УТВЕРЖДЕНО

**BY.РТНК.00002-03.01 34 01-ЛУ**

# Программно-аппаратное устройство «Клиент безопасности Bel VPN Client 3.0.1»

# РУКОВОДСТВО ОПЕРАТОРА

## Руководство пользователя

**BY.РТНК.00002-03.01 34 01**

Листов 100

| | |
|---|---|
| Подп. и дата | |
| Инв. № дубл | |
| Взам. инв. № | |
| Подп. и дата | |
| Инд. № подл | |

2012

# Содержание



  

  

# Лицензионное Соглашение

**о праве пользования Продуктом Bel VPN Client производства ИП «С-Терра Бел»**



Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного Продукта Bel VPN Client (далее - Изделия) Конечным Пользователем (физическим или юридическим лицом, указанным в Лицензии на использование Продукта, являющейся неотъемлемой частью настоящего Лицензионного Соглашения). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных непередаваемых прав пользования Изделием.

Под Изделием понимается комплекс объектов (программных средств, носителей информации, кода программных Продуктов, документации в печатной и электронной формах), включенных в Спецификацию Комплекта Изделия.

*Изделие может использоваться только в качестве персонального Агента защиты (устанавливаться на персональный компьютер пользователя) и не предназначено для использования в других целях. Использование Изделия в прочих системах и/или в иных целях является нарушением настоящего Лицензионного Соглашения.*

Изделие может включать компоненты (программные средства, информационные носители и прочее) от третьих поставщиков. Конечный Пользователь получает права на использование этих компонент на основе Лицензий и Лицензионных Соглашений этих поставщиков, которые являются в совокупности неотъемлемой частью настоящего Лицензионного Соглашения.

Изделие в полном комплекте передается Конечному Пользователю на условиях настоящего Лицензионного Соглашения.

Изделие и его компоненты являются интеллектуальной собственностью Производителя и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Республики Беларусь об авторском праве на объекты интеллектуальной собственности.

Установка Изделия после предъявления Конечному Пользователю текста Лицензионного Соглашения рассматривается как согласие Конечного Пользователя с условиями Лицензионного Соглашения и вступление его в законную силу, после чего настоящее Лицензионное Соглашение в соответствии со ст. 403 Гражданского Кодекса Республики Беларусь имеет силу договора между Конечным Пользователем и Производителем Изделия (ИП «С-Терра Бел»).

При наличии компонент третьих поставщиков Производитель является законным и полномочным представителем третьих поставщиков, если обратное не оговорено в Лицензионных Соглашениях третьих поставщиков или в других документах, регламентирующих отношения между Конечным Пользователем и третьими поставщиками.

Все компоненты третьих поставщиков объединяются в программный Продукт (комплекс) в процессе установки Изделия. Конечный Пользователь имеет право на копирование, установку и эксплуатацию всех компонент третьих поставщиков, поставленных в составе Изделия только в составе работ, связанных с эксплуатацией Изделия. Копирование, распространение, установка и эксплуатация отдельных компонент являются нарушением настоящего Лицензионного Соглашения и авторских прав как Производителя, так и третьих поставщиков (если обратное не оговорено в Лицензиях и Лицензионных Соглашениях третьих поставщиков).

Конечный Пользователь может устанавливать и использовать в рамках настоящего Лицензионного Соглашения только одну копию (единицу) Изделия и не имеет права устанавливать и использовать большее количество копий (единиц) Изделия.

Конечный Пользователь не имеет права распространять Изделие в формах предоставления доступа третьим лицам к воспроизведению или к воспроизведенным в любой форме компонентам Изделия путем продажи, проката, сдачи внаем, предоставления взаймы или иными другими способами отчуждения.

Конечный Пользователь не имеет права дисассемблировать, декомпилировать (преобразовывать бинарный код в исходный текст) программы и другие компоненты Изделия, вносить какие-либо изменения в бинарный код программ и совершать относительно Изделия другие действия, нарушающие нормы Республики Беларусь и международные нормы по авторскому праву и использованию программных средств.

Настоящее Лицензионное Соглашение вступает в силу с момента установки Изделия и действует на протяжении всего срока использования Изделия.

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Республики Беларусь от 16.05.1996 г. «Об авторском праве и смежных правах» и преследуется по закону.

Настоящее Лицензионное Соглашение предоставляет Конечному Пользователю Ограниченные гарантии, состоящие в том, что

1. В случае, если в ходе эксплуатации Изделия Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Изделия (ИП «С-Терра Бел») обеспечивает:

а) информирование доступными способами Конечного Пользователя о существовании Критичной Проблемы и о способах ее устранения

б) бесплатное предоставление обновлений программного обеспечения Производителя Изделия, в которых устранены Критичные Проблемы.

Примечание 1. Гарантийное обязательство 1 базируется на следующем определении: Критичная Проблема заключается в том, что Изделие, вследствие ошибки в программном обеспечении, не выполняет основные функции безопасности, а именно шифрование трафика и контроль доступа, что приводит к нарушению безопасности сети Конечного Пользователя.

Примечание 2. Обновления программного обеспечения в соответствии с гарантийным обязательством п.1б предоставляются по запросу Конечного Пользователя и по мере разработки обновлений.

2. Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки Изделия дефекты в составе информационных носителей или некомплектность Изделия, то информационные носители будут заменены, а комплектность Изделия восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности изделия и/или дефектам носителей информации рассматриваться не будут.

Настоящее Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию Изделия любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Изделия и его компонент в установленном порядке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

Настоящее Лицензионное Соглашение (в рамках законодательства Республики Беларусь и если противное не оговорено в виде отдельного дополнительного соглашения с Конечным Пользователем) не регламентирует вопросы технических, организационных и прочих возможных проблем, связанных с эксплуатацией Изделия и возможных материальных, финансовых и прочих потерь Конечного Пользователя в результате эксплуатации Изделия.

Срок действия настоящего Лицензионного Соглашения распространяется на весь период эксплуатации Изделия Конечным Пользователем. Действие настоящего Лицензионного Соглашения может быть прекращено по решению Конечного Пользователя. В этом случае Конечный Пользователь должен уничтожить все информационные носители, содержащие код и прочие информационные компоненты Изделия, включая информацию на внутренних носителях Изделия. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

Программный Продукт Системная Библиотека GNU libc является свободно распространяемым Продуктом и используется в составе Изделия без каких либо модификаций в соответствии с лицензией "The GNU General Public License" (http://www.gnu.org/licenses/licenses.html).

MS-DOS, Windows, Windows 98/NT/2000/XP/Vista/7 являются торговыми марками компании Microsoft Corporation в США и в других странах.

Sun Solaris и Java являются торговыми марками компании Sun Microsystems, Inc в США и в других странах.

Cisco, Cisco PIX Firewall, Cisco IOS Router, CiscoWorks, CiscoWorks VPN/Security Management Solution, CiscoWorks Management Center for VPN Routers, CiscoWorks Management Center for PIX Firewall являются торговыми марками компании Cisco Systems в США и в других странах.

Изделие включает в себя программное обеспечение, написанное Эриком Янгом (Eric Young. eay@cryptsoft.com)

Другие названия компаний и Продуктов, упомянутые в настоящем Лицензионном Соглашении и в составе информационных источников Изделия могут являться зарегистрированными торговыми марками соответствующих им компаний. Упоминание наименований, Продуктов, торговых марок третьих организаций исключительно неформально и не является ни поддержкой, рекомендацией либо рекламой. ИП «С-Терра Бел» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.

Напечатано в Республике Беларусь

ИП «С-Терра Бел»
220012, г. Минск, ул. Чернышевского, д. 12А, офис 702.
тел.: (+375 17) 280 6000
факс: (+375 17) 280 7867
эл.почта: info@s-terra.by
http://www.s-terra.by

  

# 1. Назначение и функции продукта

Продукт Bel VPN Client предназначен для защиты и фильтрации трафика протоколов семейства TCP/IP.

Защита трафика Bel VPN Client осуществляется 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.

Программный продукт Bel VPN Client обеспечивает:

- защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPsec AH и/или IPsec ESP
- аутентификацию пользователя и аутентификацию узла сети
- пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого и транспортного уровней
- событийное протоколирование
- реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения, доступ в заданном защищенном режиме только для зарегистрированных, в том числе и для мобильных партнеров по взаимодействию
- регулируемую стойкость защиты трафика
- маскировку адресных пространств защищаемых сетей (туннелирование трафика).

Все эти функции описываются в файле локальной политики безопасности (LSP- Local Security Policy). Локальная политика безопасности определяет какие из сетевых соединений следует защищать, а какие следует использовать открытыми, какие режимы и алгоритмы защиты использовать для каждого из соединений.

Продукт Bel VPN Client использует криптографические библиотеки программного средства электронной цифровой подписи и шифрования "AvCrypt ver. 5.1", разработанное компанией "Авест".

" AvCrypt ver. 5.1" реализует криптографические алгоритмы в соответствии со стандартами Республики Беларусь:

- алгоритмы криптографического преобразования в соответствии с Государственным стандартом Республики Беларусь ГОСТ 28147-89
- функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.1-99
- функции хеширования в соответствии с Государственным стандартом Республики Беларусь СТБ 34.101.31-2011
- процедура выработки и проверки электронной цифровой подписи в соответствии с Государственным стандартом Республики Беларусь СТБ 1176.2-99
- процедуру выработки псевдослучайных данных в соответствии с РД РБ 07040.1202-2003 «Банковские технологии. Процедуры выработки псевдослучайных данных с использованием секретного параметра».

Bel VPN Client является продуктом для корпоративного использования в том смысле, что политику и настройки режимов этого продукта осуществляет системный администратор или администратор безопасности предприятия.

# 2. Требования на базовые платформы и совместимость

Продукт Bel VPN Client работает под управлением операционных систем:

- MS Windows XP (32-bit, выпуск Professional) SP2/3
- MS Windows Vista (32-bit, выпуск Business / Enterprise / Ultimate) SP1/2
- MS Windows 7 (32-bit, выпуск Professional / Enterprise / Ultimate)

Продукт работает корректно на компьютерах с сетевыми адаптерами, которые поддерживают "`task offloading`".

В части реализации протоколов IPsec/IKE и их расширений Продукт совместим с Cisco IOS v.12.4.

В части удаленного мониторинга и сбора статистики управления Продукт совместим с CiscoWorks Monitoring Center for Performance 2.0.2, входящим в состав CiscoWorks VMS 2.3.

  

# 3. Атрибуты аутентификации

Технология IPsec обеспечивает аутентификацию, шифрование и целостность данных на уровне передаваемых IP-пакетов.

Для реализации этих функций технологии IPsec необходима дополнительная информация, которая поставляется протоколом IKE: ключевой материал и согласованная политика защиты.

Для аутентификации взаимодействующих сторон протоколу IKE необходима некоторая аутентификационная информация.

Такой аутентификационной информацией может быть:

- предустановленный (разделяемый) ключ (Preshared Key)
- сертификат стандарта X.509.

  

# 4. Процесс подготовки персонального инсталляционного пакета пользователя

Продукт Bel VPN Client рассчитан для применения внутри корпоративных сетей. В таких сетях пользователь не имеет право на изменение политики безопасности корпоративной сети. Поэтому продукт Bel VPN Client разработан таким образом, что администратор безопасности корпоративной сети формирует персонализованный инсталляционный пакет для каждого пользователя. При этом он производит настройки для пользователя, которые согласуются с его должностными обязанностями.

Для подготоки инсталляционного пакета пользователя администратору необходимо иметь предустановленные ключи, либо сертификаты открытых ключей пользователя, и локальную политику безопасности, предписанную для данного пользователя.

При использовании предустановленных (разделяемых) ключей (Preshared Keys) подготовка персонального инсталляционного пакета пользователя осуществляется полностью администратором.

При использовании сертификатов открытых ключей подготовка инсталляционного пакета пользователя осуществляется по одному из двух сценариев.

Секретный ключ пользователя, соответствующий открытому ключу сертификата, находится в контейнере. Контейнер имеет сложную структуру, в нем содержится личный ключ ЭЦП СТБ 1176.2-99, параметры ДСЧП на основе функции хэширования СТБ 1176.1-99 и какая-то ключевая информация, необходимая для обеспечения защиты и целостности ключа. Секретный ключ может быть расположен в контейнере, либо в файле, которые размещаются на жестком диске либо отчуждаемом носителе ключевой информации, например, AvPass и др.

Сценарии отличаются тем, кто создает ключевую пару для локального сертификата пользователя, возможна или нет проверка соответствия сертификата пользователя и секретного ключа, копируется или нет контейнер с секретным ключом во время инсталляции на компьютере пользователя.

  

# 4.1. Первый сценарий

Все действия по созданию ключевой пары, формированию запроса и созданию сертификата пользователя производятся администратором безопасности и (или) администратором CA. В этом сценарии контейнер с секретным ключом помещается либо на внешнем устройстве хранения информации, либо в инсталляционном файле, при этом будет проведена проверка соответствия сертификата пользователя и секретного ключа во время создания инсталляционного файла.

Действия администратора по этому сценарию следующие:

- администратор безопасности или администратор CA создает ключевую пару и формирует запрос на выдачу локального сертификата с помощью утилиты cryptocont.exe . Эта утилита описана в Приложении "Утилита cryptocont.exe" Запрос на выдачу сертификата передается администратору CA при этом контейнер с личным ключом пользователя остается на компьютере администратора безопасности
- администратор CA на сервере удостоверяющего центра по полученному запросу создает локальный сертификат пользователя и экспортирует его в файл. Корневой сертификат удостоверяющего центра (Trusted CA Certificate) также экспортируется в файл. Администратор безопасности получает оба эти сертификата от администратора CA
- администратор безопасности определяет для пользователя локальную политику безопасности (LSP), способ инициализации датчика случайных чисел и создает инсталляционный файл для пользователя
- подготовленный инсталляционный файл содержит исполняемый код продукта Bel VPN Client, персональные настройки, локальную политику безопасности, CA сертификат и локальный сертификат пользователя. Контайнер с секретным ключом помещается либо на внешнем устройстве хранения информации, либо в инсталляционном файле. Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из инсталляционного файла, а также контейнера с секретным ключом пользователя на на внешнем устройстве хранения информации.

Пользователь, получив инсталляционный пакет, производит установку продукта Bel VPN Client на своем компьютере.

  

## 4.2. Второй сценарий

Создание ключевой пары и формирование запроса на локальный сертификат пользователя производятся администратором безопасности или пользователем на компьютере пользователя с помощью утилиты `cryptocont.exe`. При этом контейнер с секретным ключом размещается на жестком диске на компьютере пользователя. В этом сценарии невозможна проверка соответствия сертификата пользователя и секретного ключа.

Действия администратора по этому сценарию следующие:

- администратор безопасности или пользователь на компьютере пользователя создает ключевую пару и формирует запрос на локальный сертификата пользователя. Созданный запрос посылается на сервер удостоверяющего центра сертификатов. При этом контейнер с секретным ключом пользователя размещаются на жестком диске.
- администратор CA на сервере удостоверяющего центра по полученному запросу создает локальный сертификат пользователя и экспортирует его в файл. Корневой сертификат удостоверяющего центра (Trusted CA Certificate) также экспортируется в файл. Администратор безопасности получает оба эти сертификата от администратора CA
- администратор безопасности на своем рабочем месте определяет для пользователя локальную политику безопасности (LSP), локальные настройки, определяет способ инициализации датчика случайных чисел и создает инсталляционный файл для пользователя
- подготовленный инсталляционный файл содержит исполняемый код код продукта Bel VPN Client, персональные настройки, локальную политику безопасности, локальный сертификат пользователя и CA сертификат. Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из одного инсталляционного файла.

Пользователь, получив инсталляционный пакет, производит установку продукта Bel VPN Client на своем компьютере.

  

# 4.3. Третий сценарий

Все действия по созданию ключевой пары, формированию запроса и созданию сертификата пользователя производятся администратором безопасности и(или) администратором CA. В этом сценарии контейнер с секретным ключом размещается на ключевом носителе, при этом будет проведена проверка соответствия сертификата пользователя и секретного ключа во время создания инсталляционного файла.

Действия администратора по этому сценарию следующие:

- администратор безопасности или администратор CA инициализирует ключевой носитель, создает ключевую пару и формирует запрос на выдачу локального сертификата с помощью утилиты cryptocont.exe. При этом контейнер с личным ключом пользователя размещается защищенном ключевом носителе.
- администратор CA на сервере удостоверяющего центра по полученному запросу создает локальный сертификат пользователя и экспортирует его в файл. Корневой сертификат удостоверяющего центра (Trusted CA Certificate) также экспортируется в файл. Администратор безопасности получает оба эти сертификата от администратора CA
- администратор безопасности определяет для пользователя локальную политику безопасности (LSP) и записывает ее в файл.
- подготовленный инсталляционный файл содержит исполняемый код продукта Bel VPN Client, персональные настройки, локальную политику безопасности, CA сертификат и локальный сертификат пользователя со ссылкой местоположения контейнера с секретным ключом на компьютере пользователя. Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий либо из инсталляционного файла, контейнера с секретным ключом пользователя на внешнем ключевом носителе.

Пользователь, получив инсталляционный пакет, производит установку продукта Bel VPN Client на своем компьютере.

  

# 5. Инсталляция Bel VPN Client

Продукт Bel VPN Client работает под управлением операционных систем:

- MS Windows XP (32-bit, выпуск Professional) SP2/3
- MS Windows Vista (32-bit, выпуск Business / Enterprise / Ultimate) SP1/2
- MS Windows 7 (32-bit, выпуск Professional / Enterprise / Ultimate)

Установка продукта осуществляется запуском инсталляционного файла, подготовленного и переданного администратором безопасности пользователю.

