ООО «Фактор-ТС»

Примеры конфигураций Dionis DPS

Построение защищенных VPN-туннелей (ГОСТ)

ООО «Фактор-ТС»
Москва 2023

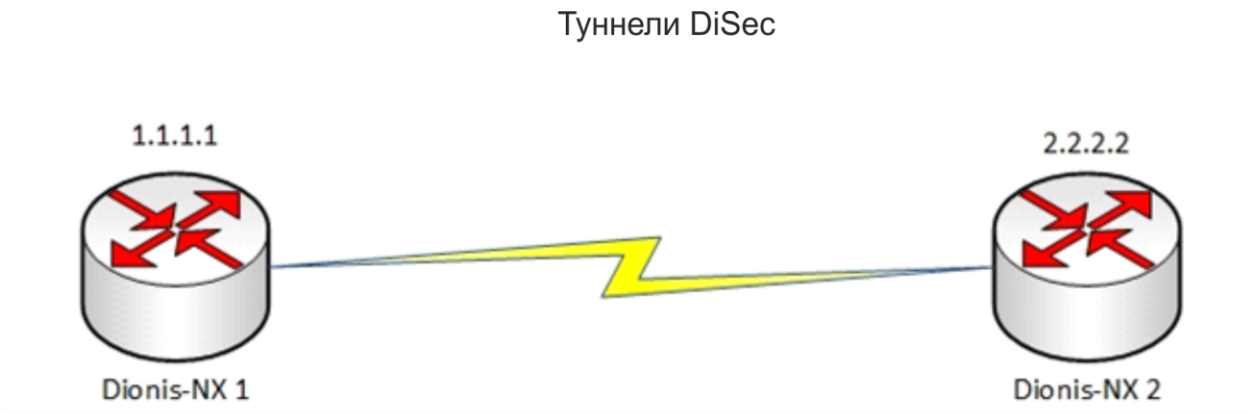
Содержание

Настройка DiSec VPN туннелей

Для создания интерфейса ditun в режиме шифрования/расшифрования в Dionis-NX должен быть предварительно создан ключ доступа и загружены ключи абонентов Disec.

Для работы интерфейса в открытом режиме (без шифрования/расшифрования) это не является необходимым.

Будем считать, что туннель DISEC инициализирован с поддержкой криптографии.




```
(config-if-ditun0)# id 1
(config-if-ditun0)# alg encrypt
(config-if-ditun0)# local 1.1.1.1
(config-if-ditun0)# remote 2.2.2.2
(config-if-ditun0)# serial 1
(config-if-ditun0)# local-cn 1
(config-if-ditun0)# remote-cn 2
(config-if-ditun0)# enable
```

```
(config-if-ditun0)# id 1
(config-if-ditun0)# alg encrypt
(config-if-ditun0)# local 2.2.2.2
(config-if-ditun0)# remote 1.1.1.1
(config-if-ditun0)# serial 1
(config-if-ditun0)# local-cn 2
(config-if-ditun0)# remote-cn 1
(config-if-ditun0)# enable
```

Для создания интерфейса, из режима конфигурации выполните команду:

```
(config)# interface ditun 0
```

В качестве номера интерфейса (в примере – 0) может быть выбрано любое число (натуральное или 0). После этого, в режиме конфигурации интерфейса необходимо задать следующие параметры:

```
(config-if-ditun0)# id 1
(config-if-ditun0)# alg encrypt
(config-if-ditun0)# local 1.1.1.1
(config-if-ditun0)# remote 2.2.2.2
(config-if-ditun0)# serial 1
(config-if-ditun0)# local-cn 1
(config-if-ditun0)# remote-cn 2
(config-if-ditun0)# enable
```

Рассмотрим по порядку параметры туннеля, которые необходимо указать при его создании:

- local: задает IP-адрес локального конца туннеля;
- remote: задает IP-адрес удаленного конца туннеля;

- id: целое число (до 5 цифр), идентифицирующее туннель; значение этого параметра должно совпадать на обоих концах туннеля;
- serial: номер серии ключей - целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети;
- local-cn: целое число (до 5 цифр), равное номеру данного узла в криптографической сети;
- remote-cn: целое число (до 5 цифр), равное номеру в криптографической сети того узла, с которым будет выполняться обмен информацией по данному туннелю;
- alg encrypt: алгоритм трансформации данных в туннеле; возможные значения:
  - compression: только сжатие данных;
  - encryption: только зашифрование данных;
  - both: и сжатие, и зашифрование данных;
  - none: никакой трансформации данных не производится.

Интерфейс будет создан в тот момент, когда будет задана минимальная необходимая информация. Для открытого туннеля (без криптографического преобразования) это набор параметров: id, local, remote. В случае крипто-туннеля (alg соответствует both или encrypt) дополнительно требуется задать параметры: local-cn, remote-cn, serial.

Параметр enable – делает созданный интерфейс активным.

Аналогичным образом настраиваем другой узел сети:

```
(config)# interface ditun 0

(config-if-ditun0)# id 1
(config-if-ditun0)# alg encrypt
(config-if-ditun0)# local 2.2.2.2
(config-if-ditun0)# remote 1.1.1.1
(config-if-ditun0)# serial 1
(config-if-ditun0)# local-cn 2
(config-if-ditun0)# remote-cn 1
(config-if-ditun0)# enable
```

Настройка криптографического туннеля по протоколу IPSec Point-to-point (аутентификация по pre-shared ключам)

Рассмотрим самый простой пример настройки соединения типа «точка-точка» со взаимной аутентификацией по ключам.

