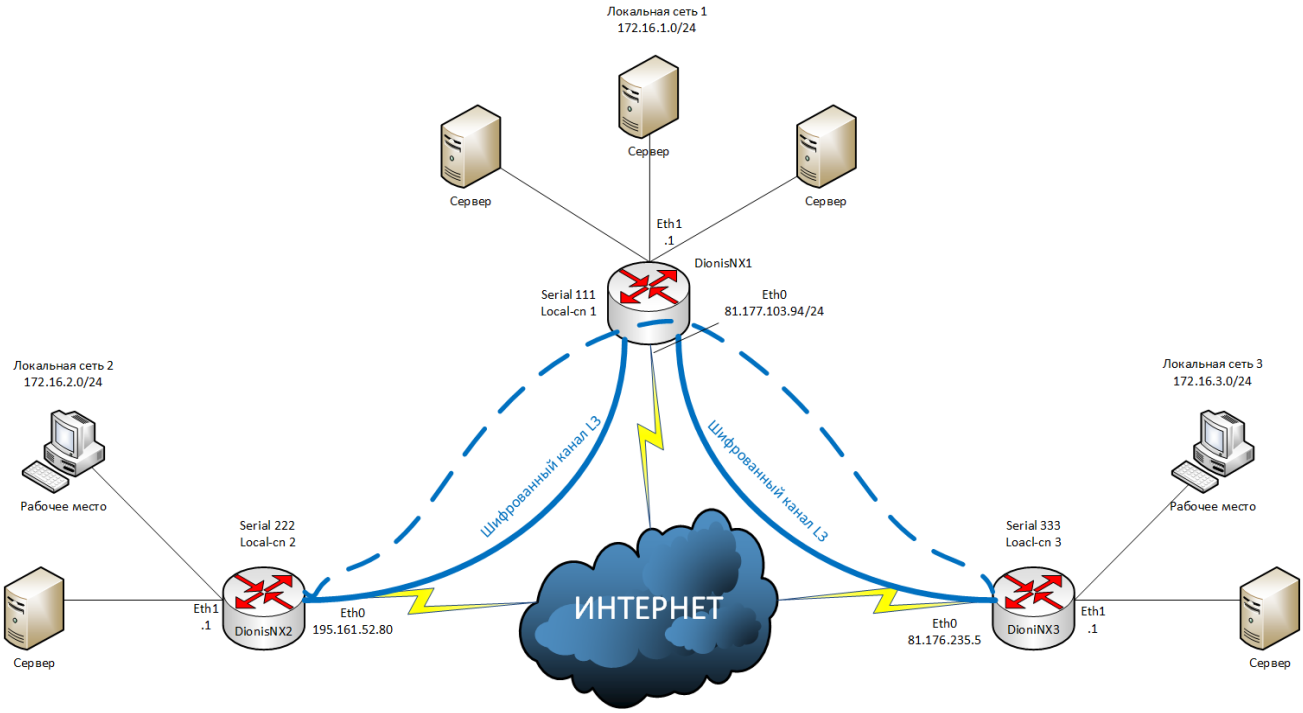
Настройка защищенных VPN-туннелей (ГОСТ) на уровне L3 топология «звезда» (Туннели DiSec)

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.