Инсталляция должна производиться пользователем, имеющим права администратора.

После запуска файла для установки Bel VPN Client инсталляция происходит в одном из 3 режимов, который был выбран администратором при подготовке инсталляционного файла:

- режим `basic` – основной режим, неинтерактивная установка с запросом на инсталляцию, вариант по умолчанию
- режим `normal` - интерактивная установка
- режим `silent` - неинтерактивная установка без запросов.

Все протоколируемые события при инсталляции Bel VPN Client будут записываться в файл, который задал администратор при создании инсталляционного пакета пользователя.

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 info@s-terra.by.

При инсталляции Bel VPN Client происходит отключение стандартного сервиса, связанного с IPsec и IKE и перевод его в состояние Manual. В Windows XP – это Служба IPSEC, внутреннее название которой PolicyAgent. В Windows Vista/7 – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности» (внутреннее название – IKEEXT). В Windows 7 отключение службы необходимо выполнить вручную.

В Windows Vista/7 производится настройка штатного FireWall сервиса (Брандмауэр Windows). При установке Bel VPN Client в Windows FireWall добавляется новое правило:

- правило для входящих подключений
- имя – CSP VPN Service – UDP allowed (predefined)
- правило включено
- действие – разрешить подключение
- протокол – UDP (все порты)
- программа – полный путь к установленному файлу `vpnsvc.exe`
- службы – применятьтолько 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.

  

## 5.1. Режим basic

В ОС **Windows Vista/7** при установке Bel VPN Client выдается окно (Рисунок 1). Необходимо разрешить запуск инсталлятора – выберите предложение `Разрешить`.

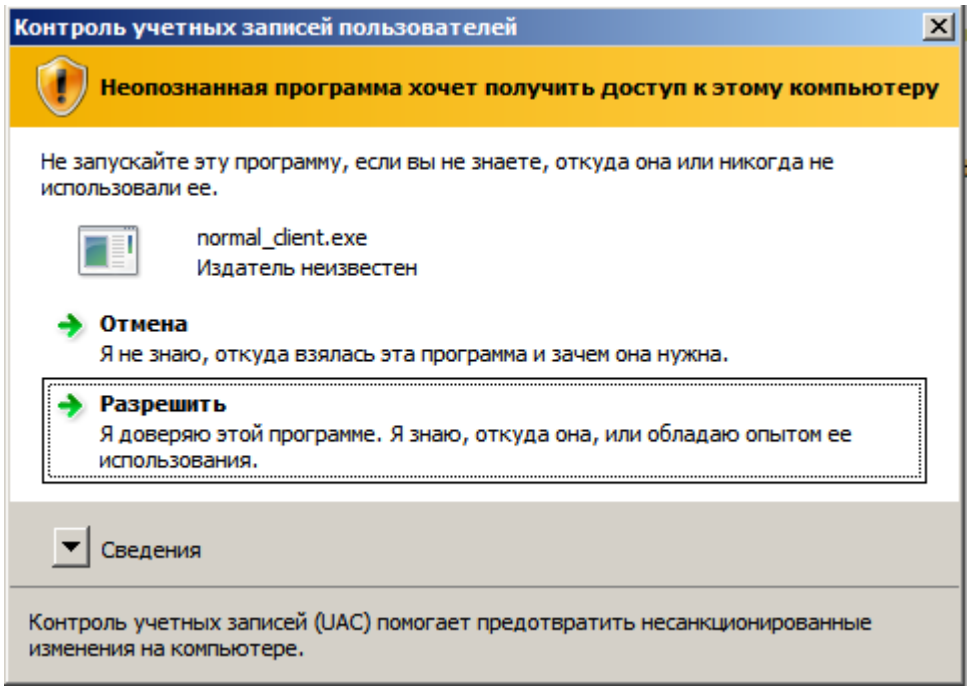


Рисунок 1

Затем выдается запрос на инсталляцию Bel VPN Client (в ОС Windows XP это окно появляется первым):

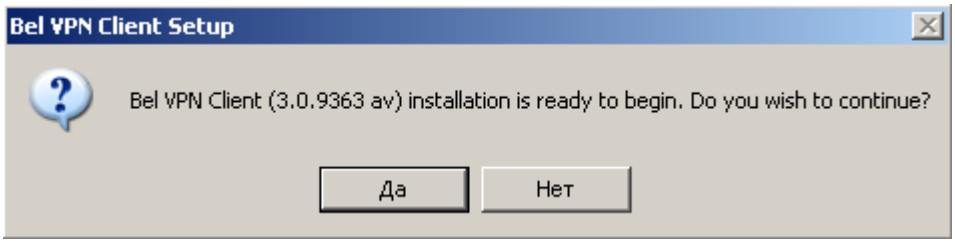


Рисунок 2

После нажатия кнопки `Да` происходит установка продукта:


Рисунок 3

Появляется окно с индикатором процесса инсталляции:

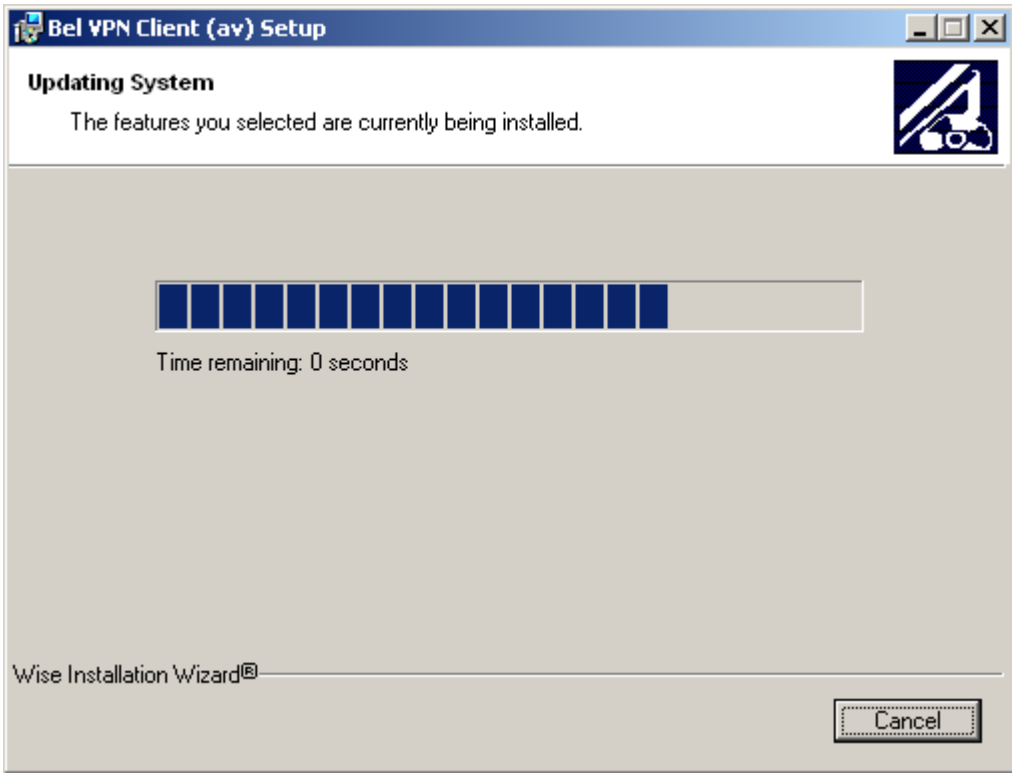


Рисунок 4

Если в процессе подготовки инсталляционного пакета был выбран способ задания данных для инициализации RNG `User biological initialization on user computer` , то появится окно, в котором просят ввести какую-то начальную информацию для датчика случайных чисел (пользователю предлагается произвольным образом нажимать на клавиши до тех пор, пока не будет собрано достаточное количество случайных данных – обычно 80 нажатий):

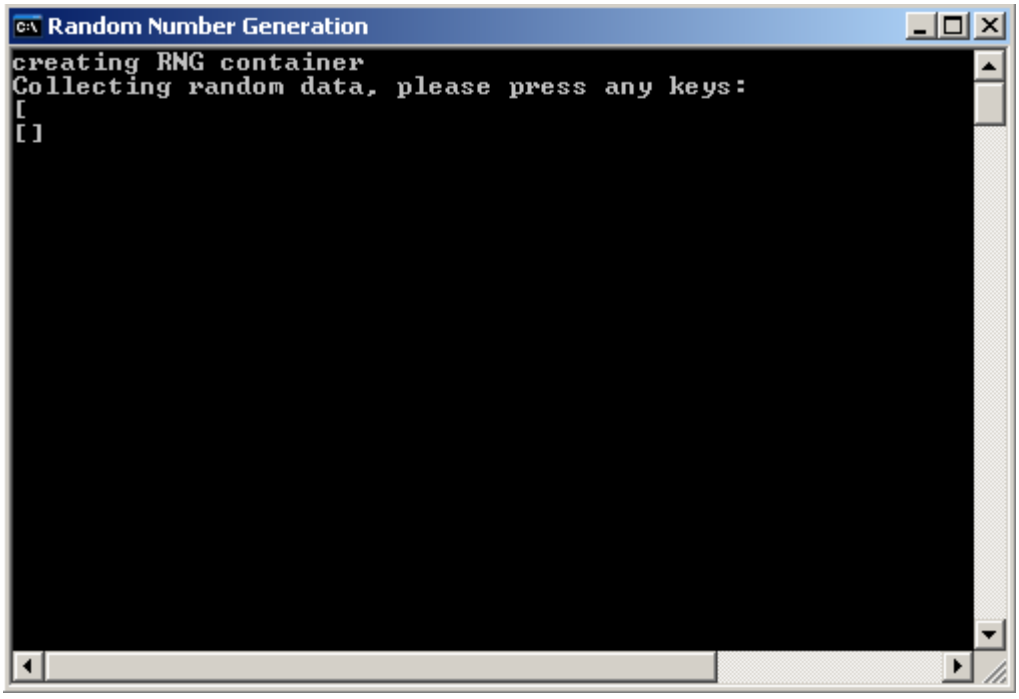


Рисунок 5

Если для инициализации RNG используются данные из существующего контейнера или происходит импорт контейнера из инсталляционного пакета, то окно Random Number Generation не появляется.

Если происходит импорт контейнера из инсталляционного пакета, а перед инсталляцией уже существует контейнер с указанным именем, то он будет замещен новым контейнером (без дополнительных запросов).

При инсталляции в ОС **Windows Vista/7** появляется окно (Рисунок 6) с запросом на установку драйверов. Выберите предложение – `Все равно установить этот драйвер`.

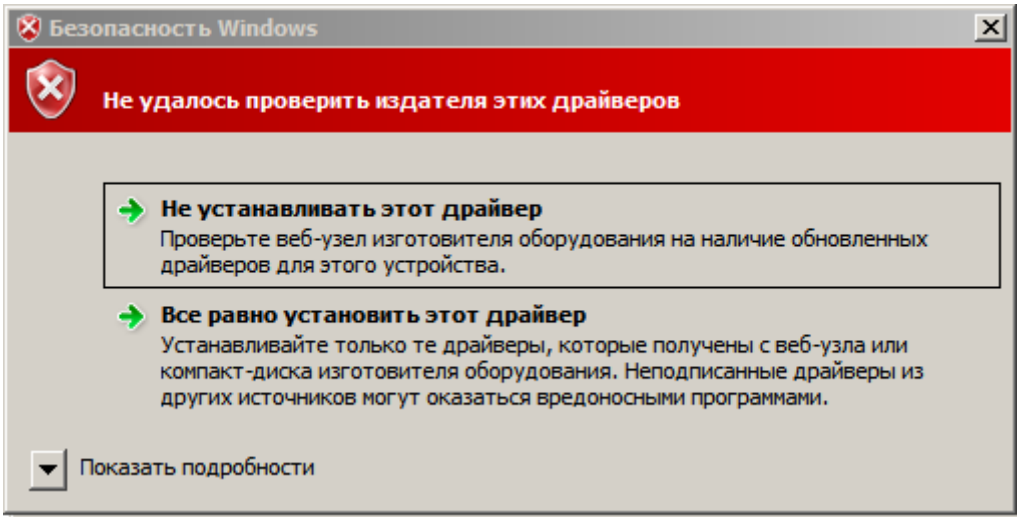


Рисунок 6

Если инсталляция происходит в ОС **Windows XP** и реакция системы Windows на установку неподписанных драйверов поставлена в положение `Предупреждать` (`Пуск – Настройка – Панель управления - Система – Свойства системы- Оборудование – Подписывание драйверов – Предупреждать`), то возможно появление окна (Рисунок 7) для подтверждения установки на интерфейс VPN Filter. Таких окон может появиться несколько. Для продолжения процесса инсталляции нажмите кнопку `Все равно продолжить` в каждом из этих окон:

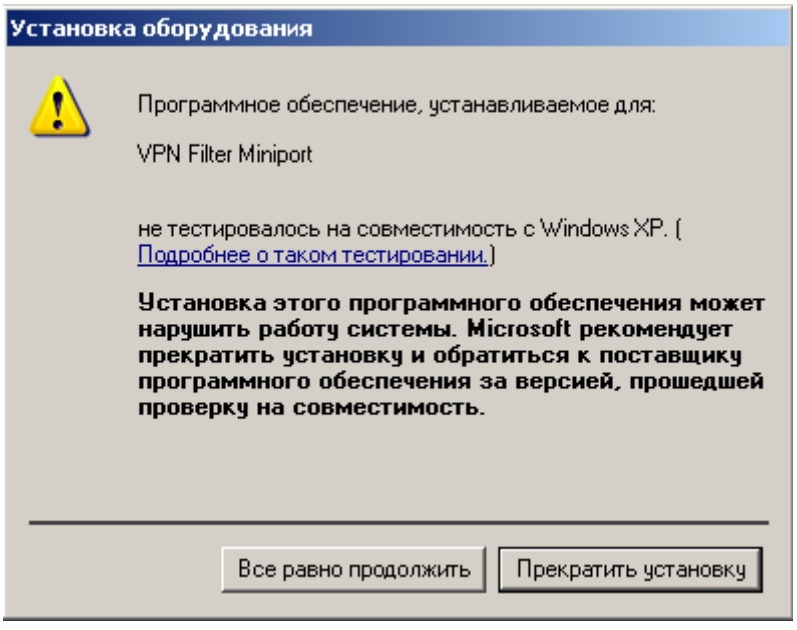


Рисунок 7

Для отключения возможности появления такого окна в операционной системе **Windows XP** войдите в окно `Параметры подписывания драйвера: Пуск – Настройка – Панель управления - Система – Свойства системы- Оборудование – Подписывание драйверов`, поставьте переключатель в положение `Пропускать` и нажмите `OK`.

По окончании установки Bel VPN Client выдается окно (Рисунок 19) с предупреждением о необходимости перезагрузки операционной системы.

# 5.2. Режим normal

Этот режим является диалоговым режимом.

В ОС **Windows Vista/7** при установке Bel VPN Client выдается окно (Рисунок 1). Необходимо разрешить запуск инсталлятора – выберите предложение `Разрешить`.