Допустим у нас есть два узла Dionis-NX с IP-адресами 192.168.1.1 и 192.168.2.1.


```
# crypto psk set key psk1 flash /psks/key1
# configure terminal
(config)# crypto psk map 192.168.1.1 192.168.2.1 psk1
 (config)# crypto ike conn t1
(config-ike-conn-t1)# auth psk
(config-ike-conn-t1)# local ip 192.168.1.1
(config-ike-conn-t1)# remote ip 192.168.2.1
(config-ike-conn-t1)# crypto ike enable
(config)# crypto ike enable conn t1
(config)#do crypto ike initiate conn t1
```

```
# crypto psk set key psk1 flash /psks/key1
# configure terminal
(config)# crypto psk map 192.168.2.1 192.168.1.1 psk1
(config)# crypto ike conn t1
(config-ike-conn-t1)# auth psk
(config-ike-conn-t1)# local ip 192.168.2.1
(config-ike-conn-t1)# remote ip 192.168.1.1
(config-ike-conn-t1)# crypto ike enable
(config)# crypto ike enable conn t1
 (config)#do crypto ike initiate conn t1
```

Настройка узла 1:

Загружаем pre-shared ключ с внешнего носителя (допустим, из файла /psks/key1):

```
# crypto psk set key psk1 flash /psks/key1
```

Ассоциируем загруженный ключ с концами туннеля:

```
# configure terminal
(config)# crypto psk map 192.168.1.1 192.168.2.1 psk1
```

Создаём соединение, указываем метод аутентификации по PSK и IP-адреса концов туннеля:

```
(config)# crypto ike conn t1
(config-ike-conn-t1)# auth psk
(config-ike-conn-t1)# local ip 192.168.1.1
(config-ike-conn-t1)# remote ip 192.168.2.1
```

Включаем туннель и службу IKE:

```
(config-ike-conn-t1)# crypto ike enable
(config)# crypto ike enable conn t1
```

Выполняем симметричные настройки узла 2:

```
# crypto psk set key psk1 flash /psks/key1
# configure terminal
(config)# crypto psk map 192.168.2.1 192.168.1.1 psk1
(config)# crypto ike conn t1
(config-ike-conn-t1)# auth psk
(config-ike-conn-t1)# local ip 192.168.2.1
(config-ike-conn-t1)# remote ip 192.168.1.1
(config-ike-conn-t1)# crypto ike enable
(config)# crypto ike enable conn t1
```

Инициируем соединение с любого из узлов:

```
(config)# do crypto ike initiate conn t1
```

Настройка туннеля по протоколу IPSec (ГОСТ) Point-to-Point (аутентификация по сертификатам X.509)

Рассмотрим самый простой пример настройки соединения типа «точка-точка» со взаимной аутентификацией по сертификатам X.509. Допустим у нас есть два узла Dionis-NX с IP-адресами 192.168.1.1 и 192.168.2.1.

# crypto pki import key from keys/router1.nam	# crypto pki import key from keys/router2.nam
# crypto pki import root ca cert from certs/ca.cer	# crypto pki import root ca cert from certs/ca.cer
# crypto pki import cert from certs/router1.cer	# crypto pki import cert from certs/router2.cer
# configure terminal	# configure terminal
(config)# crypto ike enable	(config)# crypto ike enable
(config)# crypto ike conn t1	(config)# crypto ike conn t1
(config-ike-conn-t1)# auth pubkey	(config-ike-conn-t1)# auth pubkey
(config-ike-conn-t1)# local ip 192.168.1.1	(config-ike-conn-t1)# local ip 192.168.2.1
(config-ike-conn-t1)# remote ip 192.168.2.1	(config-ike-conn-t1)# remote ip 192.168.1.1
(config-ike-conn-t1)# local cert router1.cer	(config-ike-conn-t1)# local cert router2.cer
(config-ike-conn-t1)# do crypto pki import cert from certs/router2.cer	(config-ike-conn-t1)# do crypto pki import cert from certs/router1.cer
(config-ike-conn-t1)# remote id from cert router2.cer	(config-ike-conn-t1)# remote id from cert router1.cer
(config)# crypto ike enable conn t1	(config-ike-conn-t1)# crypto ike enable conn t1

Настройка узла 1:
Импортируем сертификат узла, сертификат удостоверяющего центра и закрытый ключ узла с внешнего носителя:

```
# crypto pki import key from keys/router1.nam
# crypto pki import root ca cert from certs/ca.cer
# crypto pki import cert from certs/router1.cer
```

Входим в режим конфигурации и запускаем службу IKE:

```
# configure terminal
(config)# crypto ike enable
```

Создаём настройку соединения. Назовём его «t1»:

```
(config)# crypto ike conn t1
(config-ike-conn-t1)#
```

Вид строки приглашения говорит о том, система находится в режиме редактирования настроек соединения «t1».

По умолчанию действует режим аутентификации по сертификатам X.509, что эквивалентно опции:

```
(config-ike-conn-t1)# auth pubkey
```

Задаём IP-адреса концов туннеля - локального и удалённого:

```
(config-ike-conn-t1)# local ip 192.168.1.1
(config-ike-conn-t1)# remote ip 192.168.2.1
```

Задаём имя используемого сертификата:

```
(config-ike-conn-t1)# local cert router1.cer
```

Задаём X500-имя сертификата нашего оппонента:

```
(config-ike-conn-t1)# remote id "CN=Узел 2, O=Хорошая организация, C=RU"
```

Можно импортировать X500-имя непосредственно из сертификата оппонента. Для этого необходимо предварительно загрузить сертификат оппонента в систему:

```
(config-ike-conn-t1)# do crypto pki import cert from certs/router2.cer
(config-ike-conn-t1)# remote id from cert router2.cer
```

Новые созданные соединения изначально находятся в выключенном состоянии. Чтобы наше соединение смогло стать активным, его необходимо включить:

```
(config)# crypto ike enable conn t1
```

Теперь соединение включено и находится в «слушающем» состоянии, то есть оно готово начать установление туннеля IPsec. Установление туннеля может быть инициировано данным узлом, либо может быть инициировано нашим оппонентом.

Теперь выполним настройку узла 2, которая, по сути, будет симметричной настройке узла 1:

```
# crypto pki import key from keys/router2.nam
# crypto pki import root ca cert from certs/ca.cer
# crypto pki import cert from certs/router2.cer
# configure terminal
(config)# crypto ike enable
(config)# crypto ike conn t1
(config-ike-conn-t1)# local ip 192.168.2.1
(config-ike-conn-t1)# remote ip 192.168.1.1
(config-ike-conn-t1)# local cert router2.cer
(config-ike-conn-t1)# remote id "CN=Узел 1, O=Хорошая организация, C=RU"
(config-ike-conn-t1)# crypto ike enable conn t1
```

Теперь весь трафик (типа «точка-точка») между узлами 1 и 2 будет инкапсулироваться в протокол ESP. Важно помнить, что если к узлу 1, например, подключены другие сети, то проходящий трафик через узел 1 к узлу 2 из этих сетей НЕ будет попадать в туннель и (если не настроены фильтры) будет идти в открытом виде. Данный трафик будет являться трафиком типа «подсеть-точка» и не будет попадать в туннель типа «точка-точка».

