/logs/.
 - b) Журналирование должно производиться в соответствии с Таблицей 3.
 - 1) `apt install slapd ldap-utils migrationtools`
 - 2) `dpkg-reconfigure slapd`



Ск

DHCP

Configuring slapd

The DNS domain name is used to construct the base DN of the LDAP directory. For example, 'foo.example.org' will create the directory with 'dc=foo, dc=example, dc=org' as base DN.

DNS domain name:

skill139.wsr

<Ok>

Configuring slapd

Please enter the name of the organization to use in the base DN of your LDAP directory.

Organization name:

skill139

<Ok>

Configuring slapd

HDB and BDB use similar storage formats, but HDB adds support for subtree renames. Both support the same configuration options.

The MDB backend is recommended. MDB uses a new storage format and requires less configuration than BDB or HDB.

In any case, you should review the resulting database configuration for your needs. See /usr/share/doc/slapd/README.Debian.gz for more details.

Database backend to use:

BDB
HDB
MDB

<Ok>

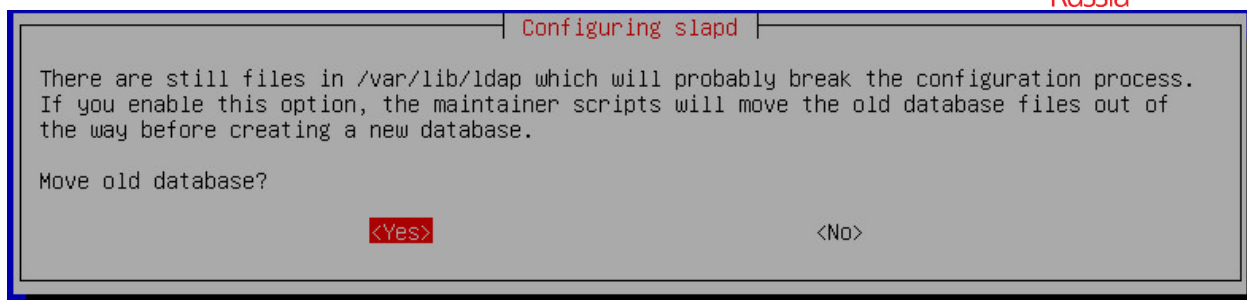
Configuring slapd

Do you want the database to be removed when slapd is purged?

<Yes> <No>

Ск

DHCP



vim ou.ldif

```
dn: ou=Admin,dc=skill39,dc=wsr
objectClass: organizationalUnit
ou: Admin

dn: ou=Users,dc=skill39,dc=wsr
objectClass: organizationalUnit
ou: Users
```

(тут вводи Guest)

ldapadd -x -W -D cn=admin,dc=skill39,dc=wsr -f ou.ldif

```
root@L-SRV:~# ldapadd -x -W -D cn=admin,dc=skill39,dc=wsr -f ou.ldif
Enter LDAP Password:
adding new entry "ou=Admin,dc=skill39,dc=wsr"

adding new entry "ou=Guest,dc=skill39,dc=wsr"

root@L-SRV:~#
```

groupadd -g 10000 Admin

groupadd -g 20000 Guest

tail -n2 /etc/group > /root/group

cd /usr/share/migrationtools

vim migrate_common.ph

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "skill39.wsr";

# Default base
$DEFAULT_BASE = "dc=skill39,dc=wsr";
```

cp migrate_common.ph /etc/perl

./migrate_group /root/group > /root/groups.ldif

vim /root/groups.ldif

#DELETE USER PASSWORD FOR GROUPS

```
dn: cn=Admin,ou=Admin,dc=skill39,dc=wsr
objectClass: posixGroup
objectClass: top
cn: Admin
gidNumber: 10000

dn: cn=Guest,ou=Guest,dc=skill39,dc=wsr
objectClass: posixGroup
objectClass: top
cn: Guest
gidNumber: 20000
```

Ск

DHCP

ldapadd -x -W -D "cn=Admin,dc=skill39,dc=wsr" -f groups.ldif

```
root@L-SRV:/usr/share/migrationtools# ldapadd -x -W -D "cn=Admin,dc=skill39,dc=wsr" -f /root/groups.
ldif
Enter LDAP Password:
adding new entry "cn=Admin,ou=Admin,dc=skill39,dc=wsr"

adding new entry "cn=Guest,ou=Guest,dc=skill39,dc=wsr"

root@L-SRV:/usr/share/migrationtools#
```

useradd -u 10001 -g 10000 tux

passwd tux

grep tux /etc/passwd > /root/tux

./migrate_passwd /root/tux > /root/tux.ldif

vim /root/tux.ldif

```
dn: uid=tux,ou=Admin,dc=skill39,dc=wsr
uid: tux
cn: tux
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {crypt}$6$KzGLFJM9EFnop7jI$syds2w1RDkzS10QkFg1hOK3brPhX50Yi09FcEwh7aCKSbIxpRqUNivYmKk
7vrJaOkJftsaCzd6hM99WILotr.
shadowLastChange: 18151
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/sh
uidNumber: 10001
gidNumber: 10000
homeDirectory: /home/tux
```

ldapadd -x -W -D "cn=Admin,dc=skill39,dc=wsr" -f /root/tux.ldif

vim /root/users.sh

```
#!/bin/bash
for i in $(seq 99); do
    useradd user$i -g 20000 -u 2000$i
    echo "user$i:P@ssw0rd" | chpasswd
done
```

sh /root/users.sh

grep user[1-99] /etc/passwd > /root/users

vim /etc/perl/migrate_common.ph

```
$NAMINGCONTEXT{'passwd'} = "ou=Guest";
```

./migrate_passwd /root/users > /root/users.ldif

Проверь, что пользователи создались в верных OU. Скорее всего у тебя там будет не так - пиши в vim такую команду - :%s/People/Guest/g

ldapadd -x -W -D "cn=Admin,dc=skill39,dc=wsr" -f /root/users.ldif

#Network folder setup on server

mkdir /homes

vim homes.sh

```
#!/bin/bash
for i in $(seq 99); do
    mkdir /homes/user$i
    chown user$i:Guest /homes/user$i
done
```

sh homes.sh

Ск

DHCP

```
mkdir /homes/tux
chown tux:Admin /homes/tux
mkdir /homes/user
chown user:user /homes/user
apt install nfs-kernel-server
```

```
Modified configuration file
exports: A new version (/usr/share/nfs-kernel-server/conf/files/etc.exports) of configuration
file /etc/exports is available, but the version installed currently has been locally
modified.

What do you want to do about modified configuration file exports?

install the package maintainer's version
keep the local version currently installed
show the differences between the versions
show a side-by-side difference between the versions
start a new shell to examine the situation

<Ok>
```

```
vim /etc/exports
```

```
/homes/ *(rw,sync,no_root_squash)
```

```
systemctl restart nfs-server
```

```
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=919b84ac-0e3c-4deb-9b6f-bbe9a5367f44 / ext4 errors=remount-ro 0
# swap was on /dev/sda5 during installation
UUID=60512f03-e4bf-4d87-9dd0-9ce547deec16 none swap sw 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
172.16.20.10:/opt/homes/ /home/ nfs defaults 0 0
~
~
~
```

CLIENT LDAP CONFIG

- 1) apt install libpam-ldapd libpam-ldapd
- 2) dpkg-reconfigure libpam-ldapd

```
Configuring libpam-ldapd
Please enter the Uniform Resource Identifier of the LDAP server. The format is
'ldap://<hostname_or_IP>:<port>/'. Alternatively, 'ldaps://' or 'ldapi://' can be used. The
port number is optional.

Using an IP address is recommended to avoid failures when domain name services are
unavailable.

LDAP server URI:
ldap://172.16.20.10
<Ok>
```

Ск

Configuring libpam-ldap

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

dc=skill39,dc=wsr

<Ok>

(Далее на два вопроса тыкай -NO, type password = clear, в пункте про галочки - ставь все и окей)

Далее в файле `/etc/passwd` - ищи строку `ram_passwd` и комментируй её
Ребутай комп

P.S. - тестить путём попытки зайти под пользователя из LDAP, если не работает - ставь libram-ldapd (мануэл по TSHOOT мы редактируем позже)

Если ты вдруг дурак, то удалять пользаков надо вот так:

```
#/bin/bash
for i in $(seq 99); do
    ldapdelete -x -D "cn=admin,dc=skill39,dc=wsr" -w 1 "uid=user$i,ou=Users,dc=skill39,dc=wsr"
done
root@kali:~#
```

```
# This will only work if netgroup service is available.
#+:@nis_group foo:ALL
-:ALL EXCEPT root (Admin):LOCAL
# User "john" should get access from ipv4 net/mask
#+:john:127.0.0.0/24
#
# User "john" should get access from ipv4 as ipv6 net/mask
```

Это на Л-СРВ. Затем удали локальных юзеров и будет тебе счастье!

$$\mathbf{C}_K$$

DHCP

```
# The PAM configuration file for the Shadow 'login' service
#
account required      pam_access.so ←
# Enforce a minimal delay in case of failure (in microseconds).
# (Replaces the 'FAIL_DELAY' setting from login.defs)
# Note that other modules may require another minimal delay. (for example,
# to disable any delay, you should add the nodelay option to pam_unix)
auth      optional    pam_faildelay.so  delay=3000000

# Outputs an issue file prior to each login prompt (Replaces the
# ISSUE_FILE option from login.defs). Uncomment for use
# auth      required    pam_issue.so issue=/etc/issue

# Disallows root logins except on tty's listed in /etc/securetty
# (Replaces the 'CONSOLE' setting from login.defs)
#
# With the default control of this module:
# [success=ok new_authtok_reqd=ok ignore=ignore user_unknown=bad default=die]
# root will not be prompted for a password on insecure lines.
# if an invalid username is entered, a password is prompted (but login
# will eventually be rejected)
#
# You can change it to a "requisite" module if you think root may mis-type
# her login and should not be prompted for a password in that case. But
# this will leave the system as vulnerable to user enumeration attacks.
#
# You can change it to a "required" module if you think it permits to
# guess valid user names of your system (invalid user names are considered
# as possibly being root on insecure lines), but root passwords may be
# communicated over insecure lines.
auth [success=ok new_authtok_reqd=ok ignore=ignore user_unknown=bad default=die] pam_securetty.so

# Disallows other than root logins when /etc/nologin exists
# (Replaces the 'NOLOGINS_FILE' option from login.defs)
auth requisite pam_nologin.so
"/etc/pam.d/login" ← 16L, 4975C written
root@L-SRV:/home/tux#
```

Службы логирования

На L-SRV прокомментируй строчки

```
module(load="imuxsock") # provides support for local system logging
module(load="imklog")   # provides kernel logging support
module(load="immark")   # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")
```

```
#
auth.* /opt/logs/L-SRV/auth.log
if $hostname contains 'L-FW' or $fromhost-ip contains "172.16.20.1" then {
    *.err /opt/logs/L-FW/error.log
}
```

И дописывай вышестоящие строчки

Ск

DHCP

Делаем на клиентах -

vim /etc/rsyslog.conf

```
#
auth,authpriv.* /var/log/auth.log
*. *;auth,authpriv.none -/var/log/syslog
*. * @172.16.20.10
#cron.* /var/log/cron.log
daemon.* -/var/log/daemon.log
kern.* -/var/log/kern.log
lpr.* -/var/log/lpr.log
mail.* -/var/log/mail.log
user.* -/var/log/user.log
```

Ребута!

Конфигурация служб удаленного доступа

1) На L-FW настройте сервер удаленного доступа на основе технологии OpenVPN:

- a) В качестве сервера выступает L-FW
- b) Параметры туннеля.
 - i) Устройство TUN.
 - ii) Протокол UDP.
 - iii) Применяется сжатие.
 - iv) Порт сервера 1122.
- c) Ключевая информация должна быть сгенерирована на R-FW.
- d) В качестве адресного пространства подключаемых клиентов использовать сеть 5.5.5.0/27.
- e) Хранение всей необходимой (кроме конфигурационных файлов) информации организовать в /opt/vpn.
- f) Подключившийся клиент должен быть автоматически сконфигурирован на использование DNS-инфраструктуры предприятия.

2) На OUT-CLI настройте клиент удаленного доступа на основе технологии OpenVPN:

- a) Запуск удаленного подключения должен выполняться скриптом start_vpn.sh
 - i) Отключение VPN-туннеля должно выполняться скриптом stop_vpn.sh.
 - ii) Скрипты должны располагаться в /opt/vpn.
 - iii) Скрипты должны вызываться из любого каталога без указания пути.
 - iv) Используйте следующий каталог для расположения файлов скриптов /opt/vpn/.
 - 1) apt install openvpn
 - v) 2) cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz /etc/openvpn
 - vi) gunzip /etc/openvpn/server.conf.gz
 - vii) vim /etc/openvpn/server.conf
 - viii)
 - ix)
 - x)
 - xi)
 - xii)

Ск

DHCP

xiii)

ОБЯЗАТЕЛЬНО! В папке /opt/vpn/ создай файл /opt/vpn/dh2048.pem -

xiv) **openssl dhparam -out dh2048.pem 2048**

xv)

xvi) Не забудь выпустит сертификат для L-FW:

1) **cd /etc/pki/tls/misc**

2) **./CA.pl -newreq-nodes**

3) **./CA.pl -sign**

4) И раскинуть его на L-FW, он находится в той же папке, что и CA.pl.
Увидишь сразу!

vim /etc/openvpn/client.conf

