

УТВЕРЖДЕНО
ВУ.РТНК.41002-01 34 02-ЛУ

Программный продукт
«Клиент безопасности Bel VPN Client-P 4.1»
Руководство пользователя

ВУ.РТНК.41002-01 34 02

Листов 97

Ин д. №	По дп. и дата	Вз ам. инд.	Ин в. № дубл.	По дп. и дата

Содержание

1	Назначение и функции	5
2	Требования на базовые платформы и совместимость	7
3	Подготовка к установке ПП Bel VPN Client-P	8
4	Установка ПП Bel VPN Client-P	9
4.1	Режим basic	10
4.2	Режим normal	12
4.3	Режим silent	17
4.4	Копирование контейнера при инсталляции.....	19
4.5	Сообщения об ошибках при инсталляции	19
5	Дополнительные настройки	23
5.1	Обеспечение работоспособности VPN сервиса	23
5.2	Настройка переменных окружения.....	23
5.2.1	Описание переменных окружения	23
5.3	Рекомендации по ручной настройке Брандмауэра Windows	24
6	Регистрация пользователя	25
6.1	Интерактивный режим логина в Продукт	25
6.1.1	Особенности регистрации для различных ОС.....	25
6.1.2	Успешная регистрация	26
6.1.3	Неуспешная регистрация.....	27
6.2	Неинтерактивный режим логина в Продукт	27
6.3	Время инициализации VPN сервиса.....	28
6.4	Неинтерактивный режим логина в ОС.....	28
6.5	Замечание.....	28
7	Стартовый и регламентный контроль целостности Продукта.....	30
7.1	Программная часть Продукта	30
7.2	Информационная часть Продукта	31
8	Отображение текущего статуса Продукта.....	32
8.1	Изменение положения иконки текущего статуса Продукта...32	
8.2	Login/Logout	33
8.3	SA Information.....	33
9	Удаление ПП Bel VPN Client-P.....	36

10	Восстановление ПП Bel VPN Client-P	37
11	Специализированные команды	38
11.1	cert_mgr show	40
11.2	cert_mgr check	41
11.3	client_login	42
11.4	client_logout	42
11.5	cspvpn_verify	43
11.6	dp_mgr show	44
11.7	dp_mgr set	45
11.8	drv_mgr	45
11.9	drv_mgr show	48
11.10	drv_mgr set	49
11.11	drv_mgr reload	50
11.12	fwconn_show	50
11.13	if_show	52
11.14	integr_mgr calc	53
11.15	integr_mgr check	53
11.16	key_mgr import	54
11.17	key_mgr remove	55
11.18	key_mgr show	56
11.19	key_mgr list	56
11.20	klogview	57
11.20.1	События группы fw_trace, fw_notif	66
11.20.2	События группы sa_minor, sa_major	67
11.20.3	События группы sa_trace	69
11.20.4	События группы sa_errors	69
11.20.5	События группы fw_tcpst, fw_tcperr, fw_tcpstat	70
11.20.6	События группы fw_obj	71
11.20.7	События группы vif_obj	73
11.20.8	События группы mtud	75
11.20.9	Сообщение об утере данных	75
11.21	lic_mgr show	76
11.22	lic_mgr set	76
11.23	log_mgr show	76

11.24	log_mgr set	77
11.25	lsp_mgr check.....	80
11.26	lsp_mgr load	81
11.27	lsp_mgr reload.....	81
11.28	lsp_mgr unload.....	82
11.29	lsp_mgr show.....	82
11.30	lsp_mgr show-info.....	83
11.31	pwd_change.....	84
11.32	sa_mgr show.....	85
11.33	sa_mgr clear	89
11.34	ver_show	90
11.35	avverify.....	91
11.36	Сообщения об ошибках	91
11.36.1	Утилиты cert_mgr show, cert_mgr import, cert_mgr check, cert_mgr create, cert_mgr remove	91
11.36.2	Утилита client_login, client_logout	93
11.36.3	Утилита cspvpn_verify.....	93
11.36.4	Утилита dp_mgr show	94
11.36.5	Утилиты drv_mgr show, drv_mgr set, drv_mgr reload	94
11.36.6	Утилита if_show.....	94
11.36.7	Утилита integr_mgr calc, integr_mgr check	95
11.36.8	Утилиты key_mgr import, key_mgr remove, key_mgr show ...	96
11.36.9	Утилита lic_mgr set.....	96
11.36.10	Утилита log_mgr show	96
11.36.11	Утилиты lsp_mgr reload, lsp_mgr unload, lsp_mgr show.....	96
11.36.12	Утилита pwd_change	97
11.36.13	Утилиты sa_mgr show, sa_mgr clear	97
11.36.14	Утилита avverify	97

1 Назначение и функции

Программный продукт «Клиент безопасности Bel VPN Client-P 4.1» (далее – ПП Bel VPN Client-P, Продукт) функционирует на аппаратных платформах в архитектуре Intel x86/x86-64 под управлением операционных систем семейства Microsoft Windows.

ПП Bel VPN Client-P выполняет роль персонального VPN клиента и персонального межсетевых экранов.

ПП Bel VPN Client-P может устанавливаться на:

- персональный компьютер пользователя – для защиты индивидуального рабочего места пользователя при работе как в локальных корпоративных сетях, так и в открытых сетях (Интернет);
- автономный сервер;
- специализированные устройства в составе платежных систем: банкоматы, расчетные терминалы, кассовые аппараты (POS-терминалы) и датчики автоматизированных систем управления технологическими процессами.

ПП Bel VPN Client-P предназначен для защиты от несанкционированного доступа, сетевых атак, создания защищенных VPN соединений между устройством, на котором он установлен, и другими взаимодействующими с ним доверенными VPN-шлюзами и VPN-клиентами.

ПП Bel VPN Client-P обеспечивает:

- создание виртуальных частных сетей (IPsec VPN) с применением белорусских криптографических стандартов;
- защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP
- пакетную и контекстную фильтрацию любого исходящего и входящего трафика на хост с использованием информации в полях заголовков сетевого, транспортного и прикладного уровней:
 - o с учетом входного и выходного сетевого интерфейса;
 - o по любым значимым полям IP-заголовка и полям данных сетевого пакета;
 - o с учетом даты и времени;
- аутентификацию пользователя (при запуске Клиента) и аутентификацию узла сети (при создании защищенного соединения);
- событийное протоколирование;
- реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения;
- регулируемую стойкость защиты трафика.

ПП Bel VPN Client-P осуществляет защиту трафика протоколов семейства TCP/IP в рамках международных стандартов IKE/IPsec:

- Security Architecture for the Internet Protocol – RFC2401.
- IP Authentication Header (AH) – RFC2402.
- IP Encapsulating Security Payload (ESP) – RFC2406.
- Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408.
- The Internet Key Exchange (IKE) – RFC2409.

- The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407.

ПП Bel VPN Client-P использует криптографическую библиотеку программного средства электронной цифровой подписи и шифрования «AvC ver.1.0» (РБ.ЮСКИ.13000-01) производства ЗАО «Авест».

ПП Bel VPN Client-P соответствует требованиям Технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» – ТР 2013/027/ВУ (взаимосвязанные ТНПА:

- хэширование – СТБ 1176.1-99, СТБ 34.101.31-2011 (подраздел 6.9 раздела 6);
- электронная цифровая подпись - СТБ 1176.2-99 (разделы 5, 6), СТБ 34.101.45-2013 (подраздел 6.2 раздела 6; подраздел 7.1 раздела 7; таблица Б1 приложения Б; приложение Д)
- шифрование и контроль целостности – ГОСТ 28147-89 (разделы 2, 4, 5), СТБ П 34.101.50-2012 (приложения Б, В, Г), СТБ 34.101.31-2011 (подраздел 6.4 раздела 6);
- генерация случайных данных – СТБ 34.101.47-2012 (подраздел 6.2 раздела 6);
- управление ключами – СТБ 34.101.66-2014 (приложение А), управление криптографическими ключами, рекомендованное ОАЦ;
- формат сертификатов и списков отозванных сертификатов – СТБ 34.101.19-2012 (разделы 6, 7, 8);
- требования безопасности – СТБ 34.101.27-2011 (класс 1), СТБ 34.101.1-2014, СТБ 34.101.2-2014, СТБ 34.101.3-2014.

Также, ПП Bel VPN Client-P поддерживает возможность работы с международными криптоалгоритмами (RSA, 3DES, AES).

ПП Bel VPN Client-P обеспечивают защиту конфиденциальной информации от внешнего нарушителя и фильтрацию входящего и исходящего сетевого трафика.

Политику безопасности и настройку режимов ПП Bel VPN Client-P осуществляет администратор безопасности, который может с помощью ПП Bel VPN Client-P запретить все внешние соединения, кроме тех, которые выполняются через защищенное VPN-соединение с Bel VPN Gate (жесткая политика), так и разрешить внешние соединения.

ПП Bel VPN Client-P поддерживает возможность централизованно-удаленного управления с использованием программного комплекса «Bel VPN КР 4.1», с помощью которого можно обновить сертификаты, ключи, политику безопасности, лицензии и др.

В ПП Bel VPN Client-P по умолчанию для всех интерфейсов задается одинаковая политика безопасности, однако поддерживается возможность задания разных политик безопасности для каждого интерфейса с помощью ручного редактирования LSP-конфигурации или с помощью программного комплекса «Bel VPN КР 4.1».

2 Требования на базовые платформы и совместимость

ПП Bel VPN Client-P работает под управлением следующих операционных систем:

- MS Windows XP SP3 Russian Edition;
- MS Windows Vista SP2 Russian Edition (32-bit, 64-bit);
- MS Windows 7 Russian Edition (32-bit, 64-bit);
- MS Windows 8 Russian Edition (32-bit, 64-bit);
- MS Windows 8.1 Russian Edition (32-bit, 64-bit);
- MS Windows 10 Pro (32-bit, 64-bit);
- MS Windows Server 2003 Edition 32-bit;
- MS Windows Server 2008 Edition (32-bit, 64-bit);
- MS Windows Server 2008R2 Edition 64-bit;
- MS Windows Server 2012 Edition 64-bit.

ПП Bel VPN Client-P может функционировать в виртуальной среде, под управлением вышеперечисленных ОС.

ПП Bel VPN Client-P совместим со следующими продуктами компании «С-Терра Бел»:

- Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 3.0.1»
- Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1»
- Программный комплекс «Шлюз безопасности виртуальный Bel VPN Gate-V 4.1»
- Программный комплекс «Bel VPN KP 4.1»

В части реализации протоколов IPsec/IKE и их расширений ПП Bel VPN Client-P совместим с Cisco IOS v.12.4 и v.15.x.x.

3 Подготовка к установке ПП Bel VPN Client-P

ВНИМАНИЕ !

Перед началом работы с продуктом
ознакомьтесь с документом
**«Программный продукт
«Клиент безопасности Bel VPN Client-P 4.1».
Подготовительные процедуры»**

Перед установкой персонализированного дистрибутива ПП Bel VPN Client-P на компьютере пользователя отключите все антивирусные программы.

Для операционных систем Microsoft Windows Vista / Windows 7 / Windows 2008
должно быть установлено обновление безопасности ОС **KB3033929**.

4 Установка ПП Bel VPN Client-P

Установка персонализированного дистрибутива ПП Bel VPN Client-P на персональный компьютер Пользователя осуществляется запуском инсталляционного файла (файл с расширением .exe), подготовленного и переданного Администратором безопасности Пользователю.

Инсталляция должна выполняться Пользователем, имеющим права администратора ОС.

После запуска файла инсталляция осуществляется в одном из 3 режимов, который был выбран Администратором при подготовке инсталляционного файла:

- **режим basic** – основной режим, интерактивная установка с запросом на инсталляцию, вариант по умолчанию;
- **режим normal** – интерактивная установка, с запросом принятия условий лицензионного соглашения, лицензии на Продукт и иных параметров;
- **режим silent** – неинтерактивная установка без запроса действий со стороны Пользователя.

Все протоколируемые события при инсталляции ПП Bel VPN Client-P будут записываться в файл, если администратор указал данную опцию при создании инсталляционного файла.

При возникновении ошибок во время инсталляции или работы Продукта устраните их и попытайтесь повторно провести инсталляцию Продукта.

При появлении сбоев во время работы Продукта – перезагрузите компьютер, но если перезагрузка не устраняет проблему – обратитесь в службу поддержки по адресу:

support@s-terra.by

При инсталляции ПП Bel VPN Client-P происходит отключение стандартного сервиса, связанного с IPsec и IKE и перевод его в состояние Manual. В Windows XP/Windows Server 2003 – это Служба IPSEC, внутреннее название которой PolicyAgent. В ОС Windows Vista и более поздних версиях – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности» (внутреннее название – IKEEXT).

В ОС Windows Vista и более поздних версиях производится настройка штатного FireWall сервиса (Брандмауэр Windows). При установке Bel VPN Client-P в Windows FireWall добавляется новое правило:

- правило для входящих подключений;
- имя – Bel VPN Service – UDP allowed (predefined);
- правило включено;
- действие – разрешить подключение;
- протокол – UDP (все порты);
- программа – полный путь к установленному файлу vpnsvc.exe;
- службы – применять только к службам;
- профили – все профили;
- остальные параметры – по умолчанию.

Эти настройки можно посмотреть следующим образом:

Панель управления → Администрирование → Брандмауэр Windows в режиме повышенной безопасности → Правила для входящих подключений.

4.1 Режим basic

1. В начале установки ПП Bel VPN Client-P выдается запрос на разрешение внесения изменений на компьютере (Рисунок 1). Необходимо выбрать вариант **Разрешить**.

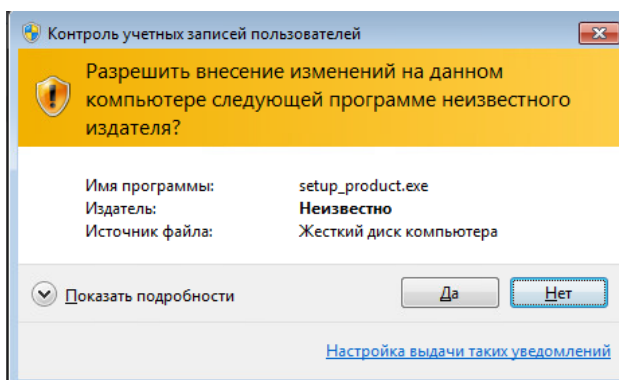


Рисунок 1

2. Затем выдается запрос на инсталляцию ПП Bel VPN Client-P (в ОС Windows XP это окно появляется первым). Для продолжения установки необходимо нажать кнопку **Да**

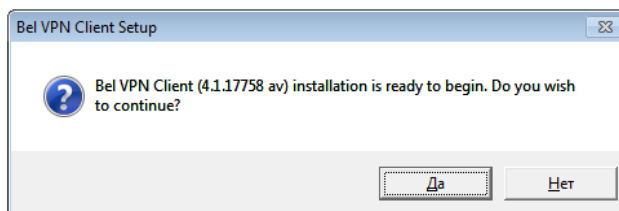


Рисунок 2

3. После нажатия кнопки **Да** происходит распаковка файлов (Рисунок 3) и установка пакета Microsoft Visual C++ 2008 Redistributable Package (Рисунок 4).



Рисунок 3

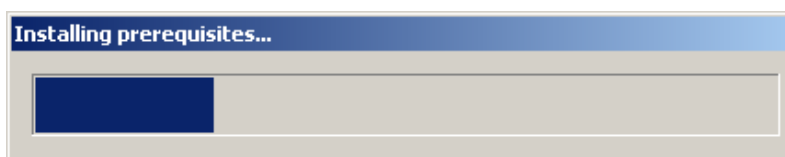


Рисунок 4

4. Далее открывается стартовое окно визарда с приглашением к инсталляции и сразу следует предупреждение о необходимости отключения всех антивирусных программ на время инсталляции ПП Bel VPN Client-P (Рисунок 5).

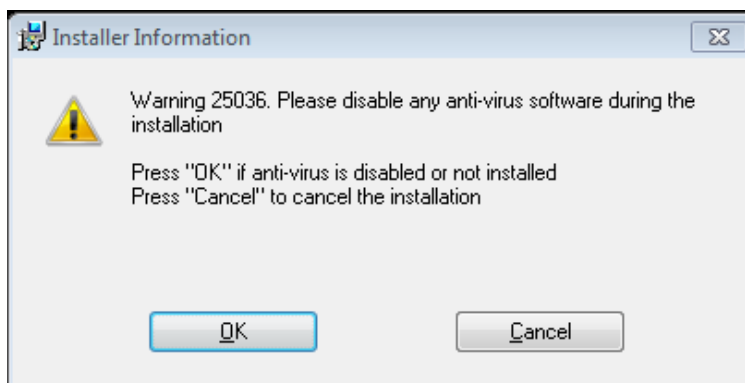


Рисунок 5

5. При нажатии кнопки **OK** инсталляция будет продолжена и появится окно с индикатором процесса инсталляции:

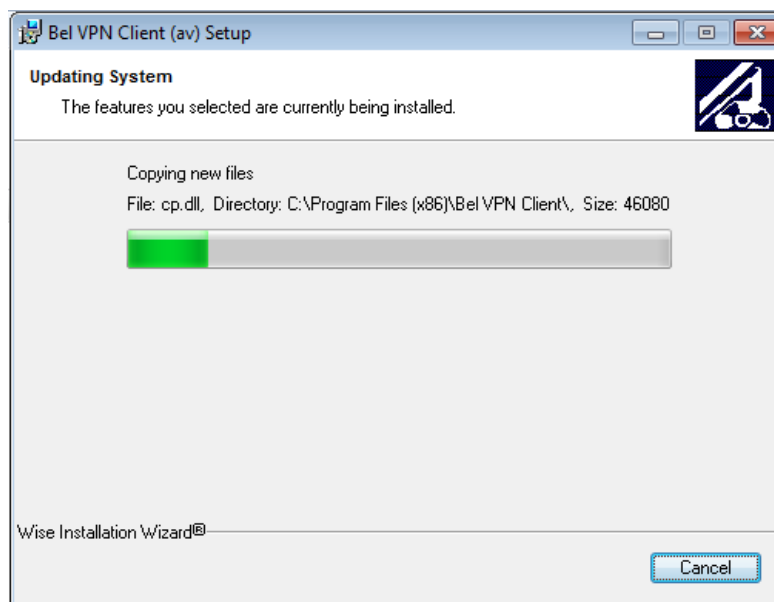


Рисунок 6

6. В случае, если датчик случайных чисел (ДСЧ) не был инициализирован администратором безопасности при создании инсталляционного пакета, предлагается «биологическая» инициализация ДСЧ – нужно нажимать случайные клавиши до заполнения индикатора.

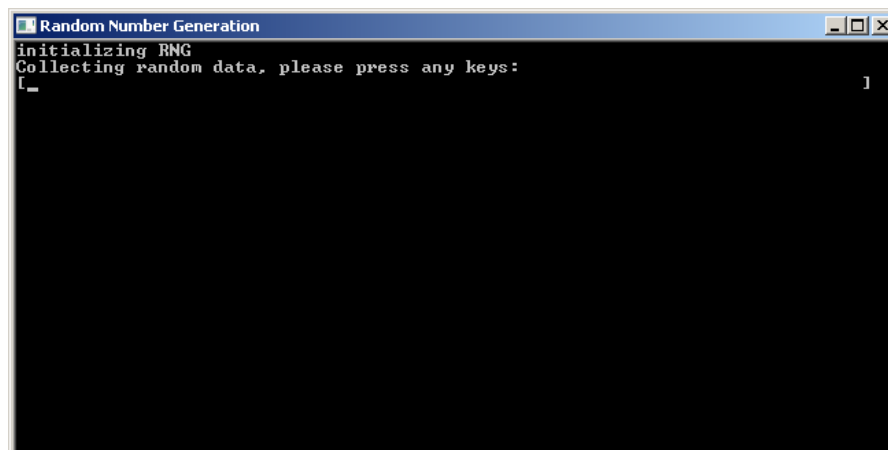


Рисунок 7

- В процессе установки может несколько раз появляться следующее окно с запросом (Рисунок 8). Следует выбрать пункт **Установить**.

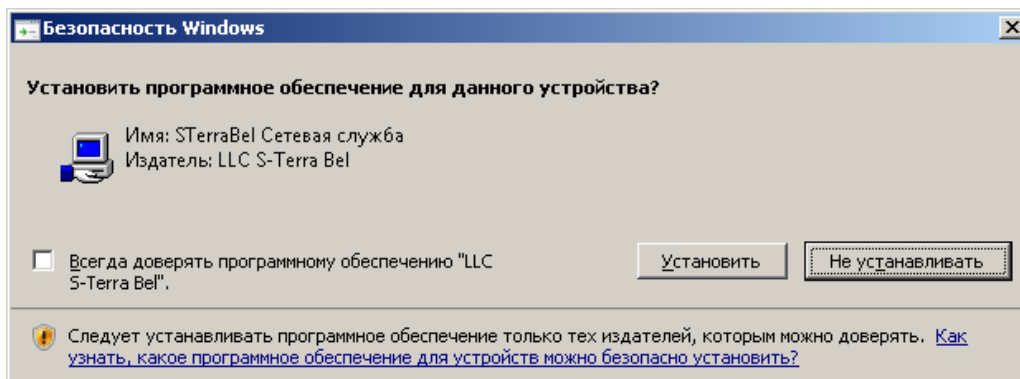


Рисунок 8

- По окончании установки ПП Bel VPN Client-P в ОС Windows XP появляется окно с предупреждением о необходимости перезагрузки операционной системы. После нажатия кнопки **Yes** происходит перезагрузка операционной системы, а нажатие кнопки **No** закрывает окно без перезагрузки. Для ОС Windows Vista и более поздних версий перезагрузка не требуется, но не исключено, что инсталлятор может запросить перезагрузку, если она будет необходима.



Note

Недопустимо удалять из ОС пакет Microsoft Visual C++ 2008 Redistributable Package, отсутствие которого может привести к неработоспособности ПП Bel VPN Client-P

4.2 Режим normal

- В ОС Windows Vista и более поздних версиях, при установке ПП Bel VPN Client-P выдается окно (Рисунок 1) с запросом на доступ к компьютеру. Выберите предложение **Разрешить**.
- Затем выдается запрос на инсталляцию ПП Bel VPN Client-P (в ОС Windows XP это окно появляется первым) (Рисунок 9):

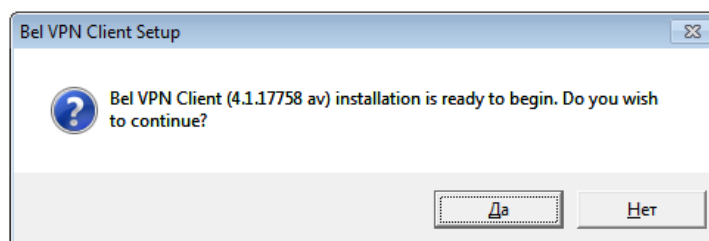


Рисунок 9

- После нажатия кнопки **Да** происходит распаковка файлов (Рисунок 10) и установка пакета Microsoft Visual C++ 2008 Redistributable Package (Рисунок 11).



Рисунок 10

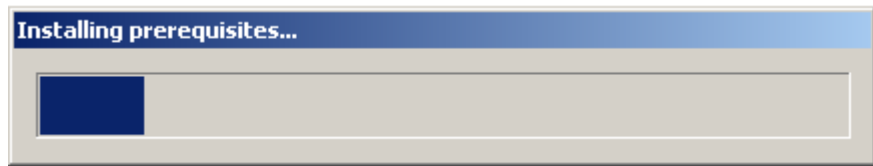


Рисунок 11

4. Этот режим является диалоговым режимом. Далее открывается стартовое окно визарда с приглашением к инсталляции и сразу следует предупреждение о необходимости отключения всех антивирусных программ на время инсталляции ПП Bel VPN Client-P (Рисунок 12).

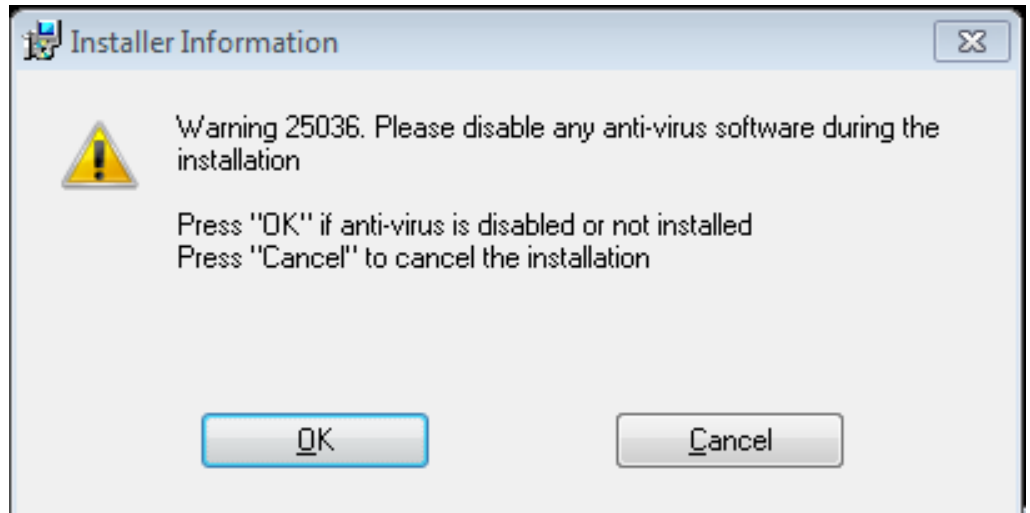


Рисунок 12

5. При нажатии кнопки **OK** инсталляция продолжается, в окне визарда меняются кнопки управления, нажмите кнопку **Next** (Рисунок 13).