Настройка защищенного VPN-туннеля (ГОСТ) на уровне L2

Для создания защищенного канала связи в режиме шифрования/дешифрования в Dionis-NX должны быть предварительно созданы ключи доступа и загружены ключи шифрования абонентов Disec.
Это описано в разделе **«Инициализация криптографических компонентов в Dionis DPS»**

Пример организации L2 туннелей с шифрованием трафика между двумя криптомаршрутизаторами Dionis DPS

Рис.1

Настройка Dionis-NX1

Будем считать, что на устройствах была произведена инициализация криптографических компонентов. (для инициализации ключей disec – на usb устройстве должен быть только один ключ)

Предварительная настройка интерфейсов на устройстве DionisNX1:
(config)# interface ethernet 0
(config-if-ethernet0)# ip address 172.16.0.1/24
(config-if-ethernet0)# enable
(config-if-ethernet0)# interface ethernet 1
(config-if-ethernet1)# enable

Создание интерфейса ditap:
(config)# interface ditap 0
В качестве номера интерфейса (в примере – 0) может быть выбрано любое число (натуральное или 0).

Далее в режиме конфигурации интерфейса необходимо задать следующие параметры:
(config-if-ditap0)# id 1
id: целое число (до 5 цифр), идентифицирующее туннель; значение этого параметра должно совпадать на обоих концах туннеля.

(config-if-ditap0)# alg encrypt
alg: алгоритм трансформации данных в туннеле; возможные значения:

- *compression: только сжатие данных;*
- *encryption: только шифрование данных;*
- *both: и сжатие, и шифрование данных;*
- *none: никакой трансформации данных не производится.*

(config-if-ditap0)# serial 222 *Число меняется в зависимости от номера серии

serial: номер серии ключей - целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети.

(config-if-ditap0)# local-cn 1 *Число меняется в зависимости от номера ключа
local-cn: целое число (до 5 цифр), равное номеру данного узла в криптографической сети.

(config-if-ditap0)# remote-cn 2 *Число меняется в зависимости от номера ключа
remote-cn: целое число (до 5 цифр), равное номеру в криптографической сети того узла, с которым будет выполняться обмен информацией по данному туннелю.

(config-if-ditap0)# local 172.16.0.1
local: задает IP-адрес локального конца туннеля.

(config-if-ditap0)# remote 172.16.0.2
remote: задает IP-адрес удаленного конца туннеля.

(config-if-ditap0)# enable
Делает интерфейс активным.

Для реализации отбора трафика в интерфейс ditap необходимо объединить физический интерфейс ethernet и интерфейс ditap при помощи интерфейса bridge:
(config-if-ditap0)# interface bridge 0
(config-if-bridge0)# port ethernet 1
(config-if-bridge0)# port ditap 0
(config-if-bridge0)# enable

Далее необходимо произвести симметричные настройки на другом криптомаршрутизаторе.

Настройка Dionis-NX2

Предварительная настройка интерфейсов на устройстве DionisNX2
(config)# interface ethernet 0
(config-if-ethernet0)# ip address 172.16.0.2/24
(config-if-ethernet0)# enable
(config-if-ethernet0)# interface ethernet 1
(config-if-ethernet1)# enable
Создание и настройка туннельного L2 интерфейса ditap:
(config)# interface ditap 0
(config-if-ditap0)# id 1
(config-if-ditap0)# alg encrypt
(config-if-ditap0)# serial 222
(config-if-ditap0)# local-cn 2
(config-if-ditap0)# remote-cn 1
(config-if-ditap0)# local 172.16.0.2
(config-if-ditap0)# remote 172.16.0.1
(config-if-ditap0)# enable
Объединение физического и туннельного интерфейса:
(config-if-ditap0)# interface bridge 0
(config-if-bridge0)# port ethernet 1
(config-if-bridge0)# port ditap 0
(config-if-bridge0)# enable

Настройка защищенного VPN-туннеля (ГОСТ) на уровне L3

Для создания защищенного канала связи в режиме шифрования/дешифрования в Dionis-NX должны быть предварительно созданы ключи доступа и загружены ключи абонентов Disec. Это описано в разделе **«Инициализация криптографических компонентов в Dionis DPS»**

Пример организации L3 туннелей с шифрованием трафика между двумя криптомаршрутизаторами Dionis DPS

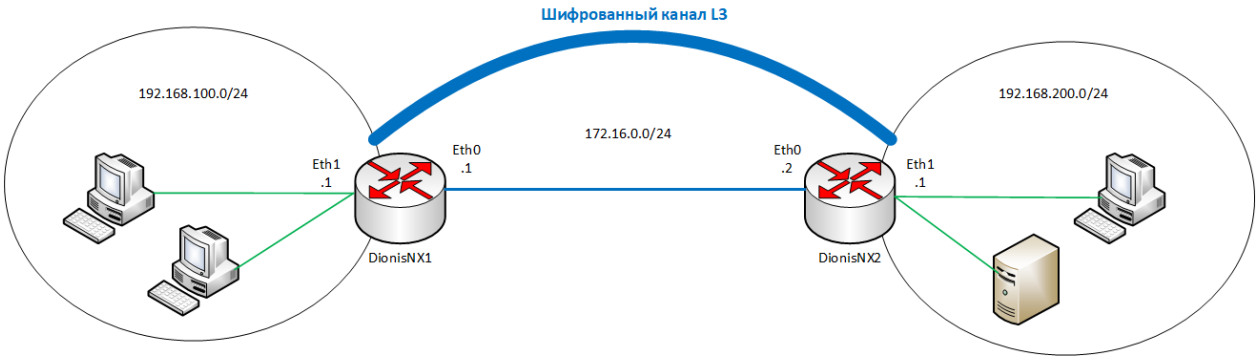


Рис.1

Будем считать, что на устройствах была произведена инициализация криптографических компонентов.

Настройка DionisNX1

Предварительная настройка интерфейсов на устройстве DionisNX1:
(config)# interface ethernet 0
(config-if-ethernet0)# ip address 172.16.0.1/24
(config-if-ethernet0)# enable
(config-if-ethernet0)# interface ethernet 1
(config-if-ethernet1)# ip address 192.168.100.1/24
(config-if-ethernet1)# enable

Создание интерфейса ditun:
(config)# interface ditun 0
В качестве номера интерфейса (в примере – 0) может быть выбрано любое число (натуральное или 0).

Далее в режиме конфигурации интерфейса необходимо задать следующие параметры:
(config-if-ditun0)# id 1
id: целое число (до 5 цифр), идентифицирующее туннель; значение этого параметра должно совпадать на обоих концах туннеля.

