Пример настройки DHCP сервера на криптошлюзе «С-Терра Шлюз»

Настоящий документ содержит описание способа совместного использования Продуктов компании ООО «С-Терра СиЭсПи» и Продуктов третьих производителей.
ООО «С-Терра СиЭсПи» осуществляет сопровождение настоящего сценария в части настроек Продуктов Компании. Упоминание наименований, продуктов, торговых марок третьих организаций исключительно неформально и не является поддержкой, рекомендацией либо рекламой. ООО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов. Документ имеет статус вспомогательного материала, который может быть использован технологическими партнерами, компаниями-интеграторами, при разработке собственных решений.
Решения, разработанные на базе данного сценария, могут применяться в действующих сетях/системах только после тестовой и/или опытной эксплуатации.

Введение

В данном документе рассматривается настройка DHCP IPv4 сервера и failover DHCP IPv4 серверов на криптошлюзах безопасности «С-Терра Шлюз».

Данная инструкция основывается на сценарии «Построение кластера на базе протокола VRRP с настройкой при помощи CLI». Построение защищенного IPsec туннеля в данном документе рассматриваться не будет. Построение защищенного IPsec туннеля описано в сценарии «Построение кластера на базе протокола VRRP с настройкой при помощи CLI».

В разделе «Дополнительные возможности» приведены примеры настройки IPv6 DHCP сервера, конфигурирование нескольких пулов и работа с TFTP сервером для IPv4 DHCP сервера.

Предварительные требования

Требования к материально-техническому обеспечению

Для переноса запросов и сертификатов между криптошлюзами и центром выпуска сертификатов требуется USB Flash накопитель.

Требования к квалификации администратора

Администратор должен обладать обширными знаниями в области сетевой информационной безопасности, иметь опыт работы с аналогичным оборудованием/программным обеспечением, знать и понимать следующие технологии и протоколы: PKI, IPsec, NAT, Firewall, routing, switching.

Также администратор должен быть ознакомлен с базовым сценарием «Организация защищенного взаимодействия между подсетями центрального офиса и филиалов посредством IPsec VPN туннеля (протокол IPv4)» и со сценарием «Построение кластера на базе протокола VRRP с настройкой при помощи CLI».

Требования к инфраструктуре

1. Требования к устройствам.
   1.1. «С-Терра Шлюз».
      1.1.1 Устройства «С-Терра Шлюз» должны быть инициализированы (подробнее на http://doc.s-terra.ru раздел С-Терра Шлюз -> С-Терра Шлюз <версия> -> «Подключение ПАК и инициализация С-Терра Шлюз на вычислительных системах архитектуры Intel x86-64»).

      В «С-Терра Шлюз» версии 5.0 появилась возможность пройти инициализацию через интерфейс управления (management) по SSH, данная процедура и ее ограничения описаны в документации и на портале https://doc.s-terra.ru.

1.2. Центр выпуска сертификатов.

1.2.1 Должен быть настроен центр выпуска сертификатов (удостоверяющий центр, далее УЦ) для IPsec. Устройство с именем Certification_authority на схеме.

1.2.2 Для выпуска цифровых сертификатов допускается использование встроенного в ОС Windows Server 2016 (или новее) удостоверяющего центра совместно с сертифицированным СКЗИ «КриптоПро» CSP 5.0 R2 (или новее).

1.2.3 Для тестовых целей можно использовать тестовый УЦ от «КриптоПро» (веб-интерфейс: https://testgost2012.cryptopro.ru/certsrv/certrqxt.asp), либо утилиту ca-tool, входящую в состав пакета auxiliary-tools (пакет auxiliary-tools предназначен для установки на «С-Терра Шлюз» 5.0, документация на ca-tool приведена в инструкции «Центр выпуска тестовых ГОСТ сертификатов для IPsec», документацию и пакет можно загрузить на портале https://doc.s-terra.ru).

Категорически запрещено использование тестового УЦ от «КриптоПро» в производственной (боевой) эксплуатации, так как в данном случае отсутствует возможность контролировать процесс выпуска сертификатов и, соответственно, процедуру аутентификации.

1.3. HTTP сервер для распространения списка отозванных сертификатов.

1.3.1 Функционирующий HTTP сервер для распространения списка отозванных сертификатов (COC). Устройство с именем CRL_distribution_point на схеме. Если по объективным причинам использование COC не представляется возможным или не требуется, то проверку COC можно отключить в CLI «С-Терра Шлюз» (при соблюдении правил пользования).

Доставка нового списка отозванных сертификатов с удостоверяющего центра на HTTP сервер должна происходить заблаговременно, до истечения срока действия предыдущего списка.

2. Требования к сетевому взаимодействию.

2.1. Между устройствами стенда должна быть обеспечена IP связность.

2.2. На защищаемых хостах Host1-b-hub1, Host2-b-hub1, Host1-b-spoke1, Host2-b-spoke1 должно быть настроено получение IP-адреса по DHCP.