```
client
dev tun
proto udp
remote 10.10.10.1 1122
resolv-retry infinite
nobind
persist-key
persist-tun
ca /opt/vpn/ca.crt
cert /opt/vpn/OUT-CLI.crt
key /opt/vpn/OUT-CLI.key
comp-lzo
~
~
~
~
~
```

Раскинь и на OUT-CLI серты и ключи!

ln -s /opt/vpn/start_vpn.sh /bin/start_vpn

xvii) **ln -s /opt/vpn/stop_vpn.sh /bin/stop_vpn**

TSHOOT: если ругается на права, ставь на clients 400!

3) Настройте защищенный канал передачи данных между L-FW и R-FW с помощью технологии IPSEC:

a) Параметры политики первой фазы IPSec:

i) Проверка целостности SHA-1

ii) Шифрование 3DES

iii) Группа Диффи-Хеллмана — 14 (2048)

iv) Аутентификация по общему ключу WSR-2019

b) Параметры преобразования трафика для второй фазы IPSec:

i) Протокол ESP

ii) Шифрование AES

iii) Проверка целостности SHA-2

Ск

DHCP

- c) В качестве трафика, разрешенного к передаче через IPsec-туннель, должен быть указан только GRE-трафик между L-FW и R-FW

`yum install libreswan -y (CentOS)`

- d) `vim /etc/ipsec.conf`

```
config setup
conn vpn
    authby=secret
    auto=start
    type=tunnel
    left=20.20.20.100
    leftprotoport=gre
    right=10.10.10.1
    rightprotoport=gre
    ike=3des-sha1:modp2048
    phase2=esp
    phase2alg=aes128-sha2_512
    pfs=no
```

`vim /etc/ipsec.secrets`

```
include /etc/ipsec.d/*.secrets
20.20.20.100 10.10.10.1 : PSK "WSR-2019"
~
~
~
```

IPSEC DEBIAN

- e) `apt install strongswan -y`
f) `vim /etc/ipsec.conf`

```
# Sample VPN connections

conn vpn
    left=10.10.10.1
    leftprotoport=gre
    right=20.20.20.100
    rightprotoport=gre
    type=tunnel
    ike=3des-sha1-modp2048
    esp=aes128-sha2_256
    authby=secret
    auto=start
```

- g)

`vim /etc/ipsec.secrets` - также, как и на CentOS, только зеркально!

4) Настройте GRE-туннель между L-FW и R-FW:8

- a) Используйте следующую адресацию внутри GRE-туннеля:
i) L-FW: 10.5.5.1/30

Ск

DHCP

ii) R-FW: 10.5.5.2/30

На виртуальной машине L-FW создаем файл -

vim /etc/gre.up и приводим к следующему виду:

```
ip tunnel add tun1 mode gre local 10.10.10.1 remote 20.20.20.100 ttl 255
ip link set tun1 up
ip addr add 10.5.5.1/30 dev tun1
```

local - адрес локальный на машине

remote - адрес удаленного соседа по GRE

chmod +x /etc/gre.up - делаем скрипт исполняемым

vim /etc/network/interfaces - создаем файл и приводим его к следующему виду:

```
auto ens160
iface ens160 inet static
address 10.10.10.1/24
gateway 10.10.10.10
    post-up /etc/gre.up
    post-down ip tunnel del tun1
```

/etc/gre.up - исполняем скрипт

На виртуальной машине R-FW создаем файл

vim /etc/gre.up и приводим к следующему виду:

chmod +x /etc/gre.up - делаем скрипт исполняемым

```
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,
# | | | | |
# * * * * * user-name command to be executed
@reboot root /etc/gre.up
~
~
~
~
```

На CentOS - добавь свой суперскрипт в /etc/crontab, как и iptables.up

5) Настройте динамическую маршрутизацию по протоколу OSPF с использованием пакета FRR:

- Анонсируйте все сети, необходимые для достижения полной связности.
- Применение статических маршрутов не допускается.
- В обмене маршрутной информацией участвуют L-RTR-A, L-RTR-B, R-RTR, L-FW и R-FW.
- Соседство и обмен маршрутной информацией между L-FW и R-FW должно осуществляться исключительно через настроенный GRE-туннель.
- Анонсируйте сети локальных интерфейсов L-RTR-A и L-RTR-B.

Ск

DHCP

- f) Запретите рассылку служебной информации OSPF в сторону клиентских машин и глобальной сети.

- 1) Установка FRR - apt install frr
- 2) Далее файл /etc/frr/daemons - редакция ospfd = yes
- 3) Ребутай службу
- 4) ifconfig lo:40 192.168.40.1 netmask 255.255.255.0 up

g)

```
#
bgpd=no
ospfd=yes
ospf6d=no
ripd=no
ripngd=no
isisd=no
pimd=no
ldpd=no
nhrpd=no
eigrpd=no
babeld=no
sharpd=no
pbrd=no
bfd=no
```

Приводи к следующему виду -

- 3) Далее пример для L-FW, задавай ospf id и вбивай подсети

```
router ospf
ospf router-id 3.3.3.3
passive-interface ens224
network 10.10.10.0/24 area 0.0.0.1
network 172.16.20.0/24 area 0.0.0.1
network 172.16.50.0/30 area 0.0.0.1
network 172.16.55.0/30 area 0.0.0.1
```

Анонс локальных подсетей:

```
ip link add dev lo1 type dummy
ip addr add 1.1.1.1/32 dev lo1
ip link set lo1 up_
```

- h) - ВОТ ТАК СОЗДАТЬ ЛУПБАК!!!!

- 4) Настройка и установка IPSEC -

L-FW - apt install libreswan strongswan -y

На CentOS настройка аналогичная, только из диска поставь libcares, все работает

НЕ надо шарить сети, которые смотрят в сторону ISP

- 6) На L-FW настройте удаленный доступ по протоколу SSH:

- a) Доступ ограничен пользователями ssh_p, root и ssh_c

Ск

DHCP

- i) В качестве пароля пользователь (кроме root) использовать ssh_pass.
- ii) root использует стандартный пароль

vim /etc/ssh/sshd_config

```
# Authentication:
AllowUsers root ssh_p ssh_c
#LoginGraceTime 2m
PermitRootLogin yes
```

- b) SSH-сервер должен работать на порту 22
- 7) На OUT-CLI настройте клиент удаленного доступа SSH:
- a) Доступ к L-FW из под локальной учетной записи exit
 - b) си root под учетной записью ssh_p должен происходить с помощью аутентификации на основе открытых ключей.

Vim /etc/ssh/sshd_config

ssh-keygen

ssh-copy-id ssh_p@10.10.10.1

Конфигурация веб-служб

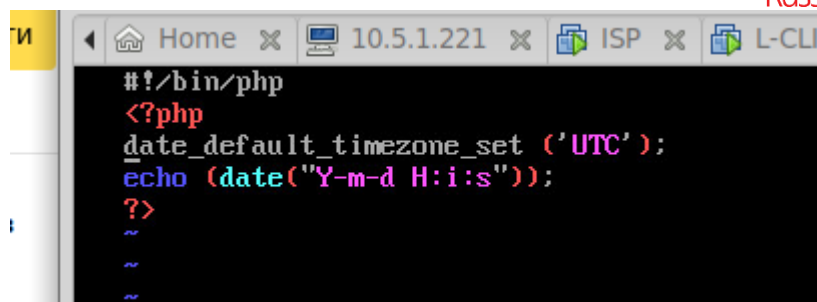
- 1) На R-SRV установите и настройте веб-сервер apache:
 - a) Настройте веб-сайт для внешнего пользования www.skill39.wsr.
 - i) Используйте директорию /var/www/html/out.
 - ii) Используйте порт 8088.
 - yum install httpd
 - iii) vim /etc/conf.d/vhosts.conf

```
<VirtualHost www.skill39.wsr:8088>
    DocumentRoot "/var/www/html/out"
    ServerName www.skill39.wsr
    <Directory /var/www/html/out>
        Require all granted
    </Directory>
</VirtualHost>
```

- iv) ~
- v) systemctl enable --now httpd
- vi) Сайт предоставляет доступ к двум файлам.
 - 1) index.html, содержимое "Hello, www.skill39.wsr is here!"
 - 2) date.php(исполняемый PHP-скрипт), содержимое:
 - a) Вызов функции date('Y-m-d H:i:s');

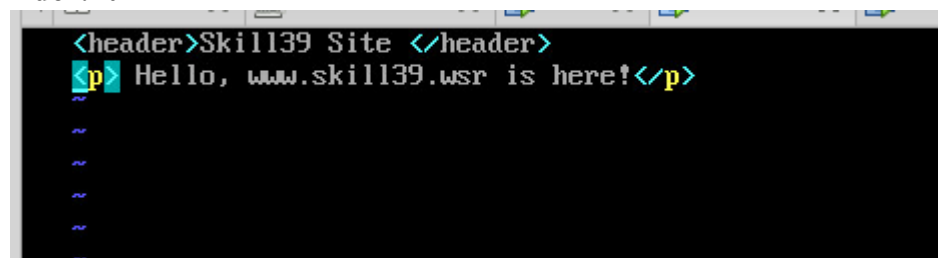
date.php - (bin/php - не надо!

Ск



```
#!/bin/php
<?php
date_default_timezone_set ('UTC');
echo (date("Y-m-d H:i:s"));
?>
```

index.html



```
<header>Skill139 Site </header>
<p> Hello, www.skill139.wsr is here!</p>
```

Также отредактируй файл /etc/httpd/conf/httpd.conf - укажи, чтобы слушал порт 8088, и DocumentRoot - /var/www/html/out

2) На R-FW настройте реверс-прокси на основе NGINX:

- a) Сайт **www.skill39.wsr** должен быть доступен из внешней сети по внешнему адресу R-FW
- b) Все настройки, связанные с заданием, должны содержаться в отдельном конфигурационном файле в каталоге /etc/nginx/conf.d/task.conf
 - i) Конфигурация основного файла должна быть минимальной и не влиять на работу NGINX в рамках выполнения задания.
- c) Настройте SSL и автоматическое перенаправление незащищенных запросов на HTTPS-порт того же самого сервера.
- d) Реализуйте пассивную проверку работоспособности бекенда.
 - i) Считать веб-сервер неработающим после 4 ошибок.
 - ii) Считать веб-сервер неработающим в течение 43 секунд.
- e) Реализуйте кэширование:
 - i) Запросы к любым PHP-скриптам не должны кэшироваться.
 - ii) Кэширование успешных запросов к остальным типам данных должно выполняться в течение 40 секунд.

DHCP

iii) vim /etc/nginx/conf.d/task.conf

```
proxy_cache_path /etc/nginx/cache keys_zone=cache:30m;
upstream backend{
    server 192.168.20.10:8088 max_fails=4 fail_timeout=43s;
}
server {
    listen 20.20.20.100:80;
    server_name www.skill39.wsr;
    return 301 https://www.skill39.wsr/$request_uri;
}

server {

    listen 20.20.20.100:443 ssl;
    server_name www.skill39.wsr;
    ssl_certificate /var/www.crt;
    ssl_certificate_key /var/www.key;

    location / {
        proxy_pass http://backend;
        proxy_cache cache;
        proxy_cache_valid 40s;

    }

    location ~* \.php$ {
        proxy_cache_bypass $cookie_nocache;
        proxy_pass http://backend;
    }

}

[root@R-FW ~]#
```

Приведи файл к следующему виду

Конфигурация служб хранения данных

1) Реализуйте синхронизацию каталогов на основе демона rsyncd.

а) В качестве сервера синхронизации используется L-SRV.

- i. Для работы синхронизации создайте специального пользователя mrsync
- ii. Домашний каталог данного пользователя должен быть расположен в /opt/sync/. Данный каталог используйте как каталог синхронизации
- iii. Домашний каталог не должен содержать никакой посторонней информации.
- iv. Для выполнения синхронизации создайте rsync-пользователя sync с паролем parol666.

v. Подключение к rsyncd должны быть разрешены исключительно от клиентов L-CLI-A и L-CLI-B

Установи службу rsync - apt install rsync

Также создай пользователя mrsync, задай ему пароль и сделай владельцем на папку /opt/sync/*

1) Далее в конфиге пиши - vim /etc/default/rsync

```
# all this does is p
# about not starting
RSYNC_ENABLE=true
```

Ск

DHCP

- vi. 3) Приведи файл /etc/rsyncd.conf к такому виду -
- vii. СВЕРХУ ФАЙЛА ПИШИ - uid=mrsync

```
[data]

    path = /opt/sync
    read only = false
    auth users = sync
    secrets file = /etc/rsyncd.secrets
    hosts allow = L-CLI-A.skill139.wsr, L-CLI-B.skill139.wsr
    hosts deny = *
```

- viii. Создай файл /etc/rsyncd.secrets

```
-bash: vcat: command not found
root@L-SRV:/opt/sync# cat /etc/rsyncd.secrets
sync:parol666
root@L-SRV:/opt/sync#
```

Дай на файл 400 права

Для L-CLI-A

```
#!/bin/bash
sleep 10
pass="/etc/pass"
chown sync:sync /root/sync/*
rsync -a --password-file $pass --delete -0 /root/sync/ sync@server.skill139.wsr::data
~
~
```

Для L-CLI-B

```
#!/bin/bash
pass="/etc/pass"
chown sync:sync /root/sync/
rsync -avz --password-file $pass sync@172.16.20.10::data /root/sync
~
~
~
```

Выдай ему максимум прав + права на исполнение , чтобы наверняка!

На клиенте в crontab пиши -