(config-if-ditun0)# alg encrypt
alg: алгоритм трансформации данных в туннеле; возможные значения:

- *compression: только сжатие данных;*
- *encryption: только шифрование данных;*
- *both: и сжатие, и шифрование данных;*
- *none: никакой трансформации данных не производится.*

(config-if-ditun0)# serial 222
serial: номер серии ключей - целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети.

(config-if-ditun0)# local-cn 1
local-cn: целое число (до 5 цифр), равное номеру данного узла в криптографической сети.

(config-if-ditun0)# remote-cn 1
remote-cn: целое число (до 5 цифр), равное номеру в криптографической сети того узла, с которым будет выполняться обмен информацией по данному туннелю.

(config-if-ditun0)# local 172.16.0.1
local: задает IP-адрес локального конца туннеля.

(config-if-ditun0)# remote 172.16.0.2
remote: задает IP-адрес удаленного конца туннеля.

(config-if-ditun0)# enable
Делает интерфейс активным.

Создание маршрута до удаленной внутренней сети:
(config)# ip route 192.168.200.0/24 ditun 0

Далее необходимо произвести симметричные настройки на другом криптомаршрутизаторе.

Настройка DionisNX2

Предварительная настройка интерфейсов на устройстве DionisNX2
(config)# interface ethernet 0
(config-if-ethernet0)# ip address 172.16.0.2/24
(config-if-ethernet0)# enable
(config-if-ethernet0)# interface ethernet 1
(config-if-ethernet1)# ip address 192.168.200.1/24
(config-if-ethernet1)# enable

Создание и настройка туннельного L3 интерфейса ditun и маршрута до удаленной сети:
(config)# interface ditun 0
(config-if-ditun0)# id 1
(config-if-ditun0)# alg encrypt
(config-if-ditun0)# serial 222
(config-if-ditun0)# local-cn 1
(config-if-ditun0)# remote-cn 1
(config-if-ditun0)# local 172.16.0.2
(config-if-ditun0)# remote 172.16.0.1
(config-if-ditun0)# enable
(config)# ip route 192.168.100.0/24 ditun 0

Настройка защищенного VPN-туннеля (ГОСТ) на уровне L2 (VLAN)

Для создания защищенного канала связи в режиме шифрования/дешифрования в Dionis-NX должны быть предварительно созданы ключи доступа и загружены ключи абонентов Disec. Это описано в разделе **«Инициализация криптографических компонентов в Dionis DPS»**

Пример организации L2 туннелей с шифрованием трафика между двумя криптомаршрутизаторами Dionis DPS

Рис.1

Настройка Dionis NX1

Будем считать, что на устройствах была произведена инициализация криптографических компонентов.

Предварительная настройка интерфейсов на устройстве Dionis NX1:
WAN интерфесй
(config)# interface ethernet 0
(config-if-ethernet0)# ip address 172.16.0.1/24
(config-if-ethernet0)# enable
VLAN интерфейс
(config-if-ethernet0)# interface ethernet 1
(config-if-ethernet1)# enable

(config-if-ethernet1)# interface ethernet 1.10
(config-if-ethernet1)# enable

Создание интерфейса ditap:
(config)# interface ditap 0
В качестве номера интерфейса (в примере – 0) может быть выбрано любое число (натуральное или 0).
Далее в режиме конфигурации интерфейса необходимо задать следующие параметры:
(config-if-ditap0)# id 1
id: целое число (до 5 цифр), идентифицирующее туннель; значение этого параметра должно совпадать на обоих концах туннеля.
(config-if-ditap0)# alg encrypt
alg: алгоритм трансформации данных в туннеле; возможные значения:

- *compression: только сжатие данных;*
- *encryption: только шифрование данных;*
- *both: и сжатие, и шифрование данных;*
- *none: никакой трансформации данных не производится.*

(config-if-ditap0)# serial 222
serial: номер серии ключей - целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети.

(config-if-ditap0)# local-cn 1
local-cn: целое число (до 5 цифр), равное номеру данного узла в криптографической сети.

(config-if-ditap0)# remote-cn 1
remote-cn: целое число (до 5 цифр), равное номеру в криптографической сети того узла, с которым будет выполняться обмен информацией по данному туннелю.

(config-if-ditap0)# local 172.16.0.1
local: задает IP-адрес локального конца туннеля.

(config-if-ditap0)# remote 172.16.0.2
remote: задает IP-адрес удаленного конца туннеля.

(config-if-ditap0)# enable
Делает интерфейс активным.
Для реализации отбора трафика в интерфейс ditap необходимо объединить физический интерфейс ethernet и интерфейс ditap при помощи интерфейса bridge:
(config-if-ditap0)# interface bridge 0
(config-if-bridge0)# port ethernet 1.10
(config-if-bridge0)# port ditap 0
(config-if-bridge0)# enable
Далее необходимо произвести симметричные настройки на другом криптомаршрутизаторе.

Настройка DionisNX2

Предварительная настройка интерфейсов на устройстве DionisNX2
(config)# interface ethernet 0
(config-if-ethernet0)# ip address 172.16.0.2/24
(config-if-ethernet0)# enable