Схема взаимодействия

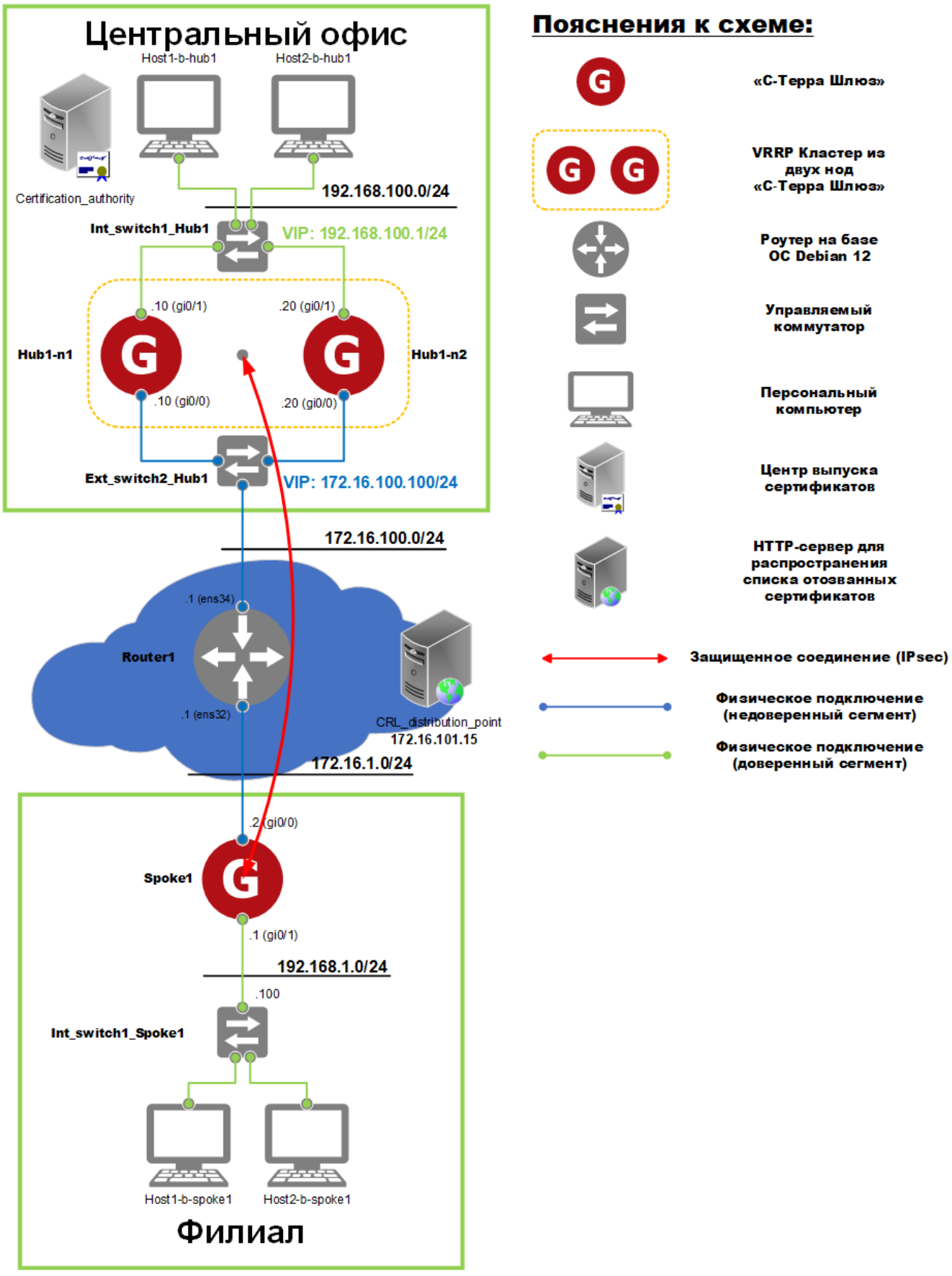


Рисунок 1. Схема взаимодействия

Общая логика работы

Размещение устройств, отказоустойчивость, подключение к сети интернет, параметры шифрования IPsec и параметры межсетевого экранирования соответствуют сценарию Построение кластера на базе протокола VRRP с настройкой при помощи CLI»

1. Размещение устройств.

   1.1. В центральном офисе размещаются: центр выпуска сертификатов (Certification_authority), криптошлюз «С-Терра Шлюз» (Hub1-n1 и Hub1-n2) версии 5.0, управляемые коммутаторы (Int_switch1_Hub1 и Ext_switch2_Hub1) и персональные компьютеры (Host1-b-hub1 и Host2-b-hub1).

   1.2. В филиале размещаются: криптошлюз «С-Терра Шлюз» (Spoke1) версии 5.0, управляемый коммутатор (Int_switch1_Spoke1) и персональные компьютеры (Host1-b-spoke1 и Host2-b-spoke1).

   1.3. В неконтролируемом сегменте (синее облако на схеме) размещаются: HTTP сервер для распространения списка отозванных сертификатов (CRL_distribution_point), маршрутизатор (Router1).

2. Отказоустойчивость.

   Криптошлюзы Hub1-n1 и Hub1-n2 объединяются в отказоустойчивый кластер, работающий на базе протокола VRRP в режиме Master/Backup.

   Нода, находящаяся в состоянии Master, владеет VIP адресами в доверенном и недоверенном сегментах и, соответственно, обрабатывает трафик. Нода, находящаяся в состоянии Backup или Fault, не владеет VIP адресами.

   На нодах есть маршрут по умолчанию через адрес доверенного сегмента другой ноды (для доступа резервной ноды в сеть интернет).

3. Параметры шифрования IPsec.

   Весь IPv4 трафик между подсетями центрального офиса (192.168.100.0/24) и филиала (192.168.1.0/24) защищается с использованием алгоритмов ГОСТ и протокола IPsec в туннельном IPv4 режиме.

4. Параметры DHCP.

   4.1. На Hub1-n1 и Hub1-n2 настроены failover DHCP и делят пул адресов 192.168.100.51-192.168.100.150/24 между собой. Hub1-n1 будет являться основным failover партнёром. Клиенты могут регистрироваться на любом failover DHCP сервере. Для балансировки Hub1-n1 может указать на каком failover DHCP сервере будет регистрироваться клиент перенаправляя DHCP запрос. При отказе одной ноды вторая нода сможет использовать весь пул адресов, при этом при регистрации на другом failover партнёра адреса на клиентах могут быть сохранены.

   4.2. Устройства центрального офиса Host1-b-hub1 и Host2-b-hub1 получают динамический адрес и адрес DNS сервера по DHCP от Hub1-n1 и Hub1-n2.

   4.3. Устройства филиала Host1-b-spoke1 и Host2-b-spoke1 получают адрес и адрес DNS сервера по DHCP от Spoke1. Host1-b-spoke1 получает динамический адрес. Host2-b-spoke1 получает статический адрес.

Настройка стенда

Настройка криптошлюза Spoke1

В данной инструкции будут описаны только настройки DHCP сервера. Остальные настройки должны быть взяты из сценария «Построение кластера на базе протокола VRRP с настройкой при помощи CLI».