```
47 6 * * 7 root test -x /usr/sb
52 6 1 * * root test -x /usr/sb
)
*/1 * * * * root /root/sync.sh
#
```

(+ измени shell на /bin/bash)

Проверить можно - путем создания на клиенте папочки, через минуту должен увидеть её на L-SRV

Ск

DHCP

- b) В качестве клиентов используются L-CLI-A и L-CLI-B
 - i. Синхронизируемый каталог располагается по адресу /root/sync/
 - ii. Каталоги должны быть зеркально идентичны по содержимому.
 - 1. Приоритетным каталогом считается каталог на L-CLI-A
 - iii. Реализуйте синхронизацию в виде скрипта:
 - 1. Скрипт находится по адресу /root/sync.sh
 - 2. Автоматизация скрипта реализована средствами cron пользователя root.

Конфигурация параметров безопасности и служб аутентификации

1) Настройте CA на R-FW, используя OpenSSL.

- a) Используйте /etc/ca в качестве корневой директории CA
- b) Атрибуты CA должны быть следующими:
 - i) Страна RU
 - ii) Организация WorldSkills Russia
 - iii) CN должен быть установлен как WSR CA
- c) Создайте корневой сертификат CA
- d) Все клиентские операционные системы должны доверять CA
- 1) yum localinstall ** - сначала установи пакетики из аддишналов
- e) 2) yum install openssl* -y - потом монтируй основной диск и ставь оттуда
- f) 3) vim /etc/pki/tls/openssl.cnf

Меняешь директорию на ту, что по заданию

```
dir = /etc/ca # Where everything is kept
```

```
[ req_distinguished_name ]
countryName           = Country Name (2 letter code)
countryName_default   = RU
countryName_min       = 2
countryName_max       = 2

stateOrProvinceName   = State or Province Name (full name)
stateOrProvinceName_default = Oblast

localityName          = Locality Name (eg, city)
localityName_default  = Ekb

0.organizationName     = Organization Name (eg, company)
0.organizationName_default = WorldSkills Russia
```

- g) Далее меняешь все, как на скриншоте
 - h) cd /etc/pki/tls/misc - идем в дир. с суперскрипт
 - i) mkdir /etc/ca - создать дир. по заданию
 - j) chmod 777 /etc/ca - выдать ему права, на всякий случай
 - k) В САТОР надо поменять директорию!
 - l) ./CA.pl -newca - выписываем новый суперсерт
 - m) ./CA.pl -newreq-nodes - выписываем серт для нодов
 - n) ./CA.pl -sign - подписываем его
 - o) mv newcert.pem /root/[www.crt](#) - серт для сайтика - серт должен быть на R-FW!
 - p) mv newcert.pem /root/[www.key](#) - ключик для сайтика
- Ск

DHCP

- q) `cp /etc/ca/cacert.pem /root/ca.crt` - копируем корневой ЦА в отдельный документ
- r) `scp ca.crt root@<ip_addr>:/root/` - раскидали серт на клиентов (настрой SSH на Debian) -

Как добавить сертификат в доверенный?

1) На CentOS - `cp ca.crt /etc/pki/ca-trust/source/anchors`

s) `update-ca-trust external`

2) На Debian -

t) `cp ca.crt /usr/share/ca-certificates` - копируй серт туда

`dpkg-reconfigure ca-certificates` - потом эту магию, там все поймешь

u)

v)

3) Настройте межсетевой экран `iptables` на L-FW и `firewalld` на R-FW

- a) Запретите прямое попадание трафика из сетей в Internal
- b) Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора L-FW
- c) Разрешите необходимый трафик для создания IPSec и GRE туннелей между организациями
- d) Разрешите SSH подключения на соответствующий порт
- e) Для VPN-клиентов должен быть предоставлен полный доступ к сети Internal
- f) Разрешите необходимый трафик к серверам L-SRV и R-SRV для работы настроенных сервисов.
- g) Остальные сервисы следует запретить.
 - i) В отношении входящих (из внешней сети) ICMP запросов поступать по своему усмотрению

На L-FW(Debian):

Ск

DHCP

```
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

-A FORWARD -i ens256 -j ACCEPT
-A FORWARD -i ens161 -j ACCEPT
-A FORWARD -i ens224 -j ACCEPT
-A FORWARD -i tun0 -j ACCEPT
-A FORWARD -i tun1 -j ACCEPT

-A INPUT -i ens256 -j ACCEPT
-A INPUT -i ens161 -j ACCEPT
-A INPUT -i ens224 -j ACCEPT
-A INPUT -i tun0 -j ACCEPT
-A INPUT -i tun1 -j ACCEPT

-A FORWARD -s 172.16.0.0/16 -o ens192 -j ACCEPT

-A INPUT -p udp -i ens192 --dport 1122 -j ACCEPT
-A INPUT -p tcp -i ens192 --dport 22 -j ACCEPT
-A INPUT -p 47 -i ens192 -j ACCEPT
-A INPUT -p esp -i ens192 -j ACCEPT
COMMIT
```

Ск

DHCP

Ha R-FW (CentOS):

