Настройка защищенного удаленного подключения по протоколу IPSec (ГОСТ)

Для создания защищенных каналов связи в режиме шифрования/дешифрования в Dionis-NX должен быть инициализирован ДСЧ и создан КД.



Рис. 1 Схема подключения

Согласно сценарию PC-1 находится за NAT

PC-1 подключается к Dionis DPS с помощью клиентского ПО Disec

## Настройка Dionis DPS

Предварительная настройка сетевых интерфейсов

#### (config)# interface ethernet 0

## (config-if-ethernet0)# ip address 83.220.32.68/24

## (config-if-ethernet0)# 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. /u1-256.p15 - закрытый ключ /root.cer – корневой сертификат /u1-256.cer – сертификат узла Dionis DPS /u2-256.cer – сертификат узла PC-1

## # crypto pki import key from flash0:/u1-256.p15

//загрузка контейнера с закрытым ключом

## # crypto pki import root ca cert from flash0:/root.cer

//загрузка корневого сертификата

## # crypto pki import cert from flash0:/u1-256.cer

//загрузка сертификата узла

Также необходимо загрузить сертификат удаленного пользователя:

## # crypto pki import cert from flash0:/u2-256.cer

И список удаленных сертификатов:

## # crypto pki import crl from flash0:/root.crl

Перейдем к настройке соединения:

(config)# crypto ike conn t1

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

(config-ike-conn-t1)# auto listen

(config-ike-conn-t1)# keying tries 1

(config-ike-conn-t1)# local cert u1-256.cer

//Указываем сертификат узла

(config-ike-conn-t1)# local ip 83.220.32.68/24

//Указываем белый адрес туннеля к которому будет подключаться удаленный пользователь

(config-ike-conn-t1)# local subnet from pool

#### (config-ike-conn-t1)# modeconfig dns 192.168.53.254 8.8.88

//Указываем какие DNS нужно назначить подключенному удаленному пользователю

(config-ike-conn-t1)# modeconfig mode pull (config-ike-conn-t1)# no rekey (config-ike-conn-t1)# pfs mode force (config-ike-conn-t1)# ph1 transforms (config-ike-conn-t1-ph1)# no strict (config-ike-conn-t1)# ph2 transforms (config-ike-conn-t1)# ph2 transforms (config-ike-conn-t1)# remote id \* (config-ike-conn-t1)# remote ig \* (config-ike-conn-t1)# remote ip \* (config-ike-conn-t1)# remote ip mypool (config-ike-conn-t1)# send cert ifasked

Перейдем к настройке адресов:

(config)# crypto ike pool mypool

## (cfg-ike-pool-mypool)# pool 10.10.1.0/24

//Указываем список виртуальных адресов, который будет назначаться удаленному пользователю

#### (cfg-ike-pool-mypool)# local subnet 192.168.0.0/16

*ШУказываем локальную сеть к которой необходимо предоставить доступ удаленному пользователю* 

(config)# crypto ike config

(config-ike)# auth-log all

(config-ike)# crl cache

(config-ike)# debug control

(config-ike)# nat traversal

#### (config)# crypto ike enable

//запуск сервиса ike

На это настройка Dionis DPS закончилась.

#### Настройка ПО Disec на PC-1

Открываем программу Disec и выбираем вкладку «Подключения», и нажимаем на кнопку «Добавить»:

тройка П	10 D	iSec					?	$\times$
щие По,	дклю	чения Драйвер	DiSec Cr	ужба DiSecSrv				
Ресурсь	ы под	цключений						
Назв	A	Режим IPSec	Имя()	ID Абонента	Пок	CEDT.		
ditun3 ditun vpn connt1 fact t1	000000000000000000000000000000000000000	ГРЗес-Фактор IPSec-Фактор IPSec-Фактор IPSec-Фактор IPSec-Фактор IPSec-Фактор IPSec-ГОСТ	римиц 192.1 192.1 192.1 192.1 83.22 192.1	CN=u1-256 CN=u1-256	u2- u2-	256 256	Вверл Вниз Экспор Импор Авто Кон ++ ВКЛ - Выкл	T T HekT
1						>	Выбрат ВСЕ	ъ
Добави	іть подк	Изменить	Удал	ить Ду	бль	-	Очистить	•
Макс одног	. чис го по	ло попыток	2 Чис	ло 0				
Провер Преду	ока с	хрока действия с кдать за	ертификато дней до око	ив нчания Пр Принять	ооверять		дней	
					ОК	Отмена	Спра	вка