Настройка DHCP сервера

1. Измените файл конфигурации `/etc/dhcp/dhcpd.conf`.

```
# Sample configuration file for ISC dhcpd
```

```
authoritative;
server-name Spoke1;
log-facility local7;
ddns-update-style none;
subnet 192.168.1.0 netmask 255.255.255.0 {
       option routers 192.168.1.1;
       option subnet-mask 255.255.255.0;
       option domain-name-servers 192.168.1.1;
       range 192.168.1.10 192.168.1.254;
       default-lease-time 21600;
       max-lease-time 28800;
}
host host2 {
       hardware ethernet 00:50:56:9e:d6:06;
       fixed-address 192.168.1.5;
}
```

где:

- `authoritative` – этот параметр рекомендуется указывать в случаях, когда данный DHCP сервер является единственным или главным DHCP сервером в сети. Этот параметр включает отправку DHCPNAK, когда DHCP клиент пытается продлить или запросить некорректный с точки зрения DHCP сервера адрес. Этот параметр можно размещать как на глобальном уровне, так внутри `subnet` (в этом случае DHCP сервер будет считаться `authoritative` для данной конкретной подсети).
- `server-name <имя>` – имя сервера;
- `log-facility <уровень>` – уровень лога syslog; при указании `local7`, файлы логов будут писаться в файл `/var/log/cspvpngate.log`;
- `ddns-update-style none;` – отключение поддержки DDNS;
- `subnet <IP-адрес> netmask <маска> {...}` – описание параметров сети, для которой будут раздаваться сетевые настройки;
- `option routers <IP-адрес>` – IP адрес шлюза по умолчанию;
- `option subnet-mask <маска>` – маска сети;
- `option domain-name-servers <IP-адрес>` – DNS сервер по умолчанию;
- `range <диапазон IP-адресов>` – диапазон, из которого будут раздаваться IP-адреса DHCP клиентам, допускается использовать несколько `range` внутри одного `subnet`;
- `default-lease-time <время>` – время аренды IP-адресов (в секундах);
- `max-lease-time <время>` – максимальное время аренды;
- `host <имя хоста> { hardware ethernet <MAC-адрес>; fixed-address <IP-адрес>; }` – хосту с соответствующим MAC-адресом статически привязать IP-адрес. Данный параметр следует размещать не внутри `subnet`, а на глобальном уровне. IP-адрес, указанный в `host`, не должен входить в диапазон адресов, которые заданы в параметрах `range`.

2. Для настройки интерфейса, на котором будут раздаваться IP-адреса, отредактируйте файл `/etc/default/isc-dhcp-server`. Имя интерфейса в переменной `INTERFACESv4` должно соответствовать имени интерфейса в нотации linux:

```
INTERFACESv4="eth1"
```

Если необходимо задать несколько интерфейсов пропишите их через пробел (в данной инструкции используется только один интерфейс):

```
INTERFACESv4="eth1 eth2"
```

Примечание - В силу особенностей реализации, DHCP сервер не сможет получить на LAN интерфейсе криптошлюза DHCP запросы, пришедшие из удаленных подсетей (например, с использованием DHCP Relay) по защищенному соединению через WAN интерфейс. Для этого нужно будет добавить WAN интерфейс в список `INTERFACESv4`, а в cisco-like консоли назначить ACL на WAN интерфейс для блокирования входящего трафика из интернета на порт DHCP сервера (например, `deny udp any host <IP адрес WAN интерфейса> eq 67`).

3. Запустите сервис DHCP сервера и добавьте его в автозагрузку:

```
root@Spoke1:~# systemctl start isc-dhcp-server.service
root@Spoke1:~# systemctl enable isc-dhcp-server.service
```

В Приложении представлены тексты конфигураций `/etc/dhcp/dhcpd.conf` и `/etc/default/isc-dhcp-server` для криптошлюза Spoke1.

Настройка криптошлюза Hub1-n1

В данной инструкции будут описаны только настройки DHCP сервера. Остальные настройки должны быть взяты из сценария «Построение кластера на базе протокола VRRP с настройкой при помощи CLI».

Настройка DHCP сервера

Для выдачи IP-адресов клиентам обоими нодами кластера из одного диапазона IP-адресов будет использоваться механизм DHCP failover, в котором обе ноды кластера работают в качестве DHCP-сервера одновременно и синхронизируют между собой информацию о выданных клиентам IP-адресах. В случае отказа одной ноды вторая нода (оставшаяся в работе) обеспечивает выдачу всего диапазона IP-адресов, с учетом IP-адресов, ранее выданных отказавшей нодой. Данный режим работы нод в качестве DHCP-серверов не связан с работой нод в составе VRRP-кластера и является штатным средством резервирования DHCP-серверов.

При настройке DHCP failover следует учитывать следующие требования и ограничения:

- Службы `isc-dhcp-server.service` должны быть настроены на автоматический запуск на обоих нодах и работать одновременно;
- Время между нодами должно быть синхронизировано, например, с помощью NTP-клиента;
- Размер пула адресов (диапазона выделяемых IP-адресов) должен быть больше или равен максимальному количеству клиентов.

  Невыполнение условия может привести к блокировке выдачи IP-адреса новому клиенту, запросившему этот IP-адрес, если ранее адрес был выдан другому клиенту отказавшей нодой. Блокировка выдачи IP-адреса, ранее выданного отказавшей нодой, новому клиенту устраняется после восстановления отказавшей ноды.

- В данный диапазон не должны попадать адреса сетевых интерфейсов и кластерные адреса криптошлюза.

Выполните следующие шаги на основной ноде кластера:

1. Измените файл конфигурации `/etc/dhcp/dhcpd.conf`.:

```
# Hub1-n1 dhcpd.conf

log-facility local7;
default-lease-time 600;
max-lease-time 3600;

failover peer "failover-partner" {
    primary;
    address 192.168.100.10;
    port 519;
    peer address 192.168.100.20;
    peer port 520;
    max-response-delay 60;
    max-unacked-updates 10;
    mclt 3600;
    split 128;
    load balance max seconds 3;
}

subnet 192.168.100.0 netmask 255.255.255.0 {
    option routers              192.168.100.1;
```

```
    option subnet-mask          255.255.255.0;
    option broadcast-address    192.168.100.255;
    option domain-name-servers  8.8.8.8;


    pool {
        failover peer "failover-partner";
        range 192.168.100.51 192.168.100.150;
    }
}
```

где:

- `log-facility <уровень>` – уровень лога syslog; при указании `local7`, файлы логов будут писаться в файл `/var/log/cspvpngate.log`;
- `default-lease-time <время>` – время аренды IP-адресов (в секундах);
- `max-lease-time <время>` – максимальное время аренды;
- `failover peer <Имя> {...}` – секция для настройки failover;
- `primary` – указывает, что DHCP сервер является первичным;
- `address <IP-адрес>` – указывает какой адрес должен прослушиваться для установления соединения с failover партнером. Также является идентификатором для установления;
- `port <номер порта>` – указывает какой tcp порт должен прослушиваться для установления соединения с failover партнером;
- `peer address <IP-адрес>` – указывает какой адрес failover партнера. Также является идентификатором для установления;
- `peer port <номер порта>` – указывает tcp порт партнера. Должен совпадать со значением `port` в настройках партнёра;
- `max-response-delay <время>` – указывает какое время в секундах должно пройти с момента получения последнего сообщения от сервера партнёра, чтобы считать, что соединение с партнёром разорвано;
- `max-unacked-updates <количество пакетов>` – указывает сколько BNDUPD сообщений (сообщение о обновлении базы привязки) может быть отправлено перед получением BNDACK сообщения (сообщении о подведении). Рекомендуется использовать 10;
- `mclt <время>` – время, на которое может быть продлена запись, когда нет соединения с партнёром. Указывается только на первичном DHCP сервере. Рекомендуется использовать 3600 секунд;
- `split <индекс>` – служит для балансировки нагрузки между серверами. Указывает значение между 0 и 256. При 128 нагрузка делится пополам. Чем выше значение, тем больше нагрузки будет на первичном DHCP сервере. При 256 нагрузка не делится. Указывается только на первичном DHCP сервере;
- `load balance max seconds <время>` – время, через которое будет остановлена балансировка нагрузки. Время обновляется каждый раз обновляется, когда от клиента получают первое `DHCPDISCOVER` или первое `DHCPREQUEST` сообщение;
- `subnet <IP-адрес> netmask <маска> {...}` – описание параметров сети, для которой будут раздаваться сетевые настройки;
- `option routers <IP-адрес>` – IP адрес шлюза по умолчанию;
- `option subnet-mask <маска>` – маска сети;
- `option broadcast-address < IP-адрес >` – широковещательный IP адрес сети;
- `option domain-name-servers <IP-адрес>` – DNS сервер по умолчанию;
- `range <диапазон IP-адресов>` – диапазон, из которого будут раздаваться IP-адреса DHCP клиентам;
- `pool {failover peer <Имя>; range <диапазон IP-адресов>;}` – диапазон, который будет выделяться обоими нодами.

2. Для настройки интерфейса, на котором будут раздаваться IP-адреса, отредактируйте файл `/etc/default/isc-dhcp-server`. Имя интерфейса в переменной `INTERFACESv4` должно соответствовать имени интерфейса в нотации linux:

```
INTERFACESv4="eth1"
```

Если необходимо задать несколько интерфейсов пропишите их через пробел (в данной инструкции используется только один интерфейс):

```
INTERFACESv4="eth1 eth2"
```

3. Запустите сервис DHCP сервера и добавьте его в автозагрузку:

```
root@Hub1-n1:~# systemctl start isc-dhcp-server.service
root@Hub1-n1:~# systemctl enable isc-dhcp-server.service
```

В Приложении представлены тексты конфигураций `/etc/dhcp/dhcpd.conf` и `/etc/default/isc-dhcp-server` для криптошлюза Hub1-n1.

Настройка криптошлюза Hub1-n2

В данной инструкции будут описаны только настройки DHCP сервера. Остальные настройки должны быть взяты из сценария «Построение кластера на базе протокола VRRP с настройкой при помощи CLI».

Настройка DHCP сервера

1. Измените файл конфигурации `/etc/dhcp/dhcpd.conf`.:

```
# Hub1-n2 dhcpd.conf
log-facility local7;
default-lease-time 600;
max-lease-time 3600;

failover peer "failover-partner" {
    secondary;
    address 192.168.100.20;
    port 520;
    peer address 192.168.100.10;
    peer port 519;
    max-response-delay 60;
    max-unacked-updates 10;
    load balance max seconds 3;
}

subnet 192.168.100.0 netmask 255.255.255.0 {
    option routers              192.168.100.1;
    option subnet-mask          255.255.255.0;
    option broadcast-address    192.168.100.255;
    option domain-name-servers  8.8.8.8;

    pool {
        failover peer "failover-partner";
        range 192.168.100.51 192.168.100.150;
    }
}
```

где:

- `secondary` – указывает, что DHCP сервер является вторичным;
- остальные параметры были описаны в настройке Hub1-n1.

2. Для настройки интерфейса, на котором будут раздаваться IP-адреса, отредактируйте файл `/etc/default/isc-dhcp-server`. Имя интерфейса в переменной `INTERFACESv4` должно соответствовать имени интерфейса в нотации linux:

```
INTERFACESv4="eth1"
```

Если необходимо задать несколько интерфейсов пропишите их через пробел (в данной инструкции используется только один интерфейс):

```
INTERFACESv4="eth1 eth2"
```

3. Запустите сервис DHCP сервера и добавьте его в автозагрузку:

```
root@Hub1-n2:~# systemctl start isc-dhcp-server.service
root@Hub1-n2:~# systemctl enable isc-dhcp-server.service
```

В Приложении представлены тексты конфигураций `/etc/dhcp/dhcpd.conf` и `/etc/default/isc-dhcp-server` для криптошлюза Hub1-n2.

Проверка работоспособности стенда

Проверка работы DHCP кластера

1. Проверьте содержимое лог-файла `/var/log/cspvpngate.log` на наличие сообщения о установления связи с failover партнёром:

```
root@Hub1-n1:~# tail -n 50 /var/log/cspvpngate.log | grep "dhcpd"
```

```
2024-05-27T13:41:07.288558+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
I move from communications-interrupted to startup
2024-05-27T13:41:07.289381+03:00 Hub1-n1 dhcpd[768]: Server starting service.
2024-05-27T13:41:10.512498+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
peer moves from normal to communications-interrupted
2024-05-27T13:41:10.514170+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
I move from startup to normal
2024-05-27T13:41:10.514241+03:00 Hub1-n1 dhcpd[768]: balancing pool 55b07134cf60
192.168.100.0/24  total 100  free 50  backup 50  lts 0  max-own (+/-)10
2024-05-27T13:41:10.514279+03:00 Hub1-n1 dhcpd[768]: balanced pool 55b07134cf60
192.168.100.0/24  total 100  free 50  backup 50  lts 0  max-misbal 15
2024-05-27T13:41:10.517309+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
peer moves from communications-interrupted to normal
2024-05-27T13:41:10.517379+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
Both servers normal
```

```
root@Hub1-n2:~# tail -n 50 /var/log/cspvpngate.log | grep "dhcpd"
```

```
2024-05-27T13:41:09.017099+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
I move from communications-interrupted to startup
2024-05-27T13:41:09.017715+03:00 Hub1-n2 dhcpd[764]: Server starting service.
2024-05-27T13:41:10.031196+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
peer moves from normal to communications-interrupted
2024-05-27T13:41:10.032547+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
I move from startup to normal
2024-05-27T13:41:10.032615+03:00 Hub1-n2 dhcpd[764]: balancing pool 55c4ad262f20
192.168.100.0/24  total 100  free 50  backup 50  lts 0  max-own (+/-)10
2024-05-27T13:41:10.032668+03:00 Hub1-n2 dhcpd[764]: balanced pool 55c4ad262f20
192.168.100.0/24  total 100  free 50  backup 50  lts 0  max-misbal 15
2024-05-27T13:41:10.032691+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
peer moves from communications-interrupted to normal
2024-05-27T13:41:10.032742+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
Both servers normal
```

Видно, что соединение с партнёром установлено. Делят 100 адресов из подсети 192.168.100.0/24.