```

102 firewall-cmd
103 firewall-cmd --zone=public --list-all
104 ip a
105 firewall-cmd --permanent --zone=trusted --add-interface=ens224
106 firewall-cmd --permanent --zone=trusted --add-interface=ens256
107 vim /etc/sysconfig/iptables
108 ip a
109 firewall-cmd --permanent --zone=trusted --add-interface=tun1
110 systemctl restart iptables
111 firewall-cmd --zone=trusted --list-all
112 systemctl status firewalld
113 systemctl start firewalld
114 firewall-cmd --zone=trusted --list-all
115 ip r
116 vtysh
117 firewall-cmd --zone=trusted --list-all
118 firewall --zone=public --list-all
119 firewall-cmd --zone=public --list-all
120 firewall-cmd --zone=public --add-masquerade
121 firewall-cmd --zone=public --list-all
122 firewall-cmd --permanent --zone=public --list-all
123 firewall-cmd --permanent --zone=public --add-masquerade
124 firewall-cmd --permanent --zone=public --add-service=http
125 firewall-cmd --permanent --zone=public --add-service=https
126 firewall-cmd --permanent --zone=public --add-protocol=gre
127 firewall-cmd --permanent --zone=public --add-protocol=esp
128 ping 10.5.5.1
129 firewall-cmd --permanent --zone=public --add-service=ssh
130 ipsec status
131 ping 10.5.5.1
132 ping 10.5.5.2
133 ping 10.5.5.1
134 ipsec status
135 ip a
136 firewall-cmd --zone=public --list-all
137 firewall-cmd --zone=trusted --list-all
138 firewall-cmd --zone=public --list-all
139 firewall-cmd --permanent --zone=public --add-service=http
140 firewall-cmd --zone=public --list-all
141 firewall-cmd --reload
142 firewall-cmd --zone=public --list-all
143 ping 10.5.5.1
144 ping 10.5.5.2
145 ipsec status
146 firewall-cmd --list-all
147 firewall-cmd --permanent --add-port=47/tcp
148 firewall-cmd --permanent --add-port=47/tcp --zone=public
149 ping 10.5.5.1

```

Ск

Таблица 1 – DNS-имена

Хост	DNS-имя
L-CLI-A	A,PTR: l-cli-a.skill39.wsr
L-CLI-B	A,PTR: l-cli-b.skill39.wsr
L-SRV	A,PTR: l-srv.skill39.wsr CNAME: server.skill39.wsr
L-FW	A: l-fw.skill39.wsr
R-FW	A: r-fw.skill39.wsr CNAME: www.skill39.wsr
R-SRV	A,PTR: r-srv.skill39.wsr

Таблица 2 – Учетные записи LDAP

Группа	CN	Пароль	Доступ
Admin	tux	toor	L-SRV, L-CLI-A L-CLI-B
Guest	user1 – user99	P@ssw0rd	L-CLI-A L-CLI-B

DHCP

Таблица 3 – Правила журналирования

Источник	Уровень журнала (строгое соответствие)	Файл
L-SRV	auth.*	/opt/logs/<HOSTNAME>/auth.log
L-FW	*.err	/opt/logs/<HOSTNAME>/error.log

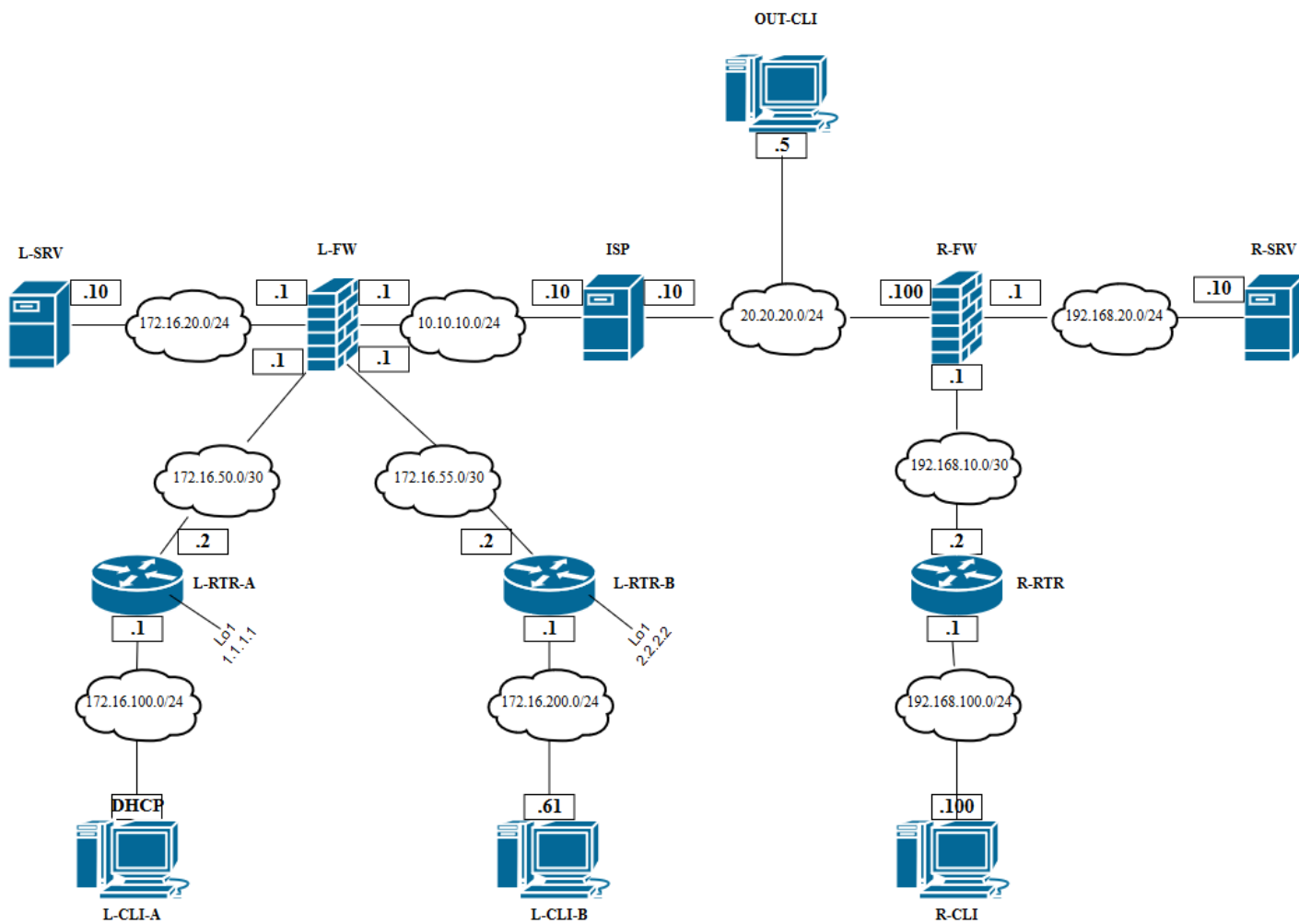
*<HOSTNAME> - название директории для журналируемого хоста

**В директории /opt/logs/ не должно быть файлов, кроме тех, которые указаны в таблице

Ск

DHCP

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



Ск

DNCP

Модуль В: «Пусконаладка инфраструктуры на основе ОС семейства Windows»

Версия 2 от 31.07.19.

ВВЕДЕНИЕ

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.

В рамках легенды конкурсного задания Вы – системный администратор компании, находящейся в городе Казань. В главном офисе вы управляете доменом **Kazan.wsr**. Вам необходимо настроить сервисы в локальной сети головного офиса.

Компания, в которой вы работаете, хочет выйти на рынки северной Европы. Для этого она устанавливает партнерские отношения с одной из компаний, находящейся в Санкт-Петербурге. Вам нужно помочь администратору партнерской компании с настройкой своего домена (**SPB.wse**), а потом настроить между доменами доверие.

Также Вам предстоит настроить канал связи между офисами с помощью статических маршрутов.

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: **Administrator/P@ssw0rd**.

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

КОМПЛЕКТАЦИЯ КОНКУРСНОГО ЗАДАНИЯ

1. Текстовые файлы:
 - данный файл с конкурсным заданием;
 - файл дополнений к конкурсному заданию, содержащий: описание вида предустановок, описание используемых операционных систем, а также рекомендации по выделению ресурсов для виртуальных машин.
2. Программное обеспечение:
 - Windows10.ADMX.

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

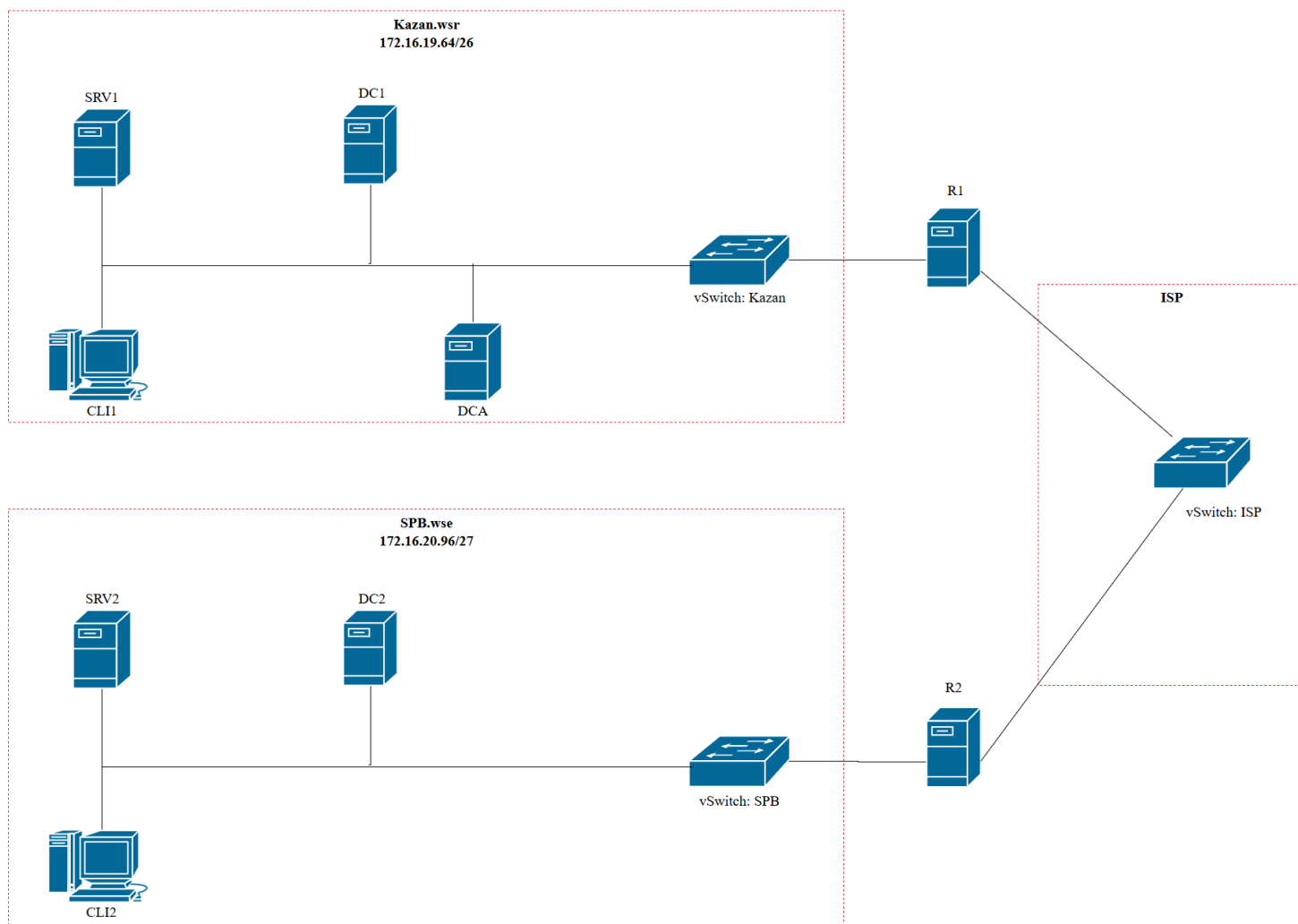
Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.

Ск

DHCP

Network diagram



Ск

Настройка DC1

Базовая настройка

- переименуйте компьютер в DC1;
- в качестве адреса DC1 используйте первый возможный адрес из подсети 172.16.19.64/26;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.

Active Directory

- сделайте сервер контроллером домена Kazan.wsr.

DHCP

- настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все незанятые серверами адреса в подсети;
- настройте failover: mode – Load balancer, partner server – SRV1, state switchover – 5 min;
- настройте дополнительные свойства области (адреса DNS-серверов и основного шлюза).

Переходи DHCP Manager - IPv4(ПКМ) - Configure Failover - Partner Server - пиши SRV1 - Next - далее все интуитивно понятно!

DNS

- настройте необходимые зоны прямого и обратного просмотра;
- создайте все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
- обеспечьте разрешение имен сайтов обеих компаний.

Если не работает DNS - ipconfig /flushdns - может помочь

DNS ты настраивать умеешь, чтобы разрешить имена для обеих компаний - вбей в Conditonal Forwarders - DC2 spb.wse

GPO

- запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;

В создании GPO - тыкай следующий путь - Computer Configuration - Admin.templates - System - Logon - и там GPO Show first sigh тыры пыры - нажимай Disabled

- 00члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;

Иди по пути Computer Manger - Policies - Windows Settings - Security - Restricted Groups - там создавай новую группу IT

В момент добавления выбирай Второй параметр - и добавляй в группу Administrators

-

в браузерах IE Explorer и Microsoft Edge должна быть настроена стартовая страница –

Ск

www.kazan.wsr;

Установи пакет из диска с административными файлами, запомни ссылку, куда установится служба.

Далее скопируй её в папку Policies - по пути - \\127.0.0.1\\sysvol\\Kazan.wsr\\Policies

Для IE - Group Policy Preferences: User Configuration - Preferences - Control Panel settings - Internet Settings

Для Edge -

Там создавай свою политику, все интуитивно понятно - когда надпись станет зеленой, значит все работает! Нажимай F5!

Для Edge - Computer Configuration -> Administrative Template -> Windows Components -> Microsoft Edge (

- члены группы Sales при обращении к общим папкам группы IT должны получать уведомление следующего вида: «У вас нет прав доступа к папке [путь к папке]! Не пытайтесь повторить!».

Для того, чтобы сделать это в GPO и делай там следующие параметры -

Computer Configuration\\Policies\\Administrative Template\\System\\Access-Denied-Assistance - далее Customize message for AD errors - переходишь в Enabled и ниже в окошке пишешь такую фразу - You do not have permissions to use this path - [Original File Path]! Do not try it again!

Готово!

-
- также, создай GPO, чтобы разрешить ICMP в сети. Для этого иди по пути - Computer Manager - Policies - Windows settings - Security - Windows Firewall - Windows Defender - Inbound Area and Outbound area. В визарде выбирай Predefined - File and Printer Sharing. В списке правил убери все галки, оставь только на ICMP. Повтори фокус на OutBound.

Элементы доменной инфраструктуры

- создайте подразделения: IT и Sales;
- в соответствующих подразделениях создайте одноименные доменные группы.
- в каждой группе создайте с помощью скрипта по 30 пользователей. Все учетные записи должны иметь возможность входа в домен с логином, созданным по следующему шаблону *НазваниеГруппы_ПорядковыйНомерПользователя@kazan.wsr*. Пароли должны быть созданы по следующему шаблону: *НазваниеГруппы_ПорядковыйНомерПользователя*, но записанному наоборот (справа-налево). Все учетные записи пользователей должны быть включены. Вход в систему должен быть обеспечен для всех пользователей со всех клиентских компьютеров домена и рядовых серверов.
- для каждого пользователя, члена группы IT, создайте автоматически подключаемую в качестве диска U:\ домашнюю папку внутри папки по адресу

Ск

SRV1→d:\shares\IT;

Сначала делаем шару - (по классике, как надо) (проверь, что диск в онлайн, что он отображается в Server Manager и все такое) (важно иметь установленным на данном сервере File Manager)

Далее, проверь что она доступна по пути - (в оснастке шары нажми опен шара)

Скопируй ссылку на шару и иди в Юзеры - выделяй их все мышкой, иди в пункт профайл, там будет хоум фолдер.

Дальше чакры помогут!

- **все пользователи при первом входе в домен с компьютера CLI1 должны видеть на рабочем столе ярлык программы *Калькулятор*.**

Для создания ярлыка Калькулятор тыкай - User Configuration - Preferences - Shortcuts - New. + Location - Desktop

В параметрах задавай действие Action, Target Type - File System - Target path - ссылка на калькулятор (C:\Windows\System32\calc.exe)

СуперСкрипт для пользователей для регионала

и

Важная поправка, скрипт не даст записать таких пользователей, так как его парольная политика говорит о большей длине символов, исправляем:

Заходим в GPO и в дефолтной политике идем по пути: Computer Manager - Windows Settings - Security Settings - Account Policies - Password Policy - там уже поймешь куда нажимать

Настройка SRV1

Базовая настройка

- **переименуйте компьютер в SRV1;**
- **в качестве адреса SRV1 используйте второй возможный адрес из подсети 172.16.19.64/26;**
- **обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.**
- **с помощью дополнительных жестких дисков создайте RAID-5 массив; назначьте ему букву D:\.**

Set-Item WSMan:\localhost\Client\TrustedHosts -Value '*' - команда для того, чтобы удаленно управлять сервером через графику

Ск

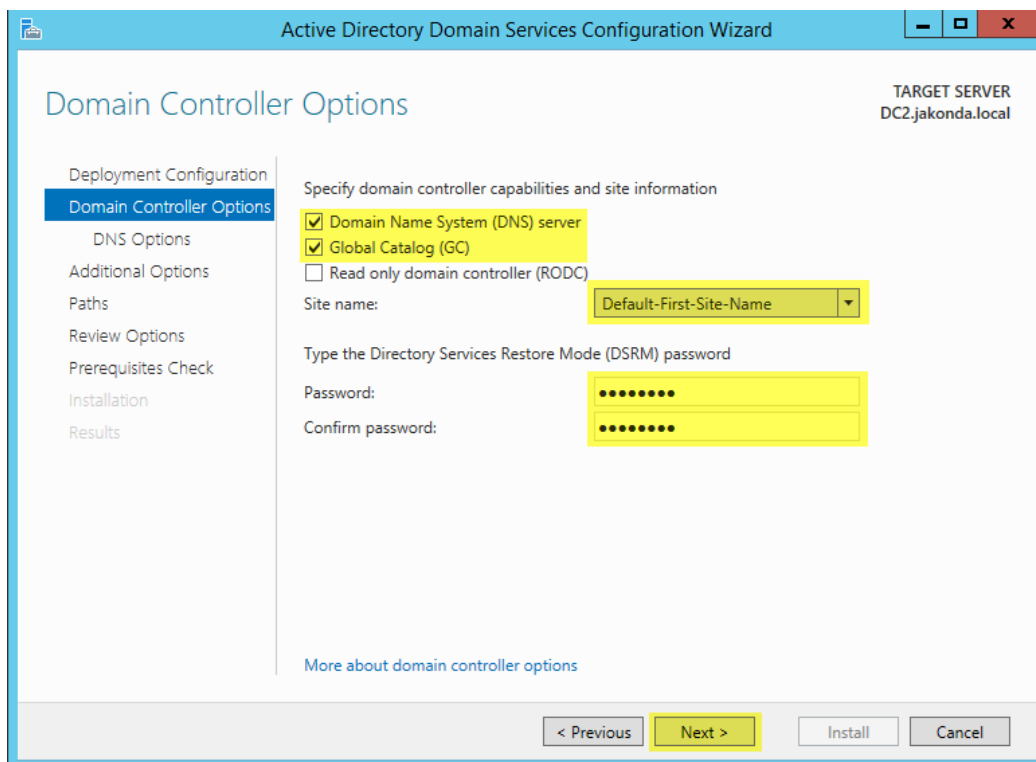
Для создание RAID через дискпарт нужно сделать -

- 1) select disk 1
- 2) attributes disk clear readonly
- 3) online disk - в режиме выбранного диска (проделай такой фокус на всех дисках)
- 3) convert dynamic (также на каждом диске)
- 4) create volume raid disk=1,2,3,4 - собери все диски вместе
- 5) list volume - проверяем, что диск создан
- 6) select volume N - переходим в диск, для того чтобы задать ему букву
- 7) assign letter=N - задаем букву!
- 8) format fs=ntfs - чтобы сразу задать ФС

Active Directory

- сделайте сервер дополнительным контроллером домена **Kazan.wsr**;
- сервер должен быть контроллером домена только для чтения.

На SRV1 в момент конфигурации крайне важно отключить галочку на DNS



DHCP

- настройте протокол DHCP для автоконфигурации клиентов;
- настройте failover: mode – Load balancer, partner server – DC1, state switchover – 5 min.

DNS

- сделайте сервер дополнительным DNS-сервером в домене **Kazan.wsr**;
- загрузите с DC1 все зоны прямого и обратного просмотра;

Ск

- на SRV1 не должно быть основных зон прямого просмотра.
(ПУНКТ ПО НЕОБХОДИМОСТИ БУДЕТ ДОПОЛНЯТЬСЯ, ВРОДЕ ТУТ НЕ СЛОЖНО)

Общие папки

- создайте общие папки для подразделений (IT, Sales) по адресу SRV1→d:\shares\departments. Просматривать и редактировать файлы в папках могут только члены соответствующей группы.
- обеспечьте привязку общей папки подразделения к соответствующей группе пользователей в качестве диска G:\.

Создаем папку на SRV1 - в директории shares/deparments

В процессе создания добавь в зону доступа все группы и дай им максимальные права,

Далее иди в GPO и делай новое правило - User Config - Preferences - Windows Settings - Folders:

1) Action: Update

2) Path - \\SRV1.Kazan.wsr\departments

Далее в той же GPO иди в Drive Maps

Создавай новое правило User Config - Preferences - Windows Settings - Drive Maps:

1) Action: Update

2) Location - путь до папки, как сверху

3) Ставь галочку на Reconnect

4) Drive Letter - Use (G/)

Далее перезапрашивай с клиента папку и будет тебе счастье!

UPD: В режиме Common нужно кликнуть на User Targeting - New Item - Security Group, надеюсь ты это запомнил, так как сам тыкался в это!

Квоты/Файловые экраны

- установите максимальный размер в 2 Gb для каждой домашней папки пользователя (U:\);
- запретите хранение в домашних папках пользователей файлов с расширениями .mp3 и .wav; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

Нужно установить инструмент(на SRV1) - File and Storage Services - File and iSCI services - Check File Server Resource Manager - далее протыкай некст

Дальше квоты и файл скрин ты умеешь делать, вроде как

IIS

- создайте сайт компании со стартовой страницей следующего содержания:
<html>

Ск

Welcome to Kazan!

</html>;

- сайт должен быть доступен по именам **www.kazan.wsr** и **kazan.wsr** только по протоколу **https** в обоих сетевых сегментах с использованием сертификатов, выданных DCA.

Не забудь, что службу IIS нужно установить на DC1 для удаленного конфигурирования, как и на сервере где будет крутиться сайт - обязательно ставь **Mangment Tools!!** Это очень важно!

По сайтику - сначала иди в **REGEDIT** - и по пути - **HKEY_LOCAL_MACHINE - Software - Microsoft- Web Manager - Server** - Там ищи параметр **EnableRemoteManagement** и ставь **1**

Далее, на DC1 через **All servers** заходи на **SRV1** через **Computer Manager** - иди во вкладку **Services** - там ищи **Web Manager Service** - выбирай **Startrype - Auto** и запусти службу. Готово! Теперь можно подключаться и делать сайт через DC1

Сертификат для сайта - идешь на DCA, в **Cert Templates** находишь темплейт про **Web Server**

Редактируешь его - во вкладке **General** - задай ему имя и поставь галочку на **Publish**
В **Subject Name** убедись, что стоит галка на **Supply in the request**, в **Security** - ставь галчку на максимальные права на Админа, Админа локального и энтерпрайзнутого, также советую добавить компы в эту политику, разрешим всем все на свете, хуже не будет! - готово!

После того, как сертификат будет сделан - публикуй его и через MMC - **Ctrl + M** добавляй сертификат оснастку, далее во вкладку **Personal** и **Enroll** новый серт, когда увидишь его на экране, переходи в режим его конфигурирования и делай следующее -

Type - выбирай **Common Name**

Value - пиши имя сайта - www.kazan.wsr - не забудь смахнуть в **ADD**

В параметрах **Alternative name** -

Type - **DNS**

В этом **Type** укажи ***.kazan.wsr**