Появляется стартовое окно визарда с приглашением к инсталляции (Рисунок 8):


Рисунок 8

После нажатия кнопки `Next` будет открыто окно визарда с текстом Лицензионного Соглашения. Установка переключателя в положение "`I accept the license agreement`" делает кнопку `Next` доступной:

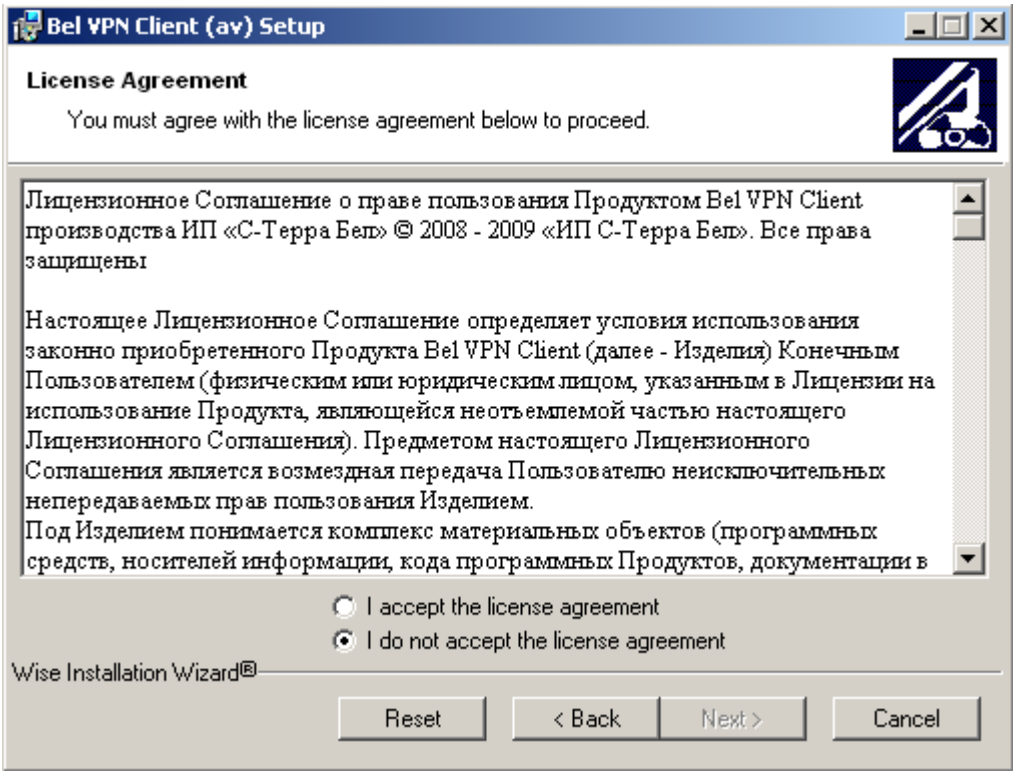


Рисунок 9

Для указания папки, в которую будет установлен продукт, нажать кнопку `Browse` и сделать выбор:

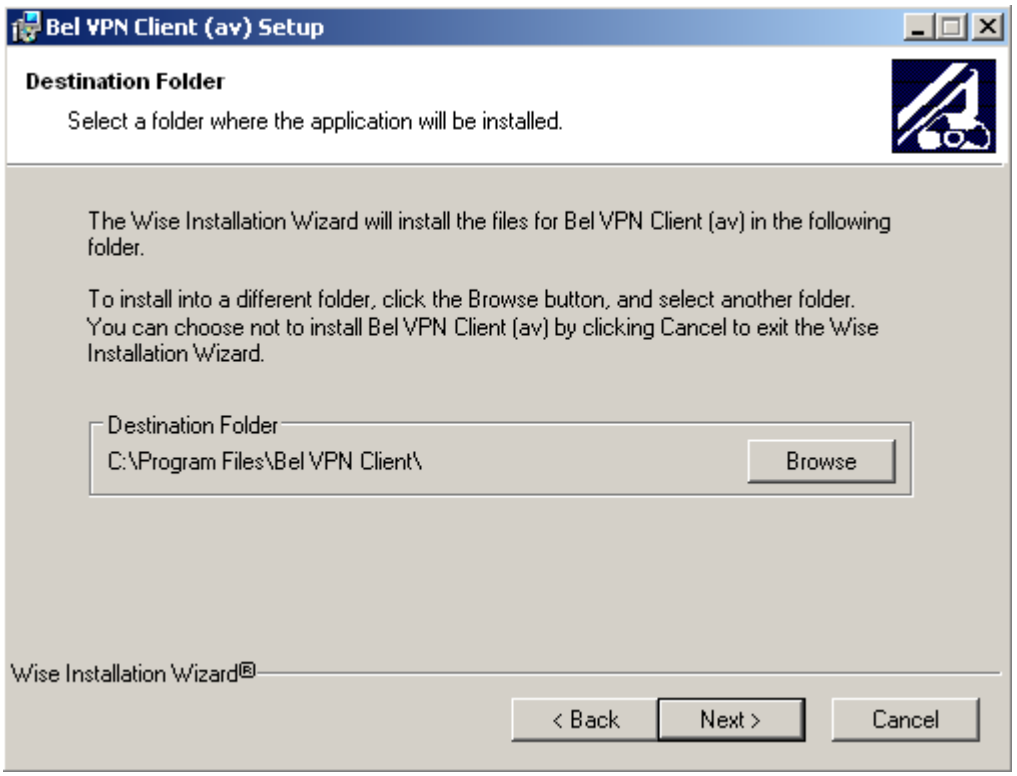


Рисунок 10

Если при создании инсталляционного файла в инсталляционный пакет не был включен контейнер с данными для инициализации RNG, то появится окно ввода информации о размещении контейнера, который содержит инициализационные данные для датчика случайных чисел (Рисунок 11). Для задания способа инициализации RNG нужно установить переключатель в одно из двух положений:

- `Use biological initialization` – пользователя попросят задать данные для инициализации датчика случайных чисел.
- `Use key container` – будет использоваться существующий контейнер. Нужно указать имя контейнера в поле `Container name` пароль к нему в поле `Container password`. Датчик случайных чисел при каждом использовании этого контейнера будет зачитывать из него информацию и модифицировать его.

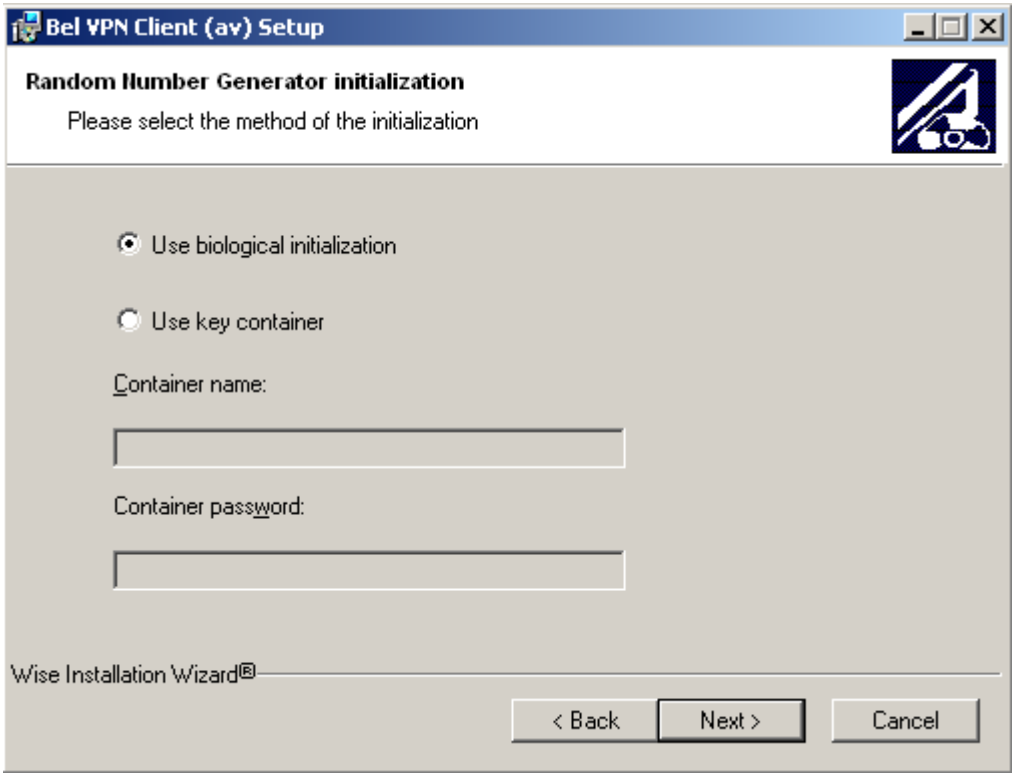


Рисунок 11

  

Если при создании инсталляционного файла регистрационные данные Лицензии на продукт Bel VPN Client не были включены в инсталляционный файл, то появится окно для ввода данных Лицензии на продукт:

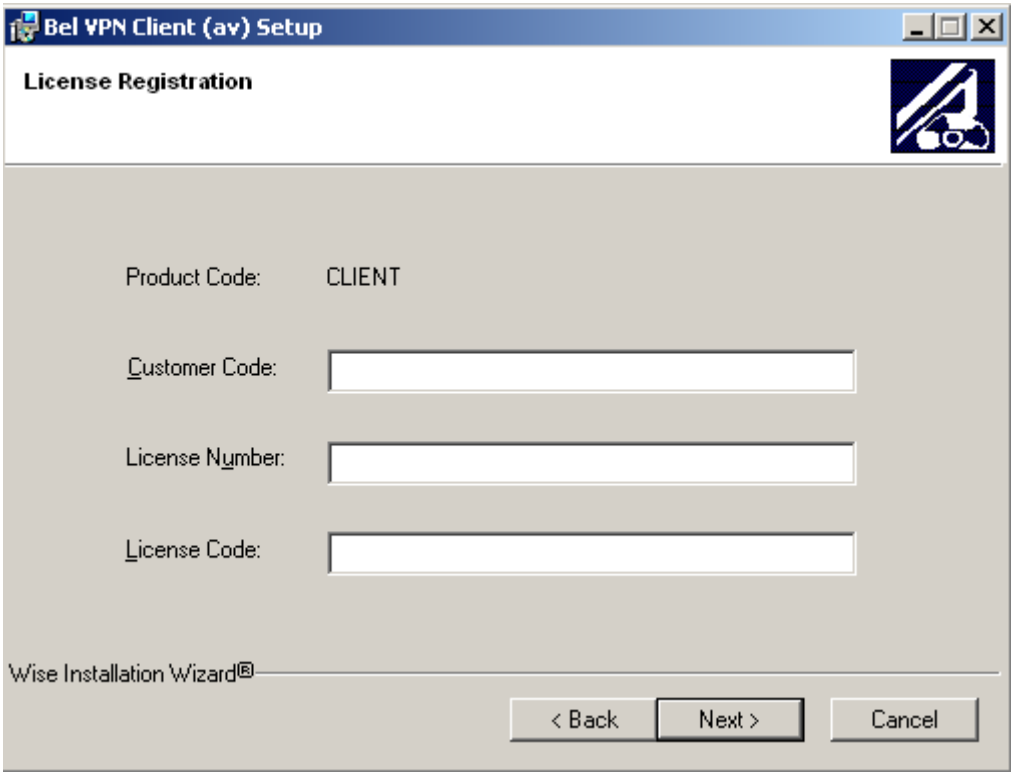


Рисунок 12

Стандартное окно визарда сообщает о готовности к инсталляции. Для начала инсталляции нажать `Next`:

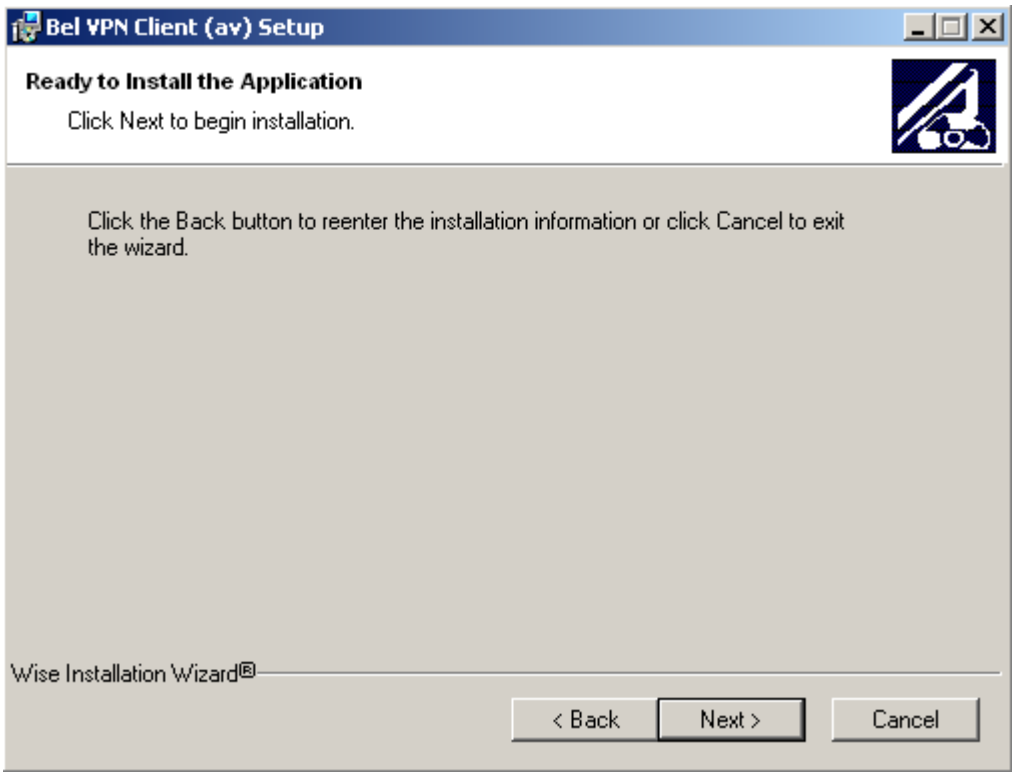


Рисунок 13

Далее появляется окно с индикатором процесса инсталляции:

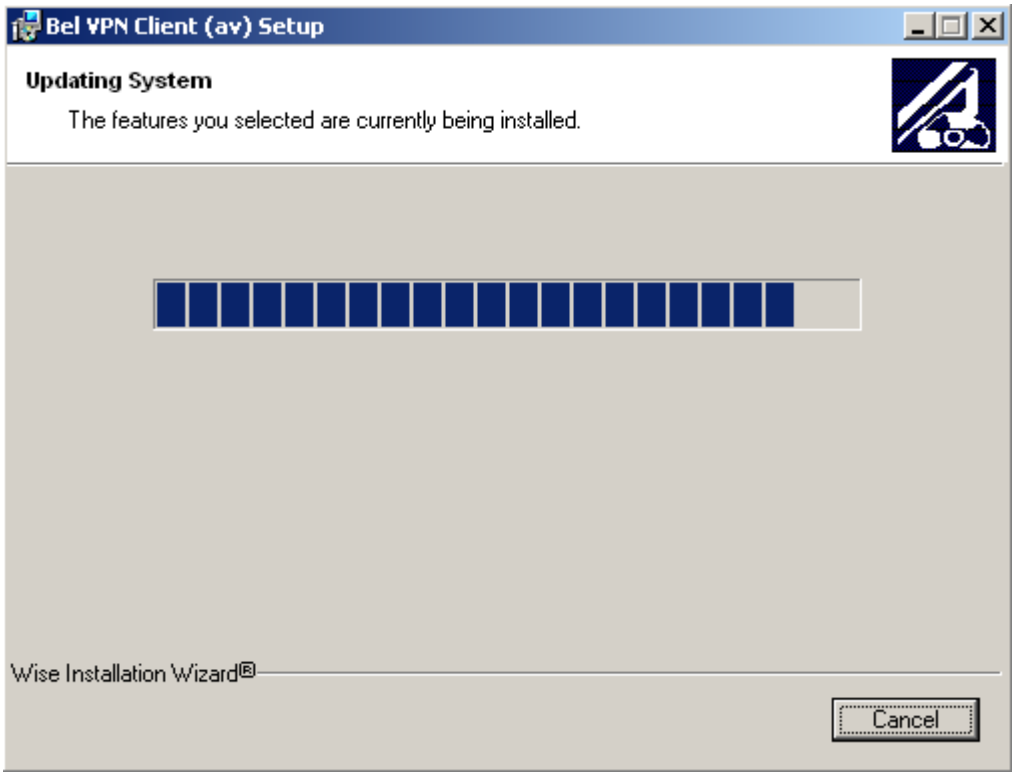


Рисунок 14

Если задан способ инициализации RNG `Use biological initialization`, то в следующем окне попросят ввести какую-то начальную информацию для датчика случайных чисел (пользователю предлагается произвольным образом нажимать на клавиши до тех пор, пока не будет собрано достаточное количество случайных данных – обычно 80 нажатий):

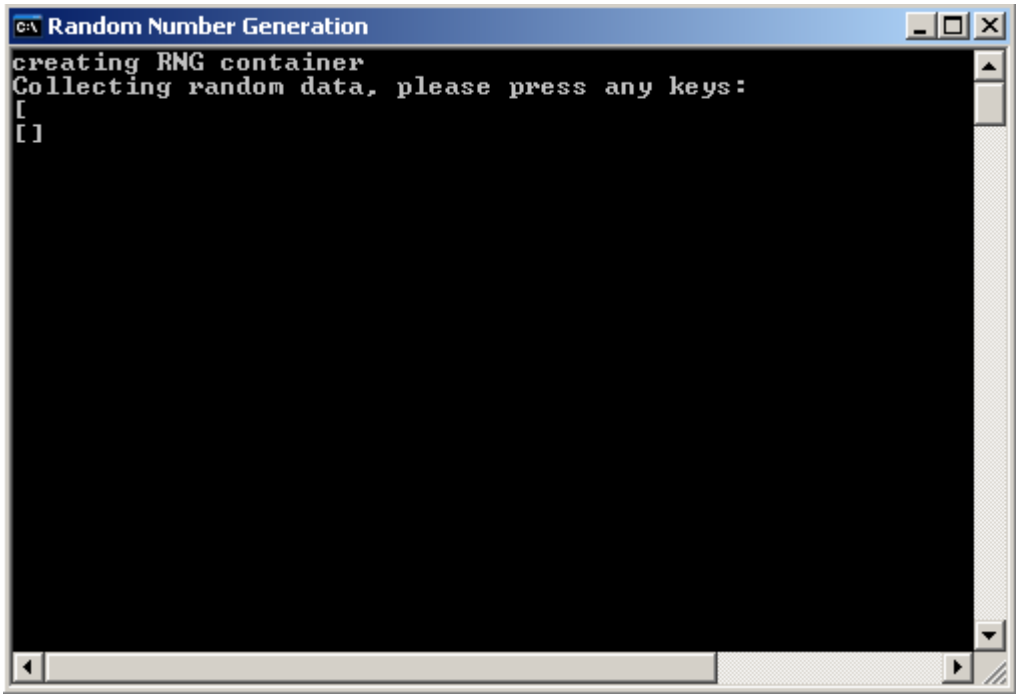


Рисунок 15

Если для инициализации RNG используются данные из существующего контейнера или происходит импорт контейнера из инсталляционного пакета, то окно Random Number Generation не появляется

Дальнейшее поведение инсталлятора зависит от ОС и установленной пользователем опции `Подписывание драйверов`, описанной в разделе "Режим basic".

После завершения процедуры инсталляции нажать Finish:

По окончании установки Bel VPN Client выдается окно (Рисунок 19) о необходимости перезагрузки операционной системы.

## 5.3. Режим silent

В ОС **Windows Vista/7** при установке Bel VPN Client выдается окно (Рисунок 1). Необходимо разрешить запуск инсталлятора – выберите предложение `Разрешить`.