(config-if-ethernet0)# interface ethernet 1
(config-if-ethernet1)# enable

(config-if-ethernet0)# interface ethernet 1.10
(config-if-ethernet1)# enable

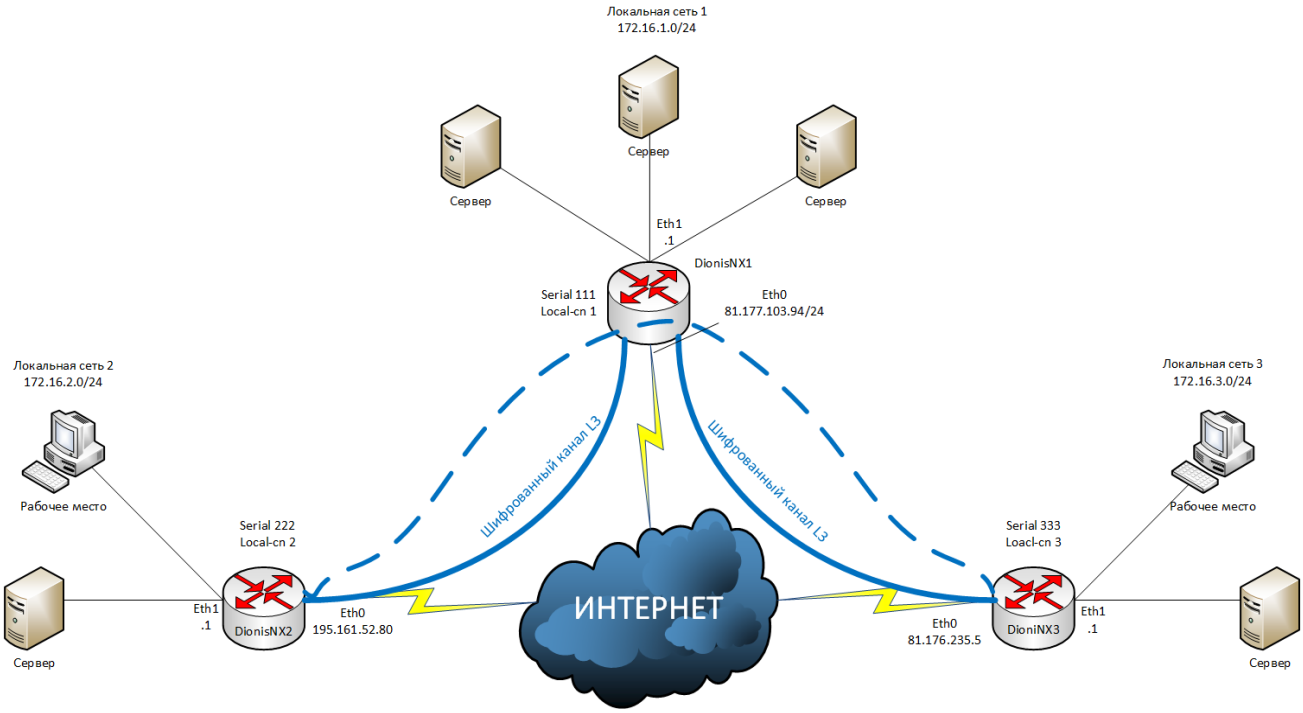
Создание и настройка туннельного L2 интерфейса ditap:
(config)# interface ditap 0
(config-if-ditap0)# id 1
(config-if-ditap0)# alg encrypt
(config-if-ditap0)# serial 222
(config-if-ditap0)# local-cn 1
(config-if-ditap0)# remote-cn 1
(config-if-ditap0)# local 172.16.0.2
(config-if-ditap0)# remote 172.16.0.1
(config-if-ditap0)# enable
Объединение физического и туннельного интерфейса:
(config-if-ditap0)# interface bridge 0
(config-if-bridge0)# port ethernet 1.10
(config-if-bridge0)# port ditap 0
(config-if-bridge0)# enable

Настройка защищенных VPN-туннелей (ГОСТ) на уровне L3 топология «звезда» (Туннели DiSec)

Для создания защищенных каналов связи в режиме шифрования/дешифрования в Dionis-NX должны быть предварительно созданы ключи доступа и загружены ключи абонентов Disec.

Это описано в разделе **«Инициализация криптографических компонентов в Dionis DPS»**

Пример организации L3 туннелей с шифрованием трафика между тремя криптомаршрутизаторами Dionis DPS топология «звезда»



Будем считать, что на устройствах была произведена инициализация криптографических компонентов и между ними есть IP связность.

Настройка DionisNX1

Предварительная настройка сетевых интерфейсов:

(config)# interface ethernet 0

(config-if-ethernet0)# ip address 81.177.103.94/24

(config-if-ethernet0)# enable

(config-if-ethernet0)# interface ethernet 1

(config-if-ethernet1)# ip address 172.16.1.1/24

(config-if-ethernet1)# enable

Создание канала связи с локальной сетью 2 (DionisNX2):

Создание туннельного интерфейса ditun:

(config)# interface ditun 0

В качестве номера интерфейса (в примере – 0) может быть выбрано любое число (натуральное или 0).

Далее в режиме конфигурации интерфейса необходимо задать следующие параметры:

(config-if-ditun0)# id 1

***id**: целое число (до 5 цифр), идентифицирующее туннель; значение этого параметра должно совпадать на обоих концах туннеля.*

(config-if-ditun0)# alg encrypt

***alg**: алгоритм трансформации данных в туннеле; возможные значения:*

***compression**: только сжатие данных;*

***encryption**: только шифрование данных;*

***both**: и сжатие, и шифрование данных;*

***none**: никакой трансформации данных не производится.*

(config-if-ditun0)# serial 111

***serial**: номер серии ключей - целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети.*

(config-if-ditun0)# local-cn 1

***local-cn**: целое число (до 5 цифр), равное номеру данного узла в криптографической сети.*

(config-if-ditun0)# remote-cn 2

***remote-cn**: целое число (до 5 цифр), равное номеру в криптографической сети того узла, с которым будет выполняться обмен информацией по данному туннелю.*

(config-if-ditun0)# local 81.177.103.94

***local**: задает IP-адрес локального конца туннеля.*

(config-if-ditun0)# remote 195.161.52.80

***remote**: задает IP-адрес удаленного конца туннеля.*

(config-if-ditun0)# enable

Делает интерфейс активным.

Создание маршрута до локальной сети 2:

(config-if-ditun0)# ip route 172.16.2.0/24 ditun 0

Создание канала связи с локальной сетью 3 (DionisNX3):

Создание туннельного интерфейса ditun:

(config)# interface ditun 1

В качестве номера интерфейса (в примере – 0) может быть выбрано любое число (натуральное или 0).

Далее в режиме конфигурации интерфейса необходимо задать следующие параметры:

(config-if-ditun0)# id 2

***id**: целое число (до 5 цифр), идентифицирующее туннель; значение этого параметра должно совпадать на обоих концах туннеля.*

(config-if-ditun0)# alg encrypt

***alg**: алгоритм трансформации данных в туннеле; возможные значения:*

***compression**: только сжатие данных;*

***encryption**: только шифрование данных;*

***both**: и сжатие, и шифрование данных;*

***none**: никакой трансформации данных не производится.*

(config-if-ditun0)# serial 111

***serial**: номер серии ключей - целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети.*

(config-if-ditun0)# local-cn 1

***local-cn**: целое число (до 5 цифр), равное номеру данного узла в криптографической сети.*

(config-if-ditun0)# remote-cn 3

***remote-cn**: целое число (до 5 цифр), равное номеру в криптографической сети того узла, с которым будет выполняться обмен информацией по данному туннелю.*

(config-if-ditun0)# local 81.177.103.94

***local**: задает IP-адрес локального конца туннеля.*

(config-if-ditun0)# remote 81.176.235.5

***remote**: задает IP-адрес удаленного конца туннеля.*

(config-if-ditun0)# enable

Делает интерфейс активным.

