Руководство пользователя

Маршрутизатор Dionis-NXe

Москва, 2018

Оглавление

1. Цель документа

Данное Руководство пользователя содержит инструкции по установке и обслуживанию маршрутизатора Dionis-NXe.

2. Аудитория

Данное руководство предназначено для сетевых администраторов, которые выполняют следующие функции:

- Установка и настройка маршрутизации;
- Установка и настройка межсетевого экранирования;
- Установка и настройка VPN.

3. Назначение

Маршрутизатор Dionis-NXe представляет собой специализированное устройство, предназначенное для маршрутизации потоков данных (на сетевом уровне модели OSI) между сегментами корпоративной сети и/или глобальной сетью передачи данных Internet с обеспечением заданного уровня защиты информационных систем пользователя от сетевых угроз. Маршрутизатор состоит из аппаратной платформы и управляющей операционной системы(ОС) Dionis-NX 2.0.

ОС Dionis-NXe реализует следующие функции:

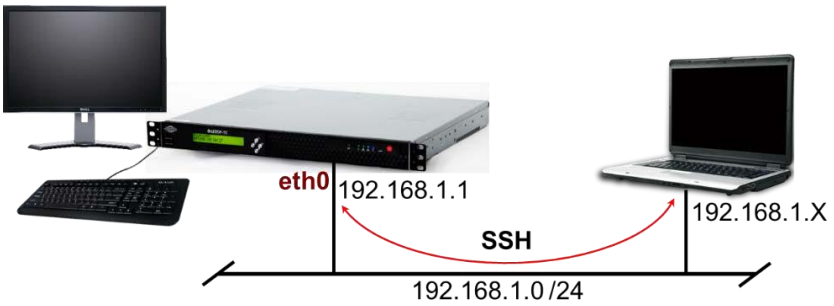
- Маршрутизатор;
- Межсетевой экран;
- Концентратор VPN (включает систему криптографии).

4. Подключение к консольному терминалу

Управление работой Dionis-NXe осуществляется с автоматизированного рабочего места (АРМ) администратора, представляющего собой персональный компьютер (ПК) с установленным программным обеспечением: эмулятор терминала или SSH-клиент, - в зависимости от способа подключения к Dionis-NXe.

Подключение к маршрутизатору Dionis-NXe для настройки и управления его работой возможно одним из следующих способов:

- Локальное подключение;
- Удалённое подключение.



4.1. Локальное подключение

На АРМ администратора должна быть предварительно установлена программа эмуляции терминала со следующими настройками:

- Скорость обмена данными – 9600bps;
- 8 бит данных без контроля четности;
- 1 стоповый бит;
- Аппаратное управление потоком данных.

Подключение АРМ администратора к Dionis-NXe выполняется консольным кабелем через USB порт.

Для подключения АРМ администратора к Dionis-NXe необходимо выполнить следующие действия:

Шаг 1	Подключить один конец кабеля к RS-232-порту АРМ администратора
Шаг 2	Подключить другой конец кабеля к порту с маркировкой «*Console*» на Dionis-NXe
Шаг 3	Включить Dionis-NXe нажатием кнопки «Пуск»

4.2. Удаленное подключение

Для организации удаленного подключения АРМ администратора к Dionis-NXe используется протокол SSH.

На АРМ администратора должно быть предварительно установлена программа SSH-Клиента (ОС Windows или Linux).

На АРМ администратора должен быть установлен IP-адрес сетевого адаптера в диапазоне 192.168.1.2-192.168.1.254 с маской сети 255.255.255.0.

Для первого удаленного подключения на заводе изготовителе на Dionis-NXe включен сервис SSH для учетной записи администратора «*cli*» и активирован интерфейс *Ethernet 0* с IP-адресом *192.168.1.1/24.*

Удалённое подключение АРМ администратора к Dionis-NXe выполняется Ethernet кабелем.

Для первого удаленного подключения АРМ администратора к Dionis-NXe необходимо выполнить следующие действия:

Шаг 1	Подключить один конец кабеля к *Ethernet* порту сетевого адаптера АРМ администратора
Шаг 2	Подключить другой конец кабеля к порту *Ethernet 0* на Dionis-NXe
Шаг 3	Включить Dionis-NXe нажатием кнопки «Пуск»
Шаг 4	Ввести имя учетной записи «cli» и пароль «cli»

5. Управление Dionis-NXe

5.1. Интерфейс управления

В качестве основного средства управления Dionis-NXe используется интерфейс командной строки. После ввода имени и пароля учетной записи пользователь может вводить с клавиатуры команды, с помощью которых осуществляется управление маршрутизатором и настройка его функций.

Команды вводятся в ответ на приглашение системы:

```
DionisNXe# _
```

где DionisNXe – имя маршрутизатора.

Команды Dionis-NXe в общем случае состоят из двух частей: имя и параметры команды. Параметры отделяются от имени команды и друг от друга пробелами.

При вводе и редактировании команд могут используются следующие клавиши:

- <Tab> или <Ctrl^I> - для автоматического дополнения имени команды или параметра (при однозначном варианте сразу выполняется дополнение; если возникает возможность выбора, выводится список вариантов);
- <?> - для вывода на экран списка команд или параметров, доступных в настоящий момент; список выводится вместе с краткой справкой по этим командам/параметрам;
- <стрелка вверх> - для вывода на экран предыдущих команд (для просмотра или повторного ввода);
- <Shift+PgUp/PgDn> - для постраничного просмотра содержимого экрана.
- <Ctrl^Z> - выход на уровень выше в дереве вложенных настроек (режим конфигурации). Соответствует выполнению команды «exit»;
- <Ctrl^Space> - просмотр конфигурации текущего уровня настроек (режим конфигурации). Соответствует выполнению команды «show»;
- <Ctrl^C> - отмена ввода и переход на новую строку;
- <Home> или <Ctrl^A> - переход в начало строки;
- <End> или <Ctrl^E> - переход в конец строки;
- <Del> или <Ctrl^D> - удаление текущего символа;
- <Backspace> или <Ctrl^H> - удаление предыдущего символа;
- <Ctrl^L> - очистка экрана;
- <Ctrl^J> или <Ctrl^M> - ввод. Соответствует нажатию клавиши <Enter>;
- <Ctrl^W> - удаление слова;
- <Ctrl^K> - удаление всей строки справа от курсора и копирование удаленной части в буфер;
- <Ctrl^U> - удаление всей строки слева от курсора и копирование удаленной части в буфер;
- <Ctrl^Y> - вставка из буфера.

Для завершения ввода команды используется клавиша <Enter>.

5.2. Учетные записи пользователей

Подключение к Dionis-NXe выполняется по имени и паролю учетной записи пользователя. В соответствии с заводскими установками при первом включении на Dionis-NXe присутствуют две учетные записи:

Имя	Пароль	Описание
cli	cli	оператор (непривилегированный пользователь)
adm	adm	администратор (привилегированный пользователь)

Для входа в систему пользователь должен ввести имя учетной записи и затем пароль учетной записи.

При первом входе в систему пользователю будет предложено сменить заводские пароли (cli и adm) на пароли, которые будут использоваться в дальнейшем.

Смена пароля производится только администратором с помощью команд:
Смена пароля оператора:

```
# passwd cli
```

Смена пароля администратора:

```
# passwd adm
```

При смене пароля необходимо сначала ввести старый пароль, а затем дважды ввести новый пароль. Пароль может содержать любые символы латинского алфавита и цифры. Длина пароля должна быть не меньше 8 символов.

При входе в систему под учетной записью оператора (cli) система предоставляет доступ к командам непривилегированного режима user - часть информационных команд, позволяющих просмотреть основную информацию об оборудовании, дисковом пространстве и версии установленного ПО и выполнить ряд действий по диагностике сетевого окружения. О работе в этом режиме будет свидетельствовать знак «>» после имени маршрутизатора:

```
DionisNXe> _
```

Для перехода в привилегированный режим необходимо ввести команду «enable» и пароль администратора (adm).