Рис.2 Добавление подключения

После этого откроется окно Общих настроек подключения

В строчке «Название подключения» необходимо ввести произвольное название соединения

В строчке «Адрес (IP) сервера VPN:» необходимо ввести адрес к которому будет подключаться удаленный клиент (нужно указывать адрес, который прописывался в local ip в настройках crypto ike conn tl)

Режим соедине	ния:	с.Фэктор	
Переподклю	нать при сбросе подн	слючения Сер	овером VPN
Тип туннела: —			
• Линамическ	ий		
Отключить	Anti-Replay защиту		

Режим соединения необходимо выбрать IPSec-ГОСТ

Рис. 3 Общие настройки

Далее необходимо перейти на следующую вкладку «Параметры»

В которой необходимо поставить галочку рядом с пунктом «Запросить IP-подсеть (MODE\_CFG)»

📑 Реквизиты подключения VPN	?	×
Общие Параметры Безопасность Задачи		
Политики IKE: Политики ESP: Создать Правка Создать Правка	a	
-Целевые объекты (доступные ресурсы):		
☑ Запросить IP-подсеть (MODE_CFG) Список объе	ктов	
Дополнительные параметры IKE Ретрансмиссии (повтор отправки сообщения) т/а (сек) 20 Макс. число 2 Макс. попыто	к 1	
Замена SAIKE (рекиинг фазы 1) Заранее Ike(сек.) 120 Задержка Ike(сек.) 1 Замена SAESP (рекиинг фазы 2)	0	
Заранее Esp(сек.) 120 Задержка Esp(сек.)	10	
ок о	тмена	

Рис. 4 Настройка парамтеров

Далее под строчкой «Политики IKE:» необходимо нажать «Правка»

И в столбце «Проверка жизнеспособности туннеля:» указать «Активный»

В «Действие при обнаружении нежизнеспособности» выбрать «Инициировать заново»

И нажать «ОК»

#### Политики IKE

Посылка локального сертификата	
По запросу	Проверка жизнеспособности туннеля:
	Активный
Параметры алгоритма 28147-89:	
id-Gost28147-89-CryptoPro-Z-ParamSet	Таймаут ожидания ответа (сек):
	90
Режим PFS:	, <u> </u>
Включён	Интервал посылки запроса (сек):
	30
Параметры алгоритма выработки сессионного ключа:	
id-tc26-gost-3410-12-512-paramSetB+id-tc26-gost3411-12-512 ▼	Макс. число ошибок 3
Период смены ключей Ike(сек):	Действие при обнаружении нежизнеспособности Инициировать заново
ОК Стандартные	Отмена

Рис. 5 Политики ІКЕ

Дальше необходимо нажать на кнопку «Правка» под строчкой «Политик ESP», поставит галочку рядом с пунктом Запрос IP-адреса в защищенной сети сети (MODECONFIG) и нажать «ОК».

Политики ES	;P	?	$\times$
Режим инка	псуляции трафика:		
Туннельны	й 💌		
Преобразов	ание ESP:		
GOST89-4M	I-IMIT-B		
,			
Параметры	ГОСТ Р 3410-2001 (только для PFS):		
как в ІКЕ	•		
Период сме			
3600			
10000	<u>•</u>		
Допустимое	количество искаженных пакетов:		
100000	- -		
Запрос І	P-адреса в защищенной сети (MODECON	IFIG)	
	Стандартные		
OK		Отме	на

Рис. 6 Политики ESP

? X

Далее переходим во вкладку «Безопасность» и в Настройках криптосистемы нажимаем «Настроить»