В режиме silent происходит установка Bel VPN Client без запросов.


Рисунок 16

Если задан способ инициализации RNG `Use biological initialization`, то в следующем окне попросят ввести какую-то начальную информацию для датчика случайных чисел (пользователю предлагается произвольным образом нажимать на клавиши до тех пор, пока не будет собрано достаточное количество случайных данных – обычно 80 нажатий):

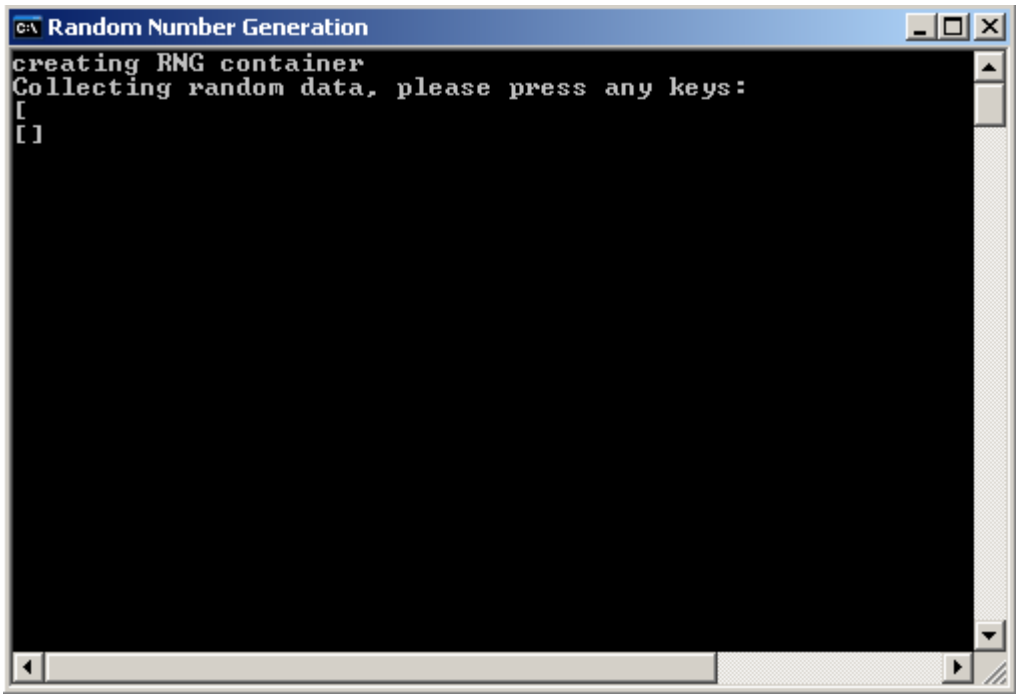


Рисунок 17

Если для инициализации RNG используются данные из существующего контейнера или происходит импорт контейнера из инсталляционного пакета, то окно Random Number Generation не появляется

При инсталляции в ОС Windows Vista/7 появится окно (Рисунок 6) с запросом на установку драйверов. Выберите предложение –Все равно установить этот драйвер.

Если инсталляция происходит в ОС **Windows XP** и реакция системы Windows на установку неподписанных драйверов поставлена в положение Предупреждать (Пуск – Настройка – Панель управления - Система – Свойства системы- Оборудование – Подписывание драйверов – Предупреждать), то возможно появление сообщения Рисунок 7. Для продолжения процесса инсталляции нажмите кнопку Все равно продолжить на каждом из этих сообщений.

По окончании установки Bel VPN Client происходит перезагрузка операционной системы без предупреждений.

  

# 5.4. Копирование контейнера при инсталляции

Если при подготовке инсталляционного файла с использованием сертификатов была указана опция –cs, то при инсталляции Bel VPN Client будет происходить копирование контейнера с секретным ключом.

Если на момент инсталляции не существовало контейнера с тем же именем, в который происходит копирование, и копирование контейнера прошло без ошибок, то никаких дополнительных сообщений и запросов пользователю не выдается.

В случае, если контейнер, в который происходит копирование уже существует, то выдается окно следующего вида:

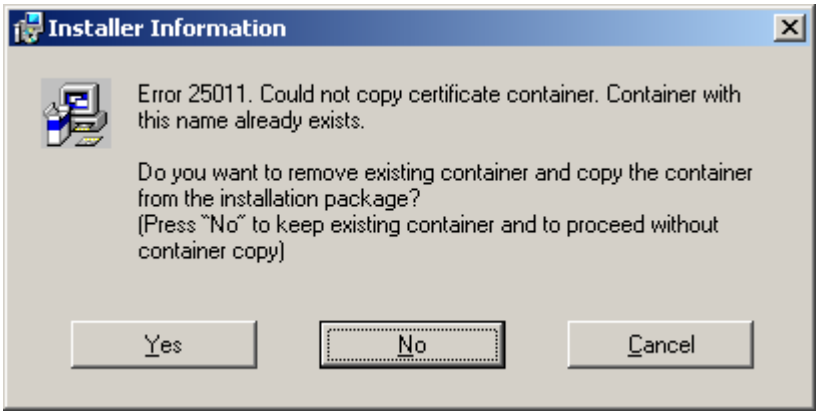


Рисунок 18

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.

# 5.5. Перезагрузка операционной системы

После установки Bel VPN Client в режимах basic и normal открывается окно, сообщающее о необходимости перезагрузки операционной системы:

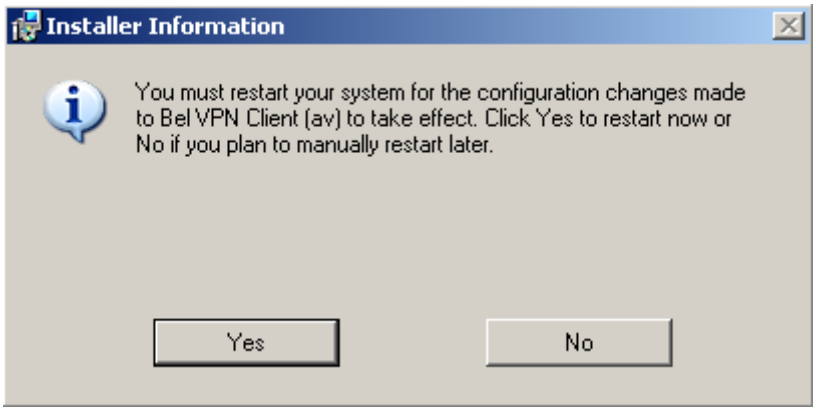


Рисунок 19

После нажатия кнопки Yes происходит перезагрузка операционной системы, а нажатие кнопки No закрывает окно без перезагрузки.

# 5.6. Сообщения об ошибках

Ниже приведены тексты сообщений об ошибках, которые могут возникать при инсталляции Bel VPN Client.

Таблица 1

| | Текст сообщения | Примечание |
|---|---|---|
| 25001 | License check failed. | Неправильная лицензия |
| 25006 | RNG container creation failed. {Reason: <Reason>} Installation aborted.{RNG container path: <RNG_container_Source>} | Не удалось инициализировать ДСЧ.<br>Если есть возможность, выдается причина <Reason> (см. **[**Ошибка! Источник ссылки не найден.**]**).<br>Для вариантов “from_container” и “from_file” выдается путь к контейнеру-источнику информации <RNG_container_Source> |
| 25007 | RNG container not found or invalid. Installation aborted.<br>RNG container path: <path><br>где <path> – путь к RNG-контейнеру. | Не найден корректный RNG контейнер. Инсталляция прервана. Путь к RNG контейнеру: <path> |
| 25008 | Copy RNG container failed. {Reason: <reason>.} Installation aborted. Source RNG container path: <src>. Destination RNG container path: <dst>. | Не удалось скопировать RNG контейнер. {Причина: <reason>} Инсталляция прервана. Путь к исходному RNG контейнеру: <src>. Путь к новому RNG контейнеру: <dst>. |
| 25009 | Copy certificate container failed. {Reason: <Reason>} Installation aborted. Source container path: <Source_container_path> Destination container path: <Destination_container_path> | Не удалось скопировать сертификатный контейнер. Причина: <Reason> – здесь и далее список возможных причин см. ниже. Инсталляция прервана. Исходный контейнер: <Source_container_path> Результирующий контейнер: <Destination_container_path> |
| 25010 | Copy secret key file failed. Installation aborted. | Не удалось скопировать файл секретного ключа. |
| 25011 | Could not copy certificate container. Container with this name already exists.<br>Do you want to remove existing container and copy the container from the installation package?<br>(Press "No" to keep existing container and to proceed without container copy) | Не удалось скопировать сертификатный контейнер. Контейнер с таким именем уже существует.<br>Хотите ли вы удалить существующий контейнер и скопировать контейнер из инсталляционного пакета?<br>(Нажмите “No” для того, чтобы оставить существующий контейнер и не проводить копирование) |
| 25017 | Product "<Product_name version>" was detected.<br>You should uninstall it first before the installation. | Был обнаружен продукт "<Product_name version>".<br>Вам необходимо сначала деинсталлировать его. |
| 25018 | You must have Administrator privileges | Вам необходимы администраторские привилегии |
| | This product needs Windows 2000 or higher | Для продукта необходима Windows 2000 или выше |

  

| | | |
|---|---|---|
| 25019 | The "<dll_path>" was wrongly marked as the previous GINA DLL. The system GINA DLL will be used instead. | **[Windows XP]**<br>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]**<br>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.<br>You should uninstall it first before the installation. | Для продукта <Product_name version> была выполнена операция объявления пользователям (advertisement).<br>Вы должны деинсталлировать его до инсталляции. |
| 25025 | Windows Firewall setup failed. | **[Windows Vista]**<br>Не удалось настроить Windows Firewall. |
| 25026 | You must have Administrator privileges. | Вам необходимы администраторские привилегии |
| 25027 | Invalid RNG initialization method. | Задано некорректное значение параметра RNG_CONTAINER_CHOICE |
| 25028 | Import of certificate container failed. {Reason: <Reason>}<br>Installation aborted.<br>Source file path: <File_path> Destination container path: <Destination_container_path> | Не удалось импортировать сертификатный контейнер. Причина: <Reason>.<br>Инсталляция прервана.<br>Путь к исходному файлу: <File_path><br>Результирующий контейнер: <Destination_container_path> |
| 25029 | Could not import certificate container. Container with this name already exists.<br>Do you want to remove existing container and import the container from the installation package?<br>(Press "No" to keep existing container and to proceed without container import) | Не удалось импортировать сертификатный контейнер. Контейнер с таким именем уже существует.<br>Хотите ли вы удалить существующий контейнер и импортировать контейнер из инсталляционного пакета?<br>(Нажмите “No” для того, чтобы оставить существующий контейнер и не проводить импорт) |
| 25030 | Could not copy or import certificate container. {<br>Reason: <Reason>}<br>где <Reason> может быть:<br>Internal error<br>Unknown operation (should be 'copy' or 'import') | Не удалось скопировать или импортировать сертификатный контейнер.<br>Причина:<br>Внутренняя ошибка<br>Неизвестная операция (должна быть “copy” или “import”) – не задан или неправильно задан параметр CSP_CONTAINER_OPERATION |

| | | |
|---|---|---|
| 25031 | Could not remove the existing container. {Reason: <Reason>}<br>Installation aborted.<br>Existing container name: <Existing_container_name> | Не удалось удалить существующий контейнер. Причина: <Reason><br>Инсталляция прервана.<br>Имя существующего контейнера: <Existing_container_name> |

# 6. Регистрация пользователя

При подготовке инсталляционного пакета можно было установить интерактивный или неинтерактивный режим логина в Продукт.

### ОС Windows XP

В ОС Windows XP после перезагрузки ОС при интерактивном режиме (см. раздел «Интерактивный режим логина в Продукт») появляется окно логина в Продукт (Рисунок 24). Это окно появляется только после инициализации VPN сервиса (см. раздел «Время инициализации VPN сервиса»). Окно логина в ОС Windows XP появляется только после регистрации пользователя в Продукте или отказе от нее. При неинтерактивном режиме логина в Продукт или переключении на него (см. раздел «Неинтерактивный режим логина в Продукт»).

### ОС Windows Vista

В ОС Windows Vista/7 после перезагрузки ОС при интерактивном режиме логина на экран выводятся иконки для выбора пользователя, иконка, отображающая текущий статус Продукта Bel VPN Client и окно логина в Продукт (Рисунок 20).

В ОС Windows Vista/7 процессы входа в систему и входа в продукт независимы друг от друга. Можно сначала зарегистрироваться в Продукте, а потом войти в ОС или наоборот.


Рисунок 20

В окне выбора пользователя (Рисунок 20) иконка, отображающая текущий статус Продукта, может смещена в нужном направлении, если ее положение неудобно (см. раздел «Изменение положения иконки текущего статуса Продукта»)

В Windows Vista/7 окно логина в Продукт автоматически появляется в интерактивном режиме, когда необходимо выбрать пользователя для входа в ОС:

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

Окно логина в Продукт будет выводиться только при запущенном VPN-сервисе. Если к моменту когда нужно вывести окно логина VPN-сервис не будет готов к работе, то Продукт будет ждать 30 секунд (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 21).

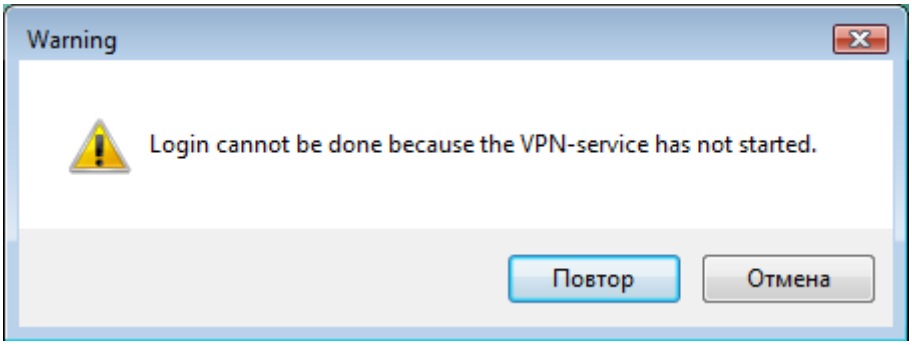


Рисунок 21

После успешной регистрации пользователя иконка статуса Продукта изменит свой вид (Рисунок 22) (см. главу «Отображение текущего статуса Продукта»).

Рисунок 22

После входа пользователя в ОС иконка статуса Продукта будет размещена в панели задач.

Если отказаться от логина, то потом войти в Продукт можно:

- нажав на иконку статуса Продукта в окне выбора пользователя и выбрав предложение Login (Рисунок 23)
- либо после входа в ОС, нажав на иконку статуса Продукта в панели задач (см. раздел «Login/Logout».

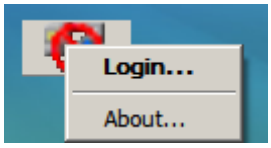


Рисунок 23

  

# 6.1. Интерактивный режим логина в Продукт

При интерактивном режиме логина в Продукт после перезагрузки операционной системы открывается окно для ввода и изменения пароля пользователя (Рисунок 24). По умолчанию пароль является пустым.


Рисунок 24

При нажатии на кнопку Change Password откроется окно, в котором можно изменить пароль пользователя:


Рисунок 25

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.

При успешной аутентификации пользователя в продукт загружается локальная политика безопасности, заданная для данного пользователя администратором и находящаяся в базе Продукта.

**Специальная политика безопасности Log-off policy**, которая задается администратором при подготовке инсталляционного пакета, загружается 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.

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

- правило `Drop All` – удалять любой трафик, приходящий на компьютер пользователя
- правило `Default Driver Policy (DDP)` – политика драйвера по умолчанию, может принимать одно из двух значений:
  - 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.

  

Политика Default Driver Policy (DDP), которая определяется 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 качеств пароля используется пустая строка). При успешном логине окно с запросом пароля (Рисунок 24) не появляется. При неуспешном логине Продукт ведет себя как при интерактивном логине - будет выдано окно запроса пароля.

При установленном Продукте Bel VPN Client можно изменить интерактивный режим логина на неинтерактивный. Включение неинтерактивного режима осуществляется установкой значения, отличного от 0, переменной в реестре NonInteractiveLogin:

`HKEY_LOCL_MACHINE\SOFTWARE\VPN Agent\NonInteractiveLogin.`

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

## 6.3. Время инициализации VPN сервиса

В ОС Windows XP и Windows Vista/7 можно задать время инициализации VPN сервиса в реестре при помощи переменной `MaxServiceStartTimeout`:

`HKEY_LOCL_MACHINE\SOFTWARE\VPN Agent\MaxServiceStartTimeout`

Эта переменная задает время в секундах, необходимое для подготовки VPN сервиса к работе. 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.

  

# 6.4. Изменение положения иконки текущего статуса Продукта

В окне выбора пользователя (Рисунок 20) положение иконки, отображающей текущий статус Продукта, если оно неудобно, можно изменить с помощью переменной в реестре:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\PLAP 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.