Создание маршрута до локальной сети 2:

(config-if-ditun0)# ip route 172.16.3.0/24 ditun 1

Настройка DionisNX2

Предварительная настройка сетевых интерфейсов:

(config)# interface ethernet 0

(config-if-ethernet0)# ip address 195.161.52.80/24

(config-if-ethernet0)# enable

(config-if-ethernet0)# interface ethernet 1

(config-if-ethernet1)# ip address 172.16.2.1/24

(config-if-ethernet1)# enable

Создание канала связи с локальной сетью 1 и 3 (DionisNX2):

Создание туннельного интерфейса ditun:

(config)# interface ditun 0

В качестве номера интерфейса (в примере – 0) может быть выбрано любое число (натуральное или 0).

Далее в режиме конфигурации интерфейса необходимо задать следующие параметры:

(config-if-ditun0)# id 1

***id**: целое число (до 5 цифр), идентифицирующее туннель; значение этого параметра должно совпадать на обоих концах туннеля.*

(config-if-ditun0)# alg encrypt

***alg**: алгоритм трансформации данных в туннеле; возможные значения:*

***compression**: только сжатие данных;*

***encryption**: только шифрование данных;*

***both**: и сжатие, и шифрование данных;*

***none**: никакой трансформации данных не производится.*

(config-if-ditun0)# serial 222

***serial**: номер серии ключей - целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети.*

(config-if-ditun0)# local-cn 2

***local-cn**: целое число (до 5 цифр), равное номеру данного узла в криптографической сети.*

(config-if-ditun0)# remote-cn 1

***remote-cn**: целое число (до 5 цифр), равное номеру в криптографической сети того узла, с которым будет выполняться обмен информацией по данному туннелю.*

(config-if-ditun0)# local 195.161.52.80

***local**: задает IP-адрес локального конца туннеля.*

(config-if-ditun0)# remote 81.177.103.94

***remote**: задает IP-адрес удаленного конца туннеля.*

(config-if-ditun0)# enable

Делает интерфейс активным.

Создание маршрута до локальных сетей 1 и 3:

(config-if-ditun0)# ip route 172.16.1.0/24 ditun 0

(config-if-ditun0)# ip route 172.16.3.0/24 ditun 0

Настройка DionisNX3

Предварительная настройка сетевых интерфейсов:

(config)# interface ethernet 0

(config-if-ethernet0)# ip address 81.176.235.5/24

(config-if-ethernet0)# enable

(config-if-ethernet0)# interface ethernet 1

(config-if-ethernet1)# ip address 172.16.3.1/24

(config-if-ethernet1)# enable

Создание канала связи с локальной сетью 1 и 2 (DionisNX2):

Создание туннельного интерфейса ditun:

(config)# interface ditun 0

В качестве номера интерфейса (в примере – 0) может быть выбрано любое число (натуральное или 0).

Далее в режиме конфигурации интерфейса необходимо задать следующие параметры:

(config-if-ditun0)# id 2

***id**: целое число (до 5 цифр), идентифицирующее туннель; значение этого параметра должно совпадать на обоих концах туннеля.*

(config-if-ditun0)# alg encrypt

***alg**: алгоритм трансформации данных в туннеле; возможные значения:*

***compression**: только сжатие данных;*

***encryption**: только шифрование данных;*

***both**: и сжатие, и шифрование данных;*

***none**: никакой трансформации данных не производится.*

(config-if-ditun0)# serial 333

***serial**: номер серии ключей - целое десятичное число, равное номеру серии ключей, используемой в данной криптографической сети.*

(config-if-ditun0)# local-cn 3

***local-cn**: целое число (до 5 цифр), равное номеру данного узла в криптографической сети.*

(config-if-ditun0)# remote-cn 1

***remote-cn**: целое число (до 5 цифр), равное номеру в криптографической сети того узла, с которым будет выполняться обмен информацией по данному туннелю.*

(config-if-ditun0)# local 81.176.235.5

***local**: задает IP-адрес локального конца туннеля.*

(config-if-ditun0)# remote 81.177.103.94

***remote**: задает IP-адрес удаленного конца туннеля.*

(config-if-ditun0)# enable

Делает интерфейс активным.

Создание маршрута до локальных сетей 1 и 2:

(config-if-ditun0)# ip route 172.16.1.0/24 ditun 0

(config-if-ditun0)# ip route 172.16.2.0/24 ditun 0

Таким образом, создаются два защищенных канала связи, причем устройства DionisNX2 и DionisNX3 напрямую друг с другом не связаны и передача данных между ними осуществляется через устройство Dionis NX1.

Настройка защищенных каналов связи по протоколу IpSec на уровне L3 (полносвязная схема)

Для создания защищенных каналов связи в режиме шифрования/дешифрования в Dionis-NX должны быть предварительно созданы ключи доступа и загружены ключи абонентов Disec.

Это описано в разделе **«Инициализация криптографических компонентов в Dionis DPS»**

Пример организации L3 туннелей с шифрованием трафика IPSec с ассиметричными ключами шифрования