В привилегированном режиме пользователю предоставляется доступ к командам управления, не меняющим конфигурацию системы. Признаком работы в привилегированном режиме служит знак «#» после имени маршрутизатора:

```
DionisNXe# _
```

Настройка функций маршрутизатора Dionis-NXe выполняется в режиме конфигурирования. Переход в режим конфигурирования выполняется по команде «configure terminal» из привилегированного режима. Признаком работы в режиме конфигурирования служит запись «(config)» после имени маршрутизатора:

```
DionisNXe(config)# _
```

5.3. Конфигурация Dionis-NXe

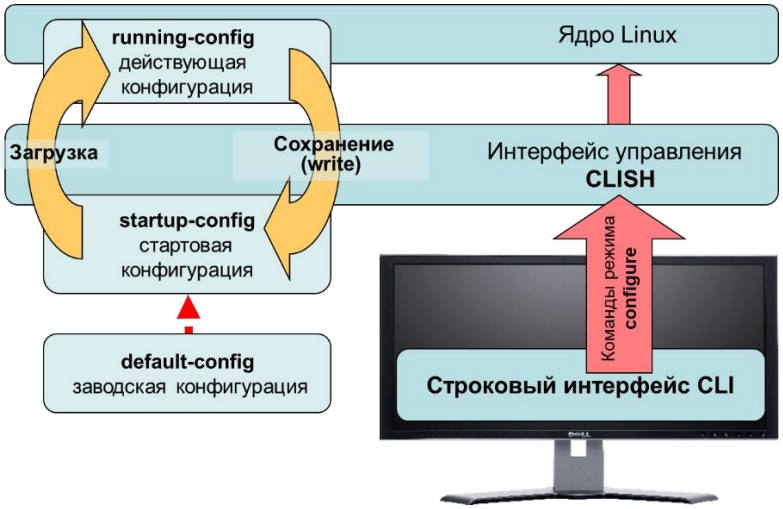
Определённая конфигурация Dionis-NXe создаётся последовательностью команд, определяющих настройку параметров маршрутизатора Dionis-NXe.

В Dionis-NXe существуют три конфигурации:

– **Действующая конфигурация (running-config)** определяет действующие в данный момент настройки маршрутизатора. Хранится в оперативной памяти маршрутизатора;

- **Стартовая конфигурация (startup-config)** загружается при включении/перезагрузке маршрутизатора. Хранится в постоянной энергонезависимой памяти Dionis-NXe;

- **Заводская конфигурация (default-config)** предназначена для создания действующей конфигурации при первоначальном включении и загрузке маршрутизатора. Хранится в постоянной энергонезависимой памяти Dionis-NXe и определяет заводские настройки Dionis-NXe, содержащие минимальный набор команд, необходимый для загрузки ОС маршрутизатора. Данная конфигурация доступна только для чтения и не может быть изменена.



Для сохранения действующей конфигурации при перезагрузке Dionis-NXe используется команда «copy running-config startup-config» или команда «write».

Для просмотра любой конфигурации используется команда «show» с наименованием конфигурации:

```
DionisNXe # show running-config

DionisNXe # show startup-config

DionisNXe # show default-config
```

5.4. Выключение и перезагрузка

Выключение Dionis-NXe выполняется из привилегированного режима командой «poweroff»:

```
DionisNXe # poweroff
```

Dionis-NXe

Перезагрузка Dionis-NXe выполняется из привилегированного режима командой «reboot»:

```
DionisNXe # reboot
```

6. Маршрутизация

В Dionis-NXe реализованы функции маршрутизатора, обеспечивающие передачу пакетов данных между сегментами корпоративной сети и/или глобальной сетью Internet в соответствии с заданной таблицей маршрутизации. Включение функции маршрутизации в Dionis-NXe выполняется в режиме конфигурации по команде «ip forwarding»:

```
(config)# ip forwarding
```

Данная команда присутствует в файле конфигурации по умолчанию (default-config).

6.1. Настройка Ethernet интерфейсов

Для настройки выбранного Ethernet интерфейса необходимо в режиме конфигурирования ввести команду входа в режим настройки интерфейса. Например, здесь и далее для интерфейса ethernet 0:

```
DionisNXe(config)# interface ethernet 0
```

Следующие команды выполняют минимально необходимую настройку интерфейса (активация и назначение IP адреса/маски подсети):

```
DionisNXe(config-if-ethernet0)# enable
DionisNXe(config-if-ethernet0)# ip address xxx.xxx.xxx.xxx/xx
```

Для автоматического назначения IP-адреса интерфейсу по протоколу DHCP необходимо ввести команду:

```
 DionisNXe(config-if-ethernet0)# ip address dhcp iponly
```

Для удаления назначенного интерфейсу IP-адреса необходимо ввести команду с префиксом «no»:

```
DionisNXe(config-if-ethernet0)# no ip address xxx.xxx.xxx.xxx/xx
```

Для переключения интерфейса в неактивное состояние (без потери настроек) необходимо выполнить команду «disable»:

```
DionisNXe(config-if-ethernet0)# disable
```

Для переключения интерфейса в неактивное состояние и удаления всех настроек необходимо выполнить команду:

```
DionisNXe(config)# no interface ethernet 0
```

Для просмотра текущей конфигурации интерфейса необходимо ввести команду «show» в режиме конфигурирования:

```
DionisNXe(config-if-ethernet0)# do show
enable
ip address xxx.xxx.xxx.xxx/xx
```

или в привилегированном режиме:

```
DionisNXe # show interface ethernet 0
enable
ip address xxx.xxx.xxx.xxx/xx
```

Для перехода в режим верхнего уровня (из режима конфигурирования в привилегированный режим, из привилегированного режима в непривилегированный режим) необходимо выполнить команду «exit» или одновременно нажать на клавиатуре АРМ администратора клавиши <Ctrl^Z>:

```
DionisNXe(config-if-ethernet0)# exit

DionisNXe(config)# _
```

Чтобы посмотреть конфигурацию всех интерфейсов Dionis-NXe в режиме конфигурирования необходимо ввести команду:

```
DionisNXe(config)# do show interface config

!
interface ethernet 0
 enable
 ip address xxx.xxx.xxx.xxx/xx
!
interface ethernet 1
 enable
 ip address xxx.xxx.xxx.xxx/xx
!
interface ethernet 2
 enable
 ip address xxx.xxx.xxx.xxx/xx
```

6.2. Типы маршрутизации

В Dionis-NXe используются два типа маршрутизации:

- Статическая маршрутизация;
- Динамическая маршрутизация.

6.3. Статическая маршрутизация

При статической маршрутизации администратор прописывает в таблице маршрутизации Dionis-NXe пути всех связанных с Dionis-NXe маршрутизаторов.

Для добавления статического маршрута в таблицу маршрутизации Dionis-NXe необходимо в режиме конфигурации ввести команду «ip route …».

6.3.1. Настройка маршрута по умолчанию:

```
DionisNXe(config)# ip route default xxx.xxx.xxx.xxx
```

где xxx.xxx.xxx.xxx – IP-адрес шлюза (например, адрес интерфейса маршрутизатора провайдера).

По данной команде все входящие и исходящие пакеты, не адресованные данному маршрутизатору и не попадающие под другие правила маршрутизации направляются на маршрутизатор с IP-адресом XXX.XXX.XXX.XXX.

6.3.2. Настройка маршрута в сеть через шлюз:

```
DionisNXe(config)# ip route xxx.xxx.xxx.xxx/xx yyy.yyy.yyy.yyy
```

По данной команде маршрутизатор направляет все входящие и исходящие пакеты адресованные сети xxx.xxx.xxx.xxx/xx, на маршрутизатор с IP-адресом yyy.yyy.yyy.yyy.