  

# 6.5. Автоматизация входа в ОС Windows XP

Для автоматического входа пользователя в систему MS **Windows XP** (не появляется окно Log On to Windows) выполните настройки, описанные для ОС Windows XP по адресу:

http://support.microsoft.com/?kbid=315231

Опишем для Windows XP настройки трех переменных в Редакторе реестра:

- нажмите Пуск – Выполнить, введите regedit, нажмите OK
- в реестре войдите в ключ

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon

- после двойного клика на переменной DefaultUserName, в открывшемся окне в поле Значение введите имя пользователя и нажмите ОК
- двойным кликом на переменной DefaultPassword в окне Изменение строкового параметра введите пароль пользователя, если эта переменная отсутствует, то создайте ее:
  - в окне Редактор Реестра войдите в меню Правка, выберите предложение Создать – Строковый параметр
  - напечатайте имя переменной - DefaultPassword и нажмите Enter
  - двойным кликом на этой переменной откройте окно, в котором введите пароль
- двойной клик на переменной AutoAdminLogon откроет окно, в котором в поле Значение введите значение 1 и нажмите OK, если эта переменная отсутствует, то создайте ее
- Выйдите из Редактора реестра
- Нажмите Пуск – Перезагрузка – OK.

После этого вход пользователя в систему будет осуществляться автоматически.

  

# 7. Отображение текущего статуса продукта

Текущий статус продукта отображает иконка, расположенная в панели задач. Эта иконка появляется при запуске сервиса и удаляется при его остановке.

Если пользователь не аутентифицировался, то иконка имеет вид:

Рисунок 26

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

Рисунок 27

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

Рисунок 28

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 29

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


Рисунок 30

  

# 7.1. Login/Logout

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

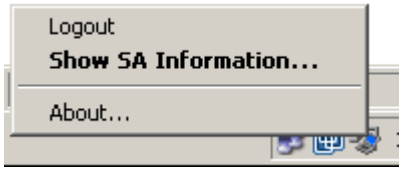


Рисунок 31

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

При выборе предложения Login появится окно ввода пароля (Рисунок 24) 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`.

# 7.2. SA Information

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

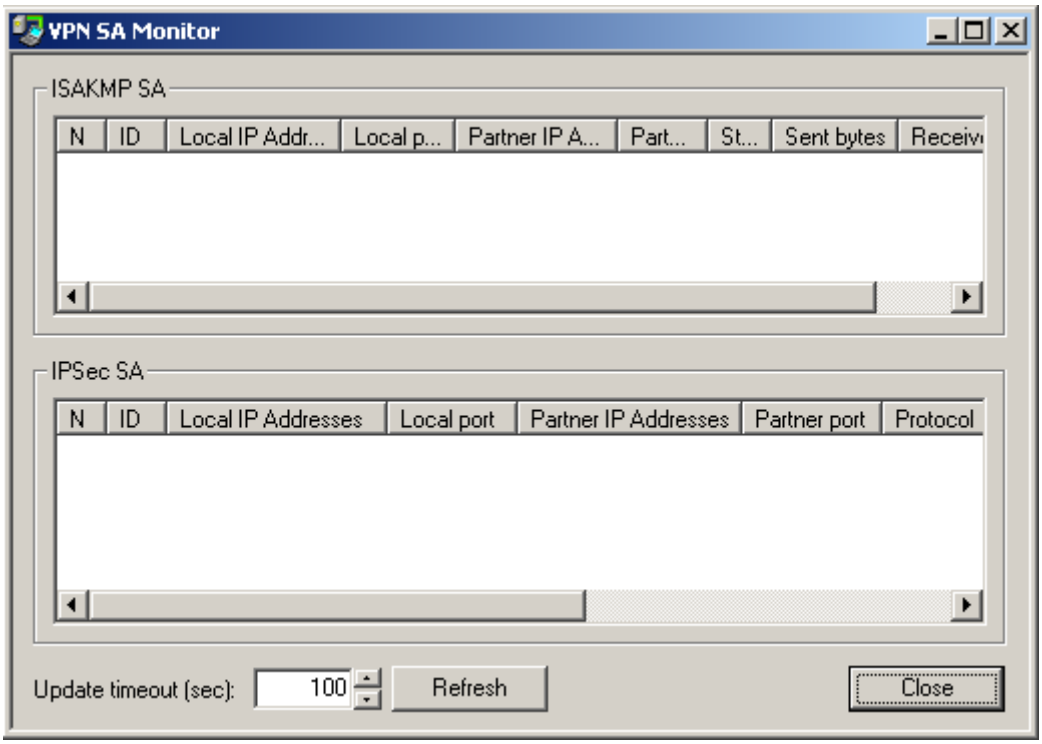


Рисунок 32

где:

IKE 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 выводится)
- `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 ports` – локальные порты
- `Partner IP Addresses` – партнерские адреса
- `Partner ports` – партнерские порты
- `Protocols` – сетевые протоколы
- `Action` – тип акции:
  - `AH`
  - `ESP`
  - `AH+ESP`
- `Type` – тип соединения:
  - `transport`
  - `tunnel`
- `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.

При выборе предложения `About` в меню выводится информация о версии продукта:

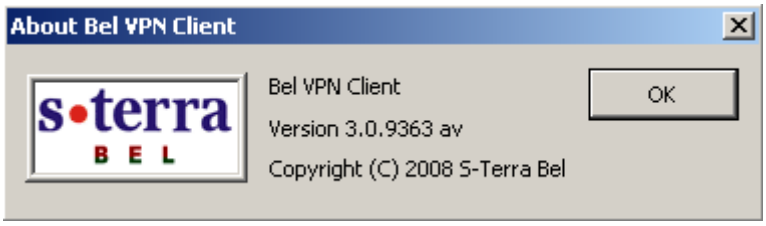


Рисунок 33

# 8. Деинсталляция Bel VPN Client

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

При деинсталляции Bel VPN Client происходит включение стандартного сервиса, связанного с IPsec и IKE. В Windows XP – это Служба IPSEC, в Windows Vista/7 – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности». В Windows 7 включение службы необходимо выполнить вручную.

В Windows Vista/7 при деинсталляции Bel VPN Client выдается окно (Рисунок 34) Необходимо разрешить запуск деинсталлятора.

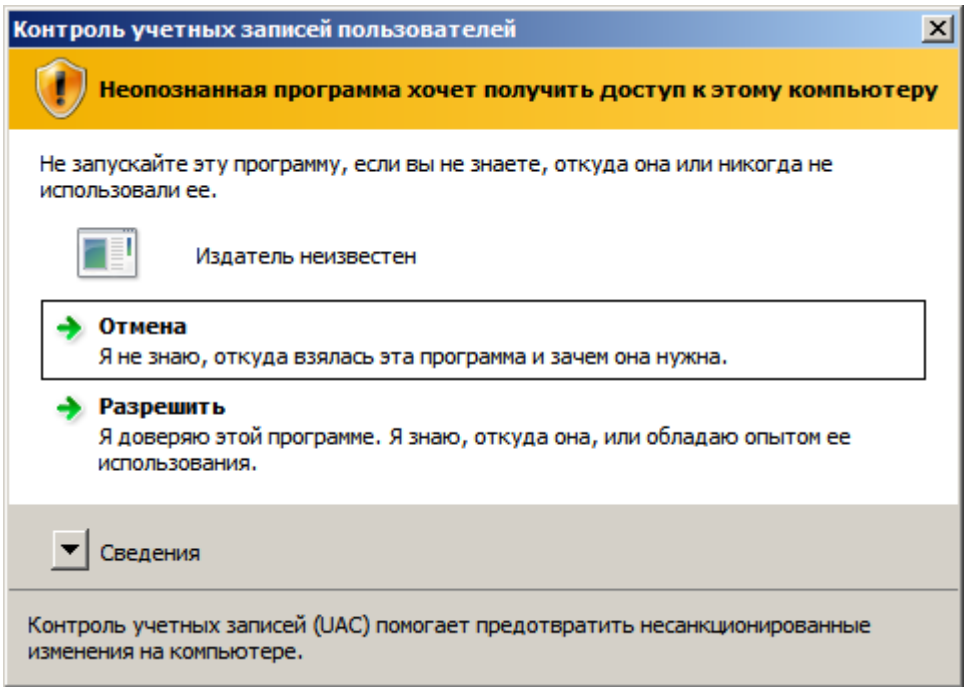


Рисунок 34

# 9. Специализированные команды

Программные утилиты, входящие в состав продукта Bel VPN Client:

**cert_show**
**cert_check**
**client login**
**client logout**
**pwd change**
**key_show**
**lsp_show**
**lsp_reload**
**log_show**
**dp_show**
**sa_show**
**klogview**

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.`

# 9.1. cert_show

Команда `cert_show` предназначена для просмотра сертификатов и списков отозванных сертификатов (CRL), лежащих в базе продукта.

**Синтаксис** **`cert_show`**

Данная команда не имеет аргументов и ключей.

**Значение по умолчанию** значение по умолчанию отсутствует

**Рекомендации по использованию**

Используйте данную команду для ознакомления со списком сертификатов и CRL, находящихся в базе продукта. В этом случае будет выведен нумерованный список сертификатов и CRL.

  

# 9.2. cert_check

Команда `cert_check` предназначена для проверки сертификатов, находящихся в базе продукта.

**Синтаксис** **`cert_check`**

**Значение по умолчанию** значение по умолчанию отсутствует

**Рекомендации по использованию**

Проверяются все сертификаты, находящиеся в базе продукта.

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

- `Certificate is invalid` – неверный формат сертификата
- `Certificate is expired` – срок действия сертификата истек или еще не наступил
- `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 accessible` – секретный ключ не подходит к сертификату
- `It is certificate request` – данный объект является сертификатным запросом.

  

# 9.3. client_login

Команда `client_login` запускается автоматически при логине пользователя в систему и представляет собой GUI-приложение (Рисунок 24), в котором нужно ввести пароль для аутентификации пользователя.

Эта команда запускается и при выборе предложения Login в меню (Рисунок 31), которое появляеся на иконке в панели задач при работающем сервисе после того, как было выбрано предложение Logout.

Может быть использована и для изменения пароля пользователя.

**Синтаксис** **`client_login`**

  

# 9.4. 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 31), которое появляеся на иконке в панели задач при работающем сервисе после того, как было выбрано предложение Login. Возможен запуск команды вручную.

**Синтаксис** **client_logout**

**Пример**

Ниже приведен пример запуска вручную команды `client_logout`:

```
client_logout
Logout OK
```

  

# 9.5. pwd_change

Команда pwd_change предназначена для изменения пароля пользователя. Эта команда запускается автоматически при нажатии кнопки `Change Password...` в окне логина пользователя (Рисунок 24) и вызовом окна `Change Password` (Рисунок 25) для ввода старого и нового пароля. Эту команду можно запускать 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
```

  

# 9.6. key_show

Команда `key_show` предназначена для просмотра предопределенных ключей, зарегистрированных в продукте.

**Синтаксис** **`key_show`**

Данная команда не имеет аргументов и ключей.

**Значение по умолчанию** Значение по умолчанию отсутствует.

**Рекомендации**

Используйте данную команду для ознакомления со списком предопределенных ключей, хранящихся в базе данных 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:**

```
Found #1 keys.
----Key----
Name   :        key1
Content         testkey1..
Content (hex):  746573746B6579310D0A
```

  

# 9.7. lsp_show

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

**Синтаксис** **`lsp_show`**

Данная команда не имеет аргументов и ключей.

**Значение по умолчанию** Значение по умолчанию отсутствует.

**Рекомендации по использованию**

Если загружена конфигурация пользователя, то по данной команде она и будет выведена..

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

```
lsp_show > current_lsp.txt
```

Политику DDP этой командой посмотреть нельзя.

  

# 9.8. lsp_reload

Команда lsp_reload предназначена для перезагрузки LSP конфигурации.

**Синтаксис** **`lsp_reload`**

**Значение по умолчанию** Значение по умолчанию отсутствует.

**Рекомендации по использованию**

Используйте команду `lsp_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**

Ниже приведен пример загрузки LSP конфигурации из базы Продукта:

```
lsp_reload
LSP is reloaded successfully.
```

  

# 9.9. log_show

Команда `log_show` предназначена для просмотра настройки уровня протоколирования событий.

**Синтаксис** **`log_show`**

Данная команда не имеет аргументов и ключей.

**Значение по умолчанию** Значение по умолчанию отсутствует.

**Рекомендации по использованию**

Данная команда выводит текущий уровень протоколирования событий:

```
Log severity level: (3) err
```

# 9.10. dp_show

Команда `dp_show` предназначена для просмотра установленных настроек политики `Default Driver Policy`.

`Default Driver Policy` – политика безопасности, загружаемая при старте продукта до загрузки конфигурации пользователя, или же при отгрузке пользовательской конфигурации. Возможные значения:

- `passall` - пропускать весь трафик
- `passdhcp` - пропускать только DHCP пакеты

**Синтаксис** **`dp_show`**

Данная команда не имеет аргументов и ключей.

**Значение по умолчанию** Значение по умолчанию отсутствует.

**Рекомендациипо использованию**

Данная команда выводит установленное значение политики DDP, например:

```
Default Driver Policy : passall
```

  

# 9.11. sa_show

Команда `sa_show` предназначена для просмотра состояний IPsec SA, ISAKMP SA, IKE info.

**Синтаксис** **`sa_show [-e]`**

Команда sa_show (без указания опции) позволяет просмотреть действующие в данный момент IPsec SA.
Команда sa_show -e выводит полную информацию– IKE info, ISAKMP SA, IPsec SA.

**Значение по умолчанию** Значение по умолчанию отсутствует.

**Рекомендации по использованию**

Используйте данную команду без указания ключа для вывода информации об IPsec SA:

- `IPsec SA` - порядковый номер IPsec SA и для каждого соединения:
  - описание партнеров (сначала удаленная часть, затем локальная) - IP-адрес или диапазон IP-адресов, номер порта (если номер порта не указан, то выдается *)
  - номер протокола (если протокол не указан, то выводится `*` )
  - описание соединения – IPsec протокол (`AH|ESP|AH+ESP`)
  - режим `tran(transport)|tunn(tunnel)`
  - статистика по соединению – количество переданных и принятых байтов.

При указании ключа –e выводится полная информация:

- `IKE sessions: ni initiated, nr responded` – количество незавершенных IKE-обменов: `ni` - в качестве инициатора, `nr` – в качестве ответчика.
- `ISAKMP SA` – порядковый номер ISAKMP SA и для каждого соединения:
  - описание партнеров (сначала удаленный, затем локальный) – IP-адрес, номер порта
    - состояние SA:
      - `incomplete` – еще недосозданный
      - `configuration` – для данного SA проводится дополнительная настройка `(IKECFG XAuth, etc.)`
      - `ready` – готовый к использованию SA
      - `deletion` – SA не используется, подготовлен к удалению.
  - статистика по соединению – количество переданных и принятых байтов.
- `IPsec SA` – выводится информация об IPsec SA.

**Пример**
Ниже приведен пример выполнения команды `sa_show –e`:

```
IKE sessions: 0 initiated, 0 responded

ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Potr) State Sent Rec
(заголовок вывода)
```

```
ISAKMP SA 1 (10.0.10.193,500)-(10.0.10.17,500) deletion 1062 1090
ISAKMP SA 2 (10.0.10.16,500)-(10.0.10.17,500) ready 1246 2602

IPsec SA Num (Remote Addr,Port)-(Local Addr,Port) Protocol Action
Type Sent Rec (заголовок вывода)

IPsec SA 1 (192.168.15.16,*)-(10.0.10.17,*) 1 ESP tunn 240 448
```

  

# 9.12. klogview

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

**Синтаксис** **`klogview`** `[-ltT] [-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 предыдущего события, показанного данным экземпляром утилиты. Например, значение 10.353245 – это 10 секунд и 353245 микросекунд. Максимальная точность – наносекунды, но реальная погрешность зависит от аппаратной плафформы 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.

`-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 на консоль сообщения, относящиеся к одной или нескольким группам событий. События, по которым выводятся сообщения, сгруппированы следующим образом:

Таблица 2

| Группа событий | Код | Описание |
|---|---|---|
| drop | 2 | 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 | 1 | Пропуск пакета. Выводится непосредственно перед отсылкой какого-либо пакета. Сообщение содержит краткий текст, поясняющий действия, которые были произведены над пакетом. |
| sa_minor | 8 | Некоторые внутренние события, происходящие с IPsec - контекстом. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста. |
| sa_major | 4 | Взаимодействия между IPsec-драйвером и приложением, касающиеся изменения состояния IPsec-контекстов. |

  

| Группа событий | Код | Описание |
|---|---|---|
| | | Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста. |
| sa_trace | 16 | Сообщения выводятся перед попыткой применения к пакету IPsec-контекста. |
| sa_errors | 32 | Ошибки, связанные с неуспешным применением IPsec-контекста к пакету. |
| filt_trace | 64 | Выводится имя и индекс правила фильтрации, если такое для пакета найдено. |

Нужный набор событий (`event_mask`) можно указать двумя способами:

- сложением кодов групп событий (см. в таблице)

  **Пример:**

  ```
  klogview –f 0x43
  или
  klogview –f 67
  ```

- перечислением названий групп событий через запятую, без пробелов между запятой и названием группы

  **Пример:**

  ```
  klogview –f drop,pass,filt_trace
  ```

**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 формата, получаемой из IPsec-драйвера.

Специальные 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[1]. |
| `<error: в выводимом сообщении` | несоответствие строки формата параметрам сообщения[2]. |

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

[1] *Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.*

[2] *Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.*

  

### 9.12.1. 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
- 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, if eth0, passed: filter flt_abc: filtered
```

Пакет был обработан по IPsec-правилу:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, passed: filter flt_cba: decapsulated
```

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, passed: packet encapsulated
```

Открытый пакет был пропущен по правилу с действием IPsec+PASS:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, passed: filter flt_cba: IPsec rule, but the packet was not decapsulated
```

Пакет был пропущен в открытом виде по правилу с действием IPsec+PASS:

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, passed: filter flt_abc: bundle not found
```

**Примеры сообщений группы drop**

Сообщения, связанные с некорректными данными заголовков пакета:

IP-заголовок испорчен:

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

TCP/UDP заголовок испорчен:

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

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

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: can't update selector
```

  

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

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: SA
33: can't prase packet 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
```

Может выводиться при внутренних ошибках работы клиентской стороны IKEcfg:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: firewall procedure's result
```

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

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
too many nested encapsulations
```

Пакет уничтожен в соответствии с `RefuseTCPPeerInit`, выставленном в правиле фильтрации:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: incoming TCP connections restricted
```

Сообщения о подпадании пакета под правило с действием `DROP`:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: packet hit a "DROP" rule
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: filtered
```

Пакет был закрыт с помощью IPsec, но подпадает под правило `PASS`:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: decapsulated packet hit a "PASS" rule
```

Открытый пакет подпадает под правило фильтрации с IPsec-действием:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
filter flt_aaa: IPsec rule, but the packet was not decapsulated
```

Правило с действием `IPsec+DROP`, и соответствующий SA bundle не был создан:

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

Ошибки IPsec:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: SA
33: decapsulation error 5: integrity verification failed
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
SA 33: encapsulation error 4: sequence number wrapped
```

  

Возможны следующие ошибки

| 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 small3 | буфер слишком мал |
| 11 | can't parse IP options | невозможно разобрать опции IP |
| 12 | padding check failed | ошибка в заполнителе |
| 13 | incorrect SA parameters (from pmod_init_sa) | неправильные параметры SA |
| 14 | encapsulation mode (tunnel/transport) doesn't match the SA | режим инкапсуляции (туннельный или транспортный) не соответствует SA |

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

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: filter flt_aaa: bundle is unusable
```

Ограничение на обработку транзитноготрафика (Server, Client):

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

Ограничение на обработку транзитноготрафика при вложенном IPsec:

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

Очередь пакетов, ожидающая создания IPsec SA bundle переполнена:

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: filter flt_aaa: waiting for a bundle: queue overflow
```

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:

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

[3] *Это является внутренней ошибкой, просьба сообщать разработчикам.*

  

Внутренние ошибки, о которых просьба сообщать разработчикам:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: ip
data is not 4-byte aligned
```

Другие сообщения:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: no
matching filtering rule
```

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

```
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
out of memory
```

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: SA
not found
```

## 9.12.2. События группы filt_trace

Сообщения этой группы позволяют определить, какое правило фильтрации используется для обработки пакета. Эти сообщения не содержат информацию о самом пакете. Такую информацию можно получить из контекста сообщения (например, из следующих сообщений группы `pass и drop`).