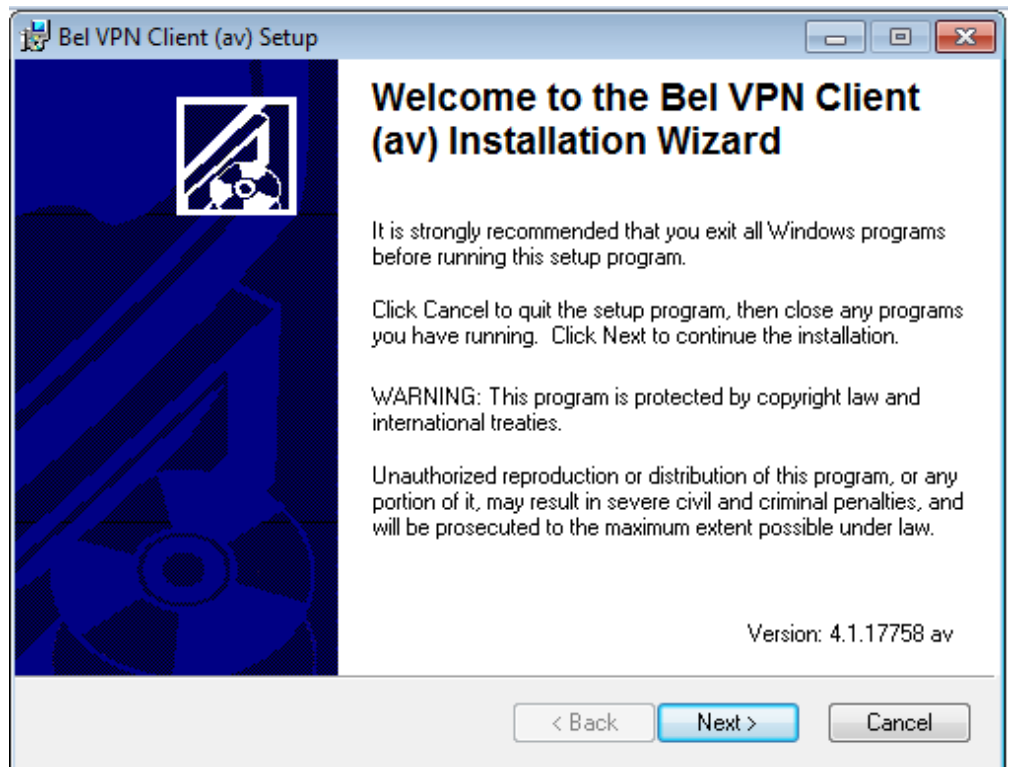


Рисунок 13

6. Далее открывается окно с текстом Лицензионного Соглашения. После установки переключателя в положение "I accept the license agreement" будет доступна кнопка Next:

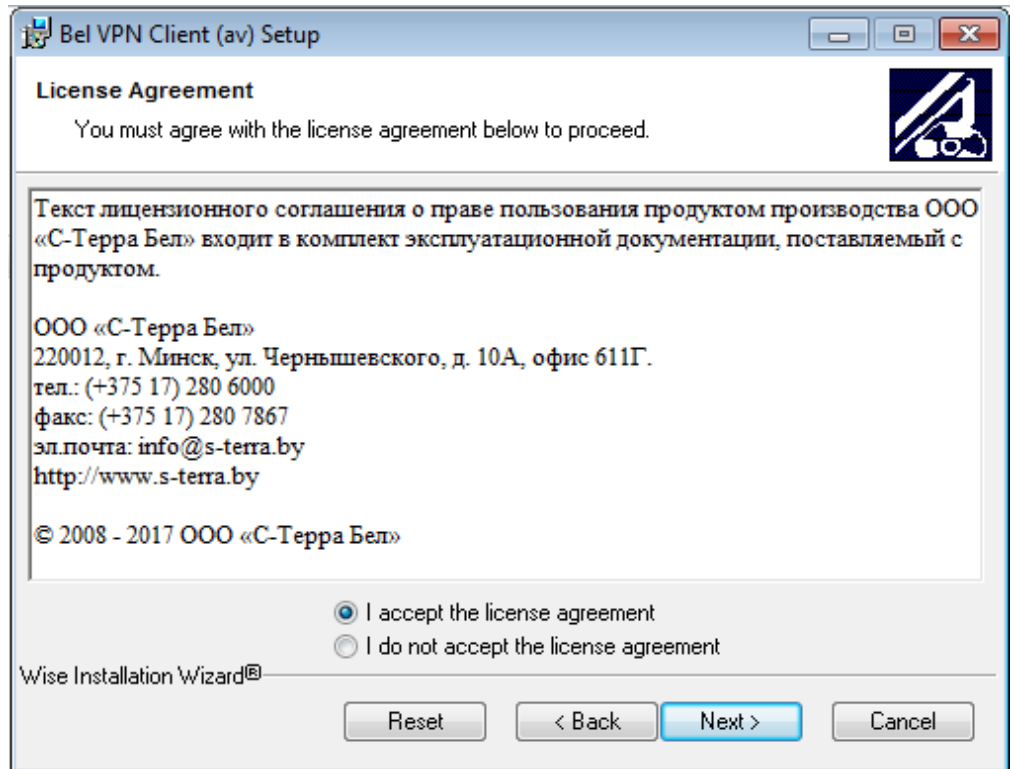


Рисунок 14

7. При необходимости сменить каталог, в который будет установлен Продукт, нажмите кнопку Browse и сделайте выбор:

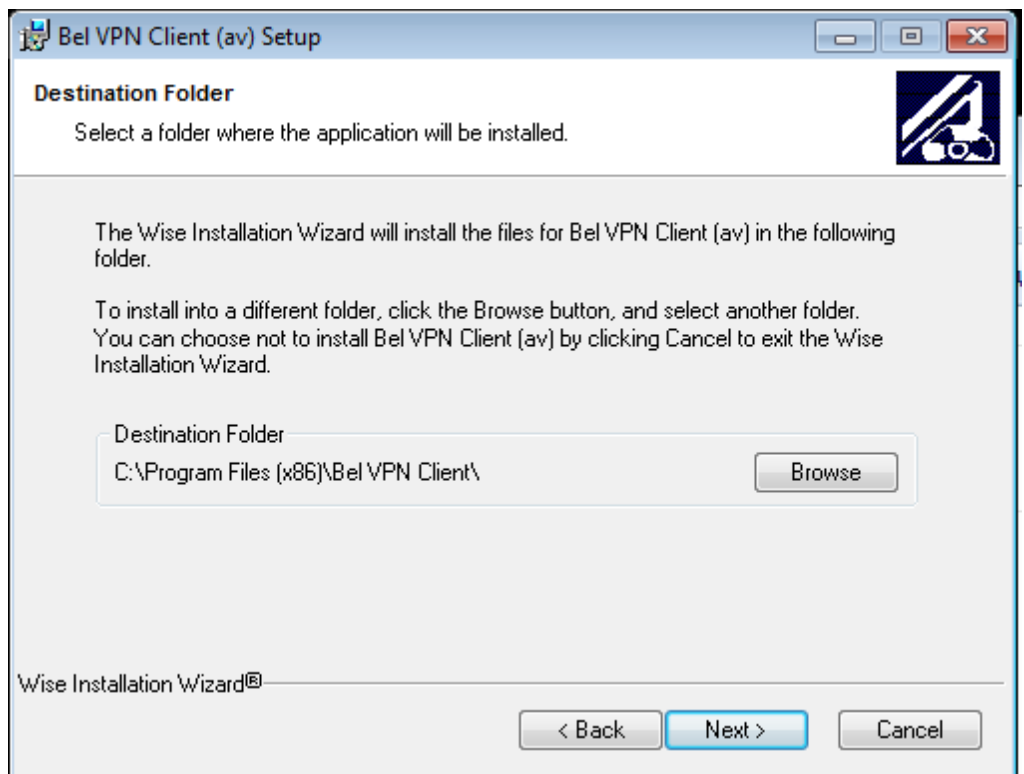


Рисунок 15

8. Если при создании инсталляционного файла был использован ключевой носитель, и регистрационные данные не были включены администратором безопасности в инсталляционный файл, то появится окно для ввода данных для доступа к ключевому носителю на Продукт (Рисунок 16):

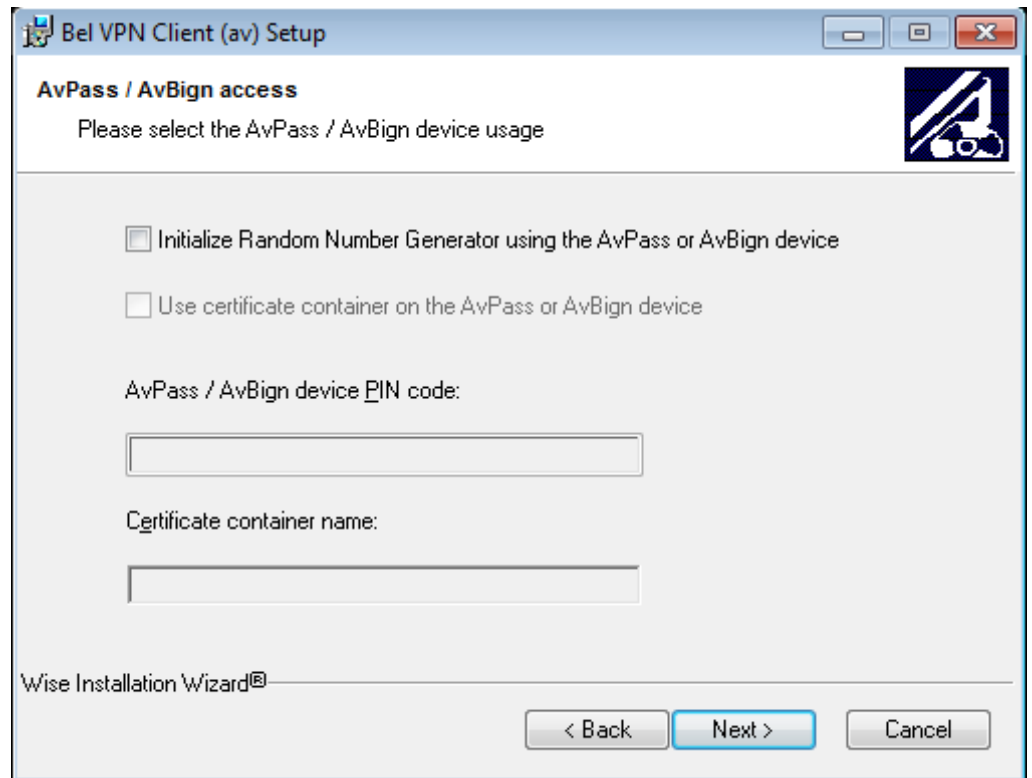


Рисунок 16

9. Стандартное окно визарда сообщает о готовности к инсталляции. Для начала инсталляции нажмите **Next**:

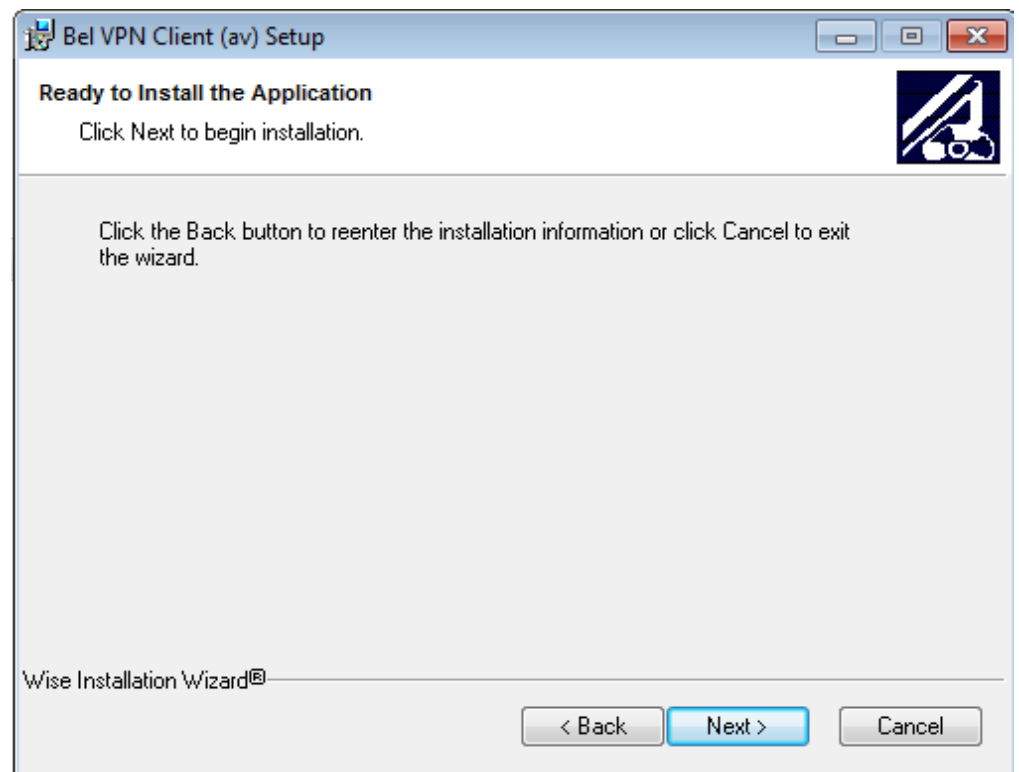


Рисунок 17

10. Далее появляется окно с индикатором процесса инсталляции:

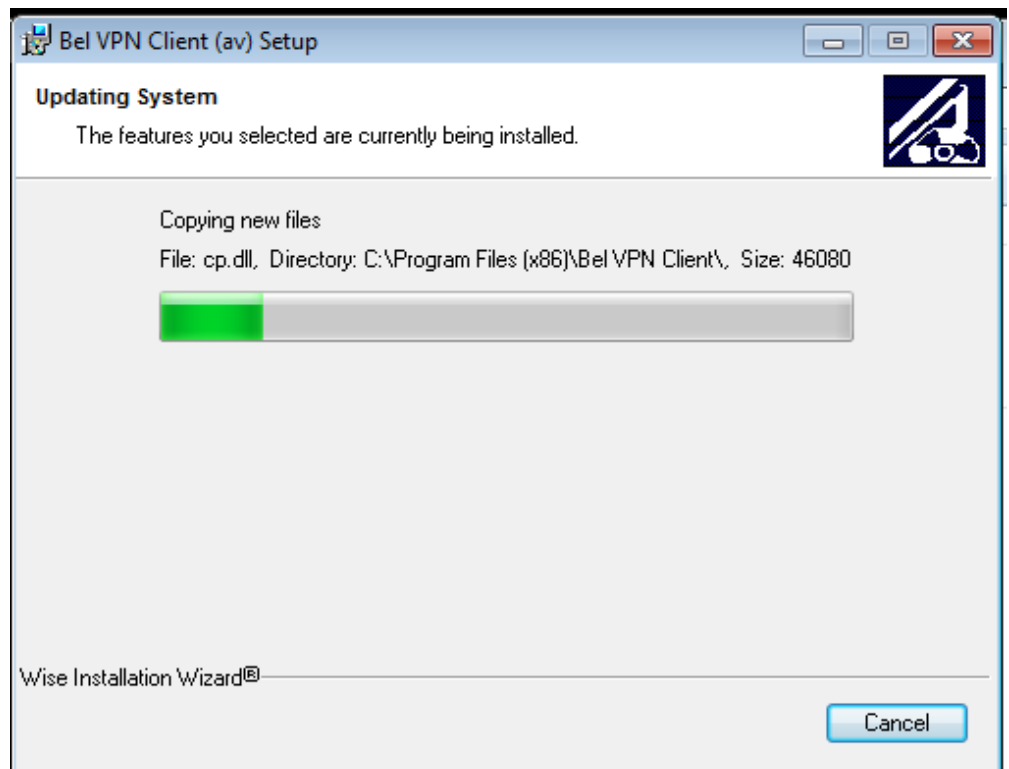


Рисунок 18

11. В случае, если датчик случайных чисел не был инициализирован администратором безопасности при создании инсталляционного пакета, предлагается «биологическая» инициализация ДСЧ – нужно нажимать случайные клавиши до заполнения индикатора (Рисунок 19).

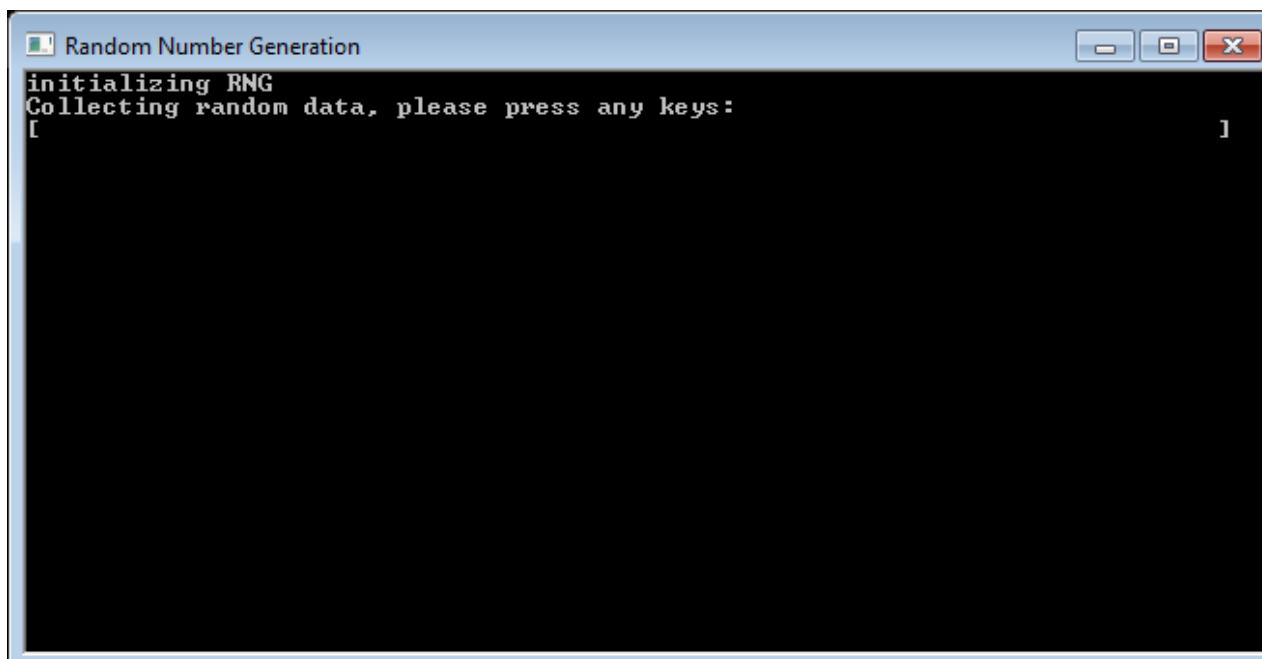


Рисунок 19

12. После завершения процедуры инсталляции нажмите **Finish**:

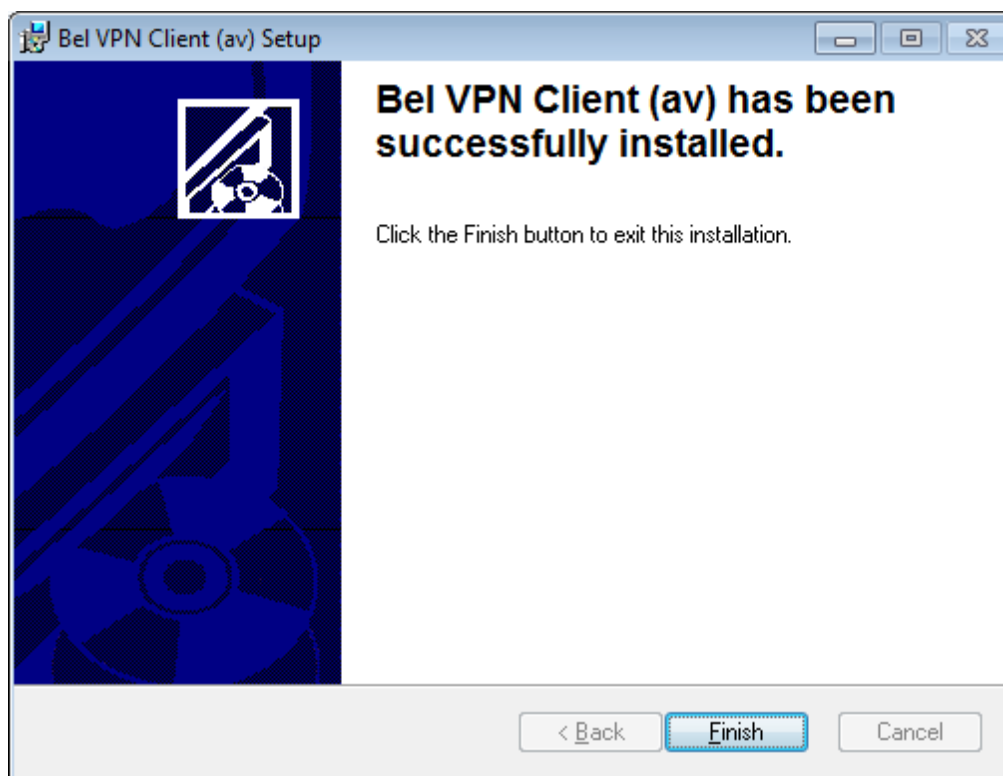


Рисунок 20

13. По окончании установки ПП Bel VPN Client-P в ОС Windows XP появляется окно (Рисунок 21) с предупреждением о необходимости перезагрузки операционной системы. После нажатия кнопки **Yes** происходит перезагрузка операционной системы, а нажатие кнопки **No** закрывает окно без перезагрузки. Для ОС Windows Vista и более поздних версий перезагрузка не требуется, но не исключено, что инсталлятор может запросить перезагрузку, если она будет необходима.

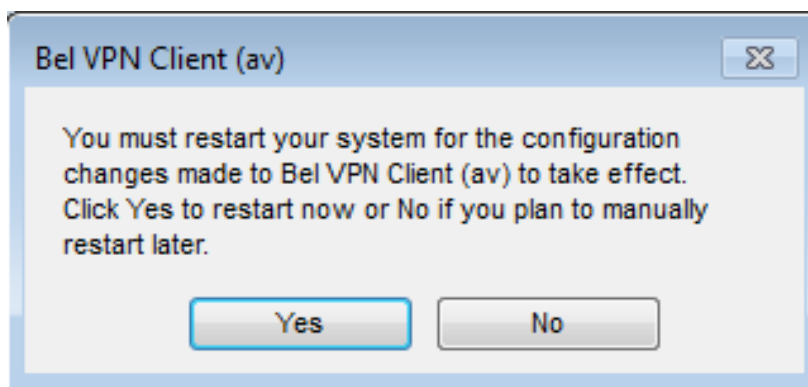


Рисунок 21



Note

Недопустимо удалять из ОС пакет Microsoft Visual C++ 2008 Redistributable Package, отсутствие которого может привести к неработоспособности ПП Bel VPN Client-P

4.3 Режим silent

В режиме silent происходит установка ПП Bel VPN Client-P без запросов, но могут появляться либо системные диалоговые окна, либо некоторые интерактивные компоненты, относящиеся к криптоподсистеме.

В ОС Windows Vista и более поздних версиях, при установке ПП Bel VPN Client-P выдается окно (Рисунок 1) с запросом на доступ к компьютеру. Выберите предложение **Разрешить**.

Далее выполняется распаковка файлов (Рисунок 2).



Рисунок 22

Устанавливается продукт Microsoft Visual C++ 2008 Redistributable Package (Рисунок 23).

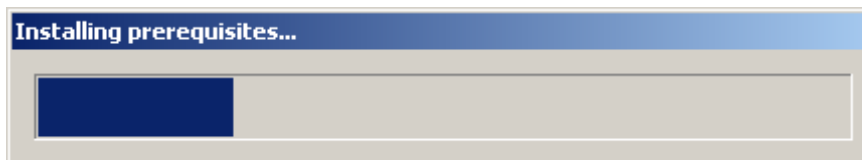


Рисунок 23

Предлагается «биологическая» инициализация ДСЧ – нужно нажимать запрашиваемые клавиши. (Рисунок 24).