6.3.3. Настройка маршрута в сеть через интерфейс:

```
DionisNXe(config)# ip route xxx.xxx.xxx.xxx/xx ethernet 1
```

Данная команда указывает маршрутизатору, что маршрут в сеть xxx.xxx.xxx.xxx/xx проходит через интерфейс ethernet 1, и все пакеты, адресованные в данную сеть, будут направлены на данный интерфейс. (Если неизвестен MAC-адрес для IP-адреса назначения, то будет выполнен ARP-запрос через указанный интерфейс).

Если задано несколько маршрутов, пересекающихся по адресам назначения, то приоритетным будет более точный маршрут (с большей маской), а менее приоритетным - общий маршрут (с меньшей маской). Маршрут по умолчанию (0.0.0.0/0) имеет наименьший приоритет.

6.3.4. Удаление статического маршрута

Удаление статического маршрута выполняется командой «no ip route …»:

```
DionisNXe(config)# no ip route default <IP-адрес>
```

6.3.5. Просмотр таблицы маршрутизации

Просмотр таблицы маршрутизации выполняется по команде «show ip route» из привилегированного режима:

```
DionisNXe# show ip route
```

```
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, A - Babel,
       > - selected route, * - FIB route

C>*   100.100.100.0/24   is   directly   connected,
ethernet0   C>*   111.111.111.0/24   is   directly
connected,  ethernet1  C>*  127.0.0.0/8  is  directly
connected, lo
S>* 0.0.0.0/0 [1/0] via 100.100.100.10, ethernet0
```

6.4. Динамическая маршрутизация

В Dionis-NXe реализованы следующие протоколы динамической маршрутизации:

- RIP (протокол маршрутизации информации);
- OSPF (протокол динамической маршрутизации внутри автономной системы);
- BGP (протокол граничного шлюза).

6.4.1. Протокол маршрутизации RIP

В Dionis-NXe реализован протокол RIP Version 2.

RIP - дистанционно-векторный протокол. Маршрутизатор Dionis-NXe присваивает маршрутам метрики (дистанции), по сумме которых выбирается наилучший путь. Маршрут и метрика составляют вектор, который передается соседнему RIP-маршрутизатору.

Протокол RIP использует UDP (порт 520) в качестве транспорта для анонсируемых маршрутов. Пакеты UDP инкапсулируются в мультикаст-датаграммы (IP-адрес: 224.0.0.9).

Настройка протокола RIP:

Шаг 1	DionisNXe(config)# router rip	Войти в режим конфигурирования протокола RIP
Шаг 2	DionisNXe (config-rip)# network <ip/m>|<iface>	Выполнить подключение клиентской сети к маршрутизатору (ip/m – IP-адрес клиентской сети, iface – интерфейс клиентской сети)
Шаг 3	DionisNXe (config-rip)#exit	Выйти из режима конфигурирования протокола RIP

6.4.2. Протокол маршрутизации OSPF

Протокол OSPF основан на технологии отслеживания состояния канала (link-state technology) и использует для нахождения кратчайшего пути алгоритм Дейкстры.

Настройка протокола OSPF

Шаг 1	DionisNXe(config)# router ospf	Войти в режим конфигурирования протокола OSPF
Шаг 2	DionisNXe (config-ospf)# network <iface_ip>/<mask> area <area_id>	Выполнить подключение клиентской сети к маршрутизатору (iface_ip – IP-адрес клиентской сети,

		mask – маска сети, area_id –область к которой подключен интерфейс)
Шаг 3	DionisNXe (config-ospf)#exit	Выйти из режима конфигурирования протокола RIP

6.4.3. Протокол маршрутизации BGP

Протокол BGP предназначен для обмена сообщениями о достижимости подсетей между автономными системами (AS), то есть группами маршрутизаторов под единым техническим и административным управлением, использующими протокол внутридоменной маршрутизации (iBGP) для определения маршрутов внутри автономной системы и протокол междоменной маршрутизации (eBGP) для определения маршрутов доставки пакетов в другие автономные системы.

BGP поддерживает бесклассовую адресацию и использует суммирование маршрутов для уменьшения таблиц маршрутизации.

В Dionis-NXe реализована четвертая версия протокола BGP (BGP-4).

Настройка протокола BGP

Шаг 1	DionisNXe(config)# router bgp <AS>	Войти в режим конфигурирования протокола BGP (AS – номер автономной системы, в которую входит Dionis-NXe
Шаг 2	DionisNXe (config-bgp-<AS>)# address-family ipv4|ipv6 unicast|multicast	Выполнить выбор семейства IP-адресов
Шаг3	DionisNXe (config-bgp-<AS>)neighbor <ip>|<group> remote-as <AS>	Прописать соседние AS (ip –адрес соседнего маршрутизатора, group- имя группы BGP-маршрутизаторов, AS – номер AS в которую входит соседний BGP-маршрутизатор или группа
Шаг 4	DionisNXe (config-bgp-<AS>))#exit	Выйти из режима конфигурирования протокола BGP

7. Межсетевое экранирование

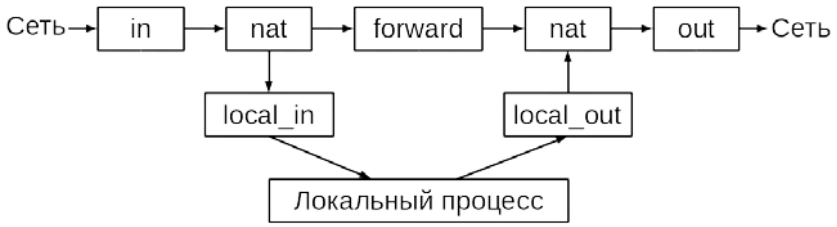
Dionis-NXe, работая в режиме межсетевого экрана, осуществляет контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами или фильтрами.

Наиболее распространённое место для установки межсетевых экранов — граница периметра локальной сети для защиты внутренних хостов от атак из сети Интернет. Однако атаки могут начинаться и с внутренних узлов — в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечёт границу сетевого периметра, и межсетевой экран не будет задействован. Поэтому в настоящее время межсетевые экраны размещают не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности.

7.1. Подсистема фильтрации

Подсистема фильтрации является базовым средством обеспечения безопасности сети и позволяет управлять прохождением трафика через интерфейсы маршрутизатора, разрешая или запрещая передачу пакетов, удовлетворяющих указанным правилам отбора. Правила отбора объединяются в IP-списки контроля доступа (ip access-list). Списки контроля доступа могут быть применены к конкретным интерфейсам (с учетом направления трафика), а также к маршрутизатору в целом (с учетом логики маршрутизации).

Ниже приведена упрощенная схема движения пакета через фильтры Dionis-NXe:



Фильтрация

Название	Назначение
in	Входной фильтр интерфейса
nat	преобразование SNAT или DNAT
local_in	Внутренний фильтр для пакетов, направленных в систему
forward	Фильтр маршрутизации транзитных пакетов
local_out	Внутренний фильтр для сгенерированных в данной системе пакетов
out	Выходной фильтр интерфейса

7.1.1. Создание списка контроля доступа

Для создания списка контроля доступа, в режиме configure необходимо выполнить команду ip access-list <acl_name>, где <acl_name> – это имя создаваемого списка, например:

```
DionisNXe(config)# ip access-list mylist
```

После выполнения команды, задаются (или модифицируются) правила фильтрации этого списка. Каждое правило содержит критерии отбора трафика и может быть разрешающим (permit) или запрещающим (deny). Все правила в списке выполняются последовательно, до первого совпадения критериям отбора. Если ни одно из правил не удовлетворяет критериям, считается, что выполняется разрешающее правило. Например:

```
DionisNXe(config-acl-mylist)# permit icmp

DionisNXe(config-acl-mylist)# permit tcp

DionisNXe(config-acl-mylist)# permit udp

DionisNXe(config-acl-mylist)# deny
```

В данном примере, разрешается прохождение пакетов трех протоколов (icmp/udp/tcp), а все остальные протоколы запрещаются.