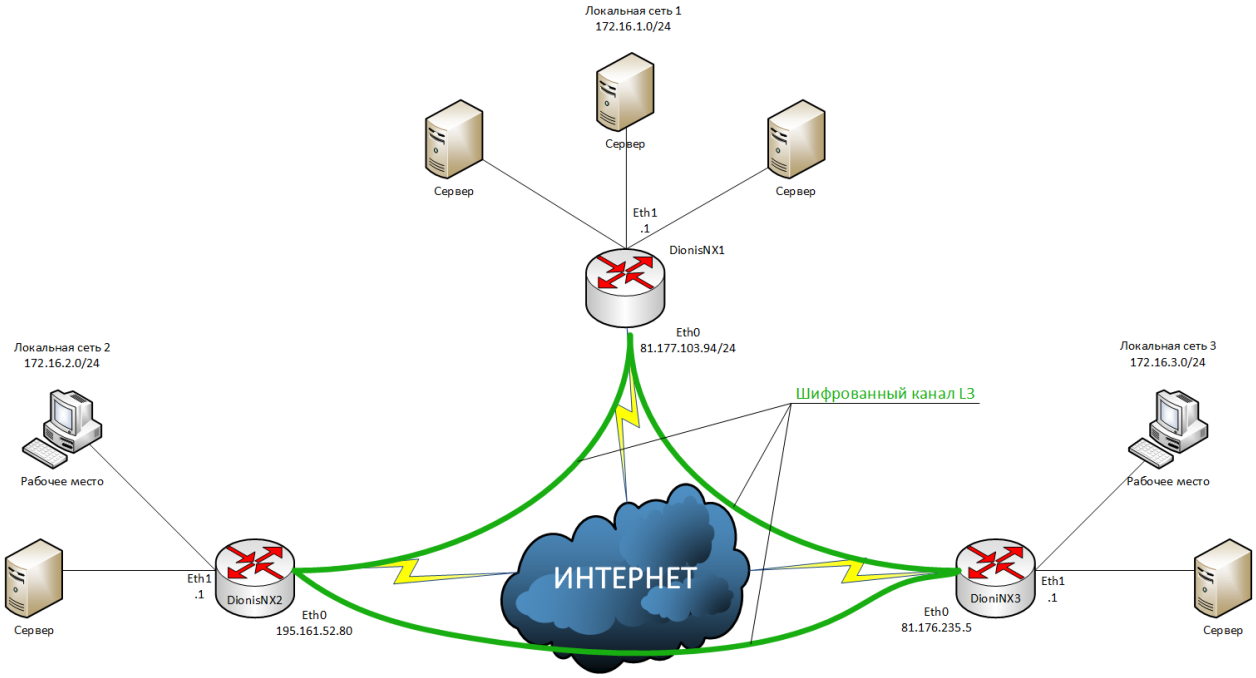


Рис.1

Будем считать, что на устройствах была произведена инициализация криптографических компонентов и между ними есть IP связность.

Настройка DionisNX1

Предварительная настройка сетевых интерфейсов:

(config)# interface ethernet 0

(config-if-ethernet0)# ip address 81.177.103.94/24

(config-if-ethernet0)# enable

(config-if-ethernet0)# interface ethernet 1

(config-if-ethernet1)# ip address 172.16.1.1/24

(config-if-ethernet1)# enable

Для работы каналов связи с ассиметричными ключами шифрования необходимо импортировать в систему закрытый ключ, сертификат узла и корневой сертификат.

Предположим, что ключ и сертификаты доставлены на внешнем флэш накопителе и находятся в его корне.

/key1.nam - закрытый ключ

/root.cer – корневой сертификат

/dionisnx1.cer – сертификат узла dionisnx1

/dionisnx2.cer – сертификат узла dionisnx2

/dionisnx3.cer – сертификат узла dionisnx3

Импорт закрытого ключа в систему:

 # crypto pki import key flash from key1.nam

Ключи могут быть в формате Фактор-ТС, вида key1.nam, либо доставляться в контейнере PKCS#15.

Импорт корневого сертификата:

 # crypto pki import root ca cert flash from root.cer

Импорт сертификата узла:

 # crypto pki import cert flash from dionisnx1.cer

Так же необходимо импортировать сертификаты узлов, с которыми будут строиться туннели:

 # crypto pki import cert flash from dionisnx2.cer

 # crypto pki import cert flash from dionisnx3.cer

Создание канала связи с локальной сетью 2 (DionisNX2):

Запуск службы IKE:

(config)# crypto ike enable

Создание соединения:

(config)# crypto ike conn tunnel-to-dionisnx2

“tunnel-to-dionisnx2” – произвольное имя соединения

Команда для автоматической инициации туннеля:

(config-ike-tunnel-to-dionisnx2)# auto route

Задание IP-адреса концов туннеля (локального и удаленного):

(config-ike-tunnel-to-dionisnx2)# local ip 81.177.103.94

(config-ike-tunnel-to-dionisnx2)# remote ip 195.161.52.80

Задание подсетей (локальной и удаленной):

(config-ike-tunnel-to-dionisnx2)# local subnet 172.16.1.0/24

(config-ike-tunnel-to-dionisnx2)# remote subnet 172.16.2.0/24

Задание используемого сертификата:

(config-ike-tunnel-to-dionisnx2)# local cert dionisnx1.cer

Импорт X500-имени из сертификата удаленного узла DionisNX2:

(config-ike-tunnel-to-dionisnx2)# remote id from cert dionisnx2.cer

Запуск созданного соединения:

(config)# crypto ike enable conn tunnel-to-dionisnx2

Создание канала связи с локальной сетью 3 (Dionis-NX3):

Запуск службы IKE:

(config)# crypto ike enable

Создание соединения:

(config)# crypto ike conn tunnel-to-dionisnx3

“tunnel-to-dionisnx3” – произвольное имя соединения

Команда для автоматической инициации туннеля:

(config-ike-tunnel-to-dionisnx3)# auto route

Задание IP-адреса концов туннеля (локального и удаленного):

(config-ike-tunnel-to-dionisnx3)# local ip 81.177.103.94

(config-ike-tunnel-to-dionisnx3)# remote ip 81.176.235.5

Задание подсетей (локальной и удаленной):

(config-ike-tunnel-to-dionisnx3)# local subnet 172.16.1.0/24

(config-ike-tunnel-to-dionisnx3)# remote subnet 172.16.3.0/24

Задание используемого сертификата:

(config-ike-tunnel-to-dionisnx3)# local cert dionisnx1.cer

Импорт X500-имени из сертификата удаленного узла DionisNX3:

(config-ike-tunnel-to-dionisnx3)# remote id from cert dionisnx3.cer

Запуск созданного соединения:

(config)# crypto ike enable conn tunnel-to-dionisnx3

Настройка DionisNX2

Предварительная настройка сетевых интерфейсов:

(config)# interface ethernet 0

(config-if-ethernet0)# ip address 195.161.52.80/24

(config-if-ethernet0)# enable

(config-if-ethernet0)# interface ethernet 1

(config-if-ethernet1)# ip address 172.16.2.1/24

(config-if-ethernet1)# enable

Для работы каналов связи с ассиметричными ключами шифрования необходимо импортировать в систему закрытый ключ, сертификат узла и корневой сертификат.

Предположим, что ключ и сертификаты доставлены на внешнем флэш накопителе и находятся в его корне.

/key2.nam - закрытый ключ

/root.cer – корневой сертификат

/dionisnx1.cer – сертификат узла dionisnx1

/dionisnx2.cer – сертификат узла dionisnx2

/dionisnx3.cer – сертификат узла dionisnx3

Импорт закрытого ключа в систему:

 # crypto pki import key flash from key2.nam

Ключи могут быть в формате Фактор-ТС, вида key2.nam, либо доставляться в контейнере PKCS#15.