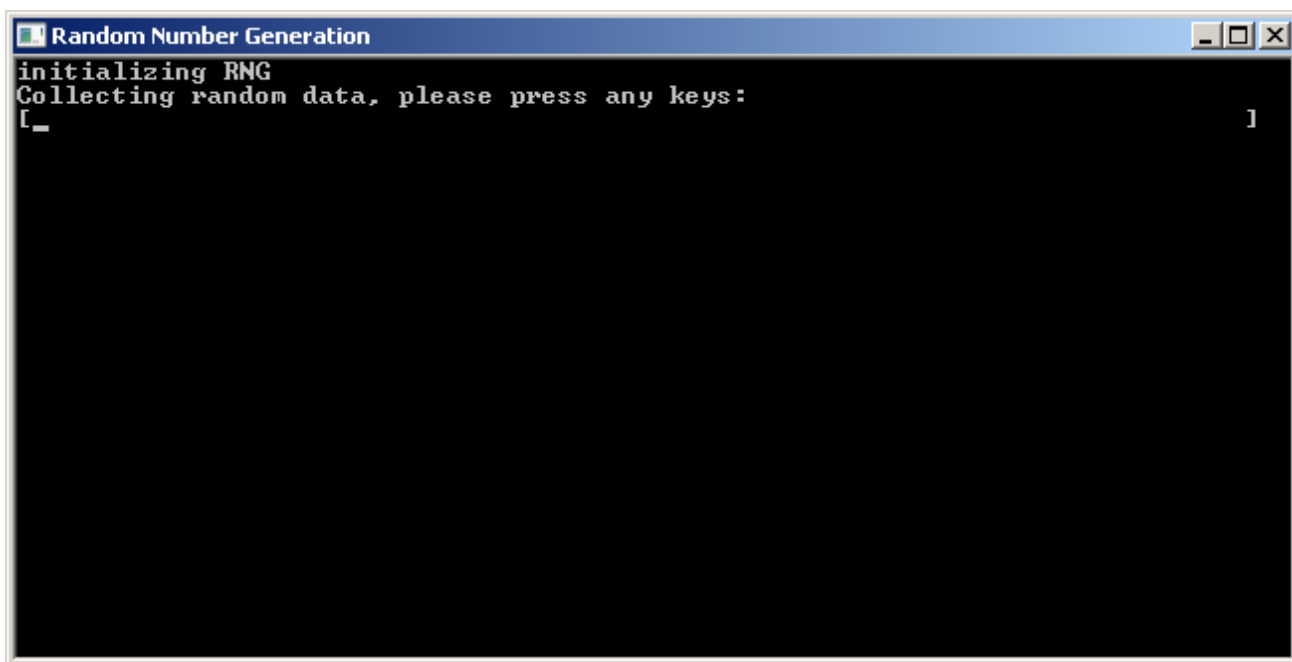


Рисунок 24

Дальнейшее поведение инсталлятора зависит от ОС и установленной пользователем опции Подписывание драйверов, описанной в разделе "[Режим basic](#)".

По окончании установки ПП Bel VPN Client-P в ОС Windows XP происходит перезагрузка операционной системы без предупреждений. Для ОС Windows Vista и более поздних версий перезагрузка не требуется, но не исключено, что инсталлятор может запустить перезагрузку, если она будет необходима.

В случае возникновения ошибок и прерывания инсталляции никакие сообщения на экран не выводятся. Эти сообщения можно посмотреть программой ОС Windows «Просмотр событий» или, если при подготовке инсталляционного пакета администратором была указана опция протоколирования событий при инсталляции в файл, то сообщения можно посмотреть в заданном файле.

Примечание: если при инсталляции будет обнаружена база локальных настроек, оставшаяся от предыдущей установки продукта, то по умолчанию происходит обновление базы локальных настроек кроме тех, которые отсутствуют при новой инсталляции. В некоторых ситуациях это может привести к неработоспособности или некорректной работе продукта (в этом случае рекомендовалось при подготовке инсталляционного файла использовать дополнительный параметр для WinInstaller AGENT_DB_REMOVE=1).



Note

Недопустимо удалять из ОС пакет Microsoft Visual C++ 2008 Redistributable Package, отсутствие которого может привести к неработоспособности ПП Bel VPN Client-P

4.4 Копирование контейнера при инсталляции

Если при подготовке инсталляционного файла с использованием сертификатов было задано копирование контейнера, то такое копирование осуществляется при инсталляции Bel VPN Client. В случае, если копирование происходит в контейнер с именем, который уже существует, то выдается окно следующего вида:

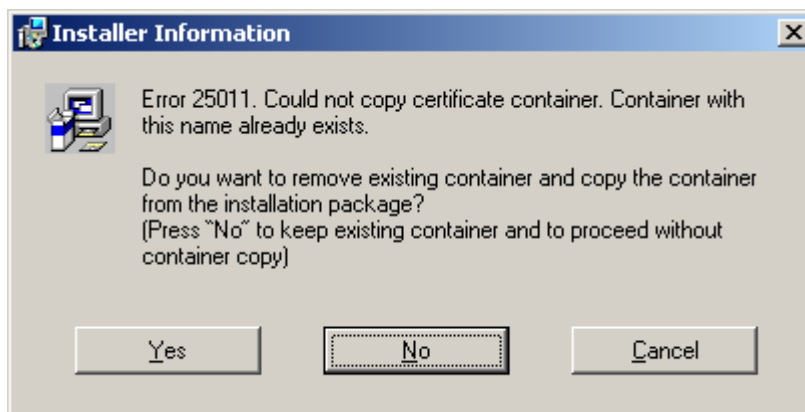


Рисунок 25

Если нажать **Yes**, то существующий контейнер будет удален и процедура копирования будет продолжена. Если нажать **No**, существующий контейнер останется, а процедура копирования будет отменена. Если нажать **Cancel**, то инсталляция клиента будет прервана.

Примечание: если инсталляции происходит в режиме **silent**, и на компьютере пользователя уже существует контейнер с указанным именем, в который происходит копирование, то инсталляция прерывается без выдачи на экран каких-либо запросов пользователю.

4.5 Сообщения об ошибках при инсталляции

Ниже приведены тексты сообщений об ошибках, которые могут появиться при инсталляции ПП Bel VPN Client-P (Таблица 1).

Таблица 1

Код ошибки	Текст сообщения	Примечание
25001	License check failed.	Неправильная лицензия
25004	Delete existing product settings?	Удалить существующие настройки продукта? (вопрос при деинсталляции)
25005	Old product settings found. Delete existing product settings?	Найдены старые настройки продукта. Удалить существующие настройки продукта?
25006	RNG initialization failed. {Reason: <reason>} Installation aborted. {RNG container path: <path>}, где <reason> может быть одним из следующих: a. Random initialization tool returned an error b. You must have Administrator privileges c. Random initialization tool not found d. Random initialization tool can't run: system error e. Random value initialization failed f. Container name generation limit exceeded	Не удалось создать RNG контейнер. {Причина: <reason>}. Инсталляция прервана. Путь к RNG контейнеру: <path> основные причины: a. Утилита для инициализации ДСЧ вернула ошибку b. Вы должны иметь администраторские привилегии c. Утилита для инициализации ДСЧ не найдена d. Не удалось запустить утилиту для инициализации ДСЧ: системная ошибка e. Инициализация ДСЧ не произошла f. Искерпан лимит генерируемых имен контейнера
25009	Copy certificate container failed. {Reason: <reason>} Installation aborted. Source container path: <src>. Destination container path: <dst>	Не удалось скопировать сертификатный контейнер. {Причина: <reason>} Инсталляция прервана. Путь к исходному контейнеру: <src>. Путь к новому контейнеру: <dst>.
25011	Could not copy certificate container. Container with this name already exists. Do you want to remove existing container and copy the container from the installation package? (Press "No" to keep existing container and to proceed without container copy)	Нельзя скопировать сертификатный контейнер, поскольку контейнер с таким именем уже есть. Хотите ли вы удалить существующий контейнер и скопировать контейнер из инсталляционного пакета? (Нажмите "No" для того, чтобы сохранить существующий контейнер и продолжить без копирования)
25018	Product "<Product_name version>" was detected. You should uninstall it first before the installation.	Был обнаружен Продукт "<Product_name version>". Вам необходимо сначала деинсталлировать его.
	This product needs Windows 2000 or higher	Для Продукта необходима Windows 2000 или выше

Код ошибки	Текст сообщения	Примечание
25019	The "<dll_path>" was wrongly marked as the previous GINA DLL. The system GINA DLL will be used instead.	[Windows XP] Файл <dll_path> был ошибочно помечен, как предыдущая GINA DLL. Будет использована системная GINA DLL.
25020	The previous GINA DLL "<dll_path>" was not found. The system GINA DLL will be used instead.	[Windows XP] Предыдущая GINA DLL <dll_path> не найдена. Будет использована системная GINA DLL.
25021	Driver "<driver_name>" installation failed. Product installation aborted.	Не удалось установить драйвер <driver_name>. Инсталляция продукта прервана.
25022	Product "<Product_name version>" was advertised. You should uninstall it first before the installation.	Для продукта <Product_name version> была выполнена операция объявления пользователям (advertisement). Вы должны деинсталлировать его до инсталляции.
25025	Failed to add Windows Firewall rule allowing network traffic for Bel VPN Service. If you intend to use Windows Firewall or other firewall, you should manually configure it to allow network traffic for Bel VPN Service.	Не удалось добавить правило Брандмауэра Windows открывающее сетевой трафик для VPN сервиса. Если Вы собираетесь использовать Брандмауэр Windows или другой firewall, вы должны настроить его вручную, чтобы пропустить сетевой трафик для VPN сервиса. Рекомендации по ручной настройке Брандмауэра Windows даны в разделе «Рекомендации по ручной настройке Брандмауэра Windows» .
25026	You must have administrator privileges.	Вам необходимы администраторские привилегии.
25028	Import of certificate container failed Installation aborted. Source file path: <src_file_path> Destination container path: <dst_cont_name> <src_file_path> – путь к файлу <dst_cont_name> – имя контейнера	Не удалось импортировать контейнер из файла.
25029	Could not import certificate container. Container with this name already exists. Do you want to remove existing container and import the container from the installation package?	Нельзя импортировать контейнер из файла, поскольку контейнер с таким именем уже есть. Хотите ли вы удалить существующий контейнер и импортировать контейнер из инсталляционного пакета? (Нажмите "No")

Код ошибки	Текст сообщения	Примечание
	(Press "No" to keep existing container and to proceed without container import)	для того, чтобы сохранить существующий контейнер и продолжить без импорта).
25030	Could not copy or import certificate container. { Reason: <reason>} <reason> – один из следующих: a. Unknown operation (should be 'copy' or 'import') b. Internal error	Не удалось скопировать контейнер или импортировать контейнер из файла. Reason: <reason>} <reason> – один из следующих: a. Неизвестная операция (должна быть 'copy' или 'import') b. Внутренняя ошибка
25031	Could not remove the existing container. Installation aborted. Existing container name: <cont_name> <cont_name> – имя контейнера, который не удалось удалить	Не удалось удалить существующий контейнер (примечание: после ответа "Yes" на вопрос [25011] или [25029])
25033	The Visual C++ Redistributable Package is absent or damaged	Visual C++ Redistributable Package отсутствует или поврежден
25034	RNG initialization was canceled. Do you want to retry RNG initialization (press "No" to cancel the installation)?	Инициализация RNG была прервана пользователем. Вы хотите повторить инициализацию RNG (нажмите "No" для прерывания инсталляции)?
25036	Please disable any anti-virus software during the installation Press "OK" if anti-virus is disabled or not installed Press "Cancel" to cancel the installation	Пожалуйста, отключите любую антивирусную программу на время инсталляции Нажмите "OK" если антивирус отключен или не установлен Нажмите "Cancel" для отмены инсталляции Примечание: появление данного сообщения может быть отключено, если установить параметр инсталляции DISABLE_ANTIVIRUS_WARNING=1

5 Дополнительные настройки

5.1 Обеспечение работоспособности VPN сервиса

Для обеспечения работоспособности VPN сервиса необходимо:

1. отключить службу «Брандмауэр Windows/Общий доступ к Интернету (ICS)» для ОС Windows XP и Windows Server 2003 или, для более поздних версий Windows, отключить службу «Общий доступ к подключению к Интернету (ICS)»
2. либо
3. в свойствах интерфейса, участвующего в построении защищенного соединения, во вкладке «Доступ» сбросить флажок «Разрешить другим пользователям сети использовать подключение к Интернету данного компьютера».

5.2 Настройка переменных окружения

Имеется возможность настроить некоторые переменные окружения, которые могут повлиять на работу ПП Bel VPN Client-P или дать возможность получить дополнительную информацию в лог-файле.

Чтобы присвоить значение переменным окружения выполните следующие действия:

1. Панель Управления → Система → Дополнительно (Дополнительные параметры системы) → Переменные среды;
2. В окне Переменные среды перейдите в область Системные переменные и нажмите кнопку Создать.
3. Введите Имя переменной и Значение переменной.
4. Перезагрузите компьютер.

5.2.1 Описание переменных окружения

CSP_SYS_RESPONSE_TIMEOUT – задает максимальное время (в секундах), на которое wrp-демон может "подвиснуть" перед тем как аварийно закончить свою работу. "Подвисание" – состояние, когда ни одна из рабочих нитей не может взяться за выполнение задания. По достижении указанного времени wrp-демон сам аварийно завершает свою работу и создает соге-файл.

Механизм слежения за зависанием wrp-демона позволяет завершить работу неработоспособного демона и запустить новую сессию, тем самым повысив отказоустойчивость системы.

Если CSP_SYS_RESPONSE_TIMEOUT = 0, то механизм слежения за зависанием wrp-демона не включается.

Переменные окружения CSP_LOG_TASK_TIME и CSP_LOG_TASK_QUEUE_PERIOD используются службой поддержки для диагностики различных ситуаций. Обе переменные задают время, по истечении которого в файл лога выдаются сообщения. CSP_LOG_TASK_QUEUE_PERIOD выдает сообщения уровня info, CSP_LOG_TASK_TIME выдает сообщения уровня warning.

CSP_LOG_TASK_TIME – задает время (в секундах), которое должно быть затрачено на выполнение одной задачи. При превышении заданного времени в файл лога будет выдаваться сообщение о большем затраченном времени на выполнение одной задачи:

```
Event Manager profiler: task time is <n> sec (src=<hex> dst=<hex> idx=<n> proc=<hex>)
```

Если CSP_LOG_TASK_TIME = 0, то сообщение в файл лога не выводится.

CSP_LOG_TASK_QUEUE_PERIOD – задает период (в секундах), с которым в файл лога будут выдаваться сообщения о времени ожидания задачи в очереди и длине очереди задач. Сообщения выводятся следующего вида:

```
Event Manager profiler: waiting time of task queue is <n> sec, queue length is <n> tasks
```

Если CSP_LOG_TASK_QUEUE_PERIOD = 0, то сообщения в файл лога не выводятся.

5.3 Рекомендации по ручной настройке Брандмауэра Windows

Рекомендации по ручной настройке брандмауэра Microsoft Windows приведены в документе «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1». Подготовительные процедуры».

6 Регистрация пользователя

При подготовке инсталляционного пакета устанавливается интерактивный или неинтерактивный режим логина пользователя в Продукт.

6.1 Интерактивный режим логина в Продукт

6.1.1 Особенности регистрации для различных ОС

Windows XP

В ОС Windows XP после перезагрузки ОС при интерактивном режиме появляется окно логина (Рисунок 26) в Продукт для ввода и изменения пароля пользователя. По умолчанию пароль является пустым.

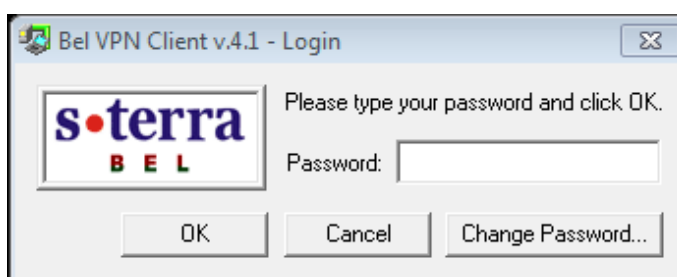


Рисунок 26

При нажатии на кнопку *Change Password* откроется окно, в котором можно изменить пароль пользователя (Рисунок 27):

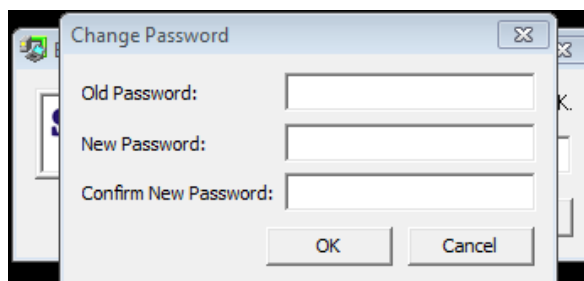


Рисунок 27

Для смены пароля необходимо ввести старый пароль и новый с подтверждением правильности нового пароля. Если старый пароль вводится трижды неправильно, то каждая последующая попытка ввода пароля будет прерываться паузой на полминуты.

Окно логина в Продукт (Рисунок 27) будет выводиться только при запущенном VPN-сервисе. Если к моменту вывода окна ОС Windows еще не запустила VPN-сервис, то Продукт будет ждать 30 секунд (по умолчанию). Если VPN-сервис не будет запущен и через 30 секунд, то появится сообщение с предложением повторить процесс логина (Рисунок 28). Чтобы данное окно не появлялось – увеличьте время инициализации сервиса (см. раздел. [«Время инициализации VPN сервиса»](#)).

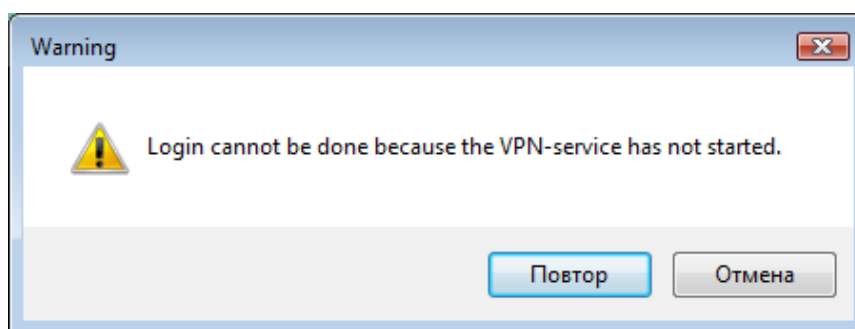


Рисунок 28

Окно логина в ОС Windows XP появляется только после регистрации пользователя в Продукте или отказе от нее.

Windows Vista и более поздние версии ОС

После перезагрузки ОС при интерактивном режиме логина на экран выводятся иконки для выбора пользователя, текущего статуса ПП Bel VPN Client-P и окно логина в Продукт.

Процессы входа в ОС и логина в Продукт независимы друг от друга. Можно сначала зарегистрироваться в Продукте, а потом войти в ОС или наоборот.

В окне выбора пользователя иконка, отображающая текущий статус Продукта, может быть смещена в нужном направлении, если ее положение неудобно (см. раздел [«Изменение положения иконки текущего статуса Продукта»](#)).

Окно логина в Продукт появляется только после инициализации VPN сервиса. Если к моменту вывода окна VPN сервис не будет готов к работе, то Продукт будет ждать 30 секунд (время по умолчанию) (см. раздел [«Время инициализации VPN сервиса»](#)). Если VPN сервис не будет готов к работе и через 30 секунд, то появится сообщение с предложением повторить процесс логина (Рисунок 28).

Окно логина в Продукт автоматически появляется в интерактивном режиме, когда необходимо выбрать пользователя для входа в ОС Windows:

- после загрузки системы
- при выходе пользователя из системы
- при смене пользователя.

6.1.2 Успешная регистрация

После успешной регистрации пользователя в Продукт загружается локальная политика безопасности, предписанная данному пользователю и находящаяся в базе Продукта.

После входа пользователя в ОС иконка статуса Продукта будет размещена в панели задач и изменит свой вид (Рисунок 29) (см. главу [«Отображение текущего статуса Продукта»](#)):



Рисунок 29

Если отказаться от логина пользователя в Продукт, то потом зарегистрироваться в Продукте можно:

- нажав на иконку статуса Продукта в окне выбора пользователя, и в выпадающем меню выбрать предложение *Login* (Рисунок 30)

- либо после входа в ОС, нажав на иконку статуса Продукта в панели задач (см. раздел “Login/Logout”).

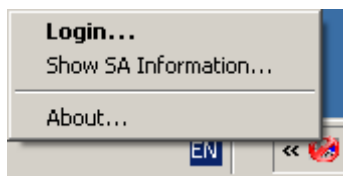


Рисунок 30

6.1.3 Неуспешная регистрация

Специальная политика безопасности **Log-off policy**, задаваемая администратором при подготовке инсталляционного пакета, служит для безопасности работы пользователя, при которой клиент не может создавать защищенных соединений, и загружается автоматически в следующих случаях:

- до тех пор, пока пользователь не ввел свой пароль,
- при вводе неверного пароля три раза,
- при отказе от регистрации (login), если нажать кнопку *Cancel*,
- при выходе пользователя из системы,
- при смене пользователя,
- при отключении пользовательского токена.

Политика **Log-off policy** работает по одному из двух правил:

- `PassDHCP` – пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для настройки TCP/IP стека по протоколу DHCP.
- `Default Driver Policy (DDP)` – политика драйвера по умолчанию, может принимать значения:
 - правило `Passall` – пропускать все пакеты. Значение по умолчанию.
 - правило `PassDHCP` – пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для настройки TCP/IP стека по протоколу DHCP.
 - правило `Dropall` – не пропускать трафик.

Политика **Default Driver Policy (DDP)**, задаваемая администратором, загружается в следующих случаях:

- при ошибочной загрузке конфигурации,
- до старта VPN сервиса,
- при остановке VPN сервиса.

6.2 Неинтерактивный режим логина в Продукт

При неинтерактивном режиме логина в Продукт автоматически производится попытка логина с пустым паролем (в качестве пароля используется пустая строка) и при успешном логине окно с запросом пароля не появляется. При неуспешном логине Продукт ведет себя как при интерактивном логине – будет выдано окно запроса пароля (Рисунок 27).

При установленном ПП Bel VPN Client-P можно изменить интерактивный режим логина на неинтерактивный. Включение неинтерактивного режима осуществляется присвоением значения, отличного от 0, переменной в реестре `NonInteractiveLogin`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VPN Agent\NonInteractiveLogin.
```

При работе продукта под управлением ОС Windows 7 x64 для переключения в неинтерактивный режим следующим переменным надо присвоить значение 1:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VPN Agent\NonInteractiveLogin
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\VPN Agent\NonInteractiveLogin
```

При значении 0 – будет включен интерактивный режим (значение по умолчанию).