7.1.2. Назначение списка контроля доступа

После создания необходимо назначить список контроля доступа соответствующему интерфейсу Dionis-NXe. Один и тот же список может быть привязан к нескольким интерфейсам.

Для назначения списка контроля доступа необходимо выполнить команду «ip access-group <имя списка> <направление>» в режиме конфигурации, где

<направление> - направление трафика относительно интерфейса. Входящий трафик обозначается как in, а выходящий как out. Например:

```
DionisNXe(config)# interface ethernet 0
DionisNXe(config-if-ethernet0)# ip access-group mylist in
DionisNXe(config-if-ethernet0)# ip access-group mylist out
```

7.1.3. Правила фильтрации

В данном разделе приведены примеры с очень простыми правилами фильтрации (отбора), в которых в качестве критерия отбора использовался протокол датаграммы. Списки контроля доступа могут содержать правила с комбинацией различных критериев отбора, которые объединяются в логическое «и», что делает фильтры простым и мощным инструментом по обеспечению безопасности в сети передачи данных.

Полный список критериев отбора находится в документе «Полный список команд Dionis-NXe».

8. Концентратор VPN

Dionis-NXe позволяет использовать его в качестве шлюза VPN при создании локальных – на базе одного или нескольких сегментов локальной сети, корпоративных (intranet VPN), объединяющих нескольких территориально удаленных друг от друга локальных сетей организации или же межкорпоративных (extranet VPN), связывающих защищенными каналами ЛВС нескольких организаций.

Основными средствами реализации данных функций являются подсистемы OpenVPN и DiSEC.

8.1. Подсистема OpenVPN

В Dionis-NXe реализована поддержка виртуальной частной сети по технологии OpenVPN. Это позволяет использовать данное устройство в качестве сервера – OpenVPN при создании собственных VPN сетевого уровня (L3), создавая криптографически защищенные каналы типа сервер-клиенты с компьютерами локальной сети и компьютерами абонентов, находящимися вне ее, или для организации взаимодействия с другими VPN, использующих технологию OpenVPN, для создания зашифрованных каналов типа точка-точка между аналогичными VPN-шлюзами. Достоинством такого подхода является использование международных стандартов криптографической защиты и возможность сопряжения создаваемой VPN с другими VPN, использующие данные стандарты.

Настройка OpenVPN в системе Dionis-NXe заключается в предварительном вводе (импортировании) необходимых для работы ключей и сертификатов, а также в создании и

конфигурировании динамических серверных SVPN-интерфейсов и клиентских VPN-интерфейсов.

8.1.1. Предварительное импортирование ключей и сертификатов

Подсистема OpenVPN в Dionis-NXe способна работать в следующих режимах:

- в режиме симметричного шифрования с pre-shared ключом защиты (PSK);
- в режиме несимметричного шифрования, основанном на инфраструктуре открытых ключей (Public Key Infrastructure - PKI) с TLS-аутентификацией.

⚠ **ВНИМАНИЕ:** Подсистема OpenVPN в Dionis-NXe не имеет механизма генерации ключей и сертификатов. Для использования ее функций необходимо использовать ключи и сертификаты, сгенерированные на АРМ с установленным на него программным обеспечением OpenVPN.

В зависимости от планируемого режима работы необходимо предварительно любым доверенным способом доставить и импортировать соответствующие ключи и сертификаты.

8.1.1.1. Подготовка к работе в режиме с pre-shared ключом защиты

При подготовке к работе в режиме симметричного шифрования с pre-shared ключом защиты необходимо импортировать:

- *psk.key* – pre-shared ключ защиты, предназначенный для симметричного шифрования при обмене защищаемой информацией.

Для этого используются команды привилегированного режима «vpn import <тип объекта> <путь к файлу>». Например:

```
DionisNXe# vpn import psk USB0:/crt/ca.crt
```

8.1.1.2. Подготовка к работе в режиме с TLS-аутентификацией

При подготовке к работе в режиме с TLS-аутентификацией необходимо импортировать:

- *ca.crt* – корневой сертификат, удостоверяющий подлинность открытого ключа, подписанный доверенным удостоверяющим центром (Certification authority, CA);
- *server.crt* или *cli.crt* – сертификат сервера или клиента (открытый ключ узла, с которым предстоит организовать защищенное соединение);
- *server.key* или *cli.key* – ключ сертификата сервера или клиента (приватный ключ – секрет, на котором будет организовано шифрование потока);

⚠ **ВНИМАНИИЕ:** Имена ключей и сертификатов «*server*» и «*cli*» здесь и далее приведены в качестве примеров. Их наименования задает оператор при генерации.

- *ta.key* – ключ для аутентификации пакетов (tls-auth ключ) обеспечивающий проверку подлинности информации, передаваемой между сторонами с целью дополнительной защиты от DoS-атак;
- *dh1024.pem* – ключ Диффи-Хеллмана, используемый для защищенного обмена данными с помощью алгоритмов симметричного шифрования. Используется при

работе изделия в качестве сервера OpenVPN, чтобы в случае похищения ключей исключить расшифрование трафика, записанного еще до этого похищения.

Для импорта ключей и сертификатов используется команда привилегированного режима. Например:

```
DionisNXe# vpn import ca USB0:/crt/ca.crt

DionisNXe# vpn import cert USB0:/crt/cli.crt

DionisNXe# vpn import cert-key USB0:/key/server.key

DionisNXe# vpn import tls-key USB0:/key/ta.key

DionisNXe# vpn import dh-key USB0:/key/dh1024.pem
```

Для удаления импортированного ключа или сертификата vpn используется команда привилегированного режима «vpn clear <тип объекта> <Импортированный объект> .

```
DionisNXe# vpn clear ca ca.crt
```

Для просмотра списка импортированных ключей или сертификатов vpn используется команда привилегированного режима «vpn show <тип объекта>».

```
DionisNXe# vpn show ca
```

8.1.2. VPN-интерфейс

8.1.2.1. Назначение и режимы работы

VPN-интерфейс настраивается на Dionis-NXe, выступающем в качестве клиента OpenVPN при клиент серверном соединении или же при организации соединений точка-точка между равноправными узлами. Его настройки включают в себя обязательные параметры, входящие в так называемый connection-блок, параметры, используемые в зависимости от используемого режима преобразования в туннеле, и дополнительные параметры.

VPN-интерфейс может работать в следующих режимах:

- Простой туннель без защиты;
- Туннель с pre-shared ключом защиты; или
- Туннель с TLS-аутентификацией;
- Работа в режиме клиента OpenVPN для подключения к мультиклиент-серверу OpenVPN.

8.1.2.2. Создание и настройка

Для создания VPN-интерфейса используется команда режима конфигурации «interface vpn <номер>».

```
DionisNXe(config)# interface vpn 1
DionisNXe(config-if-vpn1)#
```

Настройка интерфейса VPN выполняется в два этапа:

- Настройка connection-блока (настройка параметров соединения);
- Настройка дополнительных параметров.

8.1.2.3. Настройка connection-блока.

Для интерфейса VPN доступно несколько профилей подключения (connection-блоков). Интерфейс поочередно выполняет попытки установить соединение с удаленным концом из каждого блока.