2. Настройте получение сетевых параметров на соответствующих интерфейсах (в данной инструкции это `ens192`) Host1-b-hub1 по DHCP. Например, можете ввести `dhclient` для интерфейса:

```
root@Host1-b-hub1:~# dhclient ens192
```

3. Проверьте полученные по DHCP настройки (имя файла настроек: `/var/lib/dhcp/dhclient.ens192.leases`):

```
root@Host1-b-hub1:~# cat /var/lib/dhcp/dhclient.ens192.leases
```

```
lease {
  interface "ens192";
  fixed-address 192.168.100.101;
  option subnet-mask 255.255.255.0;
  option routers 192.168.100.1;
  option dhcp-lease-time 600;
  option dhcp-message-type 5;
  option domain-name-servers 8.8.8.8;
  option dhcp-server-identifier 192.168.100.10;
  option broadcast-address 192.168.100.255;
```

```
  renew 4 2024/05/27 13:50:46;
  rebind 4 2024/05/27 13:55:21;
  expire 4 2024/05/27 13:56:36;
}
```

Устройству Host1-b-hub1 выдан IP-адрес 192.168.100.101.

4. Отключите внутренний интерфейс `eth1` на Hub1-n1:

```
root@Hub1-n1:~# ifdown eth1
```

5. Настройте получение сетевых параметров на Host2-b-hub1 по DHCP:

```
root@Host2-b-hub1:~# dhclient ens192
```

6. Проверьте полученные по DHCP настройки (имя файла настроек: `/var/lib/dhcp/dhclient.ens192.leases`):

```
root@Host2-b-hub1:~# cat /var/lib/dhcp/dhclient.ens192.leases
```

```
lease {
  interface "ens192";
  fixed-address 192.168.100.51;
  option subnet-mask 255.255.255.0;
  option routers 192.168.100.1;
  option dhcp-lease-time 600;
  option dhcp-message-type 5;
  option domain-name-servers 8.8.8.8;
  option dhcp-server-identifier 192.168.100.10;
  option broadcast-address 192.168.100.255;
  renew 4 2024/05/27 14:11:06;
  rebind 4 2024/05/27 14:15:41;
  expire 4 2024/05/27 14:16:56;
}
```

Устройству Host2-b-hub1 выдан IP-адрес 192.168.100.51. Резервный сервер выдаёт из диапазона 192.168.100.51-192.168.100.100. Основной DHCP сервер выдаёт из диапазона 192.168.100.101-192.168.100.150.

7. Подождите 10 минут и посмотрите лог-файл `/var/log/cspvpngate.log`:

```
root@Hub1-n1:~# tail -n 50 /var/log/cspvpngate.log | grep "dhcpd"
```

```
2024-05-27T13:41:07.288558+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
I move from communications-interrupted to startup
2024-05-27T13:41:07.289381+03:00 Hub1-n1 dhcpd[768]: Server starting service.
2024-05-27T13:41:10.512498+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
peer moves from normal to communications-interrupted
2024-05-27T13:41:10.514170+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
I move from startup to normal
2024-05-27T13:41:10.514241+03:00 Hub1-n1 dhcpd[768]: balancing pool 55b07134cf60
192.168.100.0/24  total 100  free 50  backup 50  lts 0  max-own (+/-)10
2024-05-27T13:41:10.514279+03:00 Hub1-n1 dhcpd[768]: balanced pool 55b07134cf60
192.168.100.0/24  total 100  free 50  backup 50  lts 0  max-misbal 15
2024-05-27T13:41:10.517309+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
peer moves from communications-interrupted to normal
2024-05-27T13:41:10.517379+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
Both servers normal
2024-05-27T13:47:43.424073+03:00 Hub1-n1 dhcpd[768]: DHCPDISCOVER from
00:50:56:9e:85:bc via eth1
2024-05-27T13:47:44.425243+03:00 Hub1-n1 dhcpd[768]: DHCPOFFER on 192.168.100.101 to
00:50:56:9e:85:bc (Host1-b-hub1) via eth1
2024-05-27T13:47:44.425646+03:00 Hub1-n1 dhcpd[768]: DHCPREQUEST for 192.168.100.101
(192.168.100.10) from 00:50:56:9e:85:bc (Host1-b-hub1) via eth1
2024-05-27T13:47:44.428789+03:00 Hub1-n1 dhcpd[768]: DHCPACK on 192.168.100.101 to
00:50:56:9e:85:bc (Host1-b-hub1) via eth1
```

```
2024-05-27T13:50:47.407303+03:00 Hub1-n1 dhcpd[768]: DHCPREQUEST for 192.168.100.101
from 00:50:56:9e:85:bc (Host1-b-hub1) via eth1
2024-05-27T13:50:47.408125+03:00 Hub1-n1 dhcpd[768]: DHCPACK on 192.168.100.101 to
00:50:56:9e:85:bc (Host1-b-hub1) via eth1
2024-05-27T14:00:02.089654+03:00 Hub1-n1 dhcpd[768]: DHCPREQUEST for 192.168.100.101
from 00:50:56:9e:85:bc (Host1-b-hub1) via eth1
2024-05-27T14:00:02.091400+03:00 Hub1-n1 dhcpd[768]: DHCPACK on 192.168.100.101 to
00:50:56:9e:85:bc (Host1-b-hub1) via eth1
2024-05-27T14:07:34.735805+03:00 Hub1-n1 dhcpd[768]: timeout waiting for failover
peer failover-partner
2024-05-27T14:07:34.736070+03:00 Hub1-n1 dhcpd[768]: peer failover-partner:
disconnected
2024-05-27T14:07:34.736475+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
I move from normal to communications-interrupted
2024-05-27T14:07:39.742157+03:00 Hub1-n1 dhcpd[768]: failover peer failover-partner:
address not available
```

```
root@Hub1-n2:~# tail -n 50 /var/log/cspvpngate.log | grep "dhcpd"
```

```
2024-05-27T13:41:09.017099+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
I move from communications-interrupted to startup
2024-05-27T13:41:09.017715+03:00 Hub1-n2 dhcpd[764]: Server starting service.
2024-05-27T13:41:10.031196+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
peer moves from normal to communications-interrupted
2024-05-27T13:41:10.032547+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
I move from startup to normal
2024-05-27T13:41:10.032615+03:00 Hub1-n2 dhcpd[764]: balancing pool 55c4ad262f20
192.168.100.0/24  total 100  free 50  backup 50  lts 0  max-own (+/-)10
2024-05-27T13:41:10.032668+03:00 Hub1-n2 dhcpd[764]: balanced pool 55c4ad262f20
192.168.100.0/24  total 100  free 50  backup 50  lts 0  max-misbal 15
2024-05-27T13:41:10.032691+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
peer moves from communications-interrupted to normal
2024-05-27T13:41:10.032742+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
Both servers normal
2024-05-27T14:07:32.351399+03:00 Hub1-n2 dhcpd[764]: timeout waiting for failover
peer failover-partner
2024-05-27T14:07:32.351839+03:00 Hub1-n2 dhcpd[764]: peer failover-partner:
disconnected
2024-05-27T14:07:32.352529+03:00 Hub1-n2 dhcpd[764]: failover peer failover-partner:
I move from normal to communications-interrupted
2024-05-27T14:11:06.424073+03:00 Hub1-n2 dhcpd[764]: DHCPDISCOVER from
00:50:56:9e:38:8b via eth1
2024-05-27T14:11:07.425243+03:00 Hub1-n2 dhcpd[764]: DHCPOFFER on 192.168.100.51 to
00:50:56:9e:38:8b (Host2-b-hub1) via eth1
2024-05-27T14:11:07.067972+03:00 Hub1-n2 dhcpd[764]: DHCPREQUEST for 192.168.100.51
from 00:50:56:9e:38:8b (Host2-b-hub1) via eth1
2024-05-27T14:11:07.068361+03:00 Hub1-n2 dhcpd[764]: DHCPACK on 192.168.100.51 to
00:50:56:9e:38:8b (Host2-b-hub1) via eth1
2024-05-27T14:12:44.684094+03:00 Hub1-n2 dhcpd[764]: DHCPREQUEST for 192.168.100.101
from 00:50:56:9e:85:bc via eth1
2024-05-27T14:12:44.685387+03:00 Hub1-n2 dhcpd[764]: DHCPACK on 192.168.100.101 to
00:50:56:9e:85:bc (Host1-b-hub1) via eth1
```