Type **IPv4**

Тут укажи **ip addr** сервера - **172.16.19.66**

Как только ты его выпустил, в меню **Personal** MMC тыкай на него два раза ЛКМ, переходи во вкладку **Details** и выбирай **Copy to file**, Далее делай так -

Next - на вопрос про экспорт ключей говори **Да** - далее спросит за формат инфы, там ставь галочку на **Personal Info** - и на **Export all extended prop.** - **Next** - задавай пароль, ставь простую единичку и отправляй его на **SRV1** сразу

Ск

Далее на SRV1 - вводи команду - `certutil -importpfx C:\ssl.pfx` (твое имя серта тут будет!)

После успешного выполнения команды иди на клиента и смотри, кто дал серт!
Должен быть RootKazanCA

Настройка DCA

Базовая настройка

- переименуйте компьютер в DCA;
- в качестве адреса DCA используйте третий возможный адрес из подсети 172.16.19.64/26;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену Kazan.wsr.

Службы сертификации

- установите службы сертификации;
- настройте основной доменный центр сертификации;
- имя центра сертификации – RootKazanCA;
- срок действия сертификата – 8 лет;
- настройте шаблон выдаваемого сертификата для клиентских компьютеров ClientComps: *subject name=common name*, автозапрос только для компьютера R1;
- настройте шаблон выдаваемого сертификата ITUsers: *subject name=common name*, автозапрос только для пользователей – членов группы IT.

1) Логинься под доменным админом и устанавливай службу ADCS

2) Далее в визарде тыкаем - Enterprise CA (Убедись, что все делается в рамках домена)

3) Далее ROOT CA

4) Кучу раз некст

5) Меняй имя CA, как по заданию - RootKazanCA

6) Срок действия - 8 лет и тыщу раз некст, пока не установится

Создаем шаблоны для клиентских компов:

1) Иди в оснастку CA - далее Certificate Templates (ПКМ) - Manage

2) Находи там уже готовый темплейт - Computer

- 3) Переходи во вкладку Subject Name - выбирай галку Build from this AD info - Subject name format - Common name (также убери все галки в боксах внизу, кроме DNS Name)

4) Как опубликовать серты:

1) Certif.Temp (ПКМ) - New - Cert issue

2) Идем в GPO, создаем новую GPO, редачим её по пути - Computer Management - Policies - Windows Settings - Security - Public Key - и прям в этой штуке выбирай Cert Services Client - Enroll, включай её

Также включи политику Cert Services Client - Auto Enroll, протыкай две галочки и радуйся жизни!

Ск

- 3) тоже самое протыкай на клиенте, путь такой же! Все точно также!
(проверить можно командой - `gpresult /r` - тут глянь, что политика с сертом доехала)
- 4) Далее иди `Win + R` - `mmc`
- 5) Далее тыкай `Ctrl + M` и выбирай в левой части кнопочку `Certificates` - бахай её влево
- 6) Заходи в эту менюшу, выбирай `Personal` - и жди там серт!

Настройка CLI1

Базовая настройка

переименуйте компьютер в CLI1;

- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену *Kazan.wsr*;
- запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
- используйте компьютер для тестирования настроек в домене *Kazan.wsr*: пользователей, общих папок, групповых политик.

GPO для спящего режима

1) Создавай новую политику и иди по пути Computer Manag - Policies - Admin. Temp - System - Power Manager - Sleep Settings и гаси там все, что связано хоть как со сном (я не ебу, что именно, гасанул кучу всего - работает) Хуже точно не сделаешь!

Настройка DC2

Базовая настройка

- переименуйте компьютер в DC2;
- в качестве адреса DC2 используйте первый возможный адрес из подсети 172.16.20.96/27;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей.

Active Directory

- сделайте сервер контроллером домена *SPB.wse*;
- настройте двустороннее доверие доменом *Kazan.wsr*.

Для настройки двухстороннего доверия сначала добавь Conditional Forwardes, для звук дНС-серверов, ты умеешь как это делать, помни, что добавить надо имя домена и адрес DC, ничего больше!

DHCP

- настройте протокол DHCP для автоконфигурации клиентов – в качестве диапазона выдаваемых адресов используйте все незанятые серверами адреса в подсети.

DNS

- настройте необходимые зоны прямого и обратного просмотра;
- создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;

Ск

- обеспечьте разрешение имен сайтов обеих компаний.

Реализуется также с помощью Condit. Forwarders - только в сторону DC1

Элементы доменной инфраструктуры

- создайте учетную запись пользователя домена *User1\!P@ssw0rd*, используйте группу по умолчанию – *Domain Users*.
- для всех пользовательских учетных записей в домене используйте перемещаемые профили;
- для хранения профилей пользователей используйте общую папку по адресу *SRV2→c:\profiles*;

Установи на DC2 и SRV2 службы File Resource Manager, далее все ты знаешь как делать

- каждый пользователь должен иметь доступ к файлам только своего профиля; при обращении к указанной общей папке средствами программы *Проводник* пользователь должен видеть в списке только папку со своим профилем.

GPO

- настройте необходимые политики, обеспечивающие использование сервера *DCA.kazan.wsr* в качестве доверенного центра сертификации.

На DC2 должен оказаться файл сертификата DCA - *C:\Windows\System32\CertSrv\CertEnroll* - и там файл типа Security Cert.

Далее иди на DC2 в GPO по пути - Computer Config. - Windows Settings - Security Settings - Public Key - Trusted Root CA

Там нажимай Import.. и выбирай твой серт DCA! Победа!

Настройка SRV2

Базовая настройка

- переименуйте компьютер в SRV2;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену *SPB.wse*.

IIS

- создайте сайт компании со стартовой страницей следующего содержания:

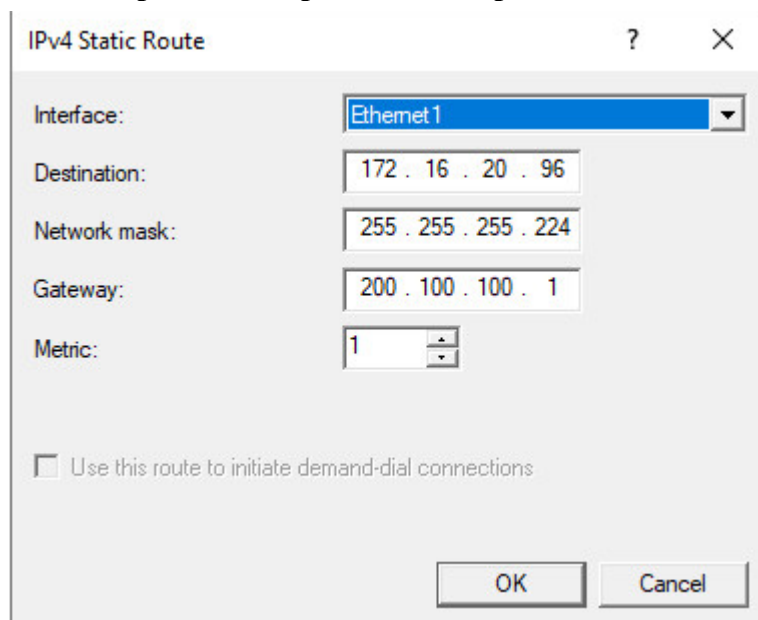
```
<html>
  Welcome to Saint-Petersburg!
</html>;
```
- сайт должен быть доступен по именам *www.spb.wse* и *spb.wse* только по протоколу https в обоих сетевых сегментах с использованием сертификатов, выданных DCA.

Настройка CLI2

Ск

Базовая настройка

- переименуйте компьютер в CLI2;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену *SPB.wse*.
- запретите использование «спящего режима» таким образом, чтобы пользователи домена не могли изменить эту настройку без участия администратора домена;
- используйте компьютер для тестирования настроек в домене *SPB.wse*



Interface - указывай выходной, внешний интерфейс

Далее все понятно

Настройка R2

Базовая настройка

- переименуйте компьютер в R2;
- задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к коммутатору ISP, используйте адрес 200.100.100.1/30; для сетевого адреса в подсети *SPB.wse* используйте последний возможный адрес из используемого адресного пространства;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену *SPB.wse*.

Настройка RRAS

- установите службу RRAS;
 - настройте статические маршруты для связи с сетевым сегментом в Казани.
- 1) Добавляй машинку в домен и установи на ней службу - RRAS

Ск

- 1) В меню выбора служб выбирай - Remote Access
- 2) В момент выбора допов выбирай - Routing - далее тыкай некст

Настройка R1

Базовая настройка

- переименуйте компьютер в R1;
- задайте настройки сети следующим образом: для сетевого интерфейса, подключенного к коммутатору ISP, используйте адрес 200.100.100.2/30; для сетевого адреса в подсети Kazan.wsr используйте последний возможный адрес из используемого адресного пространства;
- обеспечьте работоспособность протокола ICMP (для использования команды ping), при этом Windows Firewall должен быть включен для всех сетевых профилей;
- присоедините компьютер к домену Kazan.wsr.

Настройка RRAS

- установите службу RRAS;
- настройте статические маршруты для связи с сетевым сегментом в Санкт-Петербурге.

Ск

Модуль С: «Пусконаладка телекоммуникационного оборудования»

Версия 4 от 31.07.19.

ВВЕДЕНИЕ

Знание сетевых технологий на сегодняшний день становится незаменимым для тех, кто хочет построить успешную карьеру в области ИТ. Данное конкурсное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

ОПИСАНИЕ КОНКУРСНОГО ЗАДАНИЯ

Данное конкурсное задание разработано с учетом различных сетевых технологий, соответствующих уровням сертификации CCNA R/S. Задание разбито на следующие секции:

- Базовая настройка
- Настройка коммутации
- Настройка подключений к глобальным сетям
- Настройка маршрутизации
- Настройка служб
- Настройка механизмов безопасности
- Настройка параметров мониторинга и резервного копирования
- Конфигурация виртуальных частных сетей

Все секции являются независимыми друг от друга, но вместе образуют достаточно сложную сетевую инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, может подразумеваться, что IPv6 маршрутизация должна работать поверх настроенной виртуальной частной сети, которая, в свою очередь, должна работать поверх IPv4 маршрутизации, которая, в свою очередь, должна работать поверх RRPoE и Multilink и т.д. Очень важно понимать, что если вам не удастся решить какую-либо из задач по середине такого технологического стека, это не значит, что решенные задачи не будут оценены. Например, если вы не можете настроить динамическую маршрутизацию IPv4, которая необходима для работы виртуальной частной сети, вы можете использовать статическую маршрутизацию и продолжать работу над настройкой виртуальной частной сети и всем что должно работать поверх нее. В этом случае вы не получите баллы за динамическую маршрутизацию, но вы получите баллы за всё что должно работать поверх нее (в случае если функциональные тесты пройдены успешно).

Ск

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью и составить алгоритм выполнения работы. Вам предстоит вносить изменения в действующую, преднастроенную сетевую инфраструктуру предприятия, состоящую из головного офиса HQ и удаленного офиса BR1. Офисы имеют связь через провайдеров ISP1 и ISP2. Вы не имеете доступа к оборудованию провайдеров, оно полностью настроено и не требует дополнительного конфигурирования. Вам необходимо настраивать оборудование предприятия, а именно: SW1, SW2, SW3, HQ1, FW1 и BR1.

У вас отсутствует консольный доступ к устройствам, будьте очень внимательны при выполнении задания! В случае потери связи с оборудованием, вы будете виноваты сами. Разрешается перезагрузка оборудования – только техническими экспертами. Например, применили неправильный ACL, который закрыл доступ по telnet, но вы не успели сохранить конфигурацию.

Руководствуйтесь пословицей: Семь раз отмерь, один раз отрежь. Для выполнения задания у вас есть одна физическая машина (PC1 с доступом по Telnet и установленным ASDM), которую вы должны использовать в качестве:

PC2 Виртуальный ПК, Windows 10, Cisco AnyConnect, Putty. Пользователь User пароль P@ssw0rd

SRV1 Виртуальный ПК, Debian пользователь root пароль toor, с предустановленными сервисами

1) SysLog папка для проверки /Cisco_Log

2) RADIUS - FreeRadius

3) SNMP – для проверки используется пакет Net-SNMP используйте команду snmp_test

4) NTP

5) TFTP папка для проверки /Cisco_TFTP

Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. Например, задание 3 в секции «Настройка служб» предписывает вам настроить службу протокола автоматической конфигурации хостов, которая, разумеется, не будет работать пока не будут выполнены необходимые настройки в секции «Конфигурация коммутации». На вас возлагается ответственность за распределение своего рабочего времени.

Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуются тщательно проверять результаты своей работы.

Убедитесь в том, что ваши настройки на всех устройствах функционируют после перезагрузки всего оборудования.

Ск

ПОДКЛЮЧЕНИЕ К УСТРОЙСТВАМ

Для первоначального подключения используйте протокол Telnet. Для подключения к FW1 используете учетную запись с логином: **cisco** и паролем: **cisco**, для входа в привилегированный режим используйте пароль **cisco**. Для подключения к остальным сетевым устройствам используйте пароль: **cisco** и пароль для привилегированного режима: **cisco**

Для подключения к устройствам в главном офисе HQ, подключите рабочую станцию к порту F0/10 коммутатора SW2 и настройте адрес в соответствии с диаграммой L3, устройства доступны по следующим адресам:

SW1 – 192.168.254.10
SW2 – 192.168.254.20
SW3 – 192.168.254.30
HQ1 – 192.168.254.1
FW1 – 192.168.254.2
BR1 – 192.168.254.3

Ск

A. Базовая настройка

- 1) **Задайте имя всех устройств в соответствии с топологией.**
- 2) **Назначьте для всех устройств доменное имя worldskills.ru**
- 3) **Создайте на всех устройствах пользователей wsruser с паролем network**
 - a) **Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.**
 - b) **Пользователь должен обладать максимальным уровнем привилегий.**
- 4) **На всех устройствах установите пароль wsr на вход в привилегированный режим.**
 - a) **Пароль должен храниться в конфигурации в виде результата хэш-функции.**
- 5) **Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде. На FW1 используйте шифрование AES.**
- 6) **Для всех устройств реализуйте модель AAA.**
 - a) **Аутентификация на линиях виртуальных терминалов с 0 по 15 должна производиться с использованием локальной базы учётных записей. (кроме маршрутизатора HQ1)**
 - b) **После успешной аутентификации при удалённом подключении пользователи сразу должны получать права, соответствующие их уровню привилегий или роли (кроме межсетевого экрана FW1).**
 - c) **Настройте необходимость аутентификации на локальной консоли.**
 - d) **При успешной аутентификации на локальной консоли пользователи должны сразу должны получать права, соответствующие их уровню привилегий или роли.**
- 7) **На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля, назначьте IP-адреса.**
- 8) **На маршрутизаторе HQ1 на виртуальных терминальных линиях с 0 по 15 настройте аутентификацию с использованием RADIUS-сервера.**
 - a) **Используйте на линиях vty с 0 по 4 отдельный список методов с названием method_map**
 - b) **Порядок аутентификации:**
 - c) **По протоколу RADIUS**
 - d) **Локальная**
 - e) **Используйте общий ключ cisco**
 - f) **Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно**
 - g) **Адрес RADIUS-сервера 172.16.0.10**
 - h) **Настройте авторизацию при успешной аутентификации**
 - i) **Проверьте аутентификацию по протоколу RADIUS при удаленном подключении к маршрутизатору HQ1, используя учетную запись radius с паролем cisco**

Ск