Для начала настройки connection-блока необходимо выполнить команду «connection <Имя>»:

```
DionisNXe(config-if-vpn1)# connection block1
DionisNXe(config-if-vpn1-block1)
```

Команды доступные для настройки connection-блоков

команда	параметр
lport <Номер порта>	Номер порта на локальном конце туннеля. По умолчанию 1194 (Необязательный параметр)
rport <Номер порта>	Номер порта на удаленном конце туннеля. По умолчанию 1194 (Необязательный параметр)
port <Номер порта>	Номер порта на локальном и удаленном конце туннеля. По умолчанию 1194 (Необязательный параметр)
local <ip или имя хоста>	Локальный ip или имя хоста (Необязательный параметр)
proto <Протокол>	Протокол работы интерфейса. По умолчанию udp. Должен совпадать с протоколом на удаленном конце туннеля
bind	Команда связывает локальный адрес и порт
remote <ip или имя хоста>	Удаленный ip или имя хоста, к которому будет происходить подключение (Обязательный параметр)

Примечание: В connection-блоке может быть несколько команд «remote». Для удаления конкретного remote необходимо выполнить команду <no remote N>, а для удаления всех remote - команду <no remote all>:

```
DionisNXe(config-if-conn)# no remote 1
DionisNXe(config-if-conn)
```

8.1.2.4. Настройка дополнительных параметров

Дополнительные команды для настройки VPN-интерфейса:

команда	параметр
tls-client	Включить TLS и быть клиентом во время handshake. Эта команда подразумевает обязательный ввод команд <ca>, <cert>, <key>
ca <Корневой сертификат>	Предварительно импортированный корневой сертификат. ca-файл должен быть такой же как на сервере
cert <Сертификат клиента>	Предварительно импортированный сертификат клиента
key <Ключ клиента>	Предварительно импортированный ключ сертификата клиента
tls-auth <Дополнительный ключ>	Предварительно импортированный tls-auth ключ. Данная команда добавляет дополнительный слой аутентификации. tls-auth-файл должен быть такой же как на сервере (Необязательный параметр. Используется совместно с <tls-client>)
secret <Pre-shared ключ>	Предварительно импортированный pre-shared ключ в режиме работы туннеля с pre-shared ключом защиты. Файл ключа должен быть одинаковым на обоих концах туннеля
ifconfig <l_IP:r_IP>	Приватный адрес локального и удаленного конца туннеля. (Обязательная команда для всех режимов работы интерфейса кроме режима клиента openvpn. В данном режиме команда не используется)
cipher <Алгоритм>	Алгоритм шифрования.
auth <Алгоритм>	Алгоритм Аутентификации.
ping <Интервал в секундах>	ping удаленного конца туннеля, если нет передачи пакетов в течение промежутка времени, большего чем указанный интервал
ping-restart <Интервал в секундах>	Перезагрузка подключения к удаленному концу туннеля, если от него не приходило пакетов в течение промежутка времени, большего чем указанный интервал
pull	Обязательная команда при работе интерфейса в режиме клиента openvpn
ns-cert-type <nsCertType>	Требовать <nsCertType> в поле nsCertType сертификата соседа

команда	параметр
tls-cipher <Alg>	Алгоритм tls-шифра. Используется для повышения уровня безопасности контроля канала управления (TLS used only as a control channel).

8.1.3. SVPN-интерфейс

8.1.3.1. Назначение и режимы работы

Режимы работы интерфейса SVPN:

- Сервер для туннеля с TLS-аутентификацией,
- Мульти-клиент-сервер.

8.1.3.2. Создание и настройка

Для создания SVPN-интерфейса используется команда: interface svpn <номер> из режима configure. При этом номер интерфейса может начинаться с 0.

```
DionisNXe(config)# interface svpn 0
DionisNXe(config-if-svpn0)#
```

Команды для настройки svpn-интерфейса

команда	параметр
proto <Протокол>	Протокол работы интерфейса. По умолчанию udp. Должен совпадать с протоколом на удаленном конце туннеля
port <Номер порта>	Номер порта. По умолчанию 1194
local <ip или имя хоста>	Локальный IP-адрес или имя хоста (Необязательный параметр)
bind	Команда связывает локальный адрес и порт
server <ip сети:маска сети>	IP-адрес и маска создаваемой частной сети. (Только для режима работы Мульти-клиент-сервер)
remote <ip или имя хоста>	Удаленный ip или имя хоста, к которому будет происходить подключение (Режим сервера с TLS-аутентификацией)
ca <Корневой сертификат>	Предварительно импортированный корневой сертификат
cert <Сертификат сервера>	Предварительно импортированный сертификат сервера
key <Ключ сервера>	Предварительно импортированный ключ сертификата сервера

команда	параметр
dh <Ключ Диффи-Хеллмана>	Предварительно импортированный ключ Диффи-Хеллмана
tls-auth <Дополнительный ключ>	Предварительно импортированный tls-auth-ключ. Данная команда добавляет дополнительный слой аутентификации. tls-auth-файл должен быть такой же, как на клиенте (Необязательный параметр)
ifconfig <l_IP:r_IP>	Приватный адрес локального и удаленного конца туннеля. (Используется только для режима сервера в туннеле с TLS-аутентификацией)
cipher <Алгоритм>	Алгоритм шифрования.
auth <Алгоритм>	Алгоритм Аутентификации.
ping <Интервал в секундах>	ping удаленного конца, если нет передачи пакетов в течение промежутка времени, большего чем указанный интервал
ping-restart <Интервал в секундах>	Перезагрузка подключения к удаленному концу туннеля, если от него не приходило пакетов в течение промежутка времени, большего чем указанный интервал
push ping <Интервал в секундах>	Установка значения ping для подключаемых клиентов
push ping-restart <Интервал в секундах>	Установка значения ping-restart для подключаемых клиентов
push route <ip сети:маска сети>	Передача клиенту маршрутов, чтобы позволить ему связаться с другими частными подсетями
ns-cert-type <nsCertType>	Требовать <nsCertType> в поле nsCertType сертификата соседа
tls-cipher <Alg>	Алгоритм tls-шифра. Используется для повышения уровня безопасности контроля канала управления (TLS used only as a control channel).
client-to-client	Команда позволяет подключенным клиентам видеть друг друга
duplicate-cn	Команда позволяет подключаться нескольким клиентам с одинаковым common name в поле сертификата
client-net <Common Name>	Добавление подсети клиента с Common Name в поле сертификата

Пример команды:

```
DionisNXe(config-if-svpn0)# server 10.8.0.0:255.255.255.0
```

Данная команда определяет, что интерфейсу svpn0 будет назначен адрес 10.8.0.1, а подключаемым клиентам адреса с 10.8.0.4 по 10.8.0.251

Полный список параметров интерфейса VPN находится в документе «Полный список команд Dionis-NXe».

8.2. Подсистема DiSEC

Dionis-NXe поддерживает собственный протокол DiSEC, позволяющий создавать VPN на 3 и 2 уровнях (L3 и L2) модели OSI и использующий шифрование и имитозащиту пакетов по алгоритмам ГОСТ, для защиты информации передаваемой между узлами. Достоинством данного протокола является возможность создавать VPN с большей криптографической защищенностью и не доступные для других пользователей сети.

Настройка подсистемы DiSEC заключается в предварительном вводе (импортировании) необходимых для работы ключей, а также в создании и конфигурировании сетевых туннельных интерфейсов DiTUN или туннельных Ethernet интерфейсов DiTAP.

8.2.1. Ключ доступа

Протокол DiSEC, реализованный в Dionis-NXe, использует ключи шифрования, которые хранятся в зашифрованном виде в памяти изделия с использованием ключа доступа.

Поэтому для начала работы с криптографическими средствами необходимо инициализировать датчик случайных чисел (ДСЧ), а также создать ключ доступа (КД).

Начальное заполнение ДСЧ доставляется на внешнем носителе в формате random.ini - формат хранения симметричных ключей Dionis-NXe (необходимы файлы gk.db3, uz.db3, random.ini).

Ключ доступа используется для защиты шифрованием хранящихся на внутреннем носителе секретов системы:

- начального заполнения ДСЧ для следующей перезагрузки;
- узла замены для симметричных ключей DiSec;
- симметричных ключей DiSec.

После генерации ключ доступа должен быть сохранён на внешнем носителе. Данный носитель потребуется при «холодном» перезапуске системы (с выключением питания). В случае «тёплого» перезапуска (reboot) носитель с КД не потребуется, потому что КД также сохраняется в оперативной памяти Dionis-NXe.