6.3 Время инициализации VPN сервиса

Можно задать время инициализации VPN сервиса в реестре при помощи переменной `MaxServiceStartTimeout`:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VPN Agent\MaxServiceStartTimeout
```

Эта переменная задает время в секундах ожидания запуска VPN сервиса. Если эта переменная не задана, то принимается значение по умолчанию, равное 30 секундам. Максимальное значение, которое можно задать – 600 секунд. При задании большего значения – устанавливается значение в 600 секунд.

При старте vpn-сервиса выполняется стартовый контроль целостности установленного Продукта Bel VPN Client, описанный в разделе [«Стартовый и регламентный контроль целостности продукта»](#).

6.4 Неинтерактивный режим логина в ОС

При интерактивном/неинтерактивном режиме логина в ПП Bel VPN Client-P для автоматического входа пользователя в ОС Windows (не появляется окно Log On to Windows) необходимо выполнить дополнительные настройки. Конкретную информацию о настройках для определенной ОС Windows можно получить на сайте Microsoft.

6.5 Замечание

Время загрузки ОС Windows XP с продуктом ПП Bel VPN Client-P зависит от нескольких факторов, в том числе:

- аппаратной платформы (CPU, объема памяти, диска),
- количества и качества установленного программного обеспечения,
- степени фрагментации жесткого диска,
- количества накопленного «информационного мусора» в реестре.

Установленный на компьютер ПП Bel VPN Client-P позволяет создавать защищенное соединение до логина пользователя в ОС Windows XP, но для этого пользователь должен пройти дополнительную аутентификацию (окно регистрации в продукт) перед логином в ОС.

Сервис аутентификации дожидается запуска всех пользовательских сервисов и запуска Bel VPN Client. Для давно эксплуатирующейся системы, где установлено много приложений, время загрузки сервисов значительно возрастает. На компьютерах с небольшим объемом памяти процесс загрузки сервисов еще увеличивается, поскольку системе не хватает памяти, и она начинает выгружать только что загруженные приложения в swp файл на диск.

Ожидание появления дополнительного окна аутентификации может расцениваться пользователем как запуск конкретного приложения Bel VPN Client, а не запуск всех приложений ОС. Пользователю кажется, что загрузка ОС становится значительно дольше, хотя объективные замеры с секундомером доказывают обратное.

Чтобы избежать описанной выше ситуации рекомендуется выполнить некоторые действия:

- удалить неиспользуемые приложения, запускающиеся в процессе загрузки Windows,
- выполнить чистку и дефрагментацию реестра,
- выполнить дефрагментацию жесткого диска.

7 Стартовый и регламентный контроль целостности Продукта

7.1 Программная часть Продукта

При старте сервиса `vpnsvc` автоматически запускается утилита `cspvpn_verify` для проверки целостности программной части (неизменяемых файлов) установленного Продукта, перечисленных в файле `.hashes`.

При успешной проверке никакого сообщения на экран не выдается, а в файл `cspvpn_verify_err.log`, расположенный в каталоге Продукта, передается сообщение: `Verification SUCCESS: <n> files verified.`

При обнаружении ошибки работа утилиты прерывается и выдается сообщение об ошибке в файл `cspvpn_verify_err.log`.

Файл `.hashes` расположен в каталоге Продукта (по умолчанию – `Program Files\Bel VPN Client`) и содержит строки вида (между хэш-суммой и именем файла один пробел):

```
<hash> <encoded_file_path>
```

где

`<hash>` – эталонное значение хэш-суммы для данного файла

`<encoded_file_path>` – полный путь к проверяемому файлу

Регламентный контроль целостности ПП Bel VPN Client-P осуществляется во время работы Продукта запуском вручную утилиты `cspvpn_verify` из каталога установленного Продукта.

При успешной проверке и при обнаружении ошибки реакция будет такой же как и при стартовом контроле.

Возможные сообщения об ошибках

Таблица 2

Код ошибки	Сообщение об ошибке	Описание проблемы	Код возврата	Продолжение работы утилиты
1	Integrity verification tool not found	Отсутствует продукт, используемый непосредственно для подсчета контрольных сумм.	1	
2	Integrity verification list " <code><file_.hashes_full_path></code> " not found	Отсутствует файл <code>.hashes</code> .	2	
3	Integrity verification list " <code><file_.hashes_full_path></code> " is corrupted	Проблемы с чтением файла <code>.hashes</code> (например, ошибочный синтаксис файла).	3	

Код ошибки	Сообщение об ошибке	Описание проблемы	Код возврата	Продолжение работы утилиты
4	Integrity verification tool call failed on file “<product_file_full_path>”	Запуск <code>avverify</code> по каким-либо причинам не произошел (какая-то системная ошибка; например, нехватка ресурсов, проблемы с правами доступа и т.п.) или вернул неожиданный код возврата (прерывание по сигналу, необработанный exception и т.п.).	4	Утилита продолжает работать
5	File “<product_file_full_path>” is corrupted	Один или больше файлов продукта повреждены (хэш-сумма не соответствует эталонной; также возможны и другие ситуации – например, отсутствующий файл – <code>avverify</code> их не различает).	5	Утилита продолжает работать

где

<file_.hashes_full_path> – полный путь к файлу `.hashes`

<product_file_full_path> – полный путь к файлу Продукта, на котором произошла ошибка.

При обнаружении ошибки по окончании работы утилиты выдается сообщение: `Verification FAILED`. Затем проверяется сервис `vpnsvc` и, если он работает, то выполняется его аварийное прерывание.

Если обнаруживается несколько разнородных ошибок, то код возврата утилиты формируется по первому сообщению об ошибке.

При устранении ошибки перезапустите сервис `vpnsvc`:

```
net start vpnsvc
```

7.2 Информационная часть Продукта

Регламентная проверка целостности информационной части Продукта осуществляется при помощи утилиты `integr_mgr check`, описанной в разделе «Специализированные команды».

8 Отображение текущего статуса Продукта

Текущий статус Продукта отображает иконка, расположенная в панели задач.

Если пользователь не аутентифицировался, то иконка имеет вид:



Рисунок 31

Пользователь аутентифицировался, но Продукт не имеет ни одного защищенного соединения – иконка принимает вид:



Рисунок 32

Когда появляется хотя бы одно защищенное соединение, но трафик по этим соединениям отсутствует, то на иконке изменяется цвет "соединения" с серого на зеленый:



Рисунок 33

Если Продукт имеет хотя бы одно защищенное соединение и обрабатывает трафик по этим соединениям, то на иконке изменяется цвет "монитора" с синего на бирюзовый:



Рисунок 34

При наведении курсора мыши на иконку всплывает информация о количестве "живых" SA (существующих на момент наведения курсора мыши на иконку) и количестве байт обработанного трафика по всем существовавшим и существующим SA с момента загрузки операционной системы.



Рисунок 35

8.1 Изменение положения иконки текущего статуса Продукта

Положение иконки, отображающей текущий статус Продукта в окне выбора пользователя, если оно неудобно, можно изменить с помощью переменной в реестре:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\LAP Providers\{7026F7B9-3C2E-4b80-A62E-69645BFF1190}\Position

Значением переменной `Position` является строка формата:

`<int_x>,<int_y>`

где

`int_x` – целое число, задающее смещение иконки по горизонтальной оси, которое может принимать значения:

- 0 – положение иконки задается автоматически с учетом разных параметров,
- положит.знач. – положение иконки отсчитывается относительно левой стороны экрана,
- отрицат.знач. – положение иконки отсчитывается относительно правой стороны экрана.

`int_y` – целое число, задающее смещение иконки по вертикальной оси, которое может принимать значения:

- 0 – положение иконки задается автоматически с учетом разных параметров,
- положит.знач. – положение иконки отсчитывается относительно верхней стороны экрана,
- отрицат.знач. – положение иконки отсчитывается относительно нижней стороны экрана.

8.2 Login/Logout

При нажатии на иконку правой кнопкой мыши открывается меню следующего вида:

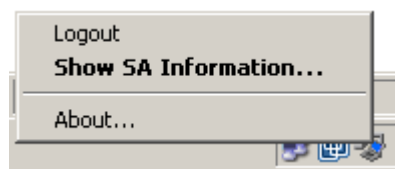


Рисунок 36

В зависимости от состояния системы (аутентифицировался пользователь или нет) будет показано предложение Login или Logout.

При выборе предложения Login появится окно ввода пароля (Рисунок 27) для аутентификации пользователя и изменения пароля.

При выборе предложения Logout выполнится следующее:

- будут уничтожены все существующие SA с данным клиентом,
- загрузится [специальная политика Log-off policy](#),
- предложение Logout изменится на Login.

8.3 SA Information

При выборе предложения Show SA Information – появится окно монитора созданных SA:

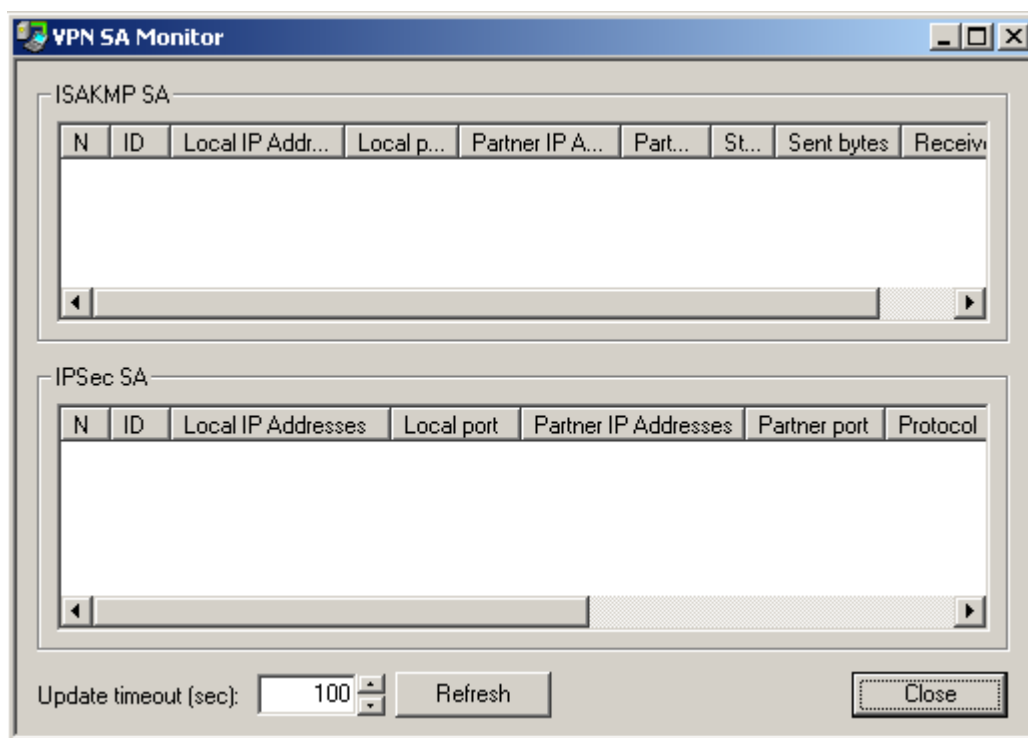


Рисунок 37

Описание полей

ISAKMP SA – список ISAKMP SA. Выводятся следующие поля:

- N – порядковый номер в таблице
- ID – уникальный номер SA
- Local IP Addresses – локальные адреса
- Local port – локальный IKE порт
- Partner IP Addresses – партнерские адреса
- Partner port – партнерский IKE порт
- State – состояние SA:
 - incomplete – недостроенный
 - ready – рабочий
 - configuration – изменяемый
 - deletion – удаляемый
 - unknown – неизвестное состояние (не должно выводиться)
- Sent bytes – количество отосланных байт
- Received bytes – количество полученных байт

IPSec SA – список IPsec SA с полями:

- N – порядковый номер в таблице
- ID – уникальный номер SA
- Local IP Addresses – локальные адреса
- Local port – локальные порты
- Partner IP Addresses – партнерские адреса

- Partner port - партнерские порты
- Protocol - сетевые протоколы
- Action - тип действия:
 - AH
 - ESP
 - AH+ESP
- Type - тип соединения:
 - transport - транспортный режим
 - tunnel - туннельный режим
 - nat-t-transport - транспортный режим через NAT
 - nat-t-tunnel - туннельный режим через NAT
- Sent bytes - количество отосланных байт
- Received bytes - количество полученных байт

Update timeout (sec) – время, через которое будут обновляться данные в таблице о созданных SA. Диапазон значений 1..9999, начальное значение – 2 секунды.

При выборе предложения **About** в меню выводится информация о версии Продукта:



Рисунок 38

9 Удаление ПП Bel VPN Client-P

Удаление ПП Bel VPN Client-P производится стандартными средствами операционной системы – вызовом модуля Add/Remove Programs и выбором из списка строки Bel VPN Client.

При деинсталляции ПП Bel VPN Client-P происходит включение стандартного сервиса, связанного с IPsec и IKE. В ОС Windows XP и ОС Windows Server 2003 – это Служба IPSEC, в ОС Windows Vista и более поздних версиях – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности».

При деинсталляции ПП Bel VPN Client-P может появиться окно (Рисунок 39). Необходимо разрешить запуск деинсталлятора.

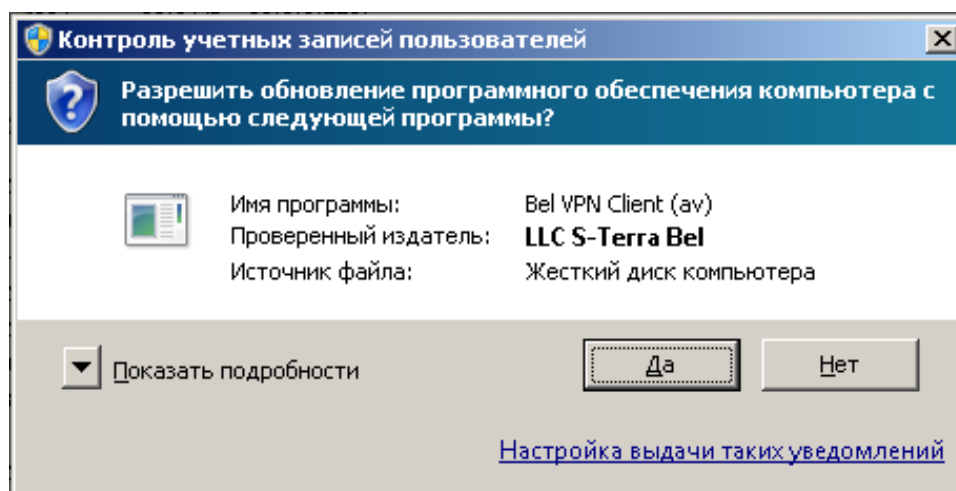


Рисунок 39

Примечание: не рекомендуется деинсталлировать ПП Bel VPN Client-P после выхода из спящего режима или режима гибернации. В этом случае сначала следует перезагрузить компьютер.

В процессе деинсталляции будет выведен запрос об удалении имеющихся настроек ПП Bel VPN Client-P (Рисунок 40). Следует выбрать вариант «Yes».

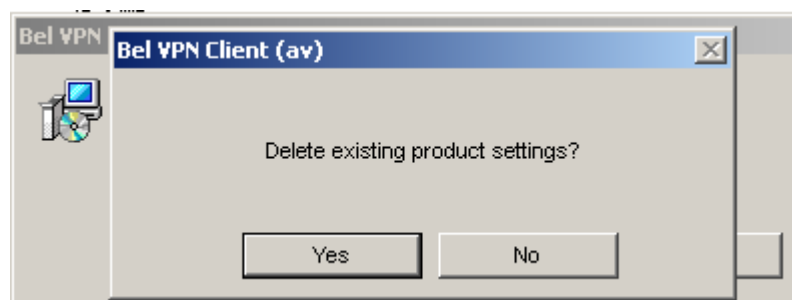


Рисунок 40

По окончании процесса деинсталляции возможно появление запрос о перезагрузке ОС ([рисунок 41]).

10 Восстановление ПП Bel VPN Client-P

Во внештатных ситуациях – сбой в работе Продукта, зависание Продукта и др. перезагрузите LSP конфигурацию командой `lsp_reload` (если это возможно) или перезапустите компьютер. Если функции продукта не восстановились, то переустановите Bel VPN Client.

11 Специализированные команды

Программные утилиты, входящие в состав Продукта Bel VPN Client:

<code>cert_mgr show</code>	для просмотра сертификатов, размещенных в файле или базе Продукта;
<code>cert_mgr check</code>	для проверки сертификатов в базе Продукта;
<code>cert_mgr import</code>	для регистрации промежуточных CA сертификатов и сертификатов партнеров в базе Продукта;
<code>cert_mgr remove</code>	для удаления сертификатов из базы Продукта;
<code>client_login</code>	для аутентификации пользователя при входе в систему;
<code>client_logout</code>	для завершения сессии пользователя;
<code>csppvpn_verify</code>	для регламентной проверки целостности установленного Продукта;
<code>dp_mgr show</code>	для просмотра настроек политики Default Driver Policy;
<code>dp_mgr set</code>	для настройки параметров Default Driver Policy;
<code>drv_mgr</code>	показывает список поддерживаемых настроек IPsec-драйвера;
<code>drv_mgr show</code>	для просмотра настроек IPsec-драйвера;
<code>drv_mgr set</code>	для изменения настроек IPsec-драйвера;
<code>drv_mgr reload</code>	для загрузки настроек IPsec-драйвера;
<code>fwconn_show</code>	для просмотра информации о TCP-соединениях;
<code>if_show</code>	для просмотра параметров сетевых интерфейсов, как защищаемых, так и не контролируемых Продуктом;
<code>integr_mgr calc</code>	для вычисления хэш-суммы указанного файла;
<code>integr_mgr check</code>	для проверки целостности информационной части Продукта;
<code>key_mgr import</code>	для импорта предопределенных ключей в базу Продукта;
<code>key_mgr remove</code>	для удаления предопределенных ключей из базы Продукта;
<code>key_mgr show</code>	для просмотра предопределенных ключей, зарегистрированных в Продукте;
<code>key_mgr list</code>	для просмотра имен предопределенных ключей, зарегистрированных в Продукте;
<code>klogview</code>	для просмотра сообщений, выдаваемых системой протоколирования IPsec-драйвера;
<code>lic_mgr show</code>	для просмотра текущей лицензии на Продукт;
<code>lic_mgr set</code>	для установки лицензии на Продукт;
<code>log_mgr show</code>	для просмотра общего уровня протоколирования всех событий, уровня протоколирования групп событий и настроек syslog-клиента;
<code>log_mgr set</code>	для настроек протоколирования;
<code>lsp_mgr check</code>	для проверки LSP конфигурации;

<code>lsp_mgr load</code>	для для загрузки конфигурации из файла в базу Продукта;
<code>lsp_mgr reload</code>	для перезагрузки LSP конфигурации;
<code>lsp_mgr unload</code>	для выгрузки LSP конфигурации и загрузки политики DDP;
<code>lsp_mgr show</code>	для просмотра LSP;
<code>lsp_mgr show-info</code>	для просмотра информации о LSP;
<code>pwd_change</code>	для изменения пароля пользователя;
<code>rnd_mgr</code>	для генерации начального значения ДСЧ;
<code>sa_mgr show</code>	для просмотра информации обо всех IPsec SA и ISAKMP SA;
<code>sa_mgr clear</code>	для удаления ISAKMP и IPsec соединений;
<code>ver_show</code>	для получения информации о Продукте.

В операционной системе Microsoft® Windows выполнение этих команд можно производить из командной строки. Для запуска утилиты из командной строки перейдите в папку, в которой находится утилита: `C:\Programs Files\Bel VPN Client`.

Запуск утилит с ключом `-h` вызывает помощь.

Все утилиты, обращающиеся к `vrpnsvc` сервису, имеют опцию `-T <timeout>`, устанавливающую максимальное время ожидания ответа от `vrpnsvc` сервиса. Опция глобальная и распознается только в начале списка опций утилиты. Например, команда `sa_mgr -T 0 show` – корректная, а `sa_mgr show -T 0` – нет.

Количество одновременно обрабатываемых запросов от утилит `vrpnsvc` сервисом не больше 3. При превышении лимита запросы отвергаются, и утилита выдает диагностику “DAEMON BUSY NOW”. Повторить запуск утилиты можно после того, как хотя бы одна из таких утилит завершит работу.

Ограничения на работу с утилитами

Для работы с некоторыми утилитами необходимо выполнение двух условий:

- Пользователь должен иметь права Администратора.

Начиная с ОС Windows Vista консольное окно “cmd”, из которого выполняются такие утилиты, должно быть запущено с помощью пункта “Запуск от имени администратора” (Run As Administrator).

Если это условие не выполнено, пользователю будет выдано сообщение: `Error: You need Administrator permissions.`

- Пользователь должен иметь право на изменение настроек Продукта

Эта возможность локального управления Продуктом задается администратором при подготовке инсталляционного пакета пользователя. Если это условие не выполнено, пользователю будет выдано сообщение: `Error: Local management is not allowed.`

11.1 cert_mgr show

Команда **cert_mgr show** предназначена для просмотра сертификатов, лежащих в файле или базе Продукта.

Синтаксис

```
cert_mgr [-T timeout] show [-f C_FILE [-p C_FILE_PWD]] [-i OBJ_INDEX1]...[-i OBJ_INDEXN] [-expired_remote]
```

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-f C_FILE	путь к файлу с сертификатами. Если данная опция не указана, то будут показаны сертификаты из базы Продукта.
-p C_FILE_PWD	пароль к файлу с сертификатами. Необязательный параметр. Используется только для доступа к файлам, защищенным паролем.
-i OBJ_INDEXN	индекс объекта (сертификата) в файле или базе Продукта. Если при написании команды указан путь к файлу, то индекс будет задавать номер искомого сертификата в файле. Если путь к файлу не указан, то индекс будет применяться к базе Продукта. Индекс задается в виде целого десятичного числа. В качестве индекса нельзя указывать 0.
-expired_remote	показать все сертификаты партнеров, срок действия которых истек. Сертификаты, не вступившие в силу, не показываются.

Значение по умолчанию значение по умолчанию отсутствует

Рекомендации по использованию

Используйте данную команду для просмотра списка сертификатов и CRL, размещенных в файле или базе Продукта. Без указания файла и индекса объекта будет показан весь нумерованный список сертификатов и CRL, лежащих в базе Продукта.

Пример

Пример просмотра сертификатов, лежащих в контейнере, который защищен паролем:

```
C:\Program Files\Bel VPN Client>cert_mgr show -f test.p12 -p pa22w0rd
```

```
Certificate/Crl from file test.p12
Found 2 certificates. Found 1 CRL.
1 O=S-Terra Bel,CN=CA Cert
2 O=S-Terra Bel,CN=Technological Cert
3 CRL: C=BY,O=STBcert,OU=QA,CN=CAUN0
```

Пример просмотра в базе Продукта сертификатов партнеров, срок действия которых истек.

```
C:\Program Files\Bel VPN Client>cert_mgr show -expired_remote
```



```

3 Status: remote
  Subject: O=TrustWorks,CN=CA Cert
  Issuer: O=TrustWorks,CN=CA Cert
  Valid from: Fri Dec 31 16:00:00 1999
  Valid to:   Sat Dec 31 16:00:00 2005
  Version: 3
  Serial number: 01
  Signature algorithm: md5RSAencryption
  Public key: RSA(1024)
  Hash MD5:  1E 8D 9D 61 2E 41 4C A1 CC BB 33 81 EF 52 42 35
  Hash SHA1: E8 4F 2C A6 2E 01 5D 36 DF 07 14 E2 9C 51 B2 F7 8B 44 1F
FF
  CRLI[0]: O=TrustWorks,CN=CA Cert
    
```

11.2 cert_mgr check

Команда **cert_mgr check** предназначена для проверки сертификатов, размещенных в базе Продукта.

Синтаксис

```
cert_mgr [-T timeout] check [-i OBJ_INDEXN]
```

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-i OBJ_INDEXN	индекс сертификата в базе Продукта, который следует проверить. Необязательный параметр.

Значение по умолчанию значение по умолчанию отсутствует.

Рекомендации по использованию

Проверяются сертификаты, находящиеся в базе Продукта. Без указания параметра **-i** проверяются все сертификаты из базы Продукта.

Утилита выводит состояние сертификата "Active" или "Inactive". В случае, если сертификат имеет состояние "Inactive", выводится краткое описание причины неактивности:

- Certificate is invalid – неверный формат сертификата
- Certificate is expired – срок использования сертификата истек
- Certificate is not valid yet – время использования сертификата не наступило
- Certificate is revoked – сертификат отозван
- Certificate can not be verified – сертификат не удается проверить:

- ◆ в базе отсутствует сертификат(ы) для построения цепочки сертификатов с корректным конечным CA сертификатом, которому мы доверяем
- ◆ в базе нет необходимого CRL для проверки одного из сертификатов цепочки, подобная ситуация может возникнуть при включении проверки CRLs (загружена DDP или в загруженной конфигурации явно задано CRLHandlingMode = ENABLE)
- Private key container is not accessible – нет доступа к контейнеру с секретным ключом
- Private key is not accessible – нет доступа к секретному ключу
- Private key is not consistent certificate – секретный ключ не подходит к сертификату
- It is certificate request – данный объект является сертификатным запросом.

Пример

Проверка сертификатов в базе Продукта:

cert_mgr check

```
1 State: Inactive CN=partner
Certificate is expired.
Valid from: Wed Sep 22 00:17:02 2013
Valid to: Thu Sep 22 00:27:02 2014
```

11.3 client_login

Команда **client_login** запускается автоматически при логине пользователя в систему и представляет собой GUI-приложение (Рисунок 26), в котором нужно ввести пароль для аутентификации пользователя.

Эта команда запускается и при выборе предложения Login в меню (Рисунок 36), которое появляется на иконке в панели задач при работающем сервисе после того, как было выбрано предложение Logout.

Синтаксис

client_login

11.4 client_logout

Команда **client_logout** предназначена для завершения сессии пользователя. При этом производится загрузка политики Log-off Policy.

Эта команда запускается при выборе предложения Logout в меню (Рисунок 36), которое появляется на иконке в панели задач при работающем сервисе после того, как было выбрано предложение Login. Возможен запуск команды вручную.

Синтаксис

client_logout [-T timeout]

-T timeout время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

Пример

Ниже приведен пример запуска вручную команды `client_logout`:

```
client_logout
```

```
Logout OK
```

11.5 cspvpn_verify

Утилита `cspvpn_verify` используется для регламентной проверки целостности программной части установленного ПП Bel VPN Client-P во время его работы. Эта же утилита автоматически запускается при каждом старте сервиса `vpnsvc`.

Синтаксис

```
cspvpn_verify [-n]
```

-n запрет на завершение работы сервиса `vpnsvc`

Рекомендации по использованию

В состав Продукта входит файл `.hashes`, который содержит список всех исполняемых файлов, библиотек и неизменяемых конфигурационных файлов, а также значение хэш-суммы для каждого файла. Этот файл содержит строки вида:

```
<hash> <full_file_path>
```

где

<hash> – эталонное значение хэш-суммы для данного файла

<full_file_path> – полный путь к проверяемому файлу.

При запуске утилита проверяет целостность именно этого списка файлов.

Используйте утилиту для проверки целостности программной части во время работы Продукта,

Если проверка прошла успешно, то никакого сообщения не выдается.

При обнаружении ошибки работа утилиты прекращается с ненулевым кодом возврата и в файл лога `cspvpn_verify_err.log` передается сообщение об ошибке. Затем, в случае запуска утилиты без ключа `-n`, проверяется работа сервиса `vpnsvc`. При его наличии – выполняется аварийное прерывание.

Если обнаруживается несколько разнородных ошибок, то код возврата утилиты формируется по первому сообщению об ошибке.

Возможные сообщения об ошибках для данной утилиты приведены в разделе [«Стартовый и регламентный контроль целостности продукта»](#).

При устранении ошибки перезапустите сервис `vpnsvc`:

```
net start vpnsvc.
```

При нарушении целостности работающего Продукта переустановите Bel VPN Client, используя инсталляционный файл.

Пример

Ниже приведен пример запуска команды:

```
cspvpn_verify
Mon Oct 03 15:00:24 2014
Verification SUCCESS: 71 files verified
```

11.6 dp_mgr show

Команда **dp_mgr show** предназначена для просмотра установленных настроек политики Default Driver Policy и Log-off policy.

Default Driver Policy (DDP) – политика безопасности по умолчанию, задается администратором, может принимать следующие значения:

passall	пропускать весь трафик.
passdhcp	пропускать пакеты только по протоколу DHCP, т.е. будут уничтожаться все пакеты, кроме исходящих UDP-пакетов на порт 67 и входящих UDP-пакетов на порт 68.
dropall	не пропускать трафик.

Политика DDP задается администратором и загружается в следующих случаях:

- при ошибке загрузки конфигурации – до старта vpnsvc сервиса
- при остановке vpnsvc.

Log-off policy – специальная политика безопасности, которая задается администратором, и служит для безопасности работы пользователя, при которой клиент не может создавать защищенных соединений. Эта политика работает по одному из двух правил:

passdhcp	пропускать пакеты только по протоколу DHCP, т.е. будут уничтожаться все пакеты, кроме исходящих UDP-пакетов на порт 67 и входящих UDP-пакетов на порт 68
ddp	политика по умолчанию.

Политика Log-off policy загружается автоматически в следующих случаях:

- до тех пор, пока пользователь не ввел свой пароль
- при вводе неверного пароля три раза
- при отказе от регистрации (login), если нажать кнопку Cancel
- при выходе пользователя из системы
- при смене пользователя.

В случае неинтерактивного логина Log-off policy при старте не загружается.

Синтаксис

```
dp_mgr [-T timeout] show [-ddp | -lop]
```

- T timeout время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд.
- ddp | -lop установка одного из параметров позволяет посмотреть либо Default Driver Policy, либо Log-off policy.

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

Данная команда выводит установленные значения DDP и Log-off-policy, например:

```
dp_mgr show
```

```
Default Driver Policy : passall
Log-off-policy: ddp
```

11.7 dp_mgr set

Команда **dp_mgr set** предназначена для настройки параметров **Default Driver Policy** (DDP) – политики по умолчанию и **Log-off policy** (см. команду **dp_mgr show**). Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
dp_mgr [-T timeout] set [-ddp {passall | passdhcp | dropall}] [-lop {ddp | passdhcp}]
```

- T timeout время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд.
- ddp {passall | passdhcp | dropall} устанавливает Default Driver Policy в один из режимов: passall (пропускать весь трафик), passdhcp (пропускать только DHCP пакеты), dropall (не пропускать трафик).
- lop {ddp | passdhcp} устанавливает Default Driver Policy или passdhcp (пропускать только DHCP пакеты).