```
radius server ACCESS_SERVER_1
address ipv4 192.168.1.1 auth-port 1111 acct-port 2222
key KEY-RADIUS
```

```
aaa group server radius ACCESS
server name ACCESS_SERVER_1
```

```
aaa authentication login default group ACCESS local
aaa authorization exec default group ACCESS local
```

- 9) Все устройства должны быть доступны для управления по протоколу SSH версии 2.

В. Настройка коммутации

- 1) Для централизованного конфигурирования VLAN в коммутируемой сети предприятия используйте протокол VTP.
 - a) В качестве сервера VTP настройте SW1.
 - b) Коммутаторы SW2 и SW3 настройте в качестве VTP клиента.
 - c) Таблица VLAN должна содержать следующие сети:
 - i) VLAN100 с именем MGT.
 - ii) VLAN200 с именем DATA.
 - iii) VLAN300 с именем OFFICE.
 - iv) VLAN500 с именем NATIVE.
 - v) VLAN600 с именем SHUTDOWN.
- 2) Между всеми коммутаторами настройте транки с использованием протокола IEEE 802.1q.
 - a) Порты F0/10 коммутаторов SW2 и SW3, а также порт F0/1 коммутатора SW1 должны работать без использования согласования. Отключите протокол DTP явным образом.
 - b) Транк между коммутаторами SW2 и SW3 должен быть настроен без использования согласования. Отключите протокол DTP явным образом.
 - c) Транки между коммутаторами SW1 и SW2, а также между SW1 и SW3, должны быть согласованы по DTP, коммутатор SW1 должен инициировать создание транка, а коммутаторы SW2 и SW3 должны ожидать начала согласования параметров от соседа, но сами не инициировать согласование.
 - d) Для всех магистральных каналов назначьте native vlan 500.
 - e) Запретите пересылку по магистральным каналам все неиспользуемые VLAN, в том числе VLAN1
- 3) Настройте агрегирование каналов связи между коммутаторами.
 - a) Номера портовых групп:
 - 1 – между коммутаторами SW1 (F0/5-6) и SW2 (F0/5-6);

Ск

2 – между коммутаторами SW1 (F0/3-4) и SW3 (F0/3-4);

- b) Агрегированный канал между SW1 и SW2 должен быть организован с использованием протокола согласования LACP. SW1 должен быть настроен в активном режиме, SW2 в пассивном.
 - c) Агрегированный канал между SW1 и SW3 должен быть организован с использованием протокола согласования PAgP. SW1 должен быть настроен в предпочтительном, SW3 в автоматическом.
- 4) Конфигурация протокола остоного дерева:
- a) Используйте протокол PVST.
 - b) Коммутатор SW1 должен являться корнем связующего дерева в сетях VLAN 100, 200 и 300, в случае отказа SW1, корнем должен стать коммутатор SW2.
 - c) Настройте порт F0/1 коммутатора SW1, таким образом, что при включении он сразу переходит в состояние forwarding не дожидаясь пересчета остоного дерева.

HA SW1 -

```
witch(config)# spanning-tree mode pvst
```

Установка коммутатора в качестве корневого:

```
Switch(config)# spanning-tree vlan номера_vlan root primary
```

HA SW2 -

Тоже самое, только приоритет задай вручную, там разберешься

- 5) Настройте порты F0/10 коммутаторов SW2 и SW3 в соответствии с L2 диаграммой. Порты должны быть настроены в режиме доступа.
- 6) Между HQ1 и FW1 настройте взаимодействие по протоколу IEEE 802.1Q.
- 7) Отключите интерфейс F0/24 коммутатора SW1 и E5 межсетевого экрана FW1, которые использовались для первоначального конфигурирования сетевой инфраструктуры офиса HQ.
- 8) На всех устройствах, отключите неиспользуемые порты.
- 9) На всех коммутаторах, неиспользуемые порты переведите во VLAN 600.

С. Настройка подключений к глобальным сетям

- 1) Подключение FW1 к ISP1 и ISP2 осуществляется с помощью IPoE, настройте интерфейсы в соответствии с диаграммами L2 и L3.
 - a) Передача данных между FW1 и ISP1 осуществляется не тегированным трафиком.
 - b) Передача данных между FW1 и ISP осуществляется тегированным трафиком с использованием VLAN 901.
- 2) ISP3 предоставляет L2 VPN между офисами HQ и BR1, настройте передачу между HQ1, FW1 и BR1 тегированного трафика, взаимодействие должно осуществляться по VLAN 10.

Ск

- 3) Настройте подключение BR1 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) BR1 должен автоматически получать адрес от ISP1.

Настройка мультилинка-

int Multilink1

ip address negotiated - чтобы получить его динамически от провайдера

ppp multilink

ppp multilink group 1

Далее на интерфейсах:

int s 0/1/0

encapsulation ppp

ppp multilink

ppp multilink group 1

int s 0/1/1

encapsulation ppp

ppp multilink

ppp multilink group 1

Проверить можно - проверь, что на интерфейс мультилинка прилетел адрес от ISPа, также попробуй пингануть адрес испа.

- 4) Настройте подключение BR1 к провайдеру ISP2 с помощью протокола HDLC.

D. Настройка маршрутизации

ВАЖНО! При настройке протоколов динамической маршрутизации, будьте предельно внимательны и анонсируйте подсети в соответствии с диаграммой маршрутизации, иначе не получите баллы за протокол, в котором отсутствует необходимая подсеть, и за тот протокол, в котором эта подсеть оказалась лишней.

Также, стоит учесть, что провайдеры фильтруют маршруты полученные по BGP, если они не соответствуют диаграмме маршрутизации.

- 1) В офисе HQ, на устройствах HQ1 и FW1 настройте протокол динамической маршрутизации OSPF.
 - a) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
 - b) HQ1 и FW1 между собой должны устанавливать соседство, только в сети 172.16.3.0/24.

Ск

- с) Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.
 - 2) Настройте протокол динамической маршрутизации OSPF в офисе BR1 с главным офисом HQ.
 - а) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
 - б) Используйте магистральную область для GRE туннелей.
 - с) Соседства между офисами HQ и BR1 должны устанавливаться, как через канал L2 VPN, так и через защищенный туннель.
 - д) Убедитесь в том, что при отказе выделенного L2 VPN, трафик между офисами будет передаваться через защищённый GRE туннель.
 - е) Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

Тут вроде ничего сложного, единственное, нужно помнить, что в туннеле может не сойтись соседство.

На туннельном интерфейсе задай - `ip ospf mtu-ignore` . Все будет окей!

- 3) Настройте протокол BGP в офисах HQ и BR1 для взаимодействия с провайдерами ISP1 и ISP2.
 - а) На устройствах настройте протокол динамической маршрутизации BGP в соответствии с таблицей 1

Таблица 1 – BGP AS

Устройство	AS
HQ1	65000
FW1	65000
ISP1	65001
ISP2	65002
BR1	65010

- б) Настройте автономные системы в соответствии с Routing-диаграммой.
 - с) Маршрутизаторы HQ1 и FW1 должны быть связаны с помощью iBGP. Используйте для этого соседства, интерфейсы, которые находятся в подсети 30.78.87.0/29.
 - д) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

Может возникнуть проблема с тем, что с HQ офиса есть будет блочиться асой. Для того, чтобы это избежать надо отключить `implicit role`. Для этого установи `asdm`:

- 1) `asdm image flash0:/асдм`
- 2) `http server enable`
- 3) `http 0.0.0.0 0.0.0.0 DATA` (интерфейс той сети, откуда хотим прийти)
- 4) Далее во вкладке Firewall натыкай все, интуитивно понятно

- 4) Настройте протокол динамической маршрутизации EIGRP поверх защищенного туннеля и выделенного канала L2 VPN между маршрутизаторами HQ1 и BR1.
 - а) Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.
 - б) Используйте номер автономной системы 6000.

Настройка очень простая, но требует внимания:

Ск

- 1) `ipv6 router eigrp <AS_NUMBER>`
- 2) `eigrp router-id <NUMBER_ID>`
- 3) Далее идем на каждый интерфейс, который засунем в eigrp 6000 и пишем там команду -
- 4) `ipv6 eigrp <AS_NUMBER>`
- 5) Супер машина делает все сама, а проверить роуты и соседство ты сможешь

Е. Настройка служб

- 1) В сетевой инфраструктуре сервером синхронизации времени является SRV1. Все остальные сетевые устройства должны использовать его в качестве сервера времени.

- a) Передача данных между осуществляется без аутентификации.
- b) Настройте временную зону с названием MSK, укажите разницу с UTC +3 часов.
`clock timezone MSK 3`
`ntp server 172.16.20.20`
`do wr`

- 2) Настройте динамическую трансляцию портов (PAT):

- a) На маршрутизаторе HQ1 и BR1 настройте динамическую трансляцию портов (PAT) для сети 192.168.2.0/24 в соответствующие адреса петлевых интерфейсов.
- b) Убедитесь в том, что для PC2 для выхода в интернет использует один из каналов до ISP1 или ISP2 от BR1, при недоступности обоих каналов, PC2 должен осуществлять выход в сеть интернет через каналы офиса HQ.
- c) Убедитесь, в том, что есть все необходимые маршруты, иначе проверить корректность настроенной трансляции портов, будет невозможно.

- 3) Настройте протокол динамической конфигурации хостов со следующими характеристиками

- a. На маршрутизаторе HQ1 для подсети OFFICE:
 - i) Адрес сети – 30.78.21.0/24.
 - ii) Адрес шлюза по умолчанию интерфейс роутера HQ1.
 - iii) Адрес TFTP-сервера 172.16.0.10.
 - iv) Компьютер PC1 должен получать адрес 30.78.21.21.

Настройка DHCP:

- 1) `ip dhcp pool <NAME>` - создал пул
- 2) `host 30.78.21.10 255.255.255.0` - указал, какой адрес получит клиент
- 3) `client-identifier` - пишешь MAC.адрес. по 4 символа в каждом тектете. Например, для винды перед маком нужно ОБЯЗАТЕЛЬНО ставить 01, для линукса - 00.

Если на винде мак - 00-0c-29-9e-27-df, то в циске ты пишешь - `client-identifier 0100.0c29.9e27.df`. Если бы это был линукс - 0000.0c29.9e27.df

- 4) `default-router <IP_ADDR>` - прописал шлюз
- 5) `option 150 ip 172.16.20.20` - прописал TFTP-сервер

Ск

Настройка PPPoE:

- 1) `ip local pool <NAME> <ADDRESS_FOR_CLIENT>` - создаем локальный пул адресов, даем ему имя и указываем какой адрес получит наш клиент - читай задание
- 2) `int virtual-template 1` - создаем виртуальный шаблон
- 3) `ip address <IP_ADDR>` - задаем ему ip адрес. задать через loopback - `ip unnumber loopback` - хотя ты, дорогой читатель, можешь сделать иначе работает 50\50
- 4) `mtu 1492` - указывай mtu. 8 байт уходит под служебную инфу PPP
- 5) `encapsulation ppp`
- 6) `peer default ip address pool <NAME>` - задали пул, с которым будет работать сервер
- 7) `ppp authentication chap ms-chap` - указали метод аутентификации
- 8) `bba-group pppoe global` -
- 9) ---- в режиме конфигурации bba пиши - `virtual-template 1`
- 10) `int g 0/1`
- 11) --- `pppoe enable group global`
- 12) В конце создай пользователей по заданию!

Далее с винды пробуй кокоситься, должно работать!

- 4) В офисе BR1 используется аутентификация клиентов с помощью протокола PPPoE. Для этого настройте сервер PPPoE на BR1.
 - с) Аутентификация PC1 на сервере PPPoE должна осуществляться по логину `pc2user` и паролю `pc2pass`.
 - д) PC2 должен получать ip адрес от PPPoE сервера автоматически.

F. Настройка механизмов безопасности

- 1) На маршрутизаторе BR1 настройте пользователей с ограниченными правами.
 - а) Создайте пользователей `user1` и `user2` с паролем `cisco`
 - б) Назначьте пользователю `user1` уровень привилегий 5. Пользователь должен иметь возможность выполнять все команды пользовательского режима, а также выполнять перезагрузку, а также включать и отключать отладку с помощью команд `debug`.
 - с) Создайте и назначьте view-контекст `sh_view` на пользователя `user2`
 - i) Команду `show cdp neighbor`
 - ii) Все команды `show ip *`
 - i) Команду `ping`
 - ii) Команду `traceroute`
 - д) Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.
- 2) На порту F0/10 коммутатора SW2, включите и настройте Port Security со следующими параметрами:
 - а) не более 2 адресов на интерфейсе
 - б) адреса должны динамически определяться, и сохраняться в конфигурации.

Ск

- с) при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.
- 3) На коммутаторе SW2 включите DHCP Snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных.
- 4) На коммутаторе SW2 включите динамическую проверку ARP-запросов в сети OFFICE.
- 5) На маршрутизаторе BR1 настройте расширенный список контроля доступа для подсети 192.168.2.0/24. Заблокируйте весь исходящий и входящий трафик от подсети 192.168.2.0/24 в интернет за исключением:
- а) Разрешите работу с DNS сервером 8.8.8.8.
 - б) Разрешите исходящий TCP трафик по портам 80 и 443.
 - в) Разрешите входящий трафик по TCP, только для тех соединений, если узел из подсети 192.168.2.0/24 инициирует это соединение.

ip access-list extended BLOCK_LOCAL_NETWORK

permit udp 192.168.2.0 0.0.0.255 host 8.8.8.8 eq domain

permit udp host 8.8.8.8 192.168.2.0 0.0.0.255

permit tcp 192.168.2.0 0.0.0.255 any eq www 443

permit tcp any 192.168.2.0 0.0.0.255 established

ПОТОМ ИДИ НА ИНТЕРФЕЙС И ДЕЛАЙ ТАМ:

interface Virtual-Template1

mtu 1492

ip unnumbered Loopback10

ip access-group BLOCK_LOCAL_NETWORK in

ip access-group BLOCK_LOCAL_NETWORK out

Ск

G. Настройка параметров мониторинга и резервного копирования

- 1) На маршрутизаторе HQ1 и межсетевом экране FW1 настройте журналирование системных сообщений на сервер SRV1, включая информационные сообщения.

HA HQ!!!!!!

logging <ip>

logging trap informational

HA FW!!!!!!!!!!!!!!

logging enable

logging trap informational

logging host ISP3_L2_VPN 172.16.20.20 format emblem

- 2) На маршрутизаторе HQ1 и межсетевом экране FW1 настройте возможность удаленного мониторинга по протоколу SNMP v3.
 - a) Задайте местоположение устройств MSK, Russia
 - b) Задайте контакт admin@wsr.ru
 - c) Используйте имя группы WSR.
 - d) Создайте профиль только для чтения с именем RO.
 - e) Используйте для защиты SNMP шифрование AES128 и аутентификацию SHA1.
 - f) Используйте имя пользователя: snmpuser и пароль: snmppass
 - g) Для проверки вы можете использовать команду snmp_test на SRV1.

HA HQ!!!

snmp-server location MSK, Russia

snmp-server contact admin@wsr.ru

snmp-server group WSR v3 priv

snmp-server community RO ro

snmp-server snmpuser v3 auth sha snmppass priv aes 128 snmppass

HA FW!!!

snmp-server location MSK, Russia

snmp-server contact admin@wsr.ru

snmp-server group WSR v3 priv

snmp-server community RO ro

snmp-server snmpuser v3 auth sha snmppass priv aes 128 snmppass

snmp-server community 0 RO ro

snmp-server community 0 RO

snmp-server community RO

snmp-server user snmpuser WSR v3 auth sha snmppass priv aes 128 snmppass

Ск