Для работы с КД действуют следующие правила:

- Один ключ доступа может относиться только к одному узлу;
- Один узел может одновременно иметь только один ключ доступа;
- Ключ доступа после генерации или замены может быть сохранён только один раз и на одном носителе;
- На одном носителе может быть только один ключ доступа.

8.2.1.1. Генерация нового КД при инициализации ДСЧ

Инициализация криптосистемы предполагает создание ключа доступа, его сохранение на внешнем носителе и установку загрузки ключа с этого носителя.

Для генерации нового КД необходимо:

- вставить внешний носитель с начальным заполнением ДСЧ;
- перейти в привилегированный режим;
- проверить наличие на внешнем носителе файлов, содержащие начальное заполнение ДСЧ:

```
DionisNXe # show crypto access key random-inis flash
```

Данная команда выведет доступные контейнеры в корневой директории флэш-накопителя:

```
HOST/
KM_K/
random.ini        old-dionis
```

Для просмотра содержимого поддиректорий, при наличии на носителе нескольких контейнеров располагающихся в разных поддиректориях, необходимо указать полный путь к контейнеру:

```
DionisNXe # show crypto access key random-inis flash HOST/KM_K/
```

Для генерации КД необходимо ввести команду:

```
DionisNXe # crypto access key init
```

По данной команде выполняется поиск первого внешнего носителя и попытка чтения контейнера random.ini/gk.db3 (также необходим файл uz.db3). При наличии нескольких контейнеров необходимо выполнить команду с точным указанием пути и имени файла контейнера:

```
DionisNXe # crypto access key init flash HOST/KM_K/random.ini
```

Для плановой замены КД следует использовать команду «crypto access key replace».

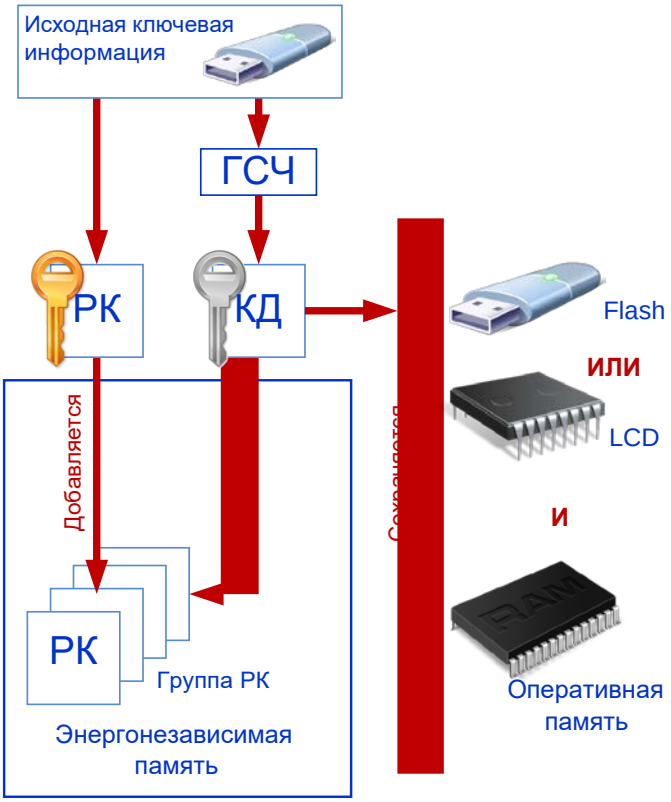
Кроме этого, в целях безопасности будет обновлено начальное заполнение ДСЧ на внешнем носителе.

8.2.1.2. Сохранение и проверка состояния КД

После успешного завершения процесса генерации ключ доступа находится в состоянии «not stored», и его необходимо сохранить на внешнем носителе. Для хранения КД используется специально выделенный для этих целей носитель.

Для сохранения КД на внешнем носителе необходимо **извлечь** носитель с начальным заполнением ДСЧ, вставить носитель для хранения ключа доступа и выполните команду:

```
DionisNXe # crypto access key store flash
```



Ключ доступа необходимо защитить паролем. При сохранении КД будет предложено ввести этот пароль.

Для определения текущего состояние ключа доступа необходимо выполнить в привилегированном режиме следующую команду:

```
DionisNXe # show crypto access key status
```

Возможные состояния:

- no key - КД не сгенерирован или не загружен в систему. ДСЧ не инициализирован. Работа криптосистемы невозможна;
- not stored - сгенерирован **новый** КД, но не сохранён на **внешнем** носителе;
- ok - КД загружен в систему. ДСЧ инициализирован.

8.2.1.3. Загрузка и удаление КД

Для автоматической загрузки КД при перезагрузке Dionis-NXe, необходимо в сохранённую конфигурацию (startup-config) включить команду «crypto access key load»:

```
DionisNXe # configure
DionisNXe(config)# crypto access key load flash
DionisNXe(config)# do copy running-config startup-config
```

По данной команде при перезагрузке Dionis-NXe будет осуществляться поиск на внешних носителях и загрузка КД.

После загрузки КД выполняется попытка расшифровки начального заполнения ДСЧ, сохранённого на внутреннем носителе. Неудачная расшифровка означает несоответствие данного КД данному узлу. При удачной расшифровке происходит инициализация ДСЧ,

формируется новое начальное заполнение ДСЧ, которое зашифровывается на КД и помещается на внутренний носитель (для следующей перезагрузки).

Для удаления КД из оперативной памяти Dionis-NXe, следует выполнить команду:

```
DionisNXe # crypto access key clear memory
```

Данная команда удаляет ключ доступа из памяти системы и из ОЗУ.

Для удаления КД с внешнего носителя используется команда:

```
DionisNXe # crypto access key clear flash
```

8.2.1.4. Плановая замена КД

Для замены с сохранением на внешнем носителе загруженного ключа доступа необходимо вставить носитель со старым КД и выполните команду:

```
DionisNXe # crypto access key replace flash
```

При замене КД перешифровываются все секреты системы на новом КД.

Если по каким-то причинам замена КД не удалась, то осуществляется откат, и старый КД продолжает действовать.

8.2.2. Рабочие ключи DiSEC

8.2.2.1. Загрузка и удаление

Чтобы добавить новый рабочий ключ DiSEC, нужно вставить флэш-носитель, хранящий новый криптоключ, и выполнить команду:

```
DionisNXe # crypto disec import key flash
```

⚠ **ВАЖНО:** Для упрощения работы крипто номер ключа должен совпадать с номером узла в криптографической сети.

Чтобы удалить установленный ключ, следует использовать команду:

```
DionisNXe # crypto disec remove key 55 1
```

Команда удалит ключ 1 серии 55.

Чтобы удалить все установленные ключи, следует использовать команду:

```
DionisNXe # crypto disec remove key all
```

8.2.2.2. Плановая смена

При плановой смене ключей (далее ПС) производится замена сетевых ключей одной из серий на ключи новой серии, которые должны уже быть введены в систему.

ПС должна быть выполнена на всех узлах, входящих в криптографическую сеть с данной серией ключей.

Алгоритм плановой смены ключей следующий:

1. После входа в систему (локально или удаленно), необходимо удостовериться в наличии новой серии ключей (например 556), выполнив следующую команду:

```
DionisNXe# show crypto disec key 556
Installed keys:
Serial: 556 , locals: 11
```

Выдача команды покажет, какие локальные криптономера доступны для данной серии ключей. Необходимо удостовериться, что необходимый криптономер (например: 12) перечислен в выдаче данной команды.

2. Далее необходимо проверить, возможен ли доступ по данной серии ключей к нужному удаленному абоненту (например: 22), выполнив следующую команду:

```
DionisNXe# show crypto disec abonent 556 11 22
Access to abonent 22 for key (sn=556;loc=11): GRANTED.
```

В нашем случае удаленный абонент является доступным по данной серии ключей.