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

Ниже приведен пример выполнения команды dp_mgr set:

```
dp_mgr set -ddp passall
```

```
Default driver policy is wrote to db successfully
```

11.8 drv_mgr

Команда **drv_mgr** показывает имена поддерживаемых настроек, режим доступа к ним, размер в байтах и диапазон допустимых значений.

Синтаксис

drv_mgr

Список выводимых настроек:

```
List of properties:
Name                access type size (in bytes) range [min-max]
pcap_minimal_mtu    read-only      4                [0-0]
fw_tcp_closed_ttl   lsp-managed    4                [1-65535]
fw_tcp_synsent_ttl   lsp-managed    4                [1-65535]
fw_tcp_synrcvd_ttl   lsp-managed    4                [1-65535]
fw_tcp_estab_ttl     lsp-managed    4                [1-65535]
fw_tcp_fin_ttl       lsp-managed    4                [1-65535]
fw_tcp_strictness    lsp-managed    4                [0-6]
fw_tcp_open_max      lsp-managed    4                [0-1000000]
fw_tcp_half_open_max lsp-managed    4                [0-1000000]
fw_tcp_half_open_low lsp-managed    4                [0-1000000]
fw_tcp_conn_rate_max lsp-managed    4                unlimited
fw_tcp_conn_rate_low lsp-managed    4                unlimited
frag_dont_grow_fragments read-write     1                [0-1]
frag_minimize_size   read-write     1                [0-1]
frag_df_options      read-write     1                [0-3]
ipsec_breq_max       read-write     4                unlimited
ipsec_breq_count     read-only      4                unlimited
ipsec_recursive_policy read-write     1                [0-1]
```

Описание настроек IPsec драйвера приведено в Таблица 3

Таблица 3

Наименование настройки	Тип доступа	Размерность	Рекомендуемые значения	Значение по умолчанию
Описание				
frag_dont_grow_fragments	чтение-запись		0-1	0
	Чтобы избежать повторной перефрагментации пакетов промежуточными маршрутизаторами, предусмотрены следующие значения: 1 – размер фрагментов не будет превышать максимальный размер оригинальных фрагментов 0 – пакет фрагментируется без учета размера оригинальных фрагментов			
frag_minimize_size	Чтение-запись		0-1	0
	Чтобы избежать повторной перефрагментации пакетов промежуточными маршрутизаторами, предусмотрены следующие значения:			

Наименование настройки	Тип доступа	Размерность	Рекомендуемые значения	Значение по умолчанию
	Описание			
	<p>1 – размер фрагментов усредняется, т.е. минимизируется максимальный размер фрагмента при сохранении минимального количества фрагментов</p> <p>0 – все фрагменты делаются максимального размера, кроме последнего.</p> <p><u>Пример:</u> MTU – 270, пакет – 276 байтов, заголовок – 20 байт. Если значение 1, то фрагменты 148 и 148 байтов. Если значение 0, то фрагменты 268 и 28 байтов.</p>			
frag_df_options	чтение запись		0-3	0
	<p>Чтобы избежать повторной перефрагментации пакетов промежуточными маршрутизаторами, предусмотрены значения, которые определяют выставлять ли DF-бит на фрагментах:</p> <p>0 – на фрагментах DF-бит всегда сбрасывается</p> <p>1 – выставлять DF-бит у фрагментов, если оригинальный пакет был фрагментирован, не инкапсулирован в IPsec, и на фрагментах был выставлен DF-бит. Это значение позволяет восстанавливать DF-бит для открытого трафика. Таким образом, хост, отправивший пакет, может проводить MTU discovery для фрагментированных пакетов.</p> <p>2 – выставлять DF-бит для фрагментированных IPsec-пакетов, если на соответствующем IPsec SA включено MTU discovery. Этот флаг позволяет проводить MTU discovery для фрагментированных пакетов драйверу и избавиться от повторной фрагментации IPsec пакетов:</p> <ul style="list-style-type: none"> – IPsec-пакет может быть фрагментирован, если в SA установлен режим сброса или копирования DF-бита (DFHandling в LSP). При этом, если установлен режим копирования, в исходном пакете DF-бит должен быть сброшен – сочетание, когда включено MTU discovery и DFHandling = CLEAR имеет смысл только при frag_df_options ≥ 2, т.к. нет смысла проводить MTU discovery, когда DF-бит всегда сброшен. <p>3 – комбинация 1 и 2.</p>			
ipsec_breq_max	чтение запись		unlimited	1000
	Максимальное количество одновременно выполняющихся запросов на создание SA bundle. В LSP можно задать отдельные ограничения для каждого правила.			
ipsec_breq_count	чтение		unlimited	0
	Текущее количество одновременно выполняющихся запросов на создание SA bundle.			
ipsec_recursive_policy	чтение		0-1	0
	Включение/выключение рекурсивного режима поиска правил IPsec для обработки пакетов. Настраивается в LSP через атрибут AllowNestedIPsec.			
pcap_minimal_mtu	чтение			1500
	Минимальное значение MTU для всех сетевых интерфейсов. Значение вычисляется на основании параметров интерфейсов, доступных для драйвера. Таким образом, минимальное значение MTU, используемое IP-драйвером может отличаться.			
fw_tcp_closed_ttl	чтение	секунды	1-65535	5

Наименование настройки	Тип доступа	Размерность	Рекомендуемые значения	Значение по умолчанию
	Описание			
fw_tcp_synsent_ttl	чтение	секунды	1-65535	30
fw_tcp_synrcvd_ttl	чтение	секунды	1-65535	60
fw_tcp_estab_ttl	чтение	секунды	1-65535	3600
fw_tcp_fin_ttl	чтение	секунды	1-65535	30
	Время жизни записи о соединении. S-Terra Client сначала определяет состояние TCP соединения для каждого из партнеров, которые создают TCP соединение через шлюз безопасности. А в LSP в зависимости от этих состояний задано время жизни записи о соединении.			
fw_tcp_strictness	чтение		0-6	3
	Уровень "жесткости" к различным ситуациям, которые воспринимаются шлюзом как ошибочные			
fw_tcp_open_max	чтение		0-1000000	65536
	Максимальное количество разрешенных TCP-соединений. При превышении данного предела новые TCP-соединения будут отвергаться. Настраивается в LSP.			
fw_tcp_half_open_max	чтение		0-1000000	500
	Максимальное количество одновременно существующих полуоткрытых сеансов TCP, при достижении которого начинается их удаление при появлении нового запроса на соединение. Настраивается в LSP.			
fw_tcp_half_open_low	чтение		0-1000000	400
	Минимальное количество одновременно существующих полуоткрытых сеансов TCP, при достижении которого прекращается их удаление. Настраивается в LSP.			
fw_tcp_conn_rate_max	чтение		unlimited	500
	Максимальная частота появления полуоткрытых сеансов TCP в минуту, по достижении которой начинается их удаление. Настраивается в LSP.			
fw_tcp_conn_rate_low	чтение		unlimited	400
	Минимальная частота появления полуоткрытых сеансов TCP в минуту, по достижении которой прекращается их удаление. Настраивается в LSP.			

11.9 drv_mgr show

Команда **drv_mgr show** предназначена для просмотра установленных значений настроек работы IPsec-драйвера.

Синтаксис

```
drv_mgr show [PROPERTY_NAME1] [PROPERTY_NAME2] ...
```

PROPERTY_NAME_n имена настроек, значения которых должны быть показаны.
Если ни одно имя не задано – будут показаны значения всех поддерживаемых настроек.

Имена настроек указаны в Таблица 3.

Пример

```
drv_mgr show
```



```

pcap_minimal_mtu      1500
fw_tcp_closed_ttl     5
fw_tcp_synsent_ttl    30
fw_tcp_synrcvd_ttl    60
fw_tcp_estab_ttl      3600
fw_tcp_fin_ttl        30
fw_tcp_strictness     3
fw_tcp_open_max       65536
fw_tcp_half_open_max  500
fw_tcp_half_open_low  400
fw_tcp_conn_rate_max  500
fw_tcp_conn_rate_low  400
frag_dont_grow_fragments 0
frag_minimize_size    0
frag_df_options       0
ipsec_breq_max        1000
ipsec_breq_count      0
ipsec_recursive_policy 0
    
```

11.10 drv_mgr set

Команда **drv_mgr set** предназначена для редактирования настроек работы IPsec-драйвера. С помощью этой команды можно изменять значения только тех настроек, которые имеют атрибуты read-write. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
drv_mgr set PROPERTY_NAME1 VALUE1 [PROPERTY_NAME2 VALUE2]
```

PROPERTY_NAME_n имена настроек, значения которых нужно изменить
 VALUE_n значения соответствующих настроек.

Рекомендации по использованию

Имена настроек указаны в Таблица 3 описания утилиты drv_mgr.

При успешной установке значения настройки будет выведено сообщение:

```
Value of "PROPERTY_NAME" is set to VALUE
```

При неуспешной установке значения настройки выводится сообщение:

```
Value of "PROPERTY_NAME" is not set to VALUE. Error:
ERROR_DESCRIPTION.
```

Значение настройки также записывается в конфигурационный файл `%PROD_DIR%\csp_ipsec_drv.cfg`, чтобы при запуске демона автоматически выставить его в IPsec-драйвере.

Редактировать этот конфигурационный файл без использования команды `drv_mgr set` нельзя.

11.11 drv_mgr reload

Команда **drv_mgr reload** загружает значения всех настроек IPsec-драйвера из конфигурационного файла %PROD_DIR%\csp_ipsec_drv.cfg. Эта команда имеет технологическое применение и используется для автоматической загрузки настроек IPsec-драйвера при запуске демона. Команда не предназначена для использования пользователем. Для работы с утилитой требуются права Администратора.

Синтаксис

```
drv_mgr reload
```

Редактировать конфигурационный файл нельзя. Установить новые значения настроек драйвера, записываемые в конфигурационный файл, можно только командой `drv_mgr set`.

При успешном завершении утилита возвращает значение 0.

11.12 fwconn_show

Команда **fwconn_show** предназначена для просмотра информации о TCP-соединениях, отслеживаемых при контекстной фильтрации трафика.

Синтаксис

```
fwconn_show [-detail] [-i conn_1_id]..[-i conn_n_id]
```

`-detail` выдается подробная информация о соединениях. Для получения подробной информации о конкретном соединении необходимо указать опцию `-detail` перед `-i`.

`-i conn_n_id` выдается информация по конкретному соединению с указанным идентификатором. Можно перечислить несколько соединений. В качестве идентификатора соединения допустимо указывать одно из двух чисел Connection ID, разделенных "/". Данные идентификаторы соединения также присутствуют в выводе утилиты `klogview` (группы сообщений FW, FR, FWTCP).

Пример

```
fwconn_show
```

```
Connection ID      Protected IP:port  Unprotected IP:port  State
0xd3e38180/0xd3e380c0  10.0.16.103:32779  -> 10.0.131.1:21
ESTAB/ESTAB

Number of TCP connections: 1
Number of established TCP connections: 1
```

где

- Connection ID (0xd3e38180/0xd3e380c0) – идентификатор соединения (используется в `fwconn_show` и выводе `klogview`)
- Protected IP:port (10.0.16.103:32779) – IP-адрес и порт, защищаемые firewall (обычно инициатор соединения)
- ➔ – направление открытия соединения

- State (ESTAB/ESTAB) – состояние TCP соединения для каждого из партнеров
- Number of TCP connections (1) – общее число отслеживаемых TCP-соединений
- Number of established TCP connections (1) – общее число отслеживаемых установившихся TCP-соединений.

fwconn_show -detail

```

Connection ID: 0xd3e38300/0xd3e38480
  Reverse connection: yes
  Protected side: 10.0.16.103:32780
    State: CLOSING
    Sequence number: 141965198
    Acknowledgement number: 1585098758
    Window size: 49232
    TTL left / TTL for current state: 27/30
  Unprotected side: 10.0.131.1:20
    State: CLOSING
    Sequence number: 1585098758
    Acknowledgement number: 141965198
    Window size: 5840
    TTL left / TTL for current state: 27/30
    
```

Дополнительные параметры, отображаемые при указании флага `-detail`:

- Reverse connection (yes) – направление установления соединения – в данном случае соединения от 10.0.131.1:20 к 10.0.16.103:32780
- Sequence number (141965198, 1585098758) – TCP sequence number для каждого из партнеров
- Acknowledgement number (1585098758, 141965198) – TCP acknowledgement number для каждого из партнеров
- Window size (49232, 5840) – размер TCP-окна для каждого из партнеров с учетом TCP window scaling¹
- TTL left² (27, 27) – время, через которое будет уничтожена запись о соединении, если не будет нового корректного пакета
- TTL for current state (30, 30) – максимальное время хранения записи о соединении при отсутствии активности.

fwconn_show -detail -i 0xffff88003f99a100

```

Connection ID: 0xffff88003f99a100/0xffff88003f99a800
  Reverse connection: no
    
```

¹ Возможна ситуация, когда firewall начинает отслеживать уже открытое соединение, не получая первых пакетов. В этом случае window scaling не учитывается.

² Запись о соединении уничтожается, если для любого из партнеров TTL Left достигает 0.

```
Protected side: 5.5.5.5:35382
    State: CLOSING
    Sequence number: 3253957880
    Acknowledgement number: 2429155619
    Window size: 92
    TTL left / TTL for current state: 536/600
Unprotected side: 6.6.6.6:21
    State: CLOSING
    Sequence number: 2429155619
    Acknowledgement number: 3253957880
    Window size: 91
    TTL left / TTL for current state: 536/600
```

11.13 if_show

Команда **if_show** предназначена для просмотра логических, физических имен и других параметров сетевых интерфейсов, защищаемых Продуктом.

Синтаксис

```
if_show [-all]
```

-all на экран выдаются все логические имена интерфейсов.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра параметров всех сетевых интерфейсов.

Фильтрация по каждому логическому интерфейсу происходит независимо, так что один и тот же физический интерфейс может быть выдан в нескольких списках, соответствующих разным логическим именам.

Примечание 1:

В выводе команды параметр `State` показывает общее состояние интерфейса. Параметр `State` отображает состояние «головного» интерфейса, и считается, что состояние логических интерфейсов совпадает с состоянием «головного» интерфейса.

Пример

```
if_show
```

```
Logical network interface "default":
    Physical name template: "*"

Physical name: ike{6405F321-8CF3-43A1-8C9E-509DF94A7B0F}
State:          UP
Index:          131076
MTU:            1500
MAC addr:      00:00:FE:AB:AB:AB
```

```
IP addr:      10.0.232.70 mask 255.255.0.0 brd 10.0.255.255

Physical name: eth{D7A013E1-9E12-4A80-9B5F-FB3D19B0E419}
State:       UP
Index:       2
MTU:         1500
MAC addr:    00:0C:29:E5:BE:C2
IP addr:     10.0.232.100 mask 255.255.0.0 brd 10.0.255.255
```

11.14 `integr_mgr calc`

Утилита `integr_mgr calc` используется для вычисления хэш-суммы указанного файла.

Синтаксис

```
integr_mgr calc -f filePath [-q]
```

`-f filePath` имя файла (включая полный путь к нему), для которого будет вычисляться хэш-сумма

`-q` запрет вывода текстовых результатов работы утилиты. Итоговый результат работы утилиты при использовании этой опции возможно узнать только из кода ошибки, возвращаемого утилитой. Допустимо указание ключа `-q` либо сразу после названия команды, либо в конце командной строки

Рекомендации по использованию

При вычислении хэш-суммы указанного файла будет создан файл с именем `filePath.hash`, содержащий значение хэш-суммы, которая в дальнейшем может применяться для контроля целостности файла.

Пример

Вычисляется хэш-сумма для файла `x509conv.ini`. В результате в том же каталоге, где расположен файл `x509conv.ini`, должен появиться файл `x509conv.ini.hash`:

```
integr_mgr calc -f x509conv.ini
```

```
SUCCESS: Operation was finished successfully
```

11.15 `integr_mgr check`

Утилита `integr_mgr check` применяется для проверки целостности отдельного файла или списка файлов. Утилиту можно использовать для проверки целостности файлов информационной части Продукта (изменяемых файлов в процессе настройки администратором).

Синтаксис

```
integr_mgr check -f filePath [-q]
integr_mgr check -l filePathList [-q]
```

-f filePath	имя проверяемого файла, включая полный путь к нему
-l filePathList	имя текстового файла со списком проверяемых файлов. Каждая строка данного файла – имя проверяемого файла с полным путем к нему
-q	запрет вывода текстовых результатов работы утилиты. Итоговый результат работы утилиты при использовании этой опции возможно узнать только из кода ошибки, возвращаемого утилитой. Допустимо указание ключа -q либо сразу после названия команды, либо в конце командной строки.

Рекомендации по использованию

В информационную часть Продукта входят каталог базы данных db и конфигурационные файлы, такие как:

```
agent.ini
s_logset.ini
syslog.ini
x509conv.ini
```

Все эти файлы лежат в каталоге Продукта, например, C:\Program Files\S-Terra Client. Значение контрольной суммы для каждого из этих файлов записано в файл с тем же именем, но с расширением hash, например, s_logset.ini.hash.

При запуске утилиты для одного файла вычисляется хэш-сумма заданного файла (filePath) и сравнивается полученное значение с контрольным значением в файле filePath.hash того же каталога.

При изменении данных файлов при помощи программных средств, предлагаемых Продуктом, пересчет хэш-сумм производится автоматически.

При изменении данных файлов вручную, без использования программных средств Продукта, необходимо пересчитать хэш-сумму измененного файла, запустив утилиту integr_mgr calc.

При проверке списка файлов работа утилиты не прерывается по первому несовпадению хэш-суммы, а также при любых других ошибках контроля целостности - ошибки доступа к файлу, отсутствие предварительно вычисленной хэш-суммы и прочих аналогичных ошибках. При каждой наступившей ошибке (если не указана опция -q) об этом выдаётся сообщение: имя обрабатываемого файла, код ошибки, расшифровка распространённых ошибок и проверка продолжается. Опцию -q удобно использовать, если есть необходимость в вызове данной утилиты из какого-либо дополнительного скрипта.

Пример

Проверяется целостность файла x509conv.ini:

```
integr_mgr check -f x509conv.ini
```

```
SUCCESS: Operation was finished successfully
```

11.16 key_mgr import

Команда **key_mgr import** предназначена для импорта предопределённых ключей из файловой системы в базу Продукта. Для работы с

утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
key_mgr [-T timeout] import -n KEY_NAME -f KEY_FILE
```

-T timeout время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

-n KEY_NAME имя предопределенного ключа.

-f KEY_FILE путь к файлу, содержащему предопределенный ключ.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для регистрации предопределенных ключей в базе Продукта.