```

do wr
wr
snmp-server host HQ 172.16.20.20 community RO version 3 snmpuser
sh route
snmp-server host ISP_3_L2_VPN 172.16.20.20 community RO version 3
snmpuser
snmp-server host IsP3_L2_VPN 172.16.20.20 community RO version 3
snmpuser

```

NAT

- 3) На маршрутизаторе HQ1 настройте резервное копирование конфигурации
 - а) Резервная копия конфигурации должна сохраняться на сервер SRV1 по протоколу TFTP при каждом сохранении конфигурации в памяти устройства
 - б) Для названия файла резервной копии используйте шаблон <hostname>-<time>.cfg

```

conf t
archive
path tftp://172.16.20.20/$H-$T
write-memory

```

Н. Конфигурация виртуальных частных сетей

- 1) Между HQ1 и BR1 настройте GRE туннель со следующими параметрами:
 - а) Используйте в качестве VTI интерфейс Tunnel1
 - б) Используйте адресацию в соответствии с L3-диаграммой
 - в) Режим — GRE
 - г) Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.
 - д) Обеспечьте работу туннеля с обеих сторон через провайдера ISP1.

Пример, как делать туннельчик:

- 1) int tun1 - создал интерфейс
- 2) ip address {IP_ADDR} - назначил айпшник
- 3) ip mtu 1400 - задал мту
- 4) tunnel source - твой публичный адрес роутера
- 5) tunnel destination - куда строить будем
- 6) no sh - включил
- ?????

Работает!

- 2) Защита туннеля должна обеспечиваться с помощью IPsec между BR1 и FW1.
 - а) Обеспечьте шифрование только GRE трафика.
 - б) Используйте аутентификацию по общему ключу.
 - в) Параметры IPsec произвольные

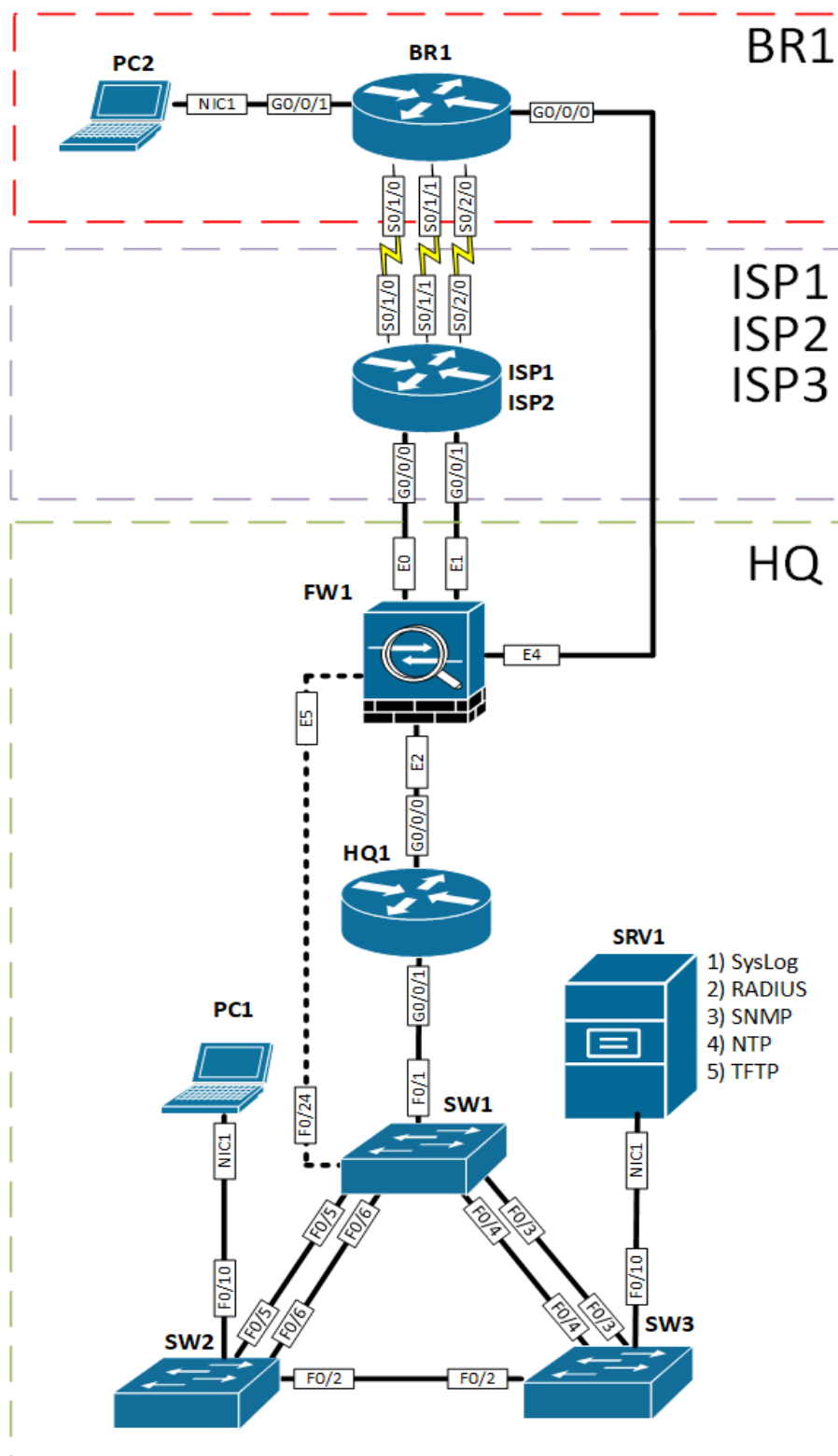
Пример конфигурации

Ск