Если удаленный абонент является недоступным (команда выдала DENIED) по данной серии ключей, то ПС не будет выполнена успешно, так как установить защищенную связь с абонентом у которого введен данный ключ невозможно.

3. Затем следует войти в настройки интерфейса ditun и выполнить следующие команды:

```
DionisNXe# configure
DionisNXe(config)# interface ditun 0
DionisNXe(config-if-ditun0)# serial 556
```

Если при смене ключей меняются еще локальный и удаленный криптономера, (например: 12 и 23), то дополнительно необходимо будет выполнить следующие команды:

```
DionisNXe(config-if-ditun0)# local-cn 12
DionisNXe(config-if-ditun0)# remote-cn 23
```

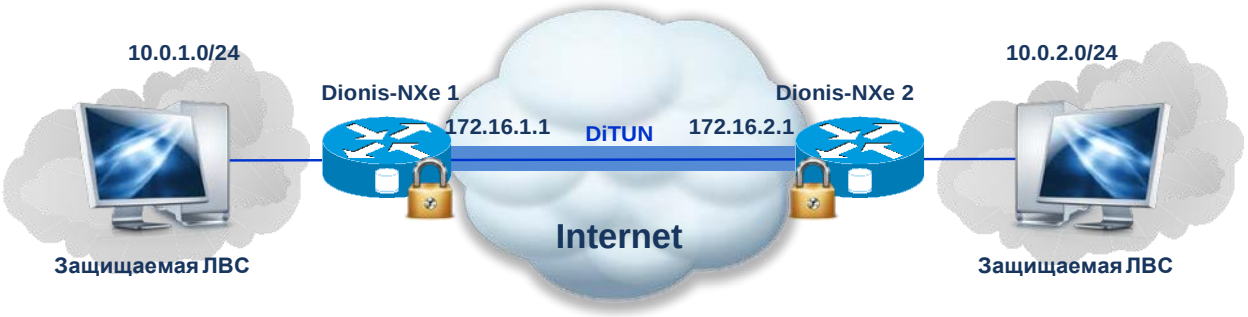
На этом плановая смена ключей завершена. Пункты 1 и 2 алгоритма не обязательны и нужны исключительно для проверки того, что необходимые номера ключей для криптосоединения в наличии и туннель будет корректно работать на новой серии ключей.

После проверки связи со всеми удаленными узлами криптографической сети, необходимо удалить старую серию ключей следующей командой:

```
DionisNXe# crypto disec remove key 555 11
```

8.2.3. DiTUN-интерфейсы

Используемый в Dionis-NXe интерфейс типа DiTUN представляет из себя сетевой интерфейс (3 уровень OSI) позволяющий организовывать туннельные соединения с инкапсуляцией зашифрованных IP-пакетов. VPN, созданные с использованием данных соединений позволяют объединять между собой защищенными виртуальными каналами территориально удаленные ЛВС



8.2.3.1. Создание и настройка

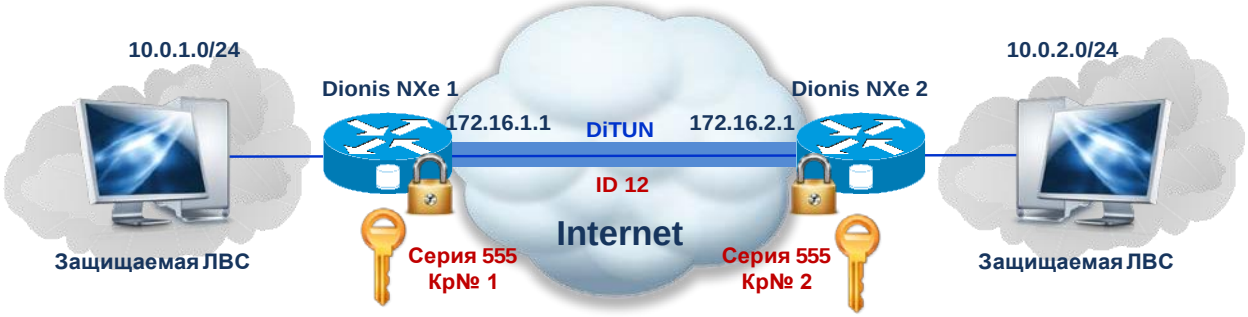
⚠ **ВАЖНО:** Для создания интерфейса DiTUN в режиме шифрования/расшифрования должен быть предварительно создан ключ доступа и загружены симметричные ключи DiSEC.

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

Для создания интерфейса, из режима конфигурации выполните команду:

```
DionisNXe(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 параметры.



Dionis-NXe

Для примера рассмотрим организацию соединения между локальным Dionis-NXe 1 и удаленным Dionis-NXe 2 согласно рисунку.
Следующими командами зададим идентификатор (id) туннеля и включим алгоритм криптографической обработки (encrypt):

```
DionisNXe(config-if-ditun0)# id 12
DionisNXe(config-if-ditun0)# alg encrypt
```

⚠ **ВАЖНО:** Параметр id на обоих Dionis-NXe, соединенных туннелем, должен быть одинаковым.

Назначим IP-адреса локального и удаленного концов туннеля:

```
DionisNXe(config-if-ditun0)# local 172.16.1.1
DionisNXe(config-if-ditun0)# remote 172.16.2.1
```

Введем серию, локальный и удаленный криптономера ключей используемые для криптографической защиты в туннеле:

```
DionisNXe(config-if-ditun0)# serial 555
DionisNXe(config-if-ditun0)# local-cn 1
DionisNXe(config-if-ditun0)# remote-cn 2
```

Активируем интерфейс:

```
DionisNXe(config-if-ditun0)# enable
```

Интерфейс будет создан в тот момент, когда будет задана минимальная необходимая информация. Для открытого туннеля (без криптопреобразования: alg соответствует compression – сжатие или none – без преобразований) это набор параметров: id, local, remote.

В случае криптотуннеля (alg соответствует encrypt – шифрование или both – шифрование с зжатием) дополнительно требуется задать параметры: local-cn, remote-cn, serial.

Для создания туннеля с инкапсуляцией в протокол UDP, необходимо выполнить команду encap, с указанием портов концов туннеля (источника и приемника), например:

```
DionisNXe(config-if-ditun0)# encap 505 505
```

Значение удаленного порта можно не указывать, если он совпадает с портом источника.

Если задать команду encap без параметров, то будут выбраны порты по умолчанию – 600.

Вы можете задать IP-адрес (или несколько адресов) интерфейсу DiTUN, а также делать другие действия, которые являются допустимы по отношению к интерфейсу, например:

```
DionisNXe(config-if-ditun0)# ip address 10.0.1.10/24
```

```
DionisNXe(config-if-ditun0)# ttl 32
```

Интерфейсы DiTUN поддерживают механизм ping-проб, при этом, отстутствие ответной пробы меняет состояние несущей и переводит интерфейс в неактивный режим no-carrier.

```
DionisNXe(config-if-ditun0)# keepalive 5 10 src 10.0.10.1 dst 10.0.20.1
DionisNXe(config-if-ditun0)# link-detect
```

В данном примере мы включаем механизм пинг-проб с периодом 5 секунд, повторить 10 раз (по умолчанию непрерывно). Параметры src и dst устанавливают IP-адрес источника и IP-адрес назначения пинг-проб и являются опциональными. Если они не указаны явно, ip-адресам источника и назначения присваиваются значения ip-адресов концов туннеля.

Также можно использовать автоматическую генерацию идентификатора id туннеля, с помощью:

```
DionisNXe(config-if-ditun0)# id auto
```

При этом, в качестве id будет выбран:

- номер интерфейса + 1 (если интерфейс не в режиме шифрования);
- локальный криптономер + удаленный криптономер (если интерфейс в режиме шифрования);

Какой именно id туннеля используются можно узнать с помощью команды show interface ditun.