Пример

Пример импорта предопределенных ключей из файлов в базу Продукта:

```
key_mgr.exe import -f c:\certs\key1 -n key1 -f key2 -n key2name -f key3 -n key3name
```

```
OK key1name
OK key2name
OK key3name
```

11.17 **key_mgr remove**

Команда **key_mgr remove** предназначена для удаления предопределенных ключей из базы Продукта. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
key_mgr [-T timeout] remove -n KEY_NAME
```

-T timeout время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

-n KEY_NAME имя предопределенного ключа.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для удаления предопределенных ключей из базы Продукта.

Пример

Ниже приведен пример удаления предопределенного ключа:

```
key_mgr remove -n key1name
```

OK key1name

11.18 key_mgr show

Команда **key_mgr show** предназначена для получения информации о предопределенных ключах, зарегистрированных в Продукте.

Синтаксис

```
key_mgr [-T timeout] show
```

-T timeout время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра списка предопределенных ключей в базе Продукта.

При выполнении этой команды будут выводиться следующие данные:

- количество предопределенных ключей
- для каждого ключа:
 - ◆ имя ключа
 - ◆ тело ключа в печатном виде. Если тело ключа содержит непечатные символы, то при выводе в печатном виде они заменяются на ' . ' (символ точка).
 - ◆ тело ключа в hex-представлении.

Пример:

```
key_mgr show
```

```
Found #1 keys.
----Key----
Name      :      key1
Content   :      testkey1..
```

11.19 key_mgr list

Команда **key_mgr list** предназначена для просмотра списка предопределенных ключей, зарегистрированных в Продукте.

Синтаксис

```
key_mgr [-T timeout] list
```

-T timeout время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра списка predetermined keys в базе Продукта.

При выполнении этой команды будут выводиться следующие данные:

- количество predetermined keys
- для каждого ключа:
 - ◆ имя ключа

Пример:

```

key_mgr list

Found #3 keys.
-- [Key] -----
Name           : key1
-- [Key] -----
Name           : key2name
-- [Key] -----
Name           : key3name
    
```

11.20 klogview

Утилита `klogview` предназначена для просмотра сообщений, выдаваемых системой протоколирования IPsec-драйвера.

Синтаксис

```

klogview [-ltTg] [-p ts_precision] [-m event_mask] [-f
event_mask]
    
```

- l ожидать сообщения из ядра и выводить их по мере поступления. Эта опция принимается по умолчанию, если не задана опция -m.
- t печатать дату и время вывода сообщения
- T печатать относительное время, когда произошло событие. Время выводится в секундах относительно последнего произошедшего события (а не по времени вывода), показанного данным экземпляром утилиты. Например, значение 10.353245 – это 10 секунд и 353245 микросекунд. Максимальная точность – наносекунды, но реальная погрешность зависит от аппаратной платформы и операционной системы. Значение, выдаваемое с первым сообщением, отображает абсолютное значение часов, которое используется для вычисления относительного времени. Абсолютное значение – это либо время со старта системы, либо время относительно какой-то даты, принятой в данной системе за точку отсчета. Возможны отрицательные значения. Время, указанное в событии, относится к началу

	формирования сообщения, а при параллельном формировании сообщений порядок их отправки не определен
-g	печатать перед сообщением в квадратных скобках идентификатор группы событий. Идентификатор группы поясняет, к какому разделу относится данное событие. При выборе фильтра, когда выводится множество сообщений различных разделов, без идентификатора трудно соотнести раздел и сообщение
-p ts_precision	количество знаков долей секунд, используемых при печати относительного времени события (-T)
-f event_mask	задать фильтр событий для данного экземпляра утилиты. Возможные события описаны в таблице
-m event_mask	задать фильтр событий по умолчанию. Заданное значение используется, если не указана опция -f
-h	вывести краткую информацию об использовании утилиты.

В настоящий момент утилита может выводить сообщения, относящиеся к одной или нескольким группам событий. События, по которым выводятся сообщения, сгруппированы двумя способами:

- группировка событий по подсистеме – сообщения, относящиеся к одной подсистеме. Например, PKT – события, относящиеся к подсистеме, реализующей логику обработки пакетов
- группировка событий по маске – позволяет выбирать сообщения более детально. Подсистема может использовать несколько масок событий. Например, PKT включает маски pass и drop.

Группировка событий по маске

Таблица 4

Группа событий	Код	Описание
drop	0x2	Уничтожение пакета. Выводится непосредственно перед уничтожением какого-либо пакета. Сообщение содержит краткий текст, поясняющий причину уничтожения и информацию из IP-заголовка пакета. В некоторых случаях IP-заголовок может быть испорчен к моменту вывода сообщения, тогда в сообщении допускаются нулевые или любые другие случайные адреса.
pass	0x1	Пропуск пакета. Выводится непосредственно перед отсылкой какого-либо пакета. Сообщение содержит краткий текст, поясняющий действия, которые были произведены над пакетом.
sa_minor	0x8	Некоторые внутренние события, происходящие с IPsec - контекстом. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста.
sa_major	0x4	Взаимодействия между IPsec-драйвером и приложением, касающиеся изменения состояния IPsec-контекстов. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста.
sa_trace	0x10	Сообщения выводятся перед попыткой применения к пакету IPsec-контекста.
sa_errors	0x20	Ошибки, связанные с неуспешным применением IPsec-контекста к пакету.

Группа событий	Код	Описание
fw_trace	0x80	Результат поиска правил firewall для пакета (если поиск производился). Сообщения, выбираемые fw_trace, включают все сообщения fw_notif.
fw_notif	0x100	Выводятся при применении правила firewall к пакету, если правило помечено в LSP.
fw_obj	0x200	Действия, производимые над правилами firewall (добавление, удаление). Идентификаторами правил являются числа двух типов. В десятичном виде выводятся идентификаторы, загружаемые из vnsvsc. В шестнадцатеричном виде (с префиксом 0x) выводятся идентификаторы динамических правил контекстной фильтрации.
vif_obj	0x400	Изменения конфигурации сетевого интерфейса (vif).
fw_tcpst	0x800	Изменения записи о состоянии TCP соединения (tcp state), ошибки и другие события контекстной фильтрации TCP. Включает все сообщения fw_tcpstat и fw_tcperr. Для идентификации сессий используются два числа (0x...), каждое из которых соответствует записи о состоянии партнера по TCP-соединению. Эти же числа являются идентификаторами соответствующих правил фильтрации в сообщениях групп fw_obj, fw_trace.
fw_tcpstat	0x1000	Вывод статистики после закрытия TCP сессии, если правило помечено в LSP.
fw_tcperr	0x2000	Вывод ошибок, связанных с контекстной фильтрацией TCP-соединения, если правило помечено в LSP.
mtud	0x4000	Действия, связанные с path mtu discovery (отсылка и обработка ICMP сообщений, ошибки). В сообщениях выводятся оригинальные заголовки пакетов, даже если к пакету применялся IPsec. Внешний заголовок можно увидеть в соответствующих сообщениях pass/drop.

Группировка событий по подсистемам

Таблица 5

Обозначение подсистемы	Описание ³
LOG	Сервисные сообщения подсистемы протоколирования. Их прием нельзя включить или отключить
SA	Работа с IPsec SA в ядре
IPSEC	Работа протоколов IPsec
PKT	Основная логика обработки пакетов
FW	Фильтрация трафика
FR	Действия над правилами фильтрации трафика
FWTCP	Контекстная фильтрация TCP
MTUD	Работа path mtu discovery
VIF	Действия над описаниями виртуальных сетевых интерфейсов.

Нужный набор событий (`event_mask`) можно указать перечислением масок событий через запятую (пробелы при перечислении не допускаются). Маска может быть задана числовым значением, именем (из таблицы «Группировка событий по маске») или именем подсистемы (из таблицы «Группировка событий по подсистемам»).

Примеры (все перечисленные команды эквивалентны):

³ Соответствие масок подсистемам можно увидеть в подсказке утилиты `klogview`.

```
klogview -f 0x1f
klogview -f 31
klogview -f drop,pass,sa_minor,sa_major,sa_trace
klogview -f PKT,SA,sa_trace
klogview -f drop,1,SA,0x10
```

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра сообщений, выдаваемых системой протоколирования.

Сообщения, выводимые утилитой

Сообщения, выводимые утилитой, формируются на основе данных, присылаемых из IPsec-драйвера. Структура большинства сообщений определяется строкой формата⁴, получаемой из IPsec-драйвера (см. [Примеры сообщений](#)).

Сервисные сообщения, выводимые утилитой:

*** N messages lost ***	выводится, если утилита не успевает обрабатывать сообщения и N сообщений поретяны.
no format string	в сообщении отсутствует строка формата ⁵ .
<error: ..	в выводимом сообщении несоответствие строки формата параметрам сообщения ⁶ .

Приведем список сообщений, которые выводятся системой протоколирования IPsec-драйвера для разных групп событий.

События группы pass и drop

Сообщения для этой группы выводятся непосредственно перед уничтожением или отправкой пакета.

Формат сообщения (в порядке следования):

- входящий или выходящий пакет
- IP-адрес источника
- порт источника
- IP-адрес получателя
- порт получателя
- номер IP-протокола
- длина IP-пакета

⁴ Строка формата по смыслу и стилю похожа на форматную строку в printf.

⁵ Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.

⁶ Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.

- логическое имя интерфейса или код интерфейса, если имя неизвестно
- действие "passed" или "dropped"
- строка, описывающая причину уничтожения или отправки пакета.

По возможности выводится дополнительная информация, например, имя правила фильтрации и идентификатор SA.

Примеры сообщений группы pass

Пакет обработан по правилу фильтрации с действием PASS:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: filtered
```

Пакет был обработан по IPsec-правилу:

```
passed in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
decapsulated
passed out packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0:
encapsulated
```

Пакет был отправлен в IP-стек для маршрутизации:

```
passed out packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0: re-routed
```

Пакет был пропущен в соответствии с конфигурацией драйвера по-умолчанию (пользовательская конфигурация не загружена):

```
passed out packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0: driver default policy
```

Примеры сообщений группы drop

Сообщения, связанные с некорректными данными заголовков пакета:

- IP-заголовок испорчен:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: corrupted IP header
```

- TCP/UDP заголовок испорчен:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: corrupted protocol headers
```

- Следующее сообщение аналогично "corrupted protocol headers", выводится после сборки (реассемблирования) IP-пакета:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: corrupted protocol headers after reassembly
```

- Испорченные заголовки после раскрытия IPsec, это может быть также связано с использованием неверного ключа для расшифровки при отсутствии проверки целостности:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA 33: corrupted protocol headers after decapsulation
```

- Испорчен ESP или AH заголовок:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: unable to fetch SPI
```

Превышено ограничение по количеству вложений IPsec, раскрываемых на одном хосте (допускается не более 16 вложений):

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0: too many nested encapsulations
```

Превышено ограничение по количеству вложений IPsec, применяемых на одном хосте (допускается не более 16 вложений), предположительно конфигурация написана таким образом, что пакет зациклился:

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0: too many nested encapsulations (recursive policy?)
```

Сообщения о подпадании пакета под правило с действием DROP:

- Пакет уничтожен на этапе фильтрации

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: firewall
```

- Пакет уничтожен на этапе проверки IPsec-фильтров.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: IPsec policy
```

- Пакет уничтожен на этапе проверки фильтров, связанных с IPsec-правилом.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0: SA filter
```

- Пакет уничтожен на этапе классификации.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0:
classification
```

Сообщения, связанные с несоответствием входящего пакета локальной конфигурации IPsec. Появление подобных сообщений может быть вызвано двумя причинами:

- несогласованные конфигурации⁷ партнеров по IKE/IPsec соединению
- попытка атаки на защищенную сеть.
- Пакет был закрыт с помощью IPsec, но подпадает под правило PASS:

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: filter
12: IPsec packet is not expected
```

- Открытый пакет подпадает под правило фильтрации с IPsec-действием:

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: filter
12: packet must be protected with IPsec
```

- При вложенной IPsec-инкапсуляции входящий пакет имеет недостаточное количество слоев IPsec-защиты:

```
dropped in packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0: packet
lacks required IPsec layer
```

- Туннельный (внешний) заголовок не соответствует параметрам SA.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: tunnel
header doesn't match SA 24
```

- Пакет пришел не с того сетевого интерфейса.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: SA
18 is bound to filter which doesn't match current vif
```

- Маловероятная ошибка, может произойти в процессе удаления SA в момент обработки пакета.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: SA 3 is
not in a bundle
```

- При вложенном IPsec пакет порядок применения слоев IPsec некорректный.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: SA 3 is
not the first SA in a bundle
```

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: SPI
0xfa849e11 is not found in SA bundle
```

После декапсуляции заголовок пакета не соответствует селектору SA.

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA 33:
decapsulated packet's IP header doesn't match the SA
```

- Неизвестный SPI (IPsec SA не найден).

```
dropped in packet 2.3.4.5->3.4.3.3, proto 50, len 140, if eth0: SPI 0xabababab
not found in hash
```

- SA не привязан к IPsec-фильтру, под который подпадает пакет.

⁷ Рассогласование может произойти "в динамике" - то есть когда один из партнеров находится в процессе конфигурирования, или параметры, которые должны согласовываться автоматически (например, IPsec SA), были рассинхронизированы из-за потерь пакетов или обрыва сетевого соединения.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: filter
12: IPsec SA doesn't match
```

Для исходящего пакета, попадающего на IPsec-фильтр, не создан SA bundle, при этом автоматическое создание SA для данного фильтра запрещено (fallback_action = DROP).

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: filter
12: SA bundle not found
```

Ошибки IPsec:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 50, len 140, if eth0: SA 33:
decapsulation error 5: integrity verification failed
```

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA 33:
encapsulation error 4: sequence number wrapped
```

Возможные ошибки представлены ниже.

Таблица 6

Код	Название	Описание проблемы
1	replay packet detected	обнаружен повторный пакет
2	call to crypto subsystem failed	ошибка крипто-подсистемы
3	last sequence number	последний номер пакета
4	sequence number wrapped	переполнение счетчика пакетов
5	integrity verification failed	проверка целостности не прошла
6	corrupted protocol headers	испорченный протокольный заголовок
7	corrupted headers after decapsulation	испорченный протокольный заголовок после декапсуляции
8	memory allocation failed	невозможно выделить память
9	IP ttl expired	счетчик IP ttl истек
10	buffer is too small ⁸	буфер слишком мал
11	can't parse IP options	невозможно разобрать опции IP
12	padding check failed	ошибка в заполнителе
13	incorrect SA configuration ⁹	неправильная конфигурация SA
14	wrong encapsulation mode for the SA	несоответствующий SA режим инкапсуляции (транспорт или туннель)
15	packet length exceeds 64K-1	длина пакета превышает максимально допустимую
16	TFC packet	TFC пакет
17	traffic limit exceeded	превышение ограничения по трафику
18	wrong tunnel source address	несоответствующий SA адрес источника в туннельном заголовке

Промежуточное состояние при IPsec-rekeying (процесс rekeying (смена ключевого материала) не успел завершиться вовремя):

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA 18
is unusable
```

Ограничение на обработку транзитного трафика:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: packet
is not local (not a security gateway)
```

⁸ Это является внутренней ошибкой, просьба сообщать разработчикам.

⁹ Тоже внутренняя ошибка, просьба сообщать разработчикам.

Ограничение на обработку транзитного трафика только для IPsec пакета:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
decapsulated packet is not local (not a security gateway)
```

Очередь пакетов, ожидающая создания IPsec SA bundle переполнена (размер очереди задается в LSP, по умолчанию 8):

```
dropped out packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0: filter
12: reached limit of 8 packets waiting for SA
```

В случае, если произойдет ошибка при построении SA bundle, для ожидающих пакетов будет выдано:

```
dropped out packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0: filter
12: failed to build SA bundle
```

Превышено общее количество одновременно выполняющихся запросов¹⁰ на создание SA (размер очереди по умолчанию 1000):

```
dropped out packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0: reached
limit of 1000 SA requests
```

Превышено количество одновременно выполняющихся запросов¹¹ на создание SA по одному фильтру (размер очереди задается в LSP, по умолчанию 8):

```
dropped out packet 10.12.33.4->11.8.3.4, proto 1, len 80, if eth0: reached
limit of 8 SA requests for filter 12
```

Следующее сообщение говорит о слишком большом количестве пакетов на обработку одним SA (более 40). Скорее всего, это означает неоптимальные настройки Продукта с точки зрения производительности. Просьба обращаться к разработчикам:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: SA 33:
queue overflow
```

Пакет после обработки IPsec может превысить максимальную длину IP. То есть к такому пакету IPsec не применим:

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 65530, if eth0: packet
is too large for IPsec, length after encapsulation 65550
```

Внутренние ошибки, о которых просьба сообщать разработчикам:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: ip data
is not 4-byte aligned
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: unknown
network interface
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: unknown
physical network interface
```

Пришел пакет ICMP destination unreachable/fragmentation needed, который обработан драйвером и далее не пропущен.

```
dropped in packet 2.3.4.5->3.4.3.3, proto 1, len 80, if eth0: ICMP PMTUD
message processed
```

Следующие сообщения связаны с тем, что драйвер находится в режиме конфигурирования, и прохождение пакетов заблокировано.

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: driver is
being configured
```

¹⁰ Ограничение касается только запросов, инициатором которых является драйвер.

¹¹ Ограничение касается только запросов, инициатором которых является драйвер.

Следующее означает, что с момента начала обработки пакета, конфигурация драйвера изменилась, и нельзя гарантировать правильность обработки данного пакета.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: packet
config id 11 don't match current id 12
```

IPsec-фильтр был уничтожен в процессе обработки пакета.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: IPsec
filter 13 is dead
```

Сообщения о нехватке ресурсов.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: filter
12: failed to send SA request: out of memory
```

```
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: can't
allocate packet buffer
```

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: can't
prepare SA list: out of memory
```

Исходящие пакеты, отправляемые с виртуального сетевого интерфейса, обязательно должны быть отправлены с использованием туннельного режима IPsec и адрес туннельного заголовка должен отличаться от изначального.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: IP
destination have not been changed for a packet which had come from IKEcfg
virtual interface
```

Исходящие пакеты, отправляемые с виртуального сетевого интерфейса, обязательно должны в качестве адреса источника иметь адрес этого виртуального интерфейса.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0: IP source
address is not an address of IKEcfg virtual interface
```

Пакет превышает MTU и не может быть фрагментирован из-за выставленного DF bit.

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: DF bit
set, can't fragment packet, path MTU 1500
```

Ошибка при попытке фрагментировать пакет.

```
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0: can't
fragment packet, path MTU 1500
```

11.20.1 События группы fw_trace, fw_notif

Сообщения этой группы позволяют определить, какое правило фильтрации используется для обработки пакета. За время обработки один пакет может проходить по нескольким спискам (например, фильтрация и классификация). Поскольку интенсивность сообщений fw_trace может быть очень высокой, fw_notif позволяет ограничить их число, получая сообщения только для правил, помеченных в LSP. Параметры пакета выводятся аналогично сообщениям pass/drop.

Примеры сообщений:

Найден фильтр, результат фильтрации в конце сообщения. Возможны следующие результаты фильтрации: PASS – пропустить пакет, ASSEMBLE – необходима сборка пакетов из фрагментов, DROP – уничтожить пакет, ERROR – ошибка обработки пакета (испорченный пакет, или нехватка ресурсов для обработки), MATCH – промежуточное состояние при фильтрации (фильтр подобран, но действие еще не определено).

```
filtration result for in packet 10.0.59.1:1680->12.1.1.1:23, proto 6, len 80,
if eth0: chain 10, filter 12, event id some_ftp_filter, status PASS
```

Отсутствие подходящего фильтра в цепочке.

```
filtration result for in packet 10.0.59.1:1680->12.1.1.1:23, proto 6, len 80,
if eth0: chain 10: no match
```

Переход к другой части цепочки фильтрации (при использовании Filter.Label в LSP).

```
intermediate filtration result for in packet 10.0.59.1:1680->12.1.1.1:23,
proto 6, len 80, if eth0: chain 10, filter 12, event id some_ftp_filter,
status MATCH, jump to 18
```

Ошибка в структуре цепочки фильтрации, просьба сообщать разработчикам о появлении.

```
filtration result for in packet 10.0.59.1:1680->12.1.1.1:23, proto 6, len 80,
if eth0: chain 10, filter 12: next filter 16 not found
```

11.20.2 События группы sa_minor, sa_major

Сообщения этой группы позволяют контролировать процессы создания, уничтожения и замены IPsec-контекстов. Сообщения о загрузке контекстов содержат детальную информацию о параметрах контекста, включая IP-параметры (адреса, порты), SPI, режимы и др.

Если сообщение содержит IP-параметры (selector), то они выводятся в следующем порядке:

- локальный адрес/диапазон адресов
- локальный порт
- удаленный адрес/диапазон адресов
- удаленный порт
- IP- протокол.

Под локальным адресом понимается адрес источника (source) для исходящих пакетов.

Примеры сообщений группы sa_major

- Превышено ограничение SA по трафику:

```
SA 55 expired
```

- Пора начинать rekeying SA (пройден барьер по трафику):

```
requesting rekeying for SA 33
```

- Сообщения о загрузке новых SA:

```
loaded SA 12: flags 0x1, IPsec flags 0x18, selector 5.4.3.2->2.3.4.5, tunnel
5.4.3.2->8.9.1.2, type 51, SPI 0xabababba
```

- Следующее сообщение говорит о замене IPsec SA без прерывания обработки трафика:

```
loaded replacement for SA 55: SA 69: flags 0x0, IPsec flags, 0x38, selector
3.4.5.1->2.3.4.0-2.3.4.255 proto 17, tunnel 3.4.5.1->1.3.4.1, type 50, SPI
0x3b7f44e0
```

Расшифровка type:

- 51 - AH
- 50 - ESP

Расшифровка некоторых¹² битов flags:

- 0x1 - входящий

¹² Остальные значения флагов не предназначены для интерпретации пользователями.

- 0x100 - включен path MTU discovery
- 0x200 - включена повторная маршрутизация (reroute)
- 0x400 - необходима сборка IP-пакетов из фрагментов перед инкапсуляцией

Расшифровка битов ipsec flags:

- 0x1 - туннельный режим
- 0x2 - сбрасывать DF-bit
- 0x4 - устанавливать DF-bit
- 0x8 - включена защита от replay-атак
- 0x10 - включена проверка целостности
- 0x20 - включено шифрование
- 0x40 - используется UDP-encapsulation (NAT traversal)

- Загрузка связки SA (SA bundle):

```
loaded bundle: chain 12, filter 98, flags 0x0, selector 3.4.5.1:98->3.4.5.2:99 proto 17, SA list 4 5
```

Расшифровка битов flags:

- 0x1 - пакеты, которые ожидают обработки данным SA bundle, должны быть уничтожены
- 0x2 - источником запроса на создание SA bundle был драйвер

- Сообщение о загрузке SA bundle, не содержащее списка SA, означает ошибку создания SA bundle приложением (демоном). Запрос SA bundle (обычно для его обработки требуется IKE-обмен):

```
SA request: filter chain 59, filter 12, selector 5.4.3.2:1->1.2.3.4:5 proto 17, expected SA selector 5.4.3.2->1.2.3.4 proto 17
```

- Пакет ожидает SA bundle.

```
waiting for SA: 10.0.59.1:1680->12.1.1.1:23, proto 17, len 90, if eth0
```

- SA заблокирован (превышено ограничение по времени/трафику), ожидается завершение процесса rekeying:

```
disabled SA 33
```

- Удаление SA:

```
removed SA 33
```

- Пришло подтверждение загрузки SA у партнера, SA активируется:

```
application request to enable SA 33 processed
```

- Автоматическое обновление SA приостановлено из-за отсутствия трафика, но при первом пакете начнется смена ключей (обновление SA).

```
first packet will trigger rekeying of SA 33
```

- Сообщения, возникающие при ошибочном/странном¹³ поведении Продукта:

```
can't add bundle: filter id 299 is not found in chain 11
```

¹³ Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

```

can't add bundle: SA id 33 not found
can't load SA: unable to unpack
can't load replacement for SA 33: SA not found
can't load replacement for SA 33: can't unpack
can't remove SA 33: sa not found
can't disable SA 33: sa not found
can't enable SA 33: sa not found
rekey trigger: can't find SA 33
can't add bundle: non-empty "drop" response
can't add bundle: illegal request size 11
can't add bundle: filter id 2 in chain 2 is not an IPsec filter
can't add bundle: filter chain id 22 is empty
can't add bundle: filter chain id 22 not found
can't add bundle: filter id 23, chain 18: request 1.2.3.4->4.3.2.1 not found
can't add bundle: filter 80 is dead
can't add bundle: SA 24 is already in a bundle
    
```

Примеры сообщений группы sa_minor¹⁴

```

destroyed SA 12
replacing SA 12 with SA 13
can't enable sa 13: it's already enabled
enabled sa 14, but didn't activate it
enabled sa 15
    
```

11.20.3 События группы sa_trace

Сообщения группы `sa_trace` позволяют увидеть факт применения IPsec-контекстов к пакету. Для исходящих пакетов – это инкапсуляция, для входящих – декапсуляция. Сообщения содержат идентификатор SA, который выводится при загрузке SA (должны быть включены сообщения группы `sa_major`). Информация о пакете выводится в том же порядке, что и для сообщений группы `pass` и `drop`.

Примеры сообщений:

```

decapsulating with SA 10: 1.2.3.4:5->5.4.3.2:1, proto 6, len 256, if iprb0
encapsulating with SA 10: 5.4.3.2:1->1.2.3.4:5, proto 6, len 256, if iprb0
    
```

11.20.4 События группы sa_errors

Сообщения этой группы выводят дополнительную информацию о специфических ошибках IPsec.

В данный момент есть только одно сообщение – о детектировании replay-атаки. Выводится состояние окна, номер пакета (`sequence number`).

¹⁴ Сообщения данного раздела предназначены для внутреннего использования. Расшифровка пользователям Продукта не предоставляется.

Пример сообщения:

```
replay packet detected: SA 10 last sequence number 92, window 0x1, packet
sequence number 4.
```

11.20.5 События группы fw_tcpst, fw_tcperr, fw_tcpstat

События группы fw_tcperr

Вывод сообщений данной группы зависит от конфигурации (LSP). Для правила фильтрации, с которым связано событие, должно быть включено протоколирование. Если включена группа fw_tcpst, то сообщения выводятся независимо от LSP.

Примеры сообщений:

```
half open session count and creation rate are ok, stopped deleting
connections: count 2 (< 10), 1-minute rate 9 (< 10)

half open sessions limit triggered by 1.1.1.2:23->1.1.1.3:1045, starting to
delete connections: count/max 22/33, 1-minute rate/max 42/42

sessions limit triggered by 1.1.1.2:23->1.1.1.3:1045, dropping packet:
session count/max 4000/4000

blocked attempt to initiate FTP passive-mode data connection 0x%#5x
(%#1,a:%,2u->% ,a:%,2u) from server side

blocked attempt to initiate FTP data connection 0x%#5x (%#1,a:%,2u->% ,a:%,2u)
from client side

blocked FTP PASV response for 0x%#5x (%#1,a:%,2u->% ,a:%,2u): user not
authenticated

blocked attempt to use priveleged port %#6d in FTP PASV response for 0x%#5x
(%#1,a:%,2u->% ,a:%,2u)

blocked FTP PORT command for 0x%#5x (%#1,a:%,2u->% ,a:%,2u): user not
authenticated

blocked attempt to use priveleged port %#6d in FTP PORT command for 0x%#5x
(%#1,a:%,2u->% ,a:%,2u)
```

Дополнительные сообщения от stateful firewall:

- TCP sequence number не попадает в TCP window (см. описание TCPStrictnessLevel в LSP). Сообщение может быть связано как с намеренным искажением TCP заголовка так и с ограниченными возможностями по отслеживанию соединений в firewall.

```
unexpected TCP sequence number for 0xfafabebe, dropping packet: seq 1040,
flags 0x10, expected seq (ack) 4050, win 1024
```

- TCP флаги не соответствуют состоянию соединения (см. описание TCPStrictnessLevel в LSP). Сообщение может быть связано как с намеренным искажением TCP заголовка так и с ограниченными возможностями по отслеживанию соединений в firewall.

```
unexpected TCP flags for 0xfafabebe, dropping packet: disallowed state change
ESTAB->SYNSENT/ESTAB->ESTAB, TCP flags 0x2
```

- Смена состояния TCP-соединения. ttl – время, через которое запись о соединении удалится при отсутствии активности. Время отслеживается для каждого из партнеров отдельно, но запись будет удалена по истечении любого из таймаутов. Состояния отображаются как старое->новое.

