Настройка защищенного канала связи (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

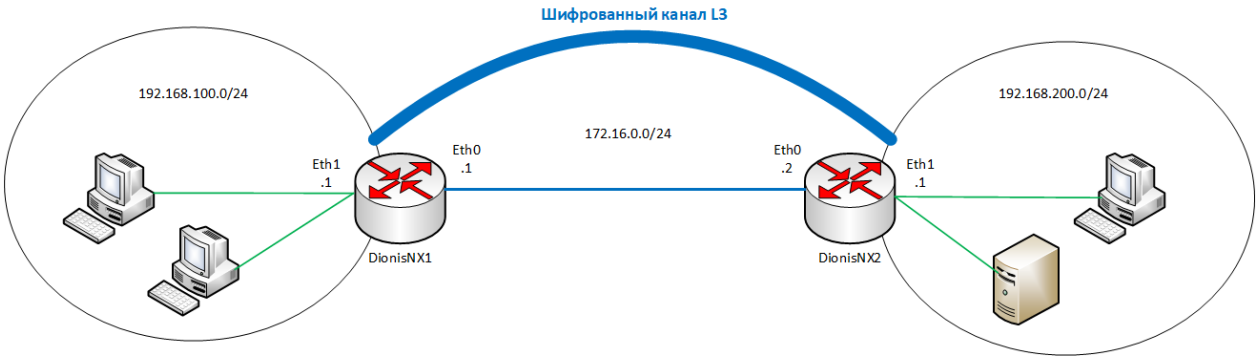

Рис.1

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

Настройка DionisNX1

Создание mangle-list на устройстве DionisNX1:
(config)# ip mangle-list mss
(config-mangle-mss)# mangle adjust-mss 1400 tcp
Рекомендуется В ip mangle-list создать правило установки MSS, чтобы избежать проблемы фрагментации пакетов из-за увеличенного MTU в туннельных интерфейсах. Необходимо привязать этот список к физическим и виртуальным интерфейсам.
Предварительная настройка интерфейсов на устройстве DionisNX1:
(config)# interface ethernet 0
(config-if-ethernet0)# ip address 172.16.0.1/24
(config-if-ethernet0)# ip mangle-group mss in
(config-if-ethernet0)# ip mangle-group mss out
Привязка ip mangle-list для исходящего и входящего трафика
(config-if-ethernet0)# enable
(config-if-ethernet0)# interface ethernet 1
(config-if-ethernet1)# ip address 192.168.100.1/24
(config-if-ethernet1)# ip mangle-group mss in
(config-if-ethernet1)# ip mangle-group mss out
(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)# ip mangle-group mss in
(config-if-ditun0)# ip mangle-group mss out
(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)# ip mangle-group mss in
(config-if-ethernet0)# ip mangle-group mss out
(config-if-ethernet0)# enable
(config-if-ethernet0)# interface ethernet 1
(config-if-ethernet1)# ip address 192.168.200.1/24
(config-if-ethernet1)# ip mangle-group mss in
(config-if-ethernet1)# ip mangle-group mss out
(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)# ip mangle-group mss in
(config-if-ditun0)# ip mangle-group mss out
(config-if-ditun0)# enable
(config)# ip route 192.168.100.0/24 ditun 0