Пример сообщения:

```
found filtering rule 102(filter_tcp)
```

## 9.12.3. 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
```

SA нигде не используются и должны быть удалены:

```
requesting to remove SA: 44,45
```

Сообщения о загрузке новых SA:

```
loaded SA: id 12; flags 0x1; ipsec flags: 0x18; selector:
5.4.3.2->2.3.4.5; type: 51; SPI: 0xabababba
```

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

```
loaded replacement for SA 55: id 12; flags 0x0; ipsec
flags: 0x38; selector: 3.4.5.1->2.3.4.0-2.3.4.255, proto
17; type: 50; SPI: 0x3b7f44e0
```

Расшифровка type:

```
51 – AH
50 - ESP
```

Расшифровка некоторых[4] битов flags:

```
0x1 – входящий
```

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 – испольуется UDP-encapsulation (NAT traversal)
```

```
Загрузка связки SA (SA bundle):
loaded bundle: filter: 298(ipsec_filter); selector: 3.4.5.1:98-
>3.4.5.2:99, proto 17; SA ids: 4, 5
```

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):
bundle request: filter: 59; selector: 5.4.3.2:1->1.2.3.4:5,
proto 17
```

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

```
disabled SA 33
```

Удаление SA:

```
removed SA 33
```

Удаление ранее заблокированного SA:

```
removed dead SA 33
```

Другие сообщения:

```
application request to enable SA 33 processed
first packet will trigger rekeying of SA 33
```

[4] *Остальные значения флагов не предназначены для интерпретации пользователями.*

Сообщения, возникающие при ошибочном/странном[5] поведении продукта:

```
can't add bundle: filter id 299 not found
can't add bundle: SA id 33 not found
can't add bundle: SA id 33 is unusable
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 load replacement for SA 33: race condition - SA is dead
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
```

**Примеры сообщений группы sa_minor** [6]**:**

```
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
```

## 9.12.4. 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, if iprb0
encapsulating with SA 10: 5.4.3.2:1->1.2.3.4:5, proto 6, if iprb0
```

## 9.12.5. События группы sa_error

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).

Пример сообщения:

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

*[5] Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.*

*[6] Сообщения данного раздела предназначены для внутреннего использования. Расшифровка пользователям продукта не предоставляется.*

# 9.13. 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 info@s-terra.by.

## Утилита sa_show

| Текст сообщения | Описание проблемы |
|---|---|
| Internal error. Код ошибки. | Внутренняя ошибка. |
| SA info is not found. Error: ACCESS DENIED. | Пользователь не аутентифицировался. |

## Утилита key_show

| Текст сообщения | Описание проблемы |
|---|---|
| Unable to obtain keys from DB.Error: ACCESS DENIED. | Не удалось получить Preshared Key из базы. |

## Утилита lsp_show

| Текст сообщения | Описание проблемы |
|---|---|
| Failed to retrieve policy from product data base.Error: ACCESS DENIED.<br>Other operations are cancelled due to error | Ошибка при повторной загрузке LSP. |

## Утилита log_show

| Текст сообщения | Описание проблемы |
|---|---|
| Failed to get severity level.Error: ACCESS DENIED. | Ошибка при получении уровня протоколирования событий. |

  

## Утилита cert_check

| Текст сообщения | Описание проблемы |
|---|---|
| Internal error. Unable to obtain certs from DB<br>No certificates found. | Неудачная попытка получить сертификаты из базы продукта. |

## Утилита dp_show

| Текст сообщения | Описание проблемы |
|---|---|
| Error %d: VPN demon is not started | Проблема со стартом демона |
| Error %d: Default driver policy is not read from db | Ошибка при чтении Default Driver Policy из базы продукта |
| Error %d: Log-off policy is not read from db | Ошибка при получении Log-off policy |
| <Описания операции>. Error: ACCESS DENIED. | Пользователь не аутентифицировался. |
| Failed to get default driver policy.Error: ACCESS DENIED. | Ошибка при загрузке DDP. |

## Утилита pwd_change

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

## Утилита client_logout

| Текст сообщения | Описание проблемы |
|---|---|
| Error %d: VPN demon is not started | Проблема со стартом демона |
| Error %d: Log-out fail | Неудачный logout |

  

# 10. Протоколирование событий

Настройка Syslog-клиента производится администратором при подготовке инсталляционного пакета пользователя. Администратор определяет IP-адрес хоста, на который будут посылаться сообщения о событиях, уровень важности сообщений, источник сообщений.

## 10.1. Получение лога в Windows

Для получения лога в Windows можно использовать продукт Kiwi Syslog Daemon (http://www.kiwisyslog.com), Tri Action Syslog Daemon и др.

## 10.2. Список протоколируемых событий

Каждому протоколируемому событию присваивается фиксированный идентификатор (MSG ID) и соответствующий ему уровень важности (Severity) для протокола Syslog:

EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, DEBUG.

Выдаваемые сообщения и описание событий по этим сообщениям представлены в таблицах 3-7.

**Сообщения уровня ERROR**

Таблица 3

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 1 | Локальный сертификат непригоден | ERR | CERT | Searching local certificate failed. Reason: %s[7]. Subject: %s Issuer: %s SN: %s |
| 2 | Секретный ключ локального сертификата недоступен | ERR | CERT | Local certificate '%{1}s' is invalid: private key %{2}s%{3}s'%{4}s' is inaccessible<br>где:<br>%{1}s – значение поля Subject локального сертификата<br>%{2}s – «», если ключ был задан явно, иначе «at container<br>%{3}s – «», если ключ был задан явно, иначе « »<br>%{4}s – путь к ключу, если он был задан явно, иначе имя контейнера |
| 3 | Контейнер ключа локального сертификата недоступен | ERR | CERT | Local certificate '%{1}s' is invalid: container '%{4}s' is inaccessible<br>где:<br>%{1}s – значение поля Subject локального сертификата<br>%{4}s – путь к ключу, если он был задан явно, иначе имя контейнера |

[7] *revoked* | *expired* | *not verified*

  

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 4 | Секретный ключ не соответствует локальному сертификату. Это возможно только после установки OCI | ERR | CERT | Local certificate '%{1}s' is invalid: private key %{2}s%{3}s'%{4}s' is inconsistent with the certificate<br>где:<br>%{1}s – значение поля Subject локального сертификата<br>%{2}s – «», если ключ был задан явно, иначе «at container»<br>%{3}s – «», если ключ был задан явно, иначе « »<br>%{4}s – путь к ключу, если он был задан явно, иначе имя контейнера |
| 5 | Неуспешная попытка установить соединение в качестве инициатора | ERR | POLICY | Connection request FAILED, Reason: %s[8], ip: %s, protocol: %s[9], IKERule: "%s", IPsecAction: "%s", FilteringRule: “%s”[10], Stopped at: %s[11] |
| 6 | Обнаружены некорректные данные в базе данных, связанные с LSP | ERR | POLICY | There is a bad lsp object in product db: '%{1}s',<br>%{1}s – имя некорректного файла описания объекта в базе данных |
| 7 | Обнаружена более чем одна активная LSP в базе данных | ERR | POLICY | There are at least two active configurations in product db: '%{1}s' and '%{2}s'<br>%{1}s – имя первого файла описания объекта в базе данных с активной LSP<br>%{2}s – имя второго файла описания объекта в базе данных с активной LSP |
| 8 | Ошибка в записи маршрутизации | ERR | SYSTEM | Invalid route to %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s<br>где:<br>%{1}s%{2}d – destination в виде одиночного IP или подсети<br>%{3}s – gw или interface<br>%{4}s – адрес gateway-я или имя интерфейса<br>%{5}s – “, metric”, если указана метрика в LSP<br>%{6}s – значение метрики<br>%{7}s – описание ошибки: inconsistency, invalid gateway (matches local address) |

[8] Session timeout | Invalid packet | No proposal chosen | Invalid ID | Authentication failed | Internal error

[9] ISAKMP либо IPsec

[10] Если на момент вывода сообщения сведения о правилах ISAKMP, IPsec либо о фильтре отсутствуют, то соответствующие сведения не выводятся

[11] Дополнительные сведения об операции, на которой прервался процесс установления соединения

  

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 9 | Ошибка при добавлении записи в таблицу маршрутизации | ERR | SYSTEM | Failed to add routing: %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s<br>где:<br>%{1}s%{2}d – destination в виде одиночного IP или подсети<br>%{3}s – gw или interface<br>%{4}s – адрес gateway-я или имя интерфейса<br>%{5}s – “, metric”, если указана метрика в LSP<br>%{6}s – значение метрики<br>%{7}s – описание ошибки: inconsistency, invalid gateway (matches local address)<br>На уровне ERROR параметр %{7}s может принимать следующие значения: system error, unknown network interface, internal error.<br>На уровне WARNING параметр %{7}s может принимать следующие значения: already exists. |
| 10 | Ошибка при удалении записи из таблицы маршрутизации | ERR | SYSTEM | Failed to delete routing: %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s<br>где:<br>%{1}s%{2}d – destination в виде одиночного IP или подсети<br>%{3}s – gw или interface<br>%{4}s – адрес gateway-я или имя интерфейса<br>%{5}s – “, metric”, если указана метрика в LSP<br>%{6}s – значение метрики<br>%{7}s – описание ошибки: inconsistency, invalid gateway (matches local address)<br>На уровне ERROR параметр %{7}s может принимать следующие значения: system error, internal error.<br>На уровне WARNING параметр %{7}s может принимать следующие значения: not found. |
| 11 | Неудачная попытка доступа Пользователя к Агенту | ERR | SYSTEM | User login failed |

**Сообщения уровня WARNING**

Таблица 4

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 1 | В файле x509conv.ini указана неподдерживаемая кодировка | WARNING | CERT | Unsupported encoding "%{1}s" has been specified in x509conv.ini, "%{2}s" will be used<br>%{1}s – неподдерживаемая кодировка<br>%{2}s – кодировка, которая будет использована для соответствующего ASN.1-типа |

  

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 2 | В файле x509conv.ini указан неизвестный параметр | WARNING | CERT | Unexpected parameter "%{1}s" has been specified in x509conv.ini, ignored<br>%{1}s – имя неизвестного параметра |
| 3 | Ошибка при перекодировке полей Issuer или Subject сертификата в UTF-8 | WARNING | CERT | Certificate with subject "%{1}s" has incompatible attribute value encoding. Probably, the connection won't be established. Please, configure x509conv.ini according to actual attribute encoding.<br>%{1}s – строковое представление поля Subject сертификата |
| 4 | LDAP запрос {1} закончился неудачей. Причина: {2} | WARNING | LDAP | LDAP request failed. Reason: %{2}s[12]. Request: "%{1}s". |
| 5 | Неуспешная попытка установить соединение в качестве ответчика | WARNING | POLICY | Incoming connection request FAILED, Reason: %s[13], ip: %s, protocol: %s[14], IKERule: "%s", IPsSecAction: "%s"[15], FilteringRule: “%s”[16], Stopped at: %s[17] |
| 6 | Значение параметра DefaultCryptoContextsPerIPsecSA задано неверно | WARNING | POLICY | DefaultCryptoContextsPerIPsecSA in "agent.ini" is not valid (must be from 1 to 128), %{1}d will be used instead.<br>%{1}d – значение, которое будет использовано для параметра DefaultCryptoContextsPerIPsecSA |
| 7 | В правиле IKERule задано несколько трансформов с различными группами. Если в качестве инициатора Агент будет использовать Aggressive Mode, то в этом случае будут высылаться только трансформы с такой же группой как у первого трансформа в правиле. | WARNING | POLICY | WARNING: IKERule '%{2}s', line %{3}d: in Aggressive Mode initiator will use %{1}s only.<br>%{1}s – название выбранной группы, по которой будет работать Агент в качестве инициатора в Aggressive Mode.<br>%{2}s – имя IKERule, для которого выведена эта диагностика<br>%{3}d – строка, на которой располагается IKERule. |

[12] *Create request failed – Не удалось сформировать корректный запрос*

*Failed to parse message – Ошибка разбора сообщения LDAP*

*Timeout*

*LDAP server is not responding – LDAP сервер недоступен*

*Request canceled – Запрос прерван (например при выгрузке конфигурации)*

*Unknown – Причина неизвестна*

[13] *Session timeout | Limit of %u responded sessions achieved | Invalid packet | No proposal chosen | No rule chosen | Invalid ID | Authentication failed | Internal error*

[14] *ISAKMP либо IPsec*

[15] *Если на момент вывода сообщения правило ISAKMP, либо IPsec не выбрано, то сведения о нём не выводятся*

[16] *Если на момент вывода сообщения сведения о правилах ISAKMP, IPsec либо о фильтре отсутствуют, то соответствующие сведения не выводятся*

[17] *Дополнительные сведения об операции, на которой прервался процесс установления соединения*

  

**Сообщения уровня NOTICE**

Таблица 5

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 1 | Результат LDAP запроса {1} – объекты не найдены | NOTICE | LDAP | LDAP request result: NOT FOUND. Request: "%{1}s". |
| 2 | Результат LDAP запроса {1} – найдено {2} объектов | NOTICE | LDAP | LDAP request result: %{2}s object(s) found. Request: "%{1}s". |
| 3 | Присвоен IP-адрес из удалённого IKE-CFG пула | NOTICE | POLICY | VPN ip-address %s obtained, Partner: %s:%d[18] |
| 4 | Партнёру присвоен IP-адрес из IKE-CFG пула | NOTICE | POLICY | VPN ip-address %s assigned to external host Partner: %s:%d[19] |
| 5 | Превышено ограничение на количество инициированных IKE-сессий. Инициированная сессия отложена до завершения любой активной инициированной IKE-сессии. | NOTICE | POLICY | [ISAKMP]: Exchange pended. Limit of %u initiated sessions achieved. Partner: %s:%d[20] |
| 6 | Превышено ограничение на количество IKE-сессий, инициированных партнерами. Запрос от партнера игнорируется, новая сессия не создается. | NOTICE | POLICY | [ISAKMP]: Exchange cancelled. Limit of %u responded sessions achieved. Partner: %s:%d[21] |
| 7 | Старт сервиса | NOTICE | SYSTEM | Service started, version %s |
| 8 | Остановка сервиса | NOTICE | SYSTEM | Service stopped |
| 9 | Доступ Пользователя к Агенту | NOTICE | SYSTEM | User logged in |
| 10 | Отключение доступа Пользователя к Агенту | NOTICE | SYSTEM | User logged out |

[18] *ip:port*

[19] *ip:port*

[20] *ip:port*

[21] *ip:port*

  