Импорт корневого сертификата:

 # crypto pki import root ca cert flash from root.cer

Импорт сертификата узла:

 # crypto pki import cert flash from dionisnx2.cer

Так же необходимо импортировать сертификаты узлов, с которыми будут строиться туннели:

 # crypto pki import cert flash from dionisnx1.cer

 # crypto pki import cert flash from dionisnx3.cer

Создание канала связи с локальной сетью 1 (DionisNX1):

Запуск службы IKE:

(config)# crypto ike enable

Создание соединения:

(config)# crypto ike conn tunnel-to-dionisnx1

“tunnel-to-dionisnx1” – произвольное имя соединения

Команда для автоматической инициации туннеля:

(config-ike-tunnel-to-dionisnx1)# auto route

Задание IP-адреса концов туннеля (локального и удаленного):

(config-ike-tunnel-to-dionisnx1)# local ip 195.161.52.80

(config-ike-tunnel-to-dionisnx1)# remote ip 81.177.103.94

Задание подсетей (локальной и удаленной):

(config-ike-tunnel-to-dionisnx1)# local subnet 172.16.2.0/24

(config-ike-tunnel-to-dionisnx1)# remote subnet 172.16.1.0/24

Задание используемого сертификата:

(config-ike-tunnel-to-dionisnx1)# local cert dionisnx2.cer

Импорт X500-имени из сертификата удаленного узла DionisNX1:

(config-ike-tunnel-to-dionisnx1)# remote id from cert dionisnx1.cer

Запуск созданного соединения:

(config)# crypto ike enable conn tunnel-to-dionisnx1

Создание канала связи с локальной сетью 3 (DionisNX3):

Запуск службы IKE:

(config)# crypto ike enable

Создание соединения:

(config)# crypto ike conn tunnel-to-dionisnx3

“tunnel-to-dionisnx3” – произвольное имя соединения

Команда для автоматической инициации туннеля:

(config-ike-tunnel-to-dionisnx3)# auto route

Задание IP-адреса концов туннеля (локального и удаленного):

(config-ike-tunnel-to-dionisnx3)# local ip 195.161.52.80

(config-ike-tunnel-to-dionisnx3)# remote ip 81.176.235.5

Задание подсетей (локальной и удаленной):

(config-ike-tunnel-to-dionisnx3)# local subnet 172.16.2.0/24

(config-ike-tunnel-to-dionisnx3)# remote subnet 172.16.3.0/24

Задание используемого сертификата:

(config-ike-tunnel-to-dionisnx3)# local cert dionisnx2.cer

Импорт X500-имени из сертификата удаленного узла DionisNX3:

(config-ike-tunnel-to-dionisnx3)# remote id from cert dionisnx3.cer

Запуск созданного соединения:

(config)# crypto ike enable conn tunnel-to-dionisnx3

Настройка DionisNX3

Предварительная настройка сетевых интерфейсов:

(config)# interface ethernet 0

(config-if-ethernet0)# ip address 81.176.235.5/24

(config-if-ethernet0)# enable

(config-if-ethernet0)# interface ethernet 1

(config-if-ethernet1)# ip address 172.16.3.1/24

(config-if-ethernet1)# enable

Для работы каналов связи с ассиметричными ключами шифрования необходимо импортировать в систему закрытый ключ, сертификат узла и корневой сертификат.

Предположим, что ключ и сертификаты доставлены на внешнем флэш накопителе и находятся в его корне.

/key3.nam - закрытый ключ

/root.cer – корневой сертификат

/dionisnx1.cer – сертификат узла dionisnx1

/dionisnx2.cer – сертификат узла dionisnx2

/dionisnx3.cer – сертификат узла dionisnx3

Импорт закрытого ключа в систему:

 # crypto pki import key flash from key3.nam

Ключи могут быть в формате Фактор-ТС, вида key3.nam, либо доставляться в контейнере PKCS#15.

Импорт корневого сертификата:

 # crypto pki import root ca cert flash from root.cer

Импорт сертификата узла:

 # crypto pki import cert flash from dionisnx3.cer

Так же необходимо импортировать сертификаты узлов, с которыми будут строиться туннели:

 # crypto pki import cert flash from dionisnx1.cer

 # crypto pki import cert flash from dionisnx2.cer

Создание канала связи с локальной сетью 1 (DionisNX1):

Запуск службы IKE:

(config)# crypto ike enable

Создание соединения:

(config)# crypto ike conn tunnel-to-dionisnx1

“tunnel-to-dionisnx1” – произвольное имя соединения

Команда для автоматической инициации туннеля:

(config-ike-tunnel-to-dionisnx1)# auto route

Задание IP-адреса концов туннеля (локального и удаленного):

(config-ike-tunnel-to-dionisnx1)# local ip 81.176.235.5

(config-ike-tunnel-to-dionisnx1)# remote ip 81.177.103.94

Задание подсетей (локальной и удаленной):

(config-ike-tunnel-to-dionisnx1)# local subnet 172.16.3.0/24

(config-ike-tunnel-to-dionisnx1)# remote subnet 172.16.1.0/24

Задание используемого сертификата:

(config-ike-tunnel-to-dionisnx1)# local cert dionisnx3.cer

Импорт X500-имени из сертификата удаленного узла DionisNX1:

(config-ike-tunnel-to-dionisnx1)# remote id from cert dionisnx1.cer

Запуск созданного соединения:

(config)# crypto ike enable conn tunnel-to-dionisnx1

Создание канала связи с локальной сетью 2 (DionisNX2):

Запуск службы IKE:

(config)# crypto ike enable

Создание соединения:

(config)# crypto ike conn tunnel-to-dionisnx2

“tunnel-to-dionisnx2” – произвольное имя соединения

Команда для автоматической инициации туннеля:

(config-ike-tunnel-to-dionisnx2)# auto route

Задание IP-адреса концов туннеля (локального и удаленного):

(config-ike-tunnel-to-dionisnx2)# local ip 81.176.235.5

(config-ike-tunnel-to-dionisnx2)# remote ip 195.161.52.80

Задание подсетей (локальной и удаленной):

(config-ike-tunnel-to-dionisnx2)# local subnet 172.16.3.0/24

(config-ike-tunnel-to-dionisnx2)# remote subnet 172.16.2.0/24

Задание используемого сертификата:

(config-ike-tunnel-to-dionisnx2)# local cert dionisnx3.cer

Импорт X500-имени из сертификата удаленного узла DionisNX2:

(config-ike-tunnel-to-dionisnx2)# remote id from cert dionisnx2.cer

Запуск созданного соединения:

(config)# crypto ike enable conn tunnel-to-dionisnx2