```
DionisNXe # show interface ditun
```

Для удаления интерфейса нужно выполнить команду:

```
DionisNXe(config)# no interface ditun 0
```

Для направления трафика в туннель используются стандартные правила маршрутизации. Правила могут быть заданы, как относительно самого интерфейса, например:

```
DionisNXe(config)# ip route default ditun 0
```

так и относительно IP-адреса удаленного интерфейса DiTUN (не путать с адресом удаленного конца туннеля!),

```
DionisNXe(config)# ip route 10.0.2.0/24 10.0.20.1
```

При этом в случае маршрутизация через адрес удаленного DiTUN интерфейса и примененных настройках: keepalive и link-detect, в случае недостижении пинг-пробами удаленной стороны, маршрут будет динамически деактивирован (а при вознобновлении прохождения проб – активирован снова).

8.2.4. -DiTAP-интерфейсы

Используемый в Dionis-NXe, интерфейс типа DiTAP представляет из себя туннельный интерфейс 2 уровня OSI позволяющий организовывать туннельные соединения в виде инкапсулирующих мостов с инкапсуляцией зашифрованных кадров. VPN, созданные с использованием данных соединений позволяют объединять между собой защищенными виртуальными каналами территориально удаленные ЛВС, работающих по протоколу стека TCP/IP, в одни единый сегмент сети, или же объединять между собой ЛВС работающие на сетевых протоколах отличных от стека TCP/IP.

8.2.4.1. Создание и настройка

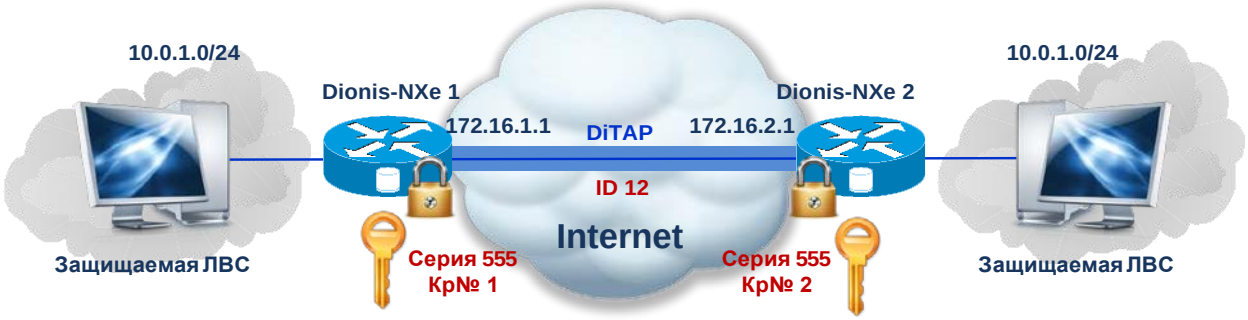
⚠ **ВАЖНО:** Для создания интерфейса DiTAP в режиме шифрования/расшифрования должен быть предварительно создан ключ доступа и загружены симметричные ключи DiSEC.

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

Для создания интерфейса, из режима конфигурации выполните команду:

```
DionisNXe(config)# interface ditap 0
```

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



Для примера рассмотрим организацию соединения между локальным Dionis-NXe 1 и удаленным Dionis-NXe 2 согласно рисунку.

Следующими командами зададим идентификатор (id) туннеля и включим алгоритм криптографической обработки (encrypt):

```
DionisNXe(config-if-ditap0)# id 12
DionisNXe(config-if-ditap0)# alg encrypt
```

⚠ **ВАЖНО:** Параметр id на обоих Dionis-NXe, соединенных туннелем, должен быть одинаковым.

Назначим IP-адреса локального и удаленного концов туннеля:

```
DionisNXe(config-if-ditap0)# local 172.16.1.1
DionisNXe(config-if-ditap0)# remote 172.16.2.1
```

Введем серию, локальный и удаленный криптономера ключей используемые для криптографической защиты в туннеле:

```
DionisNXe(config-if-ditap0)# serial 555
DionisNXe(config-if-ditap0)# local-cn 1
DionisNXe(config-if-ditap0)# remote-cn 2
```

Активируем интерфейс:

```
DionisNXe(config-if-ditap0)# enable
```

Интерфейс будет создан в тот момент, когда будет задана минимальная необходимая информация. Для открытого туннеля (без криптопреобразования: alg соответствует compression – сжатие или none – без преобразований) это набор параметров: id, local, remote.

В случае криптотуннеля (alg соответствует encrypt – шифрование или both – шифрование с сжатием) дополнительно требуется задать параметры: local-cn, remote-cn, serial.

Для создания туннеля с инкапсуляцией в протокол UDP, необходимо выполнить команду encap, с указанием портов концов туннеля (источника и приемника), например:

```
DionisNXe(config-if-ditun0)# encap 505 505
```

Значение удаленного порта можно не указывать, если он совпадает с портом источника.

Если задать команду encap без параметров, то будут выбраны порты по умолчанию – 600.

Для того чтобы связать интерфейс DiTAP с Ethernet-интерфейсом необходимо включить их в BRIDGE-интерфейс.

```
DionisNXe(config)# interface bridge 0
DionisNXe(config-if-bridge0)# port ethernet 0
DionisNXe(config-if-bridge0)# port ditap 0
```

Dionis-NXe

Интерфейс DiTAP будет принимать с Ethernet-интерфейса принимаемые им из сети кадры и после преобразования (сжатия и/или шифрования) инкапсулировать их в транспортный пакет туннеля.

Также можно использовать автоматическую генерацию идентификатора id туннеля, с помощью:

```
DionisNXe(config-if-ditap0)# id auto
```

При этом, в качестве id будет выбран:

- номер интерфейса + 1 (если интерфейс не в режиме шифрования);
- локальный криптономер + удаленный криптономер (если интерфейс в режиме шифрования);

Какой именно id туннеля используются можно узнать с помощью команды show interface ditap.

```
DionisNXe # show interface ditap
```

Для удаления интерфейса нужно выполнить команду:

```
DionisNXe(config)# no interface ditap 0
```

9. Гарантии изготовителя

В течение гарантийного срока изготовитель безвозмездно устраняет неисправности Dionis-NXe, обусловленные производственными дефектами, приведшими к нарушению его работоспособности, при условии соблюдения Заказчиком правил и условий хранения, транспортировки, эксплуатации и монтажа.

Гарантийный срок замены или ремонта Dionis-NXe согласуется с Заказчиком при заключении контракта.

Если срок гарантии в контракте не указан или Dionis-NXe поставляется без контракта (по заявке или оплаченному счету), то устанавливается гарантийный срок – 12 месяцев со дня отгрузки изделия со склада изготовителя.

Изготовитель производит гарантийный ремонт при условии возврата Dionis-NXe в полной комплектации и в упаковке. Оплату доставки по гарантийным обязательствам Dionis-NXe изготовителю и обратно осуществляется согласно условиям контракта.

Если в период гарантийного срока Dionis-NXe вышел из строя по вине Заказчика вследствие неправильного хранения, транспортировки, эксплуатации или других причин, то его ремонт производится за счет Заказчика.

По истечении срока действия гарантийных обязательств ремонт и замена Dionis-NXe
или его составных частей осуществляется предприятием-изготовителем за счет Заказчика.

Техническое сопровождение Dionis-NXe осуществляется в соответствии с регламентом по адресу http://nxe.factor-ts.ru или договором на сопровождение.

Заявки на гарантийный ремонт Dionis-NXe должны подаваться до истечения гарантийного срока и содержать сведения о Dionis-NXe и обнаруженной неисправности.

Адрес изготовителя для подачи заявок: 123290, Москва, 1-й Магистральный проезд, д. 11, стр. 1, тел. +7(495) 662-6640, факс +7(495) 662-6644, e-mail: helpdesk@factor-ts.ru.