Видно, что на каждом криптошлюзе достигнут таймаут ожидания failover партнёра и разрыв соединения. На Hub1-n1 из-за отсутствия адреса на интерфейсе eth1, dhcpd оставляется сообщения что адрес недоступен. На Hub1-n2 видно, что Host2-b-hub1 взял адрес из пула адресов Hub1-n2, и Host1-b-hub1 дальше использует адрес 192.168.100.101.

8. Включите внутренний интерфейс `eth1` на Hub1-n1:

```
root@Hub1-n1:~# ifup eth1
```

Проверка работы DHCP сервера Spoke1

1. Настройте получение сетевых параметров на соответствующих интерфейсах (в данной инструкции это `ens192`) Host1-b-spoke1 и Host2-b-spoke1 по DHCP. Например, можете ввести `dhclient` для интерфейса:

```
root@Host1-b-spoke1:~# dhclient ens192
root@Host2-b-spoke1:~# dhclient ens192
```

2. Проверьте полученные по DHCP настройки (имя файла настроек: `/var/lib/dhcp/dhclient.ens192.leases`):

```
root@Host1-b-spoke1:~# cat /var/lib/dhcp/dhclient.ens192.leases
```

```
lease {
  interface "ens192";
  fixed-address 192.168.1.10;
  server-name "Spoke1";
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option dhcp-lease-time 21600;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.1.1;
  option dhcp-server-identifier 192.168.1.1;
  renew 4 2024/04/11 05:08:04;
  rebind 4 2024/04/11 07:56:36;
  expire 4 2024/04/11 08:41:36;
}
```

```
root@Host2-b-spoke1:~# cat /var/lib/dhcp/dhclient.ens192.leases
```

```
lease {
  interface "ens192";
  fixed-address 192.168.1.5;
  server-name "Spoke1";
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option dhcp-lease-time 21600;
  option dhcp-message-type 5;
  option domain-name-servers 192.168.1.1;
  option dhcp-server-identifier 192.168.1.1;
  renew 4 2024/04/11 05:04:26;
  rebind 4 2024/04/11 08:00:26;
  expire 4 2024/04/11 08:45:26;
}
```

Устройству Host1-b-spoke1 выдан IP-адрес 192.168.1.10. Устройству Host2-b-spoke1 выдан IP-адрес 192.168.1.5.

Проверка защищенного соединения

Описание процесса проверки IP связности, проверки PKI, проверки построения защищённого соединения и проверки работы межсетевого экрана совпадает со сценарием «Построение кластера на базе протокола VRRP с настройкой при помощи CLI» с IP адресами хостов полученных по DHCP.

Дополнительные возможности

Настройка IPv6

Настройка сервиса RADVD

DHCP сервер не объявляет маршруты IPv6. Для объявления маршрутов IPv6 используется сервис маршрутных объявлений (Router Advertisement Daemon или RADVD).

1. Для объявления маршрута по умолчанию требуется изменить конфигурационный файл `/etc/radvd.conf` на криптошлюзе:

```
interface eth1
{
        AdvSendAdvert on;
        MaxRtrAdvInterval 10;
        MinRtrAdvInterval 5;
};
```

где:

- `interface <Имя_интерфейса>` – имя интерфейса в нотации linux, на котором будет работать RADVD;
- `AdvSendAdvert <on| off>` – указывает отправлять ли периодические пакеты объявления маршрута по умолчанию и ответы на запросы;
- `MaxRtrAdvInterval <Время>` – максимальное время между отправкой самостоятельных объявлений маршрутизатора с интерфейса в секундах. Должен быть больше 4 секунд и меньше 1800;
- `MinRtrAdvInterval <Время>` – минимальное время между отправкой самостоятельных объявлений маршрутизатора с интерфейса в секундах. Должен быть больше 3 секунд и меньше 0.75*`MaxRtrAdvInterval`.