Настройки криптосистемы	Х
Общие CRL/OCSP	
Хранилище сертификатов доверенных корневых УЦ	
Расположение хранилища C:\Users\User\AppData\Roaming\Factor-TS\DioNIS Security\RSST\root.sst	
, П Защитить хранилище	
Удалить имитовставку хранилища	
Текущий сертификат пользователя:	
Неизвестен	
< >	
Работа с хранилищем сертификатов Установить личный сертификат	
Предупреждать об окончании срока действия сертификата 30 дней	
Сохранить <b>Отмена</b>	

Рис. 7 Настройки криптосистемы

В графе «Текущий сертификат пользователя» необходимо нажать «Установить личный сертификат» и выбрать с носителя ключ и сертификат, который будет использоваться данным удаленным пользователем, в нашем случае это u2-256.p15 – ключевой контейнер и u2-256.cer – сертификат

юситель	Контейнер	Формат	Информация
		[DIR]	K:\
:\	u1-256.p15	P15	K:\
\$	u2-256.p15	P15	K:\

Рис. 8 Выбор ключевого контейнера

После добавления ключевого контейнера система подсказывает что необходимо добавить сертификат:



После нажатия кнопки «ОК» система будет предлагать установить сертификаты найденные на съемном носителе



Рис. 10 предложение установки сертификата

На рис. 10 необходимо нажать «Нет» т.к. система предлагает установить корневой сертификат, а в данном случае необходим сертификат удаленного пользователя – u2-256.cer , необходимо нажимать «Нет» пока система перебором не укажет необходимый сертификат

Вниман	1e	×
<u> </u>	На ключевом носителе в директории контейнера ключа НАЙДЕН файл сертификата	
	K:\u2-256.cer.	
	Установить?	
	Да Нет	1

Рис. 11 Предложение установки сертификата удаленного пользователя

Когда появится сообщение о том что найден необходимый сертификат нажимаем «Да»

После этого откроется окно в котором добавляем указанный сертификат в ранее указанное хранилище ключа:

Внимани	ie	×
<u>^</u>	Выбран ключевой носитель: P15::K:\u2-256.p15 Носитель содержит сертификат: Субъект: u2-256 Поставщик: RU, Фактор-TC, Корневой УЦ Действителен: с 17/11/2017 г. по 24/05/2026 г. Назначения: IKE-посредник IP-6езопасности Серийный номер: 00FCED4C 24000000 0E Отпечаток SHA1: 76B1B9EC 3D7D0D2B DCF51DC5 126F7810 D9A9DAD3	
	Отпечаток MD5: 93600B7D 0E2BF552 694E01CA 2BFF41BD Желаете добавить сертификат в хранилище и сделать его текущим?	
	<u>Д</u> а <u>Н</u> ет	

Рис. 12 Добавление сертификата в хранилище

На рис. 12 нажимаем «Да», если все сделано корректно то увидите следующее сообщение:

Внимание

 $\times$ 



Рис. 13 Информационное окно

После нажатия клавиши «ОК» на рис. 13 система предложит установить корневой сертификат:



Рис. 14 предложение указать корневой сертификат

После нажатия кнопки «Да» выведется окно съемного носителя с сертификатами в котором необходимо указать корневой сертификат, в данном случае это файл с названием root.cer

¥

Носитель	Контейнер	Формат	Информация
		[DIR]	K:\
K:\	root.cer	CER	K:\
K:\	u1-256.cer	CER	K:\
к:\	u2-256.cer	CER	K:\
<			
	1		
Выбрать Повтор	Удалить	Удалить ВСЕ	Отм

Выберите сертификат УЦ (\*.cer) или файл с цепочкой сертификатов УЦ (\*.p7b)

Рис. 15 Выбор корневого сертификата

После выбора на Рис. 15 корневого сертификата появится предложение Заменить предыдущий (если есть) и добавить выбранный в хранилище сертификатов

Внимани	1e	$\times$
	Сертификат доверенного корневого УЦ: Субъект: RU, Фактор-TC, Корневой УЦ Поставщик: самовыдача Действителен: с 26/05/2016 г. по 24/05/2026 г. Назначения: < Все> Серийный номер: Отпечаток SHA1: I 46А38BB2 Отпечаток MD5: 5 уже находится в хранилище сертификатов доверенн корневых УЦ(C:\Users\User\AppData\Roaming\Factor-TS\DioNIS Security\RSST\root.sst) Заменить?	ых
	Да Н	ет