```
HQSW1(config)#crypto isakmp policy 1
HQSW1(config-isakmp)#hash sha256
HQSW1(config-isakmp)#encryption 3des
HQSW1(config)#crypto isakmp policy 1
HQSW1(config-isakmp)#authentication pre-share
HQSW1(config-isakmp)#group 5
HQSW1(config)#crypto isakmp key cisco address 1.1.1.1 - только внешний адрес!
HQSW1(config)#crypto ipsec transform-set vpn esp-3des esp-sha256-hmac
HQSW1(cfg-crypto-trans)#mode tunnel
HQSW1(config)#crypto ipsec profile vpn
HQSW1(ipsec-profile)#set transform-set vpn
HQSW1(config)#int tun 0
HQSW1(config-if)#tunnel protection ipsec profile vpn
HQSW1(config-if)#end
```

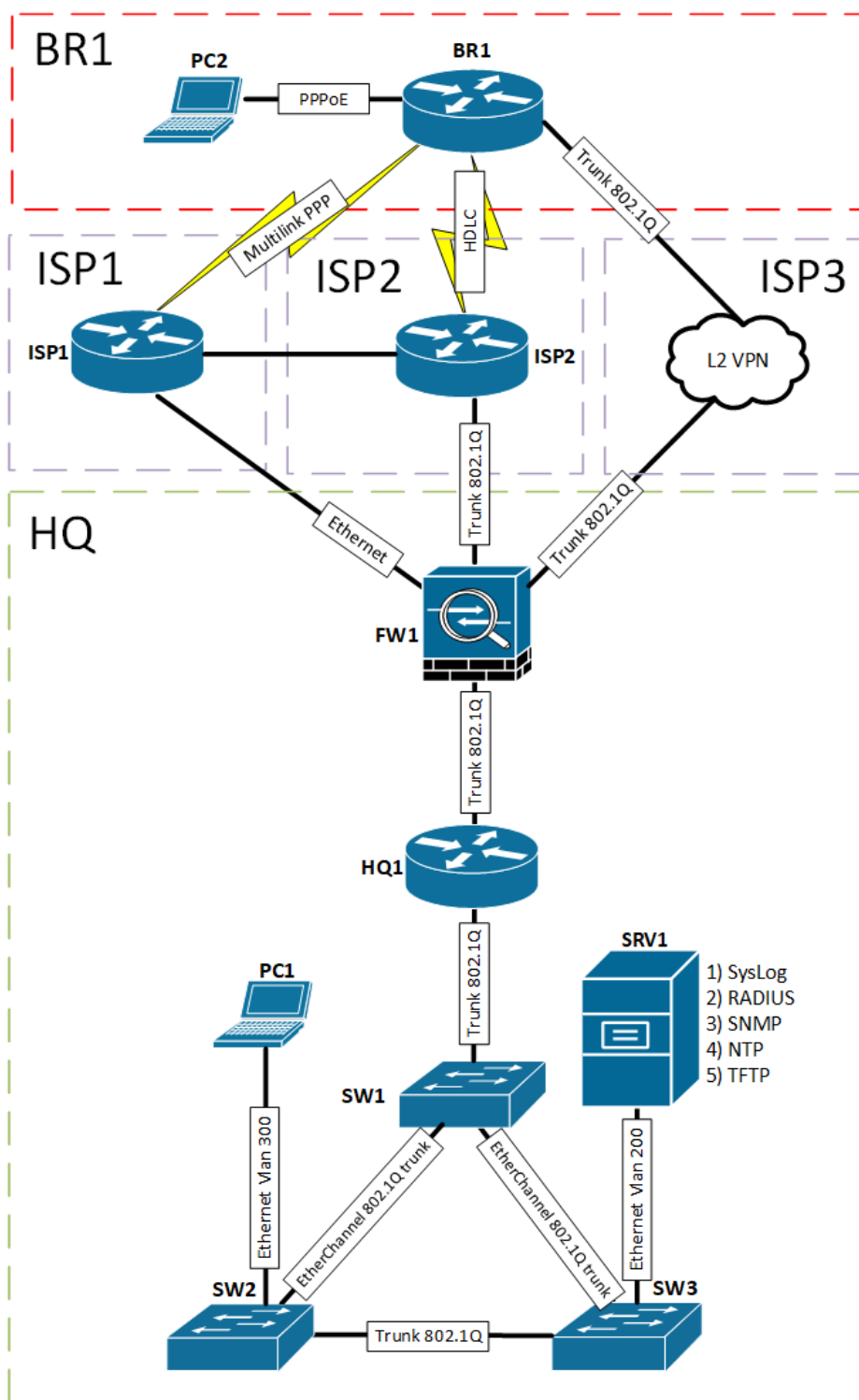
Топология L1

Ск



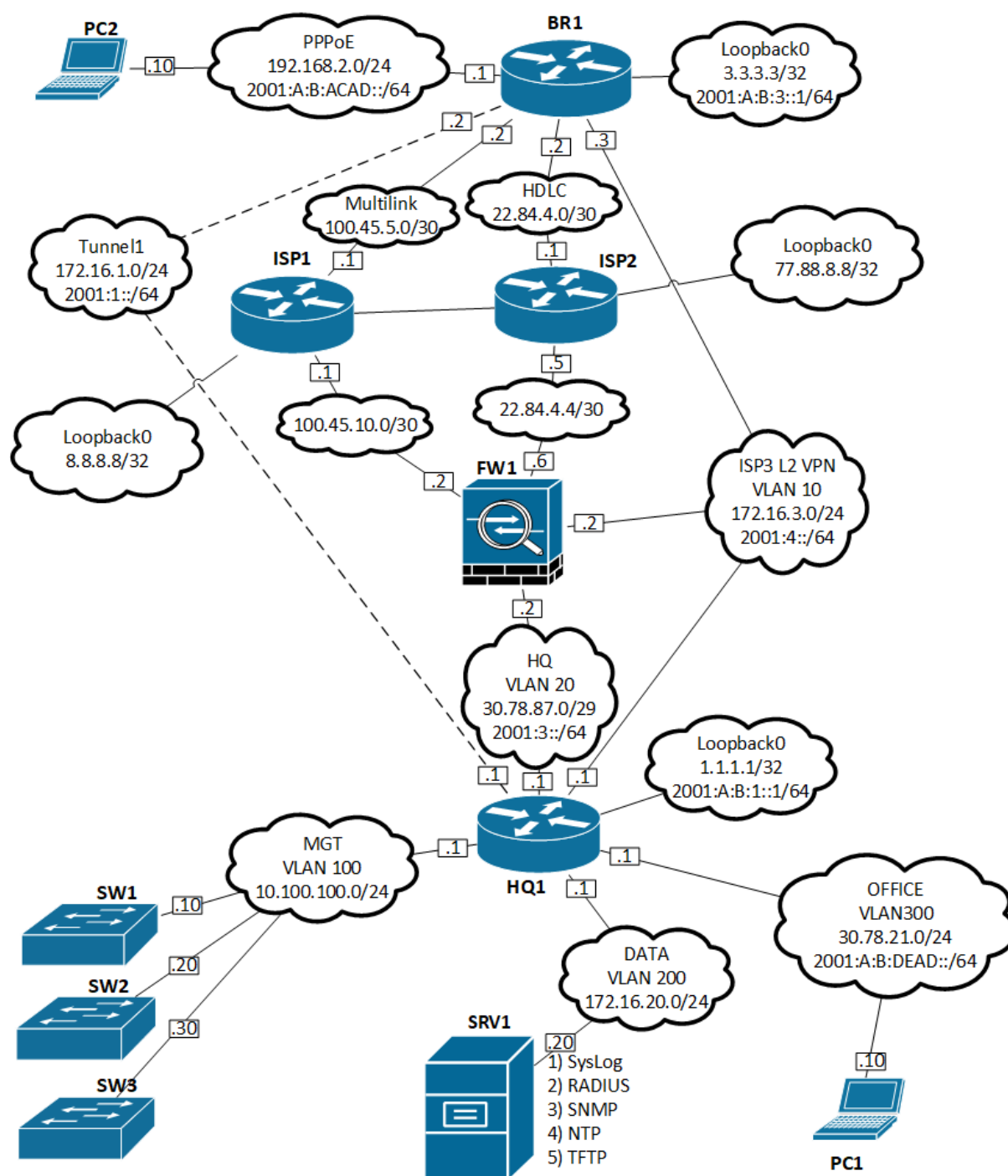
Ск

Топология L2



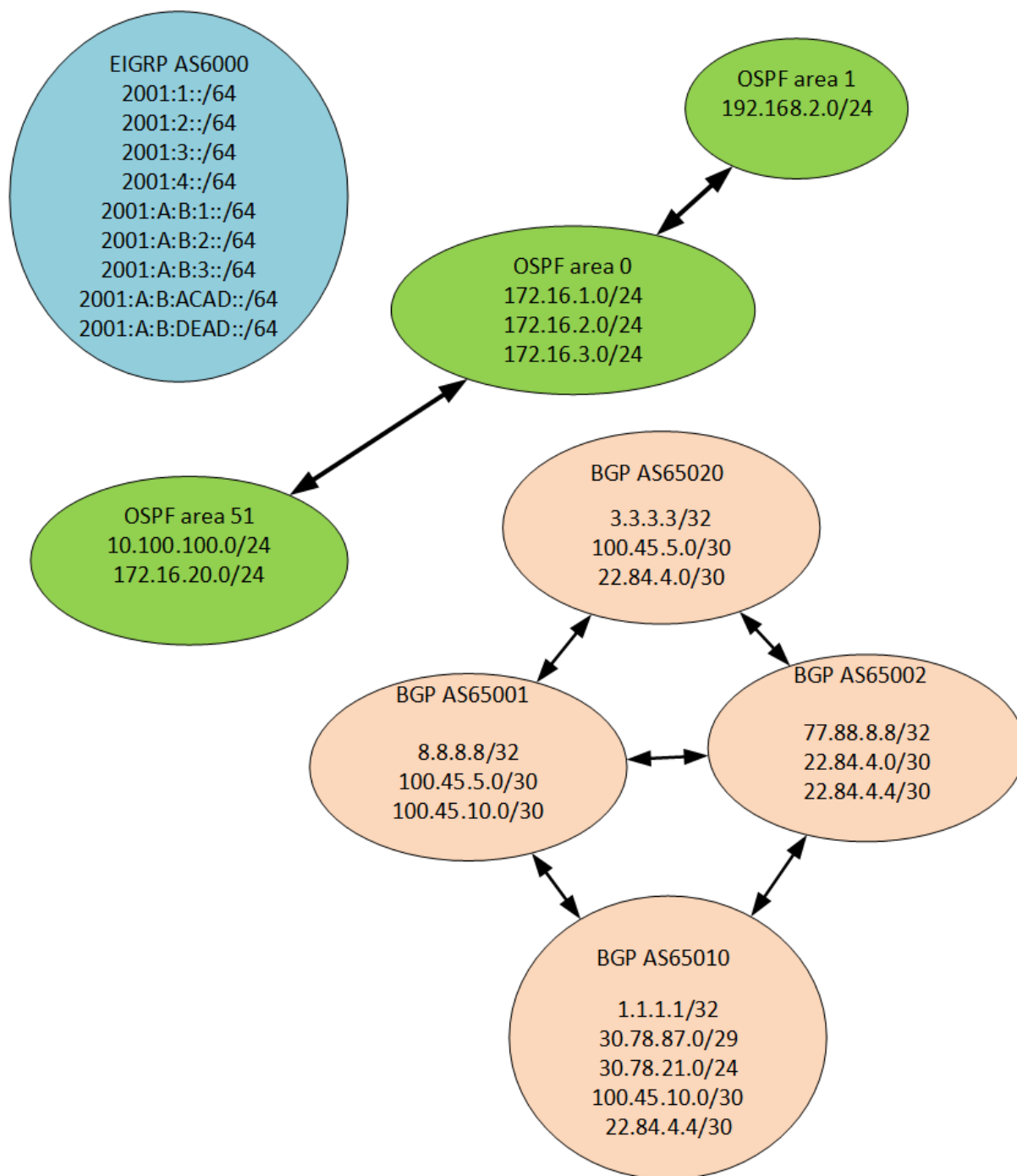
Топология L3

Ск



ШТЕ
Routing-диаграмма

Ск



Ск

4. КРИТЕРИИ ОЦЕНКИ

В данном разделе определены критерии оценки и количество начисляемых баллов (субъективные и объективные) таблица 2. Общее количество баллов задания/модуля по всем критериям оценки составляет 45.

Таблица 2 – Критерии оценки

Раздел	Критерий	Оценки		
		Субъектив	Объективная	Общая
А	Модуль А: «Пусконаладка инфраструктуры на основе ОС семейства Linux»	0	15	15
В	Модуль В: «Пусконаладка инфраструктуры на основе ОС семейства Windows»	0	15	15
С	Модуль С: «Пусконаладка телекоммуникационного оборудования»	0	15	15
Итого =		0	45	45

Ск

Ск

5. ПРИЛОЖЕНИЯ К ЗАДАНИЮ

- 1) <https://nextcloud.wsr39.ru/index.php/s/Gt7TagrrEwFjxj5> -- *Additional ISO Windows*
- 2) <https://nextcloud.wsr39.ru/index.php/s/ZRbYDLCPrRfEWjN> -- *Additional ISO Linux*
- 3) <https://nextcloud.wsr39.ru/index.php/s/YHYDN9QNoEnzWw6> -- *Windows OVA*
- 4) <https://nextcloud.wsr39.ru/index.php/s/aZLom2rXzjxQsCz> -- *Linux OVA*
- 5) https://drive.google.com/file/d/1nYKF9P_zoWNAVcBaJCZ80f95vuTwfzti/view --
Файлы предварительной конфигурации для Cisco
- 6) <https://nextcloud.wsr39.ru/index.php/s/TYm8jCjpcgGySSH> -- *SRV1 Cisco OVA*
- 7) <https://drive.google.com/file/d/17geWwpbCxa77cE2iQVFB1HKUti1KZx5a/view?usp=sharing> Набор диаграмм Cisco
- 8) <https://drive.google.com/file/d/1LW2QIWtVbwqfPieYUjCgpfzLaq1ZOYAs/view?usp=sharing> Диаграмма сети Linux
- 9) <https://drive.google.com/file/d/1Bn-RgYaahkDZY0AIsaYi00OYIYfbAWsS/view?usp=sharing> Диаграмма сети Windows

Ск

Приложение 1

Дополнительные настройки модуля В

ВВЕДЕНИЕ

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

ОПИСАНИЕ ПРЕДУСТАНОВОК

- 1) Для создания сайтов *managers.pest.com*, *www.pest.com* и *www.buda.pest.com* используйте прилагаемые шаблоны. Разместите их в качестве ISO-образа в хранилище сервера виртуализации.
- 2) Excel-файл для импорта пользователей должен находиться на DC1 по адресу *c:\users.xlsx* (либо быть доступен в качестве ISO-образа на сервере виртуализации). Базовый снимок DC1 должен содержать это файл. В качестве самого файла используйте прилагаемый шаблон.

Описание применяемых операционных систем

Имя компьютера	Операционная система
DC2	Windows Server 2016 GUI
CLI2	Windows 10 Enterprise
SRV2	Windows Server 2016 Core
BRIDGE2	Windows Server 2016 GUI
DC1	Windows Server 2016 GUI
SRV1	Windows Server 2016 Core
BRIDGE1	Windows Server 2016 Core
CLI1	Windows 10 Enterprise
DCA	Windows Server 2016 GUI

РЕКОМЕНДАЦИИ ПО ВЫДЕЛЕНИЮ ОПЕРАТИВНОЙ ПАМЯТИ ДЛЯ

ВИРТУАЛЬНЫХ МАШИН

- Windows Server 2016 Core: минимум – 1 Gb, рекомендовано – 1,5 Gb;
- Windows Server 2016 GUI: минимум – 1,5 Gb, рекомендовано – 2 Gb;
- Windows 10 Enterprise: минимум – 1,5 Gb, рекомендовано – 2 Gb.

Ск