**Сообщения уровня INFO**

Таблица 6

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 1 | Установлено соединение | INFO | POLICY | Connection established, %u.%u.%u.%u[-%u.%u.%u.%u][:%u]<->%u.%u.%u.%u[-%u.%u.%u.%u][:%u][, proto %u], FilteringRule: “%s”, IPsecAction: “%s”<br>где:<br>квадратные скобки обозначают, что данная часть сообщения может отсутствовать<br>первый аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” – IP-адрес или диапазон IP-адресов и порт, которые защищаются Агентом<br>второй аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” –IP-адрес или диапазон IP-адресов и порт, которые защищаются партнером<br>[, proto %u] – защищаемый протокол<br>FilteringRule: “%s” – фильтр, на который загружена созданная цепочка IPsec SA-ев<br>IPsecAction: “%s” – правило IPsecAction по которому создалось соединение |
| 2 | Получен ISAKMP-пакет от партнера, с которым запрещен IKE-трафик[22] | INFO | POLICY | Inbound IKE packet dropped, Reason: Access denied, Partner: %s:%d[23] |

*[22] Партнер (идентифицируется по паре ip:port) может быть помещен в «черный список», если с ним нет ни одного ISAKMP соединения, и за определенный промежуток времени он неуспешно пытался установить ISAKMP соединение достаточно большое количество раз. При получении нового IKE-пакета от такого партнера любая обработка IKE-пакетов игнорируется, поэтому невозможно определить намерение партнера: это может быть новая попытка установления ISAKMP соединения, продолжение старых попыток, информационное сообщение, либо просто пакет неправильного формата. Обмен с таким партнером разрешается спустя установленный промежуток времени, либо при инициировании соединения со стороны локального устройства.*

*[23] ip:port*

  

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 3 | Закрытие соединения | INFO | POLICY | Connection closed, %u.%u.%u.%u[-%u.%u.%u.%u][:%u]<->%u.%u.%u.%u[-%u.%u.%u.%u][:%u][, proto %u], bytes sent/received: %d / %d, Reason: %s<br>где:<br>квадратные скобки обозначают, что данная часть сообщения может отсутствовать<br>первый аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” – IP-адрес или диапазон IP-адресов и порт, которые защищаются Агентом<br>второй аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” –IP-адрес или диапазон IP-адресов и порт, которые защищаются партнером<br>[, proto %u] – защищаемый протокол<br>bytes sent/received: %d / %d – количество байт, который были отосланы и приняты под защитой этого соединения<br>Reason: %s – причина удаления соединения, возможны следующие варианты:<br>Loading new configuration – соединение уничтожено по причине загрузки новой конфигурации<br>Delete payload received – от партнера пришел запрос на удаление этого соединения<br>Time expired – истек лимит действия соединения по времени<br>Traffic expired – истек лимит действия соединения по трафику<br>Dead peer detected – партнер признан «мертвым»<br>Initial contact – соединение удалено при получении нотификации INITIAL-CONTACT<br>Cannot start DPD (no ISAKMP SA) – нет возможности инициировать DPD, партнер признается «мертвым» и соединение с ним удаляется<br>Replaced with new one – соединение удаляется в связи с тем, что построено новое<br>SA bundle destroyed – возникает в случае использования вложенного IPsec, когда удаляется одна из цепочек IPsec SAs, что приводит к уничтожению всей связки цепочек. |
| 4 | IPsec-соединение не установилось из-за превышения количества, разрешенного лицензией | INFO | POLICY | Unable to establish connection: resources exceeded |

  

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 5 | Информация о лицензии продукта | INFO | SYSTEM | Product licence: product code: %s, customer code: %s, license number: %n, license code: %s |

**Сообщения уровня DEBUG**

Таблица 7

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 1 | Не найден сертификат партнёра | DEBUG | CERT | Searching peer certificate failed. Reason: not found. Search template: %s |
| 2 | Найден непригодный сертификат партнёра | DEBUG | CERT | Searching peer certificate failed. Reason: %s[24]. Subject: %s Issuer: %s SN: %s |
| 3 | Выбран сертификат партнёра | DEBUG | CERT | Use peer certificate: Subject: %s Issuer: %s SN: %s |
| 4 | Сформирован LDAP запрос {1} | DEBUG | LDAP | LDAP request: "%{1}s[25]". |
| 5 | LDAP запрос {1} проигнорирован: не задан LDAP сервер | DEBUG | LDAP | LDAP request ignored: there is no LDAP server available. Request: "%{1}s". |
| 6 | Запрос на создание соединения | DEBUG | POLICY | Connection request, packet: %u.%u.%u.%u[:%u]-> %u.%u.%u.%u[:%u][, proto %u], FilteringRule: “%s”<br>где:<br>квадратные скобки обозначают, что данная часть сообщения может отсутствовать<br>первый аргумент вида “%u.%u.%u.%u[:%u]” – IP-адрес источника и порт, если он указан в пакете<br>второй аргумент вида “%u.%u.%u.%u[:%u]” - IP-адрес приемника и порт, если он указан в пакете<br>[,proto %u] – номер протокола, если указан в пакете, иначе не пишется<br>FilteringRule “%s” – название фильтра, под который попал пакет |

[24] *revoked | expired | not verified*

[25] *Во всех сообщениях LDAP запрос описывается в виде URL. В настоящее время если используются IP-адрес и порт, заданные в LSP, они в URL не указываются.*

  

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 7 | Ошибка инициирования создания соединения | DEBUG | POLICY | Failed to initiate connection request processing, packet: %u.%u.%u.%u[:%u]->%u.%u.%u.%u[:%u][, proto %u]<br>где:<br>квадратные скобки обозначают, что данная часть сообщения может отсутствовать<br>первый аргумент вида “%u.%u.%u.%u[:%u]” – IP-адрес источника и порт, если он указан в пакете<br>второй аргумент вида “%u.%u.%u.%u[:%u]” - IP-адрес приемника и порт, если он указан в пакете<br>[,proto %u] – номер протокола, если указан в пакете, иначе не пишется |
| 8 | Создание ISAKMP SA | DEBUG | POLICY | ISAKMP connection [%u] established, Partner: %s:%d[26], Identity: %s, IKERule: “%s” |
| 9 | Удаление ISAKMP SA | DEBUG | POLICY | ISAKMP connection [%u] closed, Partner: %s:%d[27], Identity: %s, bytes sent/received: %d / %d, Exchanges passed: %d |
| 10 | Обнаружение устройства NAT | DEBUG | POLICY | NAT detected on ...[28] side, Partner: %s:%d[29] |
| 11 | Proposals высланы партнёру | DEBUG | POLICY | (Phase I): [30]<br>Sending IKE proposals. Rule “%s”: Auth: %s<br>Transform #1: Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: %<br>Transform #2: ..<br>(Phase II):[31]<br>Sending IPsec proposals. Rule “%s”: Encapsulation mode: %s, Group: %s<br>Proposal #1:<br>Protocol AH:<br>Transform #1: Integrity: %s, Life Time: %s, Life Traffic: %s<br>Transform #2: .....<br>Protocol ESP:<br>Transform #1: Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s<br>Transform #2:<br>Proposal #2: |

[26] *ip:port*

[27] *ip:port*

[28] *local | remote*

[29] *ip:port*

[30] *Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются*

[31] *Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются*

  

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 12 | Партнёр прислал набор proposals | DEBUG | POLICY | (Phase I): [32]<br>IKE proposals received.<br>Transform #1: Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: %<br>Transform #2: |
| | | | | (Phase II):[33]<br>IPsec proposals received. Encapsulation mode: %s, Group: %s<br>Proposal #1:<br>Protocol AH:<br>Transform #1: Integrity: %s, Life Time: %s, Life Traffic: %s<br>Transform #2<br>Protocol ESP:<br>Transform #1: Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s<br>Transform #2:<br>Proposal #2 |
| 13 | Проверка proposal для правила | DEBUG | POLICY | Check proposal #%u, Protocol %s[34], Transform #%u for Rule “%s”. Result: %s[35], attribute: %s[36] |
| 14 | Выбран proposal | DEBUG | POLICY | (Phase I): [37]<br>ISAKMP proposal selected. Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: %s |
| | | | | (Phase II):[38]<br>IPsec proposal selected. Mode: %s[39], Group: %s, AH Integrity: %s, ESP Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s |
| 15 | Выбран Preshared ключ | DEBUG | POLICY | Using preshared key "%{1}s" for partner %{2}s:%{3}d,<br>где:<br>%{1}s – Идентификатор выбранного ключа, указанный в LSP<br>%{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену |
| 16 | Недоступен выбранный Preshared ключ | DEBUG | POLICY | Preshared key "%{1}s" not found,<br>где:<br>%{1}s – Идентификатор выбранного ключа, указанный в LSP |

[32] *Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются*

[33] *Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются*

[34] *ISAKMP | AH | ESP*

[35] *Not matched | OK*

[36] *Authentication method | Hash | Cipher | Oakley group | Integrity | mode – только для не совпавших proposals*

[37] *Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются*

[38] *Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются*

[39] *Transport | Tunnel*

  

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 17 | Присланный идентификатор партнера по IKE-обмену не подошел ни под одно правило ISAKMP. Предпринимается попытка идентифицировать партнера по его IP-адресу. | DEBUG | POLICY | WARNING: Unable to proceed IKE remote ID for partner %{2}s:%{3}d. Using ip-address from IKE packet instead,<br>где:<br>%{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену |
| 18 | Не удалось подобрать правило аутентификации для данного партнера по IKE-обмену | DEBUG | POLICY | Unable to choose authentication rule for partner %{2}s:%{3}d,<br>где:<br>%{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену |
| 19 | Информация об используемом локальном IKE-Identity | DEBUG | POLICY | [ISAKMP]: Sending identity "%s" to partner <ip:port> |
| 20 | Информация об IKE-Identity, присланным партнером | DEBUG | POLICY | [ISAKMP]: Identity "%s" is received from partner <ip:port> |
| 21 | Информация о сообщении (IKE-Notification), присланным партнером | DEBUG | POLICY | [ISAKMP]: Notification [%s[40]] has been received for Exchange <%u[41]>: %s[42] |
| 22 | Инициированный IKE-обмен завершился с ошибкой | DEBUG | POLICY | [ISAKMP]: Connection request FAILED. %s<br>где:<br>%s – дополнительная доступная информация о несостоявшемся обмене:<br>причина аварийного завершения [43] (см.Таблица 8)<br>стек выполняемых операций (см.Таблица 9)<br>сведения о партнере: <ip:port>, IKE-Identity [44] |

[40] *Согласно списку п. 3.14.1 в RFC 2408 и п. 4.6.3 в RFC 2407.*

[41] *Номер-идентификатор IKE-обмена.*

[42] *Реакция Агента на присланное сообщение: Ignore | Ignore unprotected Notification | Cancel target connection | Correct TTL for target connection | Start IPsec traffic | Target connection is already disabled | Peer is alive | Wrong sequence: Ignore | Peer is interested in my liveness: send acknowledgement | Clear all old connections*

[43] *Если к моменту завершения партнерам удалось договориться о применении метода аутентификации на Preshared-ключах, и в списке операций присутствует «Unable to decode packet», то, наряду с ошибкой собственно расшифрования, либо IKE-пакета, неправильно сформированного партнером, причиной отказа в соединении может быть применение неправильного ключа.*

[44] *IKE Identity указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.*

| | Описание события | Уровень важности | Раздел | Шаблоны сообщений |
|---|---|---|---|---|
| 23 | IKE-обмен, инициированный партнером, завершился с ошибкой | DEBUG | POLICY | [ISAKMP]: Incoming connection FAILED. %s<br>где:<br>%s – дополнительная доступная информация о несостоявшемся обмене:<br>причина аварийного завершения [45] (см.Таблица 8)<br>стек выполняемых операций (см.Таблица 9)<br>сведения о партнере: <ip:port>, IKE-Identity[46] |
| 24 | Пересечение соединений по адресам от разных партнеров на одном фильтре | DEBUG | POLICY | Connection to %{1}s:%{2}d conflicts with connection to %{3}s:%{4}d, conflicting address range: %{5}s<br>%{1}s:%{2}d – IP-адрес и порт партнера, который блокирует соединение к партнеру %{3}s:%{4}d в адресном пространстве %{5}s |

[45] *Если к моменту завершения партнерам удалось договориться о применении метода аутентификации на Preshared-ключах, и в списке операций присутствует «Unable to decode packet», то, наряду с ошибкой собственно расшифрования, либо IKE-пакета, неправильно сформированного партнером, причиной отказа в соединении может быть применение неправильного ключа.*

[46] *IKE Identity указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.*

## 10.2.1. Список ошибок протокола ISAKMP

(см. пункты 22 и 23 Таблица 7)

Таблица 8

| | Описание ошибки | Запись об ошибке в строке сообщения |
|---|---|---|
| 1 | Не удалось сформировать подпись | Unable to Form Signature |
| 2 | От партнера пришло сообщение неверного типа вместо ожидаемого сообщения CONNECTED (свидетельствующего о готовности IPsec-соединения на стороне партнера) | Unexpected Notification type: need CONNECTED |
| 3 | Получен компонент IKE-пакета типа 130, соответствующий компоненту для обнаружения устройства NAT, что не соответствует протоколу обмена для данного этапа | Unexpected payload found (payload type - 130, possibly NAT Discovery) |
| 4 | От партнера пришла команда дополнительной настройки ISAKMP-соединения (XAuth, IKE-CFG, и т.п.), не соответствующая протоколу обмена для данного этапа | Unexpected configuration message type |
| 5 | Потеряны внутренние данные от предыдущего пакета | Previous packet missed |
| 6 | Потеряны данные формируемого пакета | OUT packet missed |
| 7 | Потерян SA-компонент предыдущего пакета | Missing SA payload |
| 8 | Невозможно выбрать сценарий IKE-обмена для выбранного типа аутентификации | Unknown IKE-scenario for chosen Authentification method |
| 9 | Не обнаружен локальный сертификат | Local Certificate is not present |
| 10 | Не обнаружен сертификат партнера | Remote Certificate is not present |
| 11 | Не найден сертификат | Certificate not found |
| 12 | Нет доступа к публичному ключу сертификата | Cert Public Key is inaccessible |
| 13 | Не найден один из необходимых компонентов пакета | Can't find proposal |
| 14 | Потеряны данные с ключевой информацией | Encryption container missed |
| 15 | Партнер вернул неправильную идентификационную информацию ответчика IKE-обмена при создании IPsec-соединения | Bad IDcr returned |

  

| | Описание ошибки | Запись об ошибке в строке сообщения |
|---|---|---|
| 16 | Потеряны данные входящего пакета | IN packet missed |
| 17 | Партнер вернул неправильную идентификационную информацию инициатора IKE-обмена при создании IPsec-соединения | Bad IDci returned |
| 18 | Партнер прислал IKE-пакет с неправильной структурой, либо пакет не удалось правильно расшифровать. | Invalid packet (invalid structure). |

### 10.2.2. Список выполняемых действий по протоколу ISAKMP

(см. пункты 22 и 23 Таблица 7)

Таблица 9

| | Описание дествия | Информация в строке сообщения |
|---|---|---|
| 1 | Шифрование сформированного IKE-пакета перед отправкой партнеру | Coding packet |
| 2 | Расшифрование IKE-пакета, присланного партнером | Decoding packet |
| 3 | Проверка предложений, на которые согласился партнер | Check replied SA |
| 4 | Проверка сертификата, присланного партнером | Check for Remote Certificate |
| 5 | Запрос локального сертификата | Check for Local Certificate |
| 6 | Проверка идентификационной информации, присланной партнером | Check incom IDs |
| 7 | Использование в качестве идентификационной информации партнера его IP-адреса | Check IDs as IP-addresses |
| 8 | Проверка используемого алгоритма хэширования | Check for Hash method |
| 9 | Синтаксический разбор пакета, присланного партнером на отдельные компоненты (payloads) | Make payload set for received packet |
| 10 | Проверка всех компонентов присланного пакета | Check received payloads |
| 11 | Проверка формируемого пакета на наличие компонентов перед отправкой партнеру. Используется только при создании пакетов Informational обменов чтобы удостовериться, что информация не была отправлена с другим пакетом. | Check for added payloads |
| 12 | Формирование подписи | Encrypt Signature |
| 13 | Выбор правила IKE согласно текущей конфигурации по идентификационной информации партнера | Choose Rule for Partner's identity |
| 14 | Создание ключевых пар текущей IKE-сессии | Generate Keys |
| 15 | Формирование ключевого материала | Generate SKEYIDs |

  

| | Описание дествия | Информация в строке сообщения |
|---|---|---|
| 16 | Выбор политики безопасности согласно текущей конфигурации на основании предложений от партнера | Compare policy |
| 17 | Формирование SPI | Set SPI |
| 18 | Проверка и принятие параметров устанавливаемого соединения, на которые согласился партнер | Accept Transform |
| 19 | Вычисление хэша для обнаружения устройства NAT | Calculate NAT Discovery payload |
| 20 | Вычисление общего ключа | Calculate Shared Key |
| 21 | Вычисление инициализационного вектора | Calculate InitVector |
| 22 | Определение метода аутентификации | Detect Authentification Method |
| 23 | Проверка локального сертификата для метода аутентификации с использованием сертификатов | Authentification uses Certificates: Check for Local Certificates |
| 24 | Проверка метода аутентификации, предложенного партнером, на соответствие текущей политике безопасности | Check Authentification Method |
| 25 | Выбор метода аутентификации | Choose Authentification Method |
| 26 | Проверка выбранной комбинации параметров устанавливаемого соединения | Get Proposal |
| 27 | Задание выбранного алгоритма шифрации для устанавливаемого соединения | Get Algorithm |
| 28 | Запрос возможных параметров устанавливаемого соединения согласно текущей конфигурации для их согласования с партнером | Get Local Policy |
| 29 | Проверка на наличие в предложении партнера параметра, устанавливающего MODP-группу | Get DH group for QM |
| 30 | Выбор используемой идентификационной информации для отправки партнеру | Get ID from Local Policy |
| 31 | Выбор используемой идентификационной информации для отправки партнеру при создании ISAKMP-соединения в качестве инициатора | Get IDii from Local Policy |
| 32 | Выбор используемой идентификационной информации для отправки партнеру при создании ISAKMP-соединения в качестве ответчика | Get IDir from Local Policy |