Рис. 16 Добавление корневого сертификата в хранилище сертификатов

Далее система увидит на носителе файл со списком отозванных сертификатов и предложит добавить его в хранилище, необходимо нажать «Да»

Внимани	1e	$\times$
<u> </u>	На ключевом носителе в директории контейнера ключа НАЙДЕН файл со списком отозванных сертификатов (CRL)	
	K:\root.crl.	
	Добавить список в хранилище?	
	Да Нет	

Рис. 17 Добавление списка отозванных сертификатов в хранилище

Если все было сделано корректно, то система выведет следующее окно:



Рис. 18 Информационное окно о корректности установки текущего сертификата

После этого в окне «Настройки криптосистемы» Нажимаем кнопку «Сохранить»

Далее во вкладке «Безопасность», в Главе «Настройки запроса сертификата сервера VPN:» Выбираем «Не запрашивать сертификат сервера VPN» и нажимаем на кнопку «Выбрать сертификат сервера VPN...»

1	-Настройки запроса сертификата сервера VPN:
	Не запрашивать сертификат сервера VPN
	Выбрать сертификат сервера VPN

Puc. 19

После нажатия кнопки выбора сертификата сервера VPN системой будет предложено установить сертификат, в данном случае необходим сертификат с названием u1-256.cer

Система будет предлагать установить сертификаты которые найдет, если будет выбор сертификата не совпадающий с необходимым нужно нажать «Больше вариантов» в котором будет возможность Выбрать необходимый сертификат (см. рис. 20-21)

Безопасность Windows

# Выбор сертификата



Корневой УЦ

Издатель: Корневой УЦ

Действителен с: 26.05.2016 по 24.05.2026

Просмотреть свойства сертификата

Больше вариантов

ОК

Отмена

 $\times$ 

**Puc. 20** 



**Puc.** 21

После выбора необходимого сертификата нужно нажать «ОК» и вкладка «Безопасность» должно выглядеть следующим образом:

Реквизиты подключения <new> ?</new>	$\times$
Общие Параметры Безопасность Задачи	
Настройка криптосистемы:	
Настроить Инициализировать	
Субъект: u2-256	
×	
Работа с хранилищем сертификатов	
Настройки запроса сертификата сервера VPN:	1
• Не запрашивать сертификат сервера VPN	
CN=u1-256	
Выбрать сертификат сервера VPN	
О Запросить сертификат сервера VPN по X500-имени	
Получить имя субъекта из сертификата	
🔲 Запросить сертификат, выпущенный доверенным УЦ	
	1
ОК Отмена	

Рис. 22 Вкладка "Безопасность" после добавления сертификатов

После этого необходимо нажать внизу кнопку «ОК», вернемся в окно Настройки ПО Disec на вкладку «Подключения» в которой необходимо нажать кнопку «Принять» и после клавишу «ОК»

наст	роика	ΠU	DISEC
------	-------	----	-------

ſ		

Общие Подключения Драйвер DiSec Служба DiSecSrv									
Ресурсы подключений									
Назв А Режим IPSec Има(I ID Абонента Г	Іок серт								
ditun3 0 IPSec-Фактор 192.1	Decent								
ditun 0 IPSec-Фактор 192.1	Вверх								
vpn 0 IPSec-Фактор 192.1									
connt1 0 IPsec-FOCT 192.1 CN=u1-256	и <b>2-256</b> Вниз								
fact 0 IPSec-Фактор 83.22									
t1 U IPsec-I UCI 192.1 CN=u1-256 U	U2-256								
VPIN IPSec-I UC 1 83.22 CIN=U1-206 0	Экспорт								
	Импорт								
	Авто Коннект								
	++ BKU								
	Выкл.								
	Выбрать								
	BCE								
Добавить Изменить Удалить Дубль Очистить									
О Авто-подключение при запуске приложения									
Макс число полыток									
одного подключения 2 Число 0									
Предупреждать за дней до окончания Проверять	дней								
Принять									
ОК	Отмена Справка								

**Puc.** 23

На этом настройка ПО Disec закончена.