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

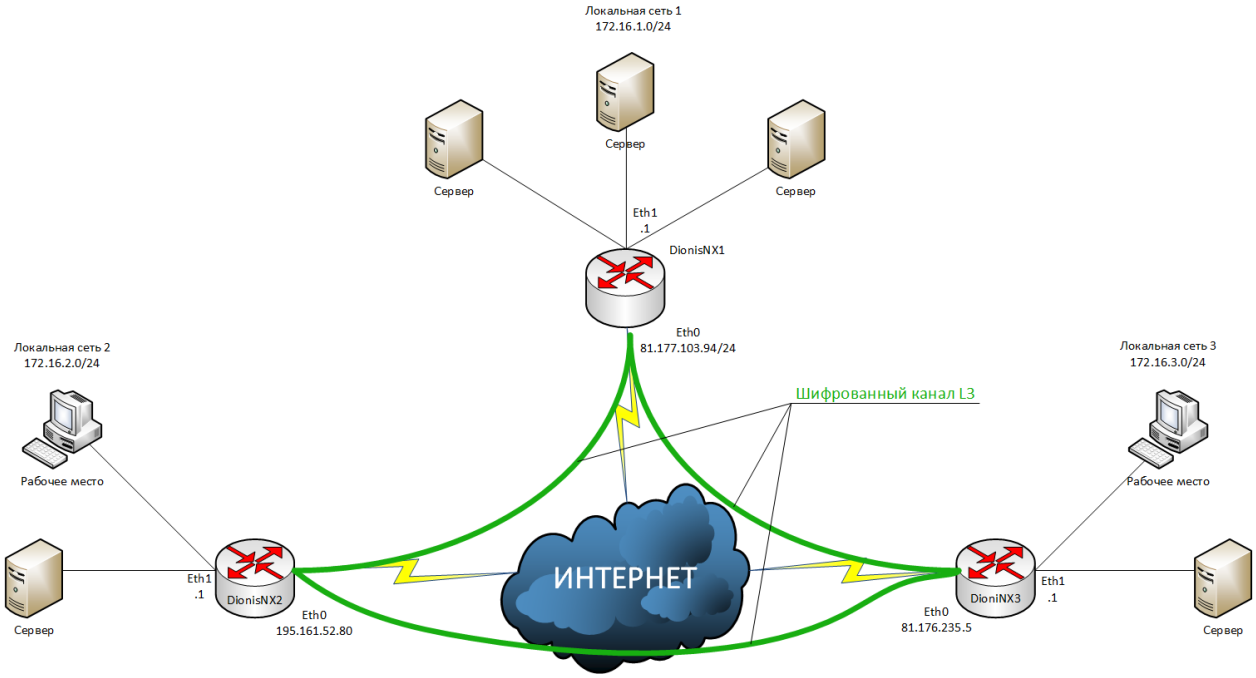

Рис.1

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