```
session state changed for 0xfafabebe: state ESTAB->ESTAB/SYNRCVD->ESTAB, ttl
100/100, TCP flags 0x10
```

- В соответствии с LSP запрещено открытие TCP-стейтов, для соединений, которые открылись раньше сброса конфигурации firewall (см. описание TCPStrictnessLevel в LSP).

```
not a SYN packet, won't create state for session 10.1.1.1:22->10.2.2.2:3532,
parent filter 8: TCP flags 0x10
```

- Открытие новой записи о TCP соединении.

```
new session 0xbebebebe/0xabababab (1.2.3.4 1.2.3.4:32 32->2.3.4.1 2.3.4.1:33
33): parent filter 18, state SYNSENT/CLOSED, TCP flags 0x2)
```

- Невозможно создать новую запись о соединении из-за ограничений на количество установившихся (established) соединений. Неустановившихся соединений для удаления нет.

```
can't delete any old half open session in favor of new session 1.2.3.4
1.2.3.4:32 32->2.3.4.1 2.3.4.1:33 33, dropping packet: half open session
count 0
```

События группы fw_tcpstat

Для правила фильтрации, с которым связано событие, должно быть включено протоколирование. , то сообщения выводятся независимо от LSP.

Пример сообщения:

```
session 0x12345678x/0x12346678 (1.1.1.2:23->1.1.1.3:1045) closed: state
CLOSED/CLOSED, transferred 200/100 bytes, 10/15 packets
```

11.20.6 События группы fw_obj

В данные группы включены сообщения об изменении состава цепочек фильтрации, изменения состояния индивидуальных фильтров. Назначение цепочки фильтрации зависит от того, в каком качестве она подключена к виртуальному интерфейсу. С точки зрения сообщений о состоянии, все цепочки (фильтрация, классификация, IPsec) – одинаковы.

Изменение состояние фильтров и цепочек правил фильтрации (аналог FilterChain в LSP). Четные номера цепочек используются для исходящих пакетов. Идентификатор фильтра отображается десятичным числом для фильтров, загружаемых из приложения, шестнадцатеричным числом с префиксом 0x для фильтров, создаваемых динамически внутри драйвера.

Примеры сообщений:

- Создание цепочки правил фильтрации:

```
created filter chain 18
```

- Удаление цепочки правил фильтрации:

```
destroyed filter chain 18
```

- Удаление фильтра из цепочки по инициативе приложения:

```
unloaded filter 12 from chain 18
```

- Групповое удаление фильтров из цепочки по инициативе приложения:

```
unloaded 9 filters with parent id 19 from chain 18
```

- Включение фильтра или фильтров (в соответствии с графиком, см. LSP, Schedule):

```
enabled filter 4 from chain 9
```

```
enabled 9 filters with id 8 from chain 9
```

- Выключение фильтра или фильтров (в соответствии с графиком, см. LSP, Schedule):

```
disabled filter 4 from chain 9
```

```
disabled 9 filters with id 8 from chain 9
```

- Уничтожение фильтра:

```
destroyed filter 19
```

- Создание фильтра:

```
created filter 8, chain 4, selector 1.2.3.4 1.2.3.5->9.1.1.1 9.1.1.1 pkttype 4, position at head, action 0x0, nextid 12
```

Селектор (selector)	фильтра определяет адресную информацию пакетов, к которым будет применяться действие данного фильтра. Селектор содержит IP-адреса и порты в формате source -> destination, номера IP-протоколов – эти значения всегда выдаются в виде перечисления диапазонов. Так значение 1.2.3.8 1.2.3.11 1.3.3.3 1.3.3.3 – это диапазон 1.2.3.8..1.2.3.11 и единичный адрес 1.3.3.3
Pkttype	битовая маска из следующих значений (описание значений есть в LSP, PacketType): 1 – LOCAL_UNICAST, 2 – LOCAL_BROADCAST, 4 – LOCAL_MISDIRECTED, 8 – TRANSIT
Nextid	переход к другому фильтру, если произошло совпадение с данным фильтром
Position	в какое место цепочки фильтр будет вставлен
action	битовая маска действий, которые связаны с совпадением данного фильтра: 2 – уничтожить пакет, 4 – пакет помечен для получения сообщений группы fw_notif, 32 – фильтр загружен в отключенном состоянии в соответствии с графиком (Schedule). Остальные значения для внутреннего использования, пользователю описание не предоставляется.

Следующие сообщения отражают изменения объекта fgrs (пара цепочек правил фильтрации), который предназначен для фильтрации трафика в обоих направлениях. В состав fgrs может входить одна цепочка правил, в случае симметричной фильтрации (например, IPsec) или две. Идентификатор fgrs совпадает с идентификатором цепочки фильтров для исходящих пакетов.

- Удаление пары цепочек правил фильтрации:

```
destroyed filter chain pair 18
```

- Удаление пары цепочек правил фильтрации из списка доступных (после этого нельзя будет заново подсоединить эту цепочку к виртуальному интерфейсу). Обычно данное действие делается непосредственно перед удалением chain pair.

```
deregistered filter chain pair 18
```

- Создание пары цепочек правил фильтрации.

```
created filter chain pair 8, type 1, visibility 1
```

Значения visibility: 1 – объект доступен для изменения из приложений, 0 – внутренний объект драйвера.

Значения type: 1 – зависимые цепочки (для контекстной фильтрации), 2 – независимые цепочки (простая пакетная фильтрация), 3 – симметричная фильтрация (используется одна цепочка, адресная информация в пакете переворачивается в зависимости от направления)

- Сообщения, возникающие при ошибочном/странном¹⁵ поведении продукта:

```
can't load filter: chain 13 is not found
can't load filter: can't create chain 13
can't load filter to chain 13: unable to unpack
can't create filter chain pair 19, type 1, visibility 1: odd id
can't create filter chain pair 8, type 1, visibility 1: out of memory
can't create filter chain pair 4, type 1, visibility 1: can't create chains
can't deregister filter chain pair 4: not found
can't load filter 18 to chain 13
can't unload filter 18: chain 13 is not found
can't unload filter 18: chain 13 is not initialized
can't unload filter 18 from chain 84: filter is not found
can't disable filter 18: chain 13 is not found
can't disable filter 18: chain 13 is not initialized
can't disable filter 18 from chain 13: filter is already disabled
can't disable filter 18 from chain 13: filter is not found
can't enable filter 18: chain 13 is not found
can't enable filter 18: chain 13 is not initialized
can't enable filter 18 from chain 13: filter is already enabled
can't enable filter 18 from chain 13: filter is not found
can't add filter to chain 13: chain is being destroyed
can't add filter to chain 13 next to filter 8: filter not found
```

11.20.7 События группы vif_obj

В данную группу включены сообщения об изменении состояния виртуальных (vif) и реальных (phy) сетевых интерфейсов.

Примеры сообщений об изменении состояния сетевого интерфейса ОС:

Параметр `flags` отображает следующие состояния:

I – для данного интерфейса имеется информация о конфигурации IP (IP адрес, маска, MTU)

P – интерфейс доступен для перехвата пакетов

V – интерфейс подключен к соответствующему виртуальному интерфейсу.

- Изменение статуса интерфейса (частичное отключение, см. `flags` выше):

```
updated phy "eth0": cleared flags I: PIV>PV
```

- Получение IP-информации:

```
updated phy "eth0": id 2, flags PV>PIV, mtu 1500, addresses 1.2.3.4 2.2.3.4,
broadcasts 1.2.3.255 2.2.3.255
```

¹⁵ Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

- Подключение к виртуальному интерфейсу:

```
updated phy "eth0": flags P>PV, vif 9 "FastEthernet0/1"
```

- Появление информации об интерфейсе в перехватчике пакетов:

```
updated phy "eth0": flags I>PI: interface appeared in pcap
```

- Создание записи о сетевом интерфейсе:

```
created phy "eth0": phy id 2, flags P
```

- Уничтожение записи о сетевом интерфейсе:

```
destroyed phy "eth0"
```

- Создание записи о виртуальном интерфейсе по инициативе приложения:

```
created vif 7 "FastEthernet0/1"
```

- Подключение цепочки фильтрации:

```
attached filter chain pair 4 to vif 19, chain type 4
```

Расшифровка type:

0 – firewall, исходящие пакеты

1 – firewall, входящие

2 – классификация, исходящие

3 – классификация, входящие

4 – IPsec

- Включение виртуального интерфейса в общем списке (после этого действия к виртуальному интерфейсу подключаются сетевые интерфейсы ОС):

```
registered vif 11 "FastEthernet0/0": pname "eth0", priority 30
```

pname – шаблон имен сетевых интерфейсов ОС

priority – приоритет: если для сетевого интерфейса ОС по шаблону pname подходит несколько виртуальных, выбирается тот, у которого значение priority больше

- Уничтожение записи о виртуальном интерфейсе.

```
destroyed vif 7 "FastEthernet0/4"
```

- Отключение цепочки фильтрации:

```
detached filter chain pair 2 from vif 9, chain type 8
```

- Отключение виртуального интерфейса:

```
deregistering vif 3 "FastEthernet0/1"
```

- Сообщения, возникающие при ошибочном/странном¹⁶ поведении продукта:

```
can't attach filter chain pair 2 to vif 3: vif is not found
can't attach filter chain pair 2 to vif 3: chain pair is not found
can't attach filter chain pair 2 to vif 3: unknown chain type 100
can't attach filter chain pair 2 to vif 3, chain type 1: vif is dead
can't attach filter chain pair 2 to vif 3: chain type 1 is occupied
```

¹⁶ Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

```
can't detach filter chain pair type 1 from vif 2: vif is not found
can't detach filter chain pair type 120 from vif 2: unknown chain type
can't detach filter chain pair type 1 from vif 2: chain pair is not attached
update phy info: can't find phy "eth140"
update phy: can't unpack
can't create vif: unable to unpack
can't deregister vif 9: not found"
```

11.20.8 События группы mtud

- ICMP сообщение destination unreachable/fragmentation needed не отослано по причине того, что в SA стоит настройка принудительного выставления DF-бита:

```
not sending ICMP because of DF bit enforced by IPsec SA options for packet
10.0.59.1:1680->12.1.1.1:23, proto 50, len 140: topmost SA 28
```

- MTU с учетом применения IPsec инкапсуляции меньше минимального MTU для IP-пакетов:

```
MTU is too low for packet 10.0.59.1:1680->12.1.1.1:23, proto 50: calculated
MTU 60, topmost SA 49
```

- Отослано ICMP сообщение о необходимости снижения MTU трассы:

```
ICMP dest unreachable/fragmentation needed sent for packet 10.0.59.1:1680-
>12.1.1.1:23, proto 50, len 1520, topmost SA 80: MTU 1430
```

- При получении сообщения ICMP не найдено SA, который был использован при обработке проблемного пакета, сообщение проигнорировано:

```
SPI 0xbebebebe not found, discarding ICMP message from 3.2.4.1
```

- При получении сообщения ICMP найден SA, который был использован при обработке проблемного пакета, но для этого SA отключена обработка ICMP path mtu discovery, сообщение проигнорировано:

```
MTU discovery is not enabled for SA 32, discarding ICMP message from 3.4.5.6
```

- ICMP сообщение обработано, MTU трассы выставлено в соответствии:

```
MTU discovery message from 3.3.3.3 processed, requested value 1400, setting
path MTU to 1400 for SA 89"
```

- Запрошенное значение MTU из ICMP сообщения не прошло проверку, сообщение проигнорировано:

```
MTU 10 is out of expected range, discarding ICMP message from 3.5.11.1
```

11.20.9 Сообщение об утере данных

Сообщение о потере данных из-за недостаточной скорости обработки сообщений приложением (например, klogview не успевает их выводить). В случае klogview можно ограничить поток сообщений, выбрав только необходимые группы (параметр -f).

```
*** 1080 messages lost17 ***
```

¹⁷ Сообщение имеет id IPISM_LOG_MID_LOST и параметр с индексом 0 типа I32, содержащий количество потерянных сообщений.

11.21 lic_mgr show

Команда **lic_mgr show** предназначена для просмотра текущей Лицензии на продукт Bel VPN Client.

Синтаксис

```
lic_mgr show
```

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

11.22 lic_mgr set

Команда **lic_mgr set** предназначена для установки текущей Лицензии. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
lic_mgr set -p PRODUCT_CODE -c CUSTOMER_CODE -n  
LICENSE_NUMBER  
-l LICENSE_CODE
```

-p PRODUCT_CODE код Продукта, возможные коды:

CLIENTB

CLIENT

-c CUSTOMER_CODE код заказчика

-n LICENSE_NUMBER номер лицензии

-l LICENSE_CODE код лицензии

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

```
lic_mgr set -p CLIENTB -c test -n 1 -l 5B271A01DF5D143A
```

Active license:

CustomerCode=test

ProductCode= CLIENTB

LicenseNumber=1

LicenseCode=5B271A01DF5D143A

11.23 log_mgr show

Команда **log_mgr show** предназначена для просмотра общего уровня протоколирования, всех событий и настроек syslog-клиента.

Синтаксис

```
log_mgr [-T timeout] show [-e [msg_group_file.ini]]  
log_mgr [-T timeout] show-syslog
```

<code>-T timeout</code>	время ожидания ответа от vnpsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд.
<code>-e msg_group_file.ini</code>	имя файла <code>msg_group_file.ini</code> , в котором указана группа событий и уровень протоколирования для них
<code>show-syslog</code>	вывод настроек syslog-клиента

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Для вывода значения общего уровня протоколирования всех событий используйте команду

```
log_mgr show
```

Для вывода измененного администратором уровня протоколирования какого-либо события используйте команду:

```
log_mgr show -e
```

При отсутствии таких изменений – команда ничего не выводит. Все события, их идентификаторы и уровень лога для каждого из них указаны в файле `s_log.ini` каталога Продукта.

Для вывода настроек syslog-клиента используйте команду:

```
log_mgr show-syslog
```

Пример

```
log_mgr show
```

```
Default log level: <6> info
```

```
log_mgr show-syslog
```

```
syslog parameters: enabled, server_ip=127.0.0.1, facility=local7
```

11.24 log_mgr set

Команда `log_mgr set` предназначена для изменения настройки уровня протоколирования всех событий, не включенных в группы, уровня протоколирования группы событий, настройки syslog-клиента, задания группы событий и др.

Для выполнения опций: `reset-syslog`, `set-syslog`, `set -e`, `save` требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
log_mgr [-T timeout] set -l log_level
log_mgr [-T timeout] set -e [msg_group_file [-f]]
log_mgr [-T timeout] save [-T timeout]
log_mgr [-T timeout] set-syslog [-y {enable|disable}] [-a
syslog_ip] [-f facility]
log_mgr [-T timeout] reset-syslog
```

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-l log_level	уровень протоколирования всех событий, не включенных в группы событий. Имеет одно из возможных значений: emerg – аварийные сообщения alert – тревожные сообщения crit – критические сообщения err – сообщения об ошибках warning – предупреждения notice – извещения info – информационные сообщения debug – отладочные сообщения.
-e msg_group_file	имя файла msg_grpXXX.ini, в котором можно задать группу событий и уровень протоколирования для нее
-f	(force) указание этой опции разрешает изменять файл с группой событий. По умолчанию опция не задана и изменение файла не допускается
-y {enable disable}	включение/выключение протоколирования.
-a syslog_ip	IP-адрес хоста, на который будут отправляться сообщения (syslog-клиент).
-f facility	источник сообщений (начальное значение: local7). Возможные значения: kern, user, mail, daemon, auth, syslog, lpr, news, uucp, cron, authpriv, ftp, ntp, audit, alert, cron2, local0, local1, local2, local3, local4, local5, local6, local7.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Задание общего уровня протоколирования всех событий, которые не включены в группы событий с заданным уровнем, выполняется командой, например:

```
log_mgr set -l warning
```

Продукт поставляется с пятью предустановленными файлами, в которых указаны группы событий и уровень лога для этих событий. Эти файлы созданы для совместимости с продуктом версии 3.0.1:

- ◆ msg_grpLDAP.ini – задан уровень лога и идентификаторы событий, связанных с доступом к LDAP-серверу
- ◆ msg_grpSYSTEM.ini – задан уровень лога и идентификаторы системных событий
- ◆ msg_grpPOLICY.ini – задан уровень лога и идентификаторы событий, связанных с применением политики безопасности
- ◆ msg_grpCERTS.ini – задан уровень лога и идентификаторы событий, связанных с сертификатами

- ◆ msg_grpKERNEL.ini – задан уровень лога и идентификаторы событий, связанных с firewall.

Для задания протоколирования группы событий, указанных в файле с заданным уровнем, обязательно выполните команду (например, для LDAP):

```
log_mgr set -e msg_grpLDAP.ini -f
```

Настройка сохраняется до перезапуска сервиса. После перезапуска сервиса протоколирование этих событий будет происходить с общим уровнем логирования.

Если отредактировать файл msg_grpLDAP.ini (или не редактировать) и повторно запустить команду без опции -f, то будет выдано сообщение об ошибке.

Для сохранения изменений в файле с группой событий и уровнем протоколирования, и после перезапуска сервиса, выполните команду:

```
log_mgr save
```

Для отмены всех установленных ранее уровней протоколирования для всех групп событий, выполните команду:

```
log_mgr set -e
```

Настройка сохраняется до перезапуска сервиса.

Создание файла с группами событий

Для создания файла с группой интересующих событий (сообщений), надо знать структуру этого файла и где взять список событий (сообщений). Опишем это далее.

Каждый такой файл должен состоять из секций вида:

```
[LOGLEVEL.<LEVEL>]
<MSG_ID1>
<MSG_ID2>
!.....
```

где

<LEVEL>	значение уровня лога для всех событий, перечисленных в группе
<MSG_ID>	идентификатор события (сообщения)
!.....	строка, начинающаяся с символа '!', является комментарием. Допустимы пустые строки.

Таких секций в файле может быть несколько. Все события (сообщения) перечислены в файле s_log.ini из состава продукта. Каждое событие в файле имеет два эквивалентных представления – текстовое и в виде индекса (8 шестнадцатеричных цифр), например,

```
[MSG_ID_PRODUCT_START]
INDEX = 0x03090001
```

Рекомендуется использовать текстовое представление, однако индекс может быть удобнее, если уже имеется файл, в котором сообщение содержит индекс.

Пример такого файла -msg_groupDEMO1.ini:

```
[LOGLEVEL.DEBUG]
! сообщение PRODUCT_START задано его индексом:
```

```
03090001
```

```
! сообщение PRODUCT_STOP задано его текстовым представлением:
PRODUCT_STOP
```

Каждое событие имеет свой уровень лога, указанный в файле `s_log.ini`. Если в группу включены события с разными уровнями логирования, то для того, чтобы выполнялось протоколирование по всем этим событиям, проще всего указать для группы уровень лога `debug`.

Установка параметров syslog-клиента для сервиса `vpnsvc`. Установленные настройки Syslog-клиента будут записаны в файл `syslog.ini`.

```
log_mgr set-syslog [-y {enable|disable}] [-a syslog_ip] [-f
facility]
```

Например,

```
log_mgr set-syslog -y enable -a 10.0.0.1
```

Неуказанный в команде параметр остается неизменным.

Установка параметров по умолчанию для syslog-клиента:

```
log_mgr reset-syslog
```

при этом действуют следующие настройки:

```
enable
syslog_ip=127.0.0.1
facility=local7
```

При установке уровня протоколирования следует помнить, что самый высокий уровень детализации дает параметр `'debug'`, а самый низкий – параметр `'emerg'`.

Пример

Пример выполнения команды `log_mgr set`:

```
log_mgr set -l warning
```

```
Default log level is set successfully
```

11.25 lsp_mgr check

Команда `lsp_mgr check` предназначена для проверки LSP конфигурации. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
lsp_mgr [-T timeout] check -f LSP_FILE
```

`-T timeout` время ожидания ответа от `vpnsvc` сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

`-f LSP_FILE` путь к файлу конфигурации.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте команду `lsp_mgr check` для проверки синтаксиса файла с политикой безопасности.

11.26 lsp_mgr load

Команда `lsp_mgr load` предназначена для загрузки конфигурации из файла в базу Продукта. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
lsp_mgr [-T timeout] load -f LSP_FILE [-l LABEL]
```

<code>-T timeout</code>	время ожидания ответа от <code>vpnsvc</code> сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
<code>-f LSP_FILE</code>	путь к файлу конфигурации.
<code>-l LABEL</code>	текстовый комментарий к конфигурации (в произвольном формате). По умолчанию в качестве LABEL задается путь до файла с конфигурацией (аргумент опции <code>-f</code>).

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Если политика безопасности написана в виде текстового конфигурационного файла, то для загрузки ее в базу Продукта используйте команду `lsp_mgr load`.

Пример

Пример загрузки LSP конфигурации из файла в базу Продукта:

```
lsp_mgr load -f default.txt
```

```
LSP successfully loaded from file default.txt
```

11.27 lsp_mgr reload

Команда `lsp_mgr reload` предназначена для перезагрузки LSP конфигурации.

Синтаксис

```
lsp_mgr [-T timeout] reload
```

<code>-T timeout</code>	время ожидания ответа от <code>vpnsvc</code> сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-------------------------	---

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте команду `lsp_mgr reload` в следующих случаях:

- если произошли какие-то изменения в сертификатах, изменения у партнера, у шлюза безопасности и др.
- для устранения всех установленных соединений с партнерами
- во внештатных ситуациях – зависание Продукта и др.

Пример

Пример загрузки LSP конфигурации из базы Продукта:

```
lsp_mgr reload
```

```
LSP is reloaded successfully
```

11.28 lsp_mgr unload

Команда `lsp_mgr unload` предназначена для выгрузки LSP конфигурации.

Синтаксис

```
lsp_mgr [-T timeout] unload
```

`-T timeout` время ожидания ответа от `vpnsvc` сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для выгрузки активной конфигурации в базу Продукта. При выгрузке конфигурации начинает действовать политика драйвера по умолчанию – DDP. Политика DDP задается администратором при создании инсталляционного файла ПП Bel VPN Client-P для пользователя.

Пример

Пример выгрузки активной конфигурации в базу Продукта:

```
lsp_mgr unload
```

```
Operation completed successfully
```

11.29 lsp_mgr show

Команда `lsp_mgr show` предназначена для просмотра локальной политики безопасности пользователя (LSP).

Синтаксис

```
lsp_mgr [-T timeout] show [-db]
```

`-T timeout` время ожидания ответа от `vpnsvc` сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.

`-db` показать конфигурацию пользователя, хранящуюся в базе локальных настроек продукта.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Если загружена конфигурация пользователя, то по данной команде она будет выведена. Если загружена Default Driver Policy на экран будет выведено сообщение: `Default Driver Policy is loaded` без вывода тела конфигурации.

В штатном режиме работы вывод команды как с указанием опции `-db`, так и без указания данной опции, должен совпадать. Однако он будет отличаться, например, после выполнения команды `lsp_mgr unload`: в этом случае команда `lsp_mgr show -db` по-прежнему выдаст текст конфигурации. При отсутствии конфигурации в базе будет выдано сообщение: `Default Driver Policy is loaded`.

При просмотре конфигурацию можно сохранить в файле, например `current_lsp.txt`, командой:

```
lsp_mgr show > current_lsp.txt
```

Пример

```
lsp_mgr show
```

```
GlobalParameters (
  Title = "This LSP was automatically generated by S-Terra Client
AdminTool (cp) at 2011.09.29 14:10:13"
  Version = LSP_4_0
  CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
  ResponseTimeout = 200
  HoldConnectTimeout = 60
  DropConnectTimeout = 5
)
IdentityEntry auth_identity_01(
)
AuthMethodPreshared auth_method_01(
  SharedIKESecret = "fg"
  LocalID = auth_identity_01
)
IKEParameters (
  DefaultPort = 500
  SendRetries = 5
  RetryTimeBase = 1
  RetryTimeMax = 30
  SessionTimeMax = 60
.....
```

11.30 lsp_mgr show-info

Команда `lsp_mgr show-info` предназначена для просмотра информации о локальной политике безопасности пользователя (LSP).

Выводится следующая информация:

Type – тип локальной политики безопасности – `DHCP only | default driver policy | user-defined`

Source – источник локальной политики безопасности

Source info – дополнительная информация об источнике локальной политики. Присутствует в выводе команды только в случае, если Type – user-defined.

Синтаксис

```
lsp_mgr [-T timeout] show-info [-db]
```

-T timeout	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд.
-db	показать информацию о конфигурации пользователя, хранящейся в базе локальных настроек продукта.

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

Ниже приведен пример вывода информации о политике безопасности сразу после установки инсталляционного пакета Bel VPN Client:

```
lsp_mgr show-info
```

```
Type: user-defined
Source: 0
```

Пример вывода информации о политике безопасности в случае загрузки конфигурации в базу продукта из файла, с использованием утилиты lsp_mgr load:

```
lsp_mgr show-info
```

```
Type: user-defined
Source: command line
Source info: lsp.txt
```

11.31 pwd_change

Команда pwd_change предназначена для изменения пароля пользователя. Эта команда запускается автоматически при нажатии кнопки Change Password... в окне логина пользователя (Рисунок 26) и вызовом окна Change Password (Рисунок 27) для ввода старого и нового пароля. Эту команду можно запустить и вручную.

Синтаксис

```
pwd_change [old_user_PWD new_user_PWD]
```

old_user_PWD	старый пароль
new_user_PWD	новый пароль

Если не задать старый и новый пароль, то в интерактивном режиме они будут запрошены. При вводе символов их печать на консоль не производится. Новый пароль будет запрошен дважды во избежание ошибки.

Пример

Ниже приведен пример изменения пароля пользователя:

```
pwd_change "old_pwd" "new_pwd"
```

```
New password is set successfully
```

pwd_change

```
Enter old password:
Enter new password:
Re-enter new password:
New password is set successfully
```

11.32 sa_mgr show

Команда `sa_mgr show` предназначена для просмотра информации обо всех IPsec SA, ISAKMP SA, их состоянии и о количестве IKE обменов.

Синтаксис

```
sa_mgr [-T timeout] show [-isakmp|-ipsec] [-i CONN1_ID]
[-i CONNn_ID] [-detail]
```

- T timeout время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд.
- isakmp выводится информация об ISAKMP соединениях.
- ipsec выводится информация об IPsec соединениях.
- i CONNn_ID выводится информация о соединении с указанным идентификатором.
- detail выводится детальная информация о соединениях.

Команда `sa_mgr show` позволяет просмотреть действующие в данный момент IPsec SA.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

sa_mgr show

В данной команде без указания опции `-detail` выводится краткая информация обо всех соединениях, например:

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connections:
Num Conn-id (Remote Addr,Port)-(Local Addr,Port) State Sent Rcvd
1 2 (10.0.10.16,500)-(10.0.10.99,500) active 1560 656
2 3 (10.0.10.18,500)-(10.0.10.99,500) active 1560 656

IPsec connections:
Num Conn-id (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type
Sent Rcvd
1 6 (192.168.15.16,*)-(10.0.10.99,*) * AH+ESP tunn 600 1120
2 8 (192.168.15.18,*)-(10.0.10.99,*) * ESP tunn 1600 3140
```

В выводе присутствует следующая информация:

ISAKMP sessions – количество незавершенных IKE-обменов:

- ◆ `ni initiated` – в качестве инициатора
- ◆ `nr responded` – в качестве ответчика.