2. Запустите сервис RADVD и добавьте его в автозагрузку:

```
root@Spoke1:~# systemctl start radvd.service
root@Spoke1:~# systemctl enable radvd.service
```

3. На хостах следует включить обработку маршрутных объявлений и маршрутов по умолчанию:

Для хостов на ОС Windows 10, включать обработку маршрутных объявлений и маршрутов по умолчанию не требуется, следовательно пункты 3 и 4 выполнять не нужно.

```
root@Host1-b-spoke1:~# echo 2 > /proc/sys/net/ipv6/conf/all/accept_ra
root@Host1-b-spoke1:~# echo 1 > /proc/sys/net/ipv6/conf/all/accept_ra_defrtr
root@Host1-b-spoke1:~# echo 2 > /proc/sys/net/ipv6/conf/ens192/accept_ra
root@Host1-b-spoke1:~# echo 1 > /proc/sys/net/ipv6/conf/ens192/accept_ra_defrtr
```

Для `accept_ra_defrtr` значение 0 или 1:

- 0 – обработка маршрута по умолчанию отключена;
- 1 – обработка маршрута по умолчанию включена.

Для `accept_ra` значение 0, 1 или 2:

- 0 – обработка отключена;
- 1 – обработка включена, если на устройстве отключен forwarding;
- 2 – обработка включена.

4. На хостах следует добавить следующие строки в `/etc/sysctl.conf`:

```
net.ipv6.conf.all.accept_ra = 2
net.ipv6.conf.all.accept_ra_defrtr = 1
net.ipv6.conf.ens192.accept_ra = 2
net.ipv6.conf.ens192.accept_ra_defrtr = 1
```

Настройка DHCP сервера

1. Измените файл конфигурации `/etc/dhcp/dhcpd6.conf`.

```
default-lease-time 21600;
dhcpv6-lease-file-name "/var/lib/dhcp/dhcpd6.leases";

option dhcp6.name-servers 2001:4860:4860::8888;
subnet6 2001:db8::192:168:1:0/112 {
        range6 2001:db8::192:168:1:10 2001:db8::192:168:1:101;
```

```
}

host Host2 {
        hardware ethernet 00:50:56:9e:d6:06;
        fixed-address6 2001:db8::192:168:1:5;
}
```

где:

- `default-lease-time <время>` – время аренды IP-адресов (в секундах);
- `dhcpv6-lease-file-name <путь до файла>` – путь до lease-файла;
- `option dhcp6.name-servers <IP-адрес>` – DNS сервер по умолчанию;
- `subnet6 <IP-адрес>/<маска> {...}` – описание параметров сети, для которой будут раздаваться сетевые настройки;
- `range6 <диапазон IP-адресов>` – диапазон, из которого будут раздаваться IP-адреса DHCP клиентам;
- `host <имя хоста> { hardware ethernet <MAC-адрес>; fixed-address <IP-адрес>; }` – хосту с соответствующим MAC-адресом статически привязать IP-адрес.

2. Для настройки интерфейса, на котором будут раздаваться IP-адреса, отредактируйте файл `/etc/default/isc-dhcp-server`. Имя интерфейса в переменной `INTERFACESv6` должно соответствовать имени интерфейса в нотации linux:

   ```
   TERFACESv6="eth1"
   ```

   Если необходимо задать несколько интерфейсов пропишите их через пробел (в данной инструкции используется только один интерфейс):

   ```
   INTERFACESv6="eth1 eth2"
   ```

3. Задайте через cisco-like консоль IP-адреса для интерфейсов из п.2 (соответствие между именами интерфейсов в нотации linux и cisco-like можно посмотреть в файле `/etc/ifaliases.cf`). IP-адреса должны быть из диапазона, который задан в параметре `subnet6` в п.1, но не входить в диапазон, который задан в `range6`.

4. Запустите сервис DHCP сервера и добавьте его в автозагрузку:

   ```
   root@Spoke1:~# systemctl start isc-dhcp-server.service
   root@Spoke1:~# systemctl enable isc-dhcp-server.service
   ```

Конфигурирование нескольких пулов

В случае необходимости, можно настроить DHCP сервер для работы на нескольких интерфейсах и раздачи с них адресов из разных пулов. В иностранной литературе такое решение называется Multihomed DHCP Server.

Настройка IPv4

Ниже показан пример конфигурации `/etc/dhcp/dhcpd.conf` для такого случая. Привязка пула к интерфейсу здесь происходит при помощи параметра `subnet` (на интерфейсе криптошлюза должен быть адрес из этой подсети).

```
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0 {
       option subnet-mask 255.255.255.0;
       option routers 192.168.1.1;
       range 192.168.1.5 192.168.1.15;
}
subnet 192.168.2.0 netmask 255.255.255.0 {
       option subnet-mask 255.255.255.0;
       option routers 192.168.2.1;
       range 192.168.2.5 192.168.2.15;
}
```

В файле /etc/default/isc-dhcp-server следует указать используемые интерфейсы через пробел. Пример:

```
INTERFACESv4="eth1 eth2"
```

Настройка IPv6

Ниже показан пример конфигурации /etc/dhcp/dhcpd6.conf для такого случая. Привязка пула к интерфейсу здесь происходит при помощи параметра subnet6 (на интерфейсе криптошлюза должен быть адрес из этой подсети).

```
default-lease-time 36000;
dhcpv6-lease-file-name "/var/lib/dhcp/dhcpd6.leases";

subnet6 2001:db8::192:168:1:0/112 {
        range6 2001:db8::192:168:1:5 2001:db8::192:168:1:15;
}

subnet6 2001:db8::192:168:2:0/112 {
        range6 2001:db8::192:168:2:5 2001:db8::192:168:2:15;
}
```

В файле /etc/default/isc-dhcp-server следует указать используемые интерфейсы через пробел. Пример:

```
INTERFACESv6="eth1 eth2"
```

Настройка опций для работы с TFTP сервером

В некоторых случаях, помимо IP-адреса, устройству необходимо получать адрес TFTP сервера для скачивания файлов. Для этого, сервисом DHCP предусмотрены опции под номерами 66 и 67. Для того, чтобы осуществить настройку данных опций, необходимо произвести некоторые настройки на DHCP сервере и на DHCP клиенте. Настройка происходит, только для IPv4. Данная опция отсутствует для IPv6.