ISAKMP connections – информация обо всех ISAKMP SA и для каждого соединения:

- ◆ `Num` – порядковый номер ISAKMP соединения
- ◆ `Conn-id` – уникальный идентификатор ISAKMP соединения
- ◆ `Remote Addr, Port` – адрес и порт партнера, если порт любой – *
- ◆ `Local Addr, Port` – локальный адрес и порт, если порт любой – *
- ◆ `State` – состояние SA:
 - `incomplete` – недостроенное соединение
 - `active` – активное соединение
 - `configuration` – для данного SA проводится дополнительная настройка (`IKECFG`, `XAuth`, etc.)
 - `deleted` – SA не используется, подготовлен к удалению
 - `unknown` – статус соединения неизвестен
- ◆ `Sent` – количество переданной информации (в байтах)
- ◆ `Rcvd` – количество принятой информации (в байтах)

IPsec connections – информация обо всех IPsec SA и для каждого соединения:

- ◆ `Num` – порядковый номер IPsec соединения
- ◆ `Conn-id` – уникальный идентификатор IPsec соединения
- ◆ `Remote Addr, Port` – адрес и порт партнера, если порт любой – *
- ◆ `Local Addr, Port` – локальный адрес и порт, если порт любой – *
- ◆ `Protocol` – сетевой протокол, если протокол любой – *
- ◆ `Action` – действие – {`AH+ESP` | `AH` | `ESP`}
- ◆ `Type` – тип:
 - `tunn` – туннельный режим
 - `trans` – транспортный режим
 - `nat-t-tunn` – туннельный режим через NAT
 - `nat-t-trans` – транспортный режим через NAT
- ◆ `Sent` – количество переданной информации (в байтах)
- ◆ `Rcvd` – количество принятой информации (в байтах)

```
sa_mgr show -ipsec -i 8
```

Данная команда выводит информацию о соединении с заданными свойствами.

```
IPsec connections:
```

```
Num Conn-id (Remote Addr,Port)-(Local Addr,Port) Protocol Action Type
Sent Rcvd
1 8 (192.168.15.18,*)-(10.0.10.99,*) * ESP tunn 1600 3140
```

sa_smgr show -detail

Команда с опцией detail выводит полную информацию обо всех соединениях.

```
ISAKMP sessions: 0 initiated, 0 responded

ISAKMP connection id: 2
  cookies: 613E427395946DFE.DE99B25554306A75
  local peer (addr/port): 10.0.10.99/500
  remote peer (addr/port): 10.0.10.16/500

  local identity (IPV4_ADDR): 10.0.10.99
  remote identity (IPV4_ADDR): 10.0.10.16
  IKERule name: ike_rule_without_ikecfg
  auth: preshared key
  mode: main

  sa:
    transform: gost2814789cp-cbc gostr341194cp
    Oakley group: 5
    sa limits: key lifetime (qm/k/sec): -/200/28800
    sa timing: remaining key lifetime (qm/k/sec): -/198/26622
    status: active

IPsec connection id: 6
  local ident (addr/prot/port): 10.0.10.99/0/0
  remote ident (addr/prot/port): 192.168.15.16/0/0

  #pkts sent/rcvd: 32/6777
  #send/recv errors: 2/0

  local crypto endpt.: 10.0.10.99, remote crypto endpt.: 10.0.10.16
  connection status: {initiated locally, }

  remote identity (IPV4_ADDR): 10.0.10.16
  IPsecAction name: IPsec_action_01
  FilteringRule name: filter_rule_00_00
  PFS: none
```

```

inbound esp sa:
  spi: 0x94857A70(2491775600)
  transform: esp-gost2814789cp-cbc esp-gostr341194cp-hmac
  in use settings = {Tunnel, }
  sa limits: key lifetime (k/sec): 4608000/3600
  sa timing: remaining key lifetime (k/sec): 4607998/1426

inbound ah sa:
  spi: 0x6CD88232(1826128434)
  transform: ah-gostr341194cp-hmac
  in use settings = {Tunnel, }
  sa limiting: key lifetime (k/sec): 4608000/3600
  sa timing: remaining key lifetime (k/sec): 4607999/1426

outbound esp sa:
  spi: 0xF40CDEE0(4094484192)
  transform: esp-gost2814789cp-cbc esp-gostr341194cp-hmac
  in use settings = {Tunnel, }
  sa limits: key lifetime (k/sec): 4608000/3600
  sa timing: remaining key lifetime (k/sec): 4607999/1426

outbound ah sa:
  spi: 0xFBE599CD(4226128333)
  transform: ah-gostr341194cp-hmac
  in use settings = {Tunnel, }
  sa limiting: key lifetime (k/sec): 4608000/3600
  sa timing: remaining key lifetime (k/sec): 4607998/1426
    
```

В выводе присутствует следующая информация:

ISAKMP sessions – количество незавершенных IKE-обменов:

- ◆ ni initiated – в качестве инициатора
- ◆ nr responded – в качестве ответчика.

ISAKMP connection – в выводе будет присутствовать:

- ◆ поле IKECFG address, если был получен IKECFG адрес:

```

ISAKMP connection id: 1
cookies: F86F80B571D2240F.A0455C78E9DE66C
local peer (addr/port): 10.0.10.193/500
remote peer (addr/port): 10.0.10.178/500
IKECFG address: 192.168.15.193
    
```

- ◆ поле Status может принимать следующие значения:
 - incomplete – недостроенное соединение

- active – активное соединение
- configuration – для данного SA проводится дополнительная настройка (IKECFG, XAuth, etc.)
- deleted – SA не используется, подготовлен к удалению
- unknown – статус соединения неизвестен

IPsec connection :

- ◆ поле connection status может принимать значения:
 - initiated locally – локальный хост выступает инициатором
 - initiated remotely – локальный хост выступает ответчиком
 - rekeyed – произведено досрочное пересоздание соединения
 - no rekeying – досрочное пересоздание соединения в качестве инициатора запрещено
- ◆ поле in use settings может принимать значения:
 - Tunnel – туннельный режим
 - Transport – транспортный режим
 - Tunnel NAT-T – туннельный режим через NAT
 - Transport-NAT-T – транспортный режим через NAT

11.33 sa_mgr clear

Команда **sa_mgr clear** предназначена для удаления ISAKMP и IPsec соединений. Для работы с утилитой требуются права Администратора. Пользователь также должен иметь право изменять настройки Продукта.

Синтаксис

```
sa_mgr [-T timeout] clear [-isakmp|-ipsec] [-i CONN1_ID]
[-i CONNn_ID] [-silent]
sa_mgr [-T timeout] clear -all [-silent]
```

- | | |
|-------------|---|
| -T timeout | время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд. |
| -isakmp | удаляет ISAKMP соединения. |
| -ipsec | удаляет IPsec соединения. |
| -i CONN1_ID | удаляет соединения с указанным идентификатором. |
| -silent | удаляет соединения без уведомления партнера. |
| -all | удаляет все IPsec и ISAKMP соединения во всех состояниях, прекращаются все ранее начатые IKE-обмены. |

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Для выборочного удаления используются опции -isakmp, -ipsec, -i.

При этом ISAKMP соединения не удаляются сразу, а только подготавливаются к удалению (см. Status – deleted) и в течение заданного в политике безопасности времени еще могут быть переиспользованы.

Пример

Удаление ISAKMP соединений с идентификаторами 1 и 4:

```
sa_mgr clear -isakmp -i 1 -i 4
```

```
ISAKMP connection 1 is removed
ISAKMP connection 4 is not found
```

Удаление всех IPsec соединений:

```
sa_mgr clear -ipsec
```

```
IPsec connection 1 is removed
IPsec connection 3 is removed
```

Удаление всех соединений:

```
sa_mgr clear -all
```

```
All connections are removed
```

или

```
Not all connections are removed
```

11.34 ver_show

Команда `ver_show` предназначена для просмотра информации об установленном продукте.

Синтаксис

```
ver_show [-a|-i|-n|-r|-w|-d|-l|-p|-h]
```

Параметры:

- a выводит всю информацию (значение по умолчанию)
- i выводит информацию об установленной ОС
- n показывает имя продукта
- r показывает версию продукта
- w показывает версию и номер сборки продукта
- d показывает дату сборки продукта
- l показывает лицензию продукта
- p показывает информацию о криптопровайдере
- h показывает подсказку

Пример

```
ver_show
```

```
Build information:
product name:      Bel VPN Client
product release:   4.1
```

```
product build number: 4.1.17758
product build date: 2017-05-10 10:08:12
product target CPU: i386

System information:
OS information: Windows 7 Professional (6.1.7601) Service Pack 1
license information: CLIENT, STERRABEL, 12347
crypto provider: Avest
```

11.35 avverify

Утилита avverify предназначена для проверки хэш-значений и электронной цифровой файлов программного продукта, вызывается в утилите cspvpn_verify

Синтаксис

```
avverify -h | -e <полное_имя_файла>
<хэш|электронная_цифровая_подпись>
```

Параметры:

- h режим проверки хэша
- e режим проверки ЭЦП

11.36 Сообщения об ошибках

Ниже приведены тексты сообщений об ошибках, которые могут возникать при работе с программными утилитами.

Если в тексте полученного сообщения присутствует фраза "Internal error:", то обращайтесь в службу поддержки по адресу support@s-terra.by.

11.36.1 Утилиты cert_mgr show, cert_mgr import, cert_mgr check, cert_mgr create, cert_mgr remove

Текст сообщения	Описание проблемы
User Error: no source file specified	Не указан путь к файлу (cert_mgr ... -f)
User Error: FILENAME unable to open file	Ошибка при открытии файла
Internal Error: No memory	Нет свободной оперативной памяти
User Error. No password specified to open FILENAME	Не задан пароль доступа к файлу
FILENAME wrong password PASSWORD	Неверный пароль
User Error. No password specified	Не указан пароль (cert_mgr-p)
Internal Error. Unable obtain certs from DB	Не удается получить сертификаты из базы продукта
User Error: no number specified\n	Не указан индекс сертификата (cert_mgr -i)

Текст сообщения	Описание проблемы
User Error: NUMBER exceeds number of objects	Указанный индекс превышает количество объектов в базе продукта
User Error. No subject	Не задано поле Subject сертификата
User Error: Key KEY1 is not compatible with key KEY2	Несовместимость заданных параметров (ключей)
User Error: Key KEY is useless	Задан лишний параметр
User Error: Key KEY is used twice	Повторное задание параметра (ключа)
User Error: Unable remove. Base is empty	Попытка удаления сертификата из пустой базы продукта
Internal Error:Unable remove object from base	Неудачная попытка удаления объекта из базы продукта
User Error. Missing parameter	Отсутствует параметр
User Error. No file name specified	Не указано имя файла
Internal Error. Storage error.	Ошибка при открытии хранилища
User Error: INDEX exceeds number of objects in NAME	Значение индекса превышает количество объектов в хранилище NAME
User Error: Container name is not specified	Не указано имя контейнера
User Error: CRL can not be removed from base	CRL не может быть удален из базы продукта
User Error: Object index INDEX exceeds number of certificates and CRLs in base	Индекс объекта превышает количество сертификатов и CRL в базе продукта
User Error. Missing index of object to be removed from base. Specify 'i' key and index	Не указан индекс объекта для удаления из базы продукта
User Error. Specify certificate request subject	Ошибка задания поля Subject в запросе на сертификат
Internal Error. Unable to create certificate request ERRCODE	Ошибка при создании запроса на сертификат
Internal Error. Unable to put certificate request into base ERRCODE	Ошибка при сохранении запроса на сертификат
User Error. Missing index of object to be imported from <FILENAME>. Specify 'i' key and index	Не указан индекс объекта для регистрации в базе продукта.
User Error. Container 'CONTAINER_NAME' is not exists or access denied	Не удалось получить доступ к контейнеру (убедиться в наличии и доступности контейнера)
User Error. Failed to read private key: ERROR_DESCRIPTION	Не удалось получить секретный ключ (убедиться в доступности ключа в контейнере)
User Error. Cannot connect to the IPsec service: service is not running.	Не удалось соединиться с демоном (убедиться, что демон запущен)
User Error. Unable to set trusted status to certificate CERT_DSC	Не удалось выставить сертификату статус TRUSTED (убедиться, что сертификат CA)
User Error. Key is not consistent to cert CERT_DSC	Секретный ключ не подходит к сертификату или проверка закончилась неудачей (убедиться, что задан верный контейнер)
User Error. Unable to associate key and crt CERT_DSC	Не удалось ассоциировать секретный ключ и сертификат (убедиться, что сертификат не CA)
User Error: attempt to import a CRL as certificate	Задан недопустимый ключ "-t -kf -kfp -kc -kcp" при импорте CRL

Текст сообщения	Описание проблемы
User Error: Key -t is not compatible with key -l -kf -kfp -kc -kcp	Задан недопустимый ключ “ -kf -kfp -kc -kcp” при импорте Trusted CA сертификата
Error: Cannot import Trusted or Local cert in current TokenLogin mode	Невозможен импорт Trusted или Local сертификата в режиме TokenLogin
Error: Cannot Cannot create request in current TokenLogin mode	Невозможен создать запрос на сертификат в режиме TokenLogin
Error: You need the Administrator permissions	Недостаточно прав пользователя

11.36.2 Утилита client_login, client_logout

Текст сообщения	Описание проблемы
User Error %d: VPN demon is not started	Проблема со стартом демона
User Error %d: Logout fail	Неудачный logout
VPN demon is not ready. Try again later	Демон недоступен
VPN service has returned error code: <код ошибки>	Ошибка при попытке входа
VPN service does not know how to provide the operation	Демон не понимает запроса на вход. Возникает при изменениях настроек без перезапуска демона
Old password is incorrect	Неверный старый пароль
The password is not changed. File or directory of DB cannot be created, removed or renamed	Ошибка при внесении изменений в DB
The password is not changed. Error: <код ошибки>	Ошибка при установке пароля

11.36.3 Утилита csrvpn_verify

Текст сообщения	Описание проблемы
Integrity verification tool not found	Отсутствует продукт, используемый непосредственно для подсчета контрольных сумм.
Integrity verification list “file_.hashes_full_path” not found	Отсутствует файл .hashes.
Integrity verification list “file_.hashes_full_path” is corrupted	Проблемы с чтением файла .hashes (например, ошибочный синтаксис файла).
Integrity verification tool call failed on file “product_file_full_path”	Запуск avverify по каким-либо причинам не произошел (какая-то системная ошибка; например, нехватка ресурсов, проблемы с правами доступа и т.п.) или вернул неожиданный код возврата (прерывание по сигналу, необработанный exception и т.п.).
File “product_file_full_path” is corrupted	Один или больше файлов продукта повреждены. (хэш-сумма не соответствует эталонной; также возможны и другие ситуации, например, отсутствует файл).

11.36.4 Утилита dp_mgr show

Текст сообщения	Описание проблемы
User Error: "ddd" is unknown parameter	Введен неизвестный параметр
User Error %d: VPN demon is not started	Проблема со стартом демона
Internal Error %d: Default driver policy is not wrote to db	Ошибка при записи Default Driver Policy в базу продукта
Internal Error %d: Default driver policy is not read from db	Ошибка при чтении Default Driver Policy из базы продукта

11.36.5 Утилиты drv_mgr show, drv_mgr set, drv_mgr reload

Текст сообщения	Описание проблемы
User Error: Value for "NAME" is missing	Не задано значение настройки
User Error: Property name "NAME " is unknown	Имя настройки введено не верно
User Error: Required parameters are missing	Не задан обязательный параметр
User Error: command "NAME" is unknown	Введена неизвестная команда
Internal Error: Value of "NAME" cannot be read. Error: DESC	Не удалось получить значение настройки из драйвера
User Error: Value of "NAME" is not set to VALUE. Error: DESC	Не удалось выставить значение настройки в драйвер
User Error: Value of "NAME" is not saved to file.\n	Не удалось сохранить значение настройки в cfg файл (убедиться, что файл доступен на запись)
User Error: Values are not saved to file NAME.Error:DESC.	Не удалось сохранить cfg файл
User Error: File NAME cannot be loaded	Не удалось загрузить значения настроек из cfg файла (убедиться, что файл доступен на чтение).
Error: You need the Administrator permissions	Недостаточно прав пользователя

11.36.6 Утилита if_show

Текст сообщения	Описание проблемы
Internal error. Couldn't initialize local network interface list	Не удается получить информацию о сетевых интерфейсах
Internal error. Couldn't receive local network interface information	Не удается получить информацию об именах логических интерфейсов
User Error. Couldn't load network interface aliases file	Невозможно загрузить файл "ifaliases.cf", хотя пакет установлен
User Error. Couldn't access PRODUCT driver	Драйвер пакета недоступен, хотя пакет установлен
Warning: PRODUCT is not located	Предупреждение. Установленный пакет не найден. Не является ошибкой

11.36.7 Утилита `integr_mgr calc`, `integr_mgr check`

Код ошибки	Текст сообщения	Описание проблемы
0	SUCCESS: Operation was finished successfully.	Успешное окончание.
9	ERROR: Missing required command or parameters. (Try 'integr_mgr -h' for help)	Недостаточное количество параметров в командной строке.
9	ERROR: Invalid command 'имя_команды'. (Try 'integr_mgr -h' for help)	Введено имя операции, которое утилита распознать не может. Допустимы операции 'calc' и 'check'.
9	ERROR: Missing or invalid target file definition. (Try 'integr_mgr -h' for help)	В командной строке отсутствует имя файла для выполнения операции с единичным файлом..
9	ERROR: Missing target file name. (Try 'integr_mgr -h' for help)	В командной строке отсутствует имя файла со списком объектов для выполнения операции.
9	ERROR: Too long target file name 'имя файла'. (Try 'integr_mgr -h' for help)	Указанное имя файла превышает в длину 500 символов.
9	ERROR: Hash library initialization error.	Внутренняя ошибка инициализации системы вычисления хеша.
50	ERROR:: Missing file '<имя_файла>' or missing access to this file.	Указано имя несуществующего файла либо отсутствуют права на чтение содержимого этого файла. Данная ошибка может возникнуть как при обработке списка, так и при обработке единичного файла.
50	ERROR:: Missing file '<имя_файла_с_расширением_hash>'.	При попытке операции проверки выявлено отсутствие файла с контрольной информацией.
54	ERROR: Read file is fault.	Ошибка чтения содержимого проверяемого файла.
54	ERROR: Invalid hash calculation.	Внутренняя ошибка вычисления контрольной информации.
54	ERROR: Invalid contents file '<имя_файла_с_расширением_hash>'.	Файл с контрольной информацией поврежден.
54	ERROR: Corrupted file '<имя_проверяемого_файла>'	Проверяемый файл поврежден.
54	ERROR: Invalid format of list file.	Формат файла списка проверяемых файлов нарушен.
54	ERROR: File '<имя_файла_из_списка>' was corrupted.	Поврежден проверяемый файл из списка.
75	ERROR: Can't create file '<имя_файла_с_расширением_hash>'.	Невозможно создать файл с контрольной информацией.
75	ERROR: Can't write file '<имя_файла_с_расширением_hash>'	Невозможно записать файл с контрольной информацией

11.36.8 Утилиты key_mgr import, key_mgr remove, key_mgr show

Текст сообщения	Описание проблемы
Internal Error: No memory to open file FILENAME	Недостаточно памяти, чтобы открыть файл
User Error: Key file no specified	Не указан файл с ключом
User Error: Key name no specified	Не указано имя ключа
Internal Error. Unable to append key into base KEYNAME	Ошибка при попытке импорта ключа в базу Продукта

11.36.9 Утилита lic_mgr set

Текст сообщения	Описание проблемы
User Error: <parameter> undefined	Не указан один из параметров
User Error: Wrong license	Неверная лицензия
Internal Error: Can't write license file	Ошибка при записи лицензии
Error: You need the Administrator permissions	Недостаточно прав пользователя

11.36.10 Утилита log_mgr show

Текст сообщения	Описание проблемы
User Error: "ddd" is unknown parameter	Введен неизвестный параметр.
User Error: %d: VPN demon is not started	Проблема со стартом демона
Internal Error %d: Failed to set default log level	Ошибка при установке уровня протоколирования
Internal Error %d: Failed to get default log level	Ошибка при получении уровня протоколирования
User Error: Parameter is missing	Пропущен параметр команды
User Error: Too many parameters	Слишком много параметров команды
Internal Error: Failed to set log levels for msg group	Ошибка установки группы log levels
Internal Error: Failed to load the msg group file	Ошибка загрузки файла группы
Internal Error: Failed to get the msg group	Ошибка получения группы log levels
Internal Error: Failed to save log levels	Ошибка сохранения log levels

11.36.11 Утилиты lsp_mgr reload, lsp_mgr unload, lsp_mgr show

Текст сообщения	Описание проблемы
User Error.FILENAME unable to open file	Ошибка при попытке открыть файл (убедиться в доступности файла).
Internal Error: Unable to set LSP as active	Не удалось загрузить LSP из файла в базу продукта
Internal Error: No memory to open file FILENAME	Недостаточно памяти для открытия файла
Internal Error: unrecognized error	Внутренняя ошибка
Internal Error: Unable to reload lsp from base	Не удалось перезагрузить LSP из базы продукта

Текст сообщения	Описание проблемы
Error: Cannot change LSP in current TokenLogin mode	В режиме TokenLogin изменение LSP запрещено

11.36.12 Утилита pwd_change

Текст сообщения	Описание проблемы
User Error %d: VPN demon is not started	Проблема со стартом демона
User Error %d: Old password is wrong	Неверный старый пароль
User Error %d: New password is not set	Ошибка при установке пароля

11.36.13 Утилиты sa_mgr show, sa_mgr clear

Текст сообщения	Описание проблемы
Internal Error: SAs' clearing failed. Error: %s.	Не удалось удалить ISAKMP или IPsec соединения.
Internal Error: ISAKMP info not available. Error: %s	Не удается получить информацию об ISAKMP
Internal Error Connections info not available. Error: %s	Не удается получить информацию о соединениях
Timeout expired. Please ensure that all chosen SAs are cleared.	Закончилось время ожидания завершения удаления соединений. Убедитесь, что все выбранные соединения удалены.

11.36.14 Утилита avverify

Текст сообщения	Описание проблемы
Verification COMPLETED	Не удалось удалить ISAKMP или IPsec соединения.
USAGE: avverify -h <full_name_with_path_of_file> <hash> or avverify -e <full_name_with_path_of_file> <EDS>c	Недостаточное количество параметров в командной строке вызывает вывод подсказки в использовании.
ERROR: Initialization errorc	Внутренняя ошибка инициализации системы.
ERROR: Invalid check valuec	Отсутствует или имеет неверный формат значение контрольной информации для проверки.
ERROR Open file error. <далее строка описания ошибки в формате операционной системы>	Ошибка открытия проверяемого файла.
ERROR: Read file error. <далее строка описания ошибки в формате операционной системы>	Ошибка чтения содержимого проверяемого файла.
ERROR: Verification unsuccessfulc	Проверка выявила несоответствие предложенного значения контрольной информации и вычисленного значения. Возможно, проверяемый файл поврежден.
ERROR: Calculation unsuccessfulc	Ошибка вычисления контрольной информации.c