Файл /etc/dhcp/dhcpd.conf должен иметь вид:

```
root@Spoke1:~# cat /etc/dhcp/dhcpd.conf
```

```
# Sample configuration file for ISC dhcpd

server-name Spoke1;
log-facility local7;
ddns-update-style none;
subnet 192.168.1.0 netmask 255.255.255.0 {
       option routers 192.168.1.1;
       option subnet-mask 255.255.255.0;
       option domain-name-servers 192.168.1.1;
       option tftp-server-name "ftp://login:password@192.168.30.245";
       option bootfile-name "serial";
       range 192.168.1.10 192.168.1.254;
       default-lease-time 21600;
       max-lease-time 28800;
}
```

где:

- option tftp-server-name – опция под номером 66, которая передаёт в качестве аргумента строку с адресом TFTP сервера;
- option bootfile-name – опция под номером 67, которая передаёт в качестве аргумента строку с путём до файла, который необходимо скачать с TFTP сервера.

После редактирования данного файла, необходимо перезапустить сервис isc-dhcp-server:

```
root@Spoke1:~# systemctl restart isc-dhcp-server.service
```

На DHCP клиенте необходимо отредактировать файл `/etc/dhcp/dhclient.conf`, добавив в список запросов (после ключевого слова `request`) опции `tftp-server-name` и `bootfile-name`. Файл `/etc/dhcp/dhclient.conf` должен иметь следующий вид:

```
root@Spoke1:~# cat /etc/dhcp/dhcpd.conf
```

```
...
option rfc3442-classless-static-routes code 121 = array of unsigned integer 8;

send host-name = gethostname();
request subnet-mask, broadcast-address, time-offset, routers,
        domain-name, domain-name-servers, domain-search, host-name,
        dhcp6.name-servers, dhcp6.domain-search, dhcp6.fqdn, dhcp6.sntp-servers,
        netbios-name-servers, netbios-scope, interface-mtu,
        rfc3442-classless-static-routes, ntp-servers, tftp-server-name, bootfile-name;
...
```

После запроса на получение адреса, можно увидеть отправленные сервером настройки на стороне DHCP клиента:

```
root@Host1-b-Spoke1:~# cat /var/lib/dhcp/dhclient.ens192.leases
```

```
...
lease {
  interface "ens32";
  fixed-address 192.168.1.10;
  server-name "Spoke1";
  option subnet-mask 255.255.255.0;
  option routers 192.168.1.1;
  option dhcp-lease-time 21600;
  option tftp-server-name "192.168.30.245";
  option bootfile-name "serial";
  option dhcp-message-type 5;
  option domain-name-servers 192.168.1.1;
  option dhcp-server-identifier 192.168.1.1;
  renew 3 2021/03/03 15:40:57;
  rebind 3 2021/03/03 17:58:25;
  expire 3 2021/03/03 18:43:25;
}
...
```

При запросе адреса со стороны DHCP клиента, DHCP сервер выдал адрес TFPT сервера и путь для скачивания файла с этого сервера.

Приложение

Конфигурации криптошлюза Hub1-n1

1. Текст конфигурации `/etc/dhcp/dhcpd.conf`:

```
# Hub1-n1 dhcpd.conf

log-facility local7;
default-lease-time 600;
max-lease-time 3600;

failover peer "failover-partner" {
    primary;
    address 192.168.100.10;
    port 519;
    peer address 192.168.100.20;
    peer port 520;
    max-response-delay 60;
    max-unacked-updates 10;
```

```
    mclt 3600;
    split 128;
    load balance max seconds 3;
}

subnet 192.168.100.0 netmask 255.255.255.0 {
    option routers              192.168.100.1;
    option subnet-mask          255.255.255.0;
    option broadcast-address    192.168.100.255;
    option domain-name-servers  8.8.8.8;


    pool {
        failover peer "failover-partner";
        range 192.168.100.51 192.168.100.150;
    }
}
```

2. Текст конфигурации `/etc/default/isc-dhcp-server`:

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       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="eth1"
INTERFACESv6=""
```

Конфигурации криптошлюза Hub1-n2

1. Текст конфигурации `/etc/dhcp/dhcpd.conf`:

```
# Hub1-n2 dhcpd.conf

log-facility local7;
default-lease-time 600;
max-lease-time 3600;

failover peer "failover-partner" {
    secondary;
    address 192.168.100.20;
    port 520;
    peer address 192.168.100.10;
    peer port 519;
    max-response-delay 60;
    max-unacked-updates 10;
    load balance max seconds 3;
}

subnet 192.168.100.0 netmask 255.255.255.0 {
    option routers              192.168.100.1;
```

```
    option subnet-mask          255.255.255.0;
    option broadcast-address    192.168.100.255;
    option domain-name-servers  8.8.8.8;


    pool {
        failover peer "failover-partner";
        range 192.168.100.51 192.168.100.150;
    }
}
```

2. Текст конфигурации `/etc/default/isc-dhcp-server`:

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       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="eth1"
INTERFACESv6=""
```

Конфигурации криптошлюза Spoke1

1. Текст конфигурации `/etc/dhcp/dhcpd.conf`:

```
# Sample configuration file for ISC dhcpd

authoritative;
server-name Spoke1;
log-facility local7;
ddns-update-style none;
subnet 192.168.1.0 netmask 255.255.255.0 {
       option routers 192.168.1.1;
       option subnet-mask 255.255.255.0;
       option domain-name-servers 192.168.1.1;
       range 192.168.1.10 192.168.1.254;
       default-lease-time 21600;
       max-lease-time 28800;
}
host host2 {
       hardware ethernet 00:50:56:9e:d6:06;
       fixed-address 192.168.1.5;
}
```

2. Текст конфигурации `/etc/default/isc-dhcp-server`:

```
# Defaults for isc-dhcp-server (sourced by /etc/init.d/isc-dhcp-server)

# Path to dhcpd's config file (default: /etc/dhcp/dhcpd.conf).
#DHCPDv4_CONF=/etc/dhcp/dhcpd.conf
#DHCPDv6_CONF=/etc/dhcp/dhcpd6.conf

# Path to dhcpd's PID file (default: /var/run/dhcpd.pid).
```

```
#DHCPDv4_PID=/var/run/dhcpd.pid
#DHCPDv6_PID=/var/run/dhcpd6.pid

# Additional options to start dhcpd with.
#       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="eth1"
INTERFACESv6=""
```