  

| | Описание дествия | Информация в строке сообщения |
|---|---|---|
| 33 | Выбор используемой идентификационной информации для отправки партнеру при создании IPsec-соединения в качестве инициатора IKE-обмена | Get IDci from Local Policy |
| 34 | Выбор используемой идентификационной информации для отправки партнеру при создании IPsec-соединения в качестве ответчика IKE-обмена | Get IDcr from Local Policy |
| 35 | Инициализация ключевой информации для формирования IPsec-соединения | Initialize Encryption Container for QM |
| 36 | Формирование готового IPsec-соединения | Create contexts |
| 37 | Распознавание метода дополнительной настройки ISAKMP-соединения (XAuth, IKE-CFG, и т.п.) | Determine IKE configuration method |
| 38 | Распознавание команды дополнительной настройки ISAKMP-соединения (XAuth, IKE-CFG, и т.п.) | Determine ike-cfg message type |
| 39 | Распаковка параметров присланного запроса на дополнительную аутентификацию (XAuth) и формирование соответствующего графического пользовательского диалога | Analyse attributes and fill user dialog fields |
| 40 | Запуск графического пользовательского диалога дополнительной аутентификации (XAuth). | Start dialog for user extended authentication |
| 41 | Проверка наличия компонента IKE-пакета | Check payload %s[47] |
| 42 | Проверка структуры компонента IKE-пакета | Analyse payload structure %s[48] |
| 43 | Формирование компонента IKE-пакета | Form payload %s[49] |
| 44 | Заполнение блока данных указанного компонента IKE-пакета | Fill payload %s[50] |
| 45 | Проверка содержимого компонента IKE-пакета | Check %s[51] |
| 46 | Вычисление хэша – содержимого указанного компонента | Calculate %s[52] |

[47] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408
[48] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408
[49] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408
[50] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408
[51] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408
[52] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

| | Описание дествия | Информация в строке сообщения |
|---|---|---|
| 47 | Выполнение сценария инициации информационного обмена IKE согласно RFC 2409 | [Informational Exchange, Initiator, Packet 1] |
| 48 | Выполнение сценария обработки пакета информационного обмена IKE согласно RFC 2409 | [Informational Exchange, Responder, Packet 1] |
| 49 | Выполнение шага сценария формирования 1-го пакета IKE Main Mode согласно RFC 2409 | [Main Mode, Initiator, Packet 1] |
| 50 | Выполнение шага сценария обработки 1-го пакета IKE Main Mode согласно RFC 2409 и формирование ответного пакета | [Main Mode, Responder, Packets 1,2] |
| 51 | Выполнение шага сценария начала обработки 2-го пакета IKE Main Mode согласно RFC 2409 | [Main Mode, Initiator, Packets 2,3] |
| 52 | Выполнение шага сценария продолжения обработки 2-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета | [Main Mode, Initiator, Packets 2,3, Pre-Shared Key] |
| 53 | Выполнение шага сценария продолжения обработки 2-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета | [Main Mode, Initiator, Packets 2,3, Signature] |
| 54 | Выполнение шага сценария обработки 3-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета | [Main Mode, Responder, Packets 3,4, Pre-Shared Key] |
| 55 | Выполнение шага сценария обработки 3-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета | [Main Mode, Responder, Packets 3,4, Signature] |
| 56 | Выполнение шага сценария обработки 4-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета | [Main Mode, Initiator, Packets 4,5, Pre-Shared Key] |
| 57 | Выполнение шага сценария обработки 4-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета | [Main Mode, Initiator, Packets 4,5, Signature] |
| 58 | Выполнение шага сценария обработки 5-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета | [Main Mode, Responder, Packets 5,6, Pre-Shared Key] |

  

| | Описание дествия | Информация в строке сообщения |
|---|---|---|
| 59 | Выполнение шага сценария обработки 5-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета | [Main Mode, Responder, Packets 5,6, Signature] |
| 60 | Выполнение шага сценария обработки 6-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 | [Main Mode, Initiator, Packet 6, Pre-Shared Key] |
| 61 | Выполнение шага сценария обработки 6-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 | [Main Mode, Initiator, Packet 6, Signature] |
| 62 | Выполнение шага сценария начала формирования 1-го пакета IKE Aggressive Mode Mode согласно RFC 2409 | [Aggressive Mode, Initiator, Packet 1] |
| 63 | Выполнение шага сценария продолжения формирования 1-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 | [Aggressive Mode, Initiator, Packet 1, Pre-Shared Key] |
| 64 | Выполнение шага сценария продолжения формирования 1-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 | [Aggressive Mode, Initiator, Packet 1, Signature] |
| 65 | Выполнение шага сценария начала обработки 2-го пакета IKE Aggressive Mode согласно RFC 2409 | [Aggressive Mode, Responder, Packets 1,2] |
| 66 | Выполнение шага сценария продолжения обработки 1-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета | [Aggressive Mode, Responder, Packets 1,2, Pre-Shared Key] |
| 67 | Выполнение шага сценария продолжения обработки 1-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета | [Aggressive Mode, Responder, Packets 1,2, Signature] |
| 68 | Выполнение шага сценария обработки 2-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета | [Aggressive Mode, Initiator, Packets 2,3, Pre-Shared Key] |
| 69 | Выполнение шага сценария обработки 2-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета | [Aggressive Mode, Initiator, Packets 2,3, Signature] |
| 70 | Выполнение шага сценария обработки 3-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 | [Aggressive Mode, Responder, Packet 3, Pre-Shared Key] |

  

| | Описание дествия | Информация в строке сообщения |
|---|---|---|
| 71 | Выполнение шага сценария обработки 3-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 | [Aggressive Mode, Responder, Packet 3, Signature] |
| 72 | Выполнение шага сценария формирования 1-го пакета IKE New Group Mode согласно RFC 2409 | [New Group Mode, Initiator, Packet 1] |
| 73 | Выполнение шага сценария обработки 1-го пакета IKE New Group Mode согласно RFC 2409 и формирование ответного пакета | [New Group Mode, Responder, Packets 1,2] |
| 74 | Выполнение шага сценария обработки 2-го пакета IKE New Group Mode согласно RFC 2409 | [New Group Mode, Initiator, Packet 2] |
| 75 | Выполнение шага сценария формирования 1-го пакета служебного обмена IKE | [Transaction Exchange, Initiator, Packet 1] |
| 76 | Выполнение шага сценария обработки 1-го пакета служебного обмена IKE и формирование ответного пакета | [Transaction Exchange, Responder, Packets 1,2] |
| 77 | Выполнение шага сценария обработки 2-го пакета служебного обмена IKE | [Transaction Exchange, Initiator, Packet 2] |
| 78 | Выполнение шага сценария формирования 1-го пакета IKE Quick Mode согласно RFC 2409 | [Quick Mode, Initiator, Packet 1] |
| 79 | Выполнение шага сценария обработки 1-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета | [Quick Mode, Responder, Packets 1,2] |
| 80 | Выполнение шага сценария обработки 2-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета | [Quick Mode, Initiator, Packets 2,3] |
| 81 | Выполнение шага сценария обработки 3-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета (при поддержке партнером Commit Bit) | [Quick Mode, Responder, Packet 3,(4)] |
| 82 | Выполнение шага сценария обработки 4-го пакета IKE Quick Mode (при поддержке партнером Commit Bit) | [Quick Mode, Initiator, Packet 4] |
| 83 | Вычисление ключевого материала | [Make SKEYID] |
| 84 | Выбор ISAKMP либо IPsec правила | [Choose Rule] |
| 85 | Проверка присланного атрибута – компонента пакета IKE | [Check Attr] |

  

| | Описание дествия | Информация в строке сообщения |
|---|---|---|
| 86 | Проверка присланного сертификата – компонента пакета IKE | [Check Cert] |
| 87 | Проверка присланного хэша – компонента пакета IKE | [Check HASH] |
| 88 | Проверка присланного идентификатора – компонента пакета IKE | [Check ID] |
| 89 | Проверка присланного ключа – компонента пакета IKE | [Check KE] |
| 90 | Проверка присланного NAT-детектора – компонента пакета IKE | [Check NAT-D] |
| 91 | Проверка присланного NAT Original Address – компонента пакета IKE | [Check NAT-OA] |
| 92 | Проверка присланного Nonce – компонента пакета IKE | [Check Nonce] |
| 93 | Проверка присланного сообщения – компонента пакета IKE | [Check Notif] |
| 94 | Проверка присланного запроса на сертификат – компонента пакета IKE | [Check REQ] |
| 95 | Проверка присланных предложений на создание соединения – компонента пакета IKE | [Check SA] |
| 96 | Проверка присланной подписи – компонента пакета IKE | [Check SIG] |
| 97 | Проверка вендор-идентификатора – компонента пакета IKE | [Check VID] |
| 98 | Формирование атрибута – компонента пакета IKE | [Form Attr] |
| 99 | Формирование сертификата – компонента пакета IKE | [Form Cert] |
| 100 | Формирование хэша – компонента пакета IKE | [Form HASH] |
| 101 | Формирование идентификатора – компонента пакета IKE | [Form ID] |
| 102 | Формирование ключа – компонента пакета IKE | [Form KE] |
| 103 | Формирование NAT-детектора – компонента пакета IKE | [Form NAT-D] |

  

| | Описание дествия | Информация в строке сообщения |
|---|---|---|
| 104 | Формирование NAT Original Address – компонента пакета IKE | [Form NAT-OA] |
| 105 | Формирование Nonce – компонента пакета IKE | [Form Nonce] |
| 106 | Формирование запроса на сертификат – компонента пакета IKE | [Form CertReq] |
| 107 | Формирование подписи – компонента пакета IKE | [Form SIG] |
| 108 | Формирование вендор-идентификатора – компонента пакета IKE | [Form VendorID] |
| 109 | Проверка на наличие устройства NAT | [NAT existence check] |

  

# 11. Мониторинг

Мониторинг Bel VPN Client осуществляется по протоколу обмена SNMPv1 или SNMPv2c.

Настройка SNMP-агента произведена администратором при подготовке инсталляционного пакета для пользователя.

SNMP-менеджер имеет возможность только запрашивать содержимое базы данных агента. SNMP-менеджер инициирует запрос на значения одной или нескольких переменных, который посылает SNMP-агенту. SNMP-агент, отвечая на запрос, возвращает значения одной или нескольких переменных. Другие типы сообщений между менеджером и агентом не поддерживаются.

В качестве SNMP-менеджера могут быть использованы:

- программный продукт CiscoWorks VPN Monitor, который входит в состав комплекта CiscoWorks VMS 2.2.
- бесплатная утилита NET-SNMP (http://www.net-snmp.org/), которая является простейшим SNMP-менеджером. При работе с SNMP-агентом нужно указывать версию SNMP –v 1 или – v 2c.

## 11.1. Выдача статистики

База данных MIB, поддерживаемая SNMP-агентом, разделена на группы. В приведенной ниже таблице перечислены переменные из стандартной группы `system`, глобальной статистики IKE и IPsec, которые могут быть запрошены SNMP-менеджером.

**Примечание 1:** при принудительном перезапуске сервиса IKE-статистика сбрасывается и начинает считаться со старта Агента. IPsec-статистика считается со старта компьютера и при принудительном перезапуске сервиса не сбрасывается.

**Примечание 2:** в IKE-статистике при подсчете трафика учитывается только количество байт в ISAKMP-пакете. У Cisco же в IKE-статистике учитываются данные из IP-заголовка, UDP-заголовка и Ethernet-заголовка пакета.

Таблица 10

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| **Статистика по стандартной группе System и специфичным константным значениям** | | | | |
| sysDescr | 1.3.6.1.2.1.1.1.0 | DisplayString | Текстовое описание сетевого объекта.<br>Строка вида "Bel VPN Gate 3.0.<build>" | RFC1213-MIB |
| sysObjectID | 1.3.6.1.2.1.1.2.0 | OID | Идентификатор фирмы-производителя (внутри поддерева 1.3.6.1.4.1):<br>1.3.6.1.4.1.9.1.467(cisco2611XM из CISCO-PRODUCTS-MIB) | RFC1213-MIB |
| sysUpTime | 1.3.6.1.2.1.1.3.0 | TimeTicks | The time (in hundredths of a second) since the network management portion of the system was last re-initialized.<br>Время в сотых долях секунды с момента последней загрузки системы | RFC1213-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| sysContact | 1.3.6.1.2.1.1.4.0 | DisplayString | Имя контактной персоны и способ контакта | RFC1213-MIB |
| sysName | 1.3.6.1.2.1.1.5.0 | DisplayString | Полное имя домена <hostname>.<domain-name> | RFC1213-MIB |
| sysLocation | 1.3.6.1.2.1.1.6.0 | DisplayString | Физическое местоположение агента | RFC1213-MIB |
| sysServices | 1.3.6.1.2.1.1.7.0 | int32 | Значение, которое характеризует сервисы, предоставляемые узлом. Это значение есть сумма номеров уровней модели OSI в зависимоти от того, какие сервисы поддерживаются: 0x01 (физический), 0x02 (канальный), 0x04 (сетевой), 0x08 (точка-точка), 0x40 (прикладной). Например, если поддерживается IP уровень (маршрутизация) и транспортный уровень (точка-точка), то значение sysServices есть сумма 4 и 8.<br>78 (c2611XM) | RFC1213-MIB |
| chassisType | 1.3.6.1.4.1.9.3.6.1.0 | int32 | 335 (c2611XM) | OLD-CISCO-CHASSIS-MIB |
| cipSecMibLevel | 1.3.6.1.4.1.9.9.171.1.1.1.0 | int32 | The level of the IPsec MIB<br>1 | CISCO-IPSEC-FLOW-MONITOR-MIB |
| snmpSetSerialNo | 1.3.6.1.6.3.1.1.6.1.0 | int32 | <An advisory lock used to allow several cooperating SNMPv2 entities, all acting in a manager role, to coordinate their use of the SNMPv2 set operation.<br>Используется как значение, которое ограничивает сверху Cisco-specific значения. Фактически является неформальным обозначением конца MIB-а. Служит для предотвращения возможных коллизий при отработке GET-NEXT операций.<br>0 | SNMPv2-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| ciscoImageString | 1.3.6.1.4.1.9.9.25.1.1.1.2.<i> | DisplayString | <The string of this entry.> (описание таблицы – <A table provides content information describing the executing IOS image.>).<br>Выдаются данные для агента:<br>1: "CW_BEGIN$-csp-vpn$"<br>2: "CW_IMAGE$C2600-CSP-VPN$"<br>3: "CW_FAMILY$C2600$"<br>4: "CW_FEATURE$IP\|FIREWALL 2 PLUS 3DES$"<br>5: "CW_VERSION$12.2(13)T5, $"<br>6: "CW_MEDIA$RAM$"<br>7: "CW_SYSDESCR$CSP VPN {Gate\|Server\|Client} <major>.<minor>.<build>$""<br>8: "CW_MAGIC$$"<br>9: "CW_END$-csp-vpn$" | CISCO-IMAGE-MIB |
| **Глобальная IKE-статистика** | | | | |
| cikeGlobalActiveTunnels | 1.3.6.1.4.1.9.9.171.1.2.1.1.0 | uint32 | <The number of currently active IPsec Phase-1 IKE Tunnels><br>Все существующие на данный момент активные ISAKMP SA. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalPreviousTunnels | 1.3.6.1.4.1.9.9.171.1.2.1.2.0 | uint32 | <The total number of previously active IPsec Phase-1 IKE Tunnels><br>Количество ISAKMP SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalInOctets | 1.3.6.1.4.1.9.9.171.1.2.1.3.0 | uint32 | <The total number of octets received by all currently and previously active IPsec Phase-1 IKE Tunnels><br>Количество байт, принятых в течение всех IKE-сессий с момента старта Агента | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalInPkts | 1.3.6.1.4.1.9.9.171.1.2.1.4.0 | uint32 | <The total number of packets received by all currently and previously active IPsec Phase-1 IKE Tunnels><br>Количество ISAKMP-пакетов, принятых в течение всех IKE-сессий с момента старта Агента | CISCO-IPSEC-FLOW-MONITOR-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| cikeGlobalInDropPkts | 1.3.6.1.4.1.9.9.171.1.2.1.5.0 | uint32 | <The total number of packets which were dropped during receive processing by all currently and previously active IPsec Phase-1 IKE Tunnels><br>Количество ISAKMP-пакетов, отвергнутых в течение всех IKE-сессий с момента старта Агента | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalInP2Exchgs | 1.3.6.1.4.1.9.9.171.1.2.1.7.0 | uint32 | <The total number of IPsec Phase-2 exchanges received by all currently and previously active IPsec Phase-1 IKE Tunnels><br>Количество успешных Quick Modes в качестве респондера. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalInP2ExchgInvalids | 1.3.6.1.4.1.9.9.171.1.2.1.8.0 | uint32 | <The total number of IPsec Phase-2 exchanges which were received and found to be invalid by all currently and previously active IPsec Phase-1 IKE Tunnels><br>Общее количество IKE-сессий по созданию IPsec соединений, инициированных партнёрами, не состоявшихся по причине ошибки обмена. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalInP2ExchgRejects | 1.3.6.1.4.1.9.9.171.1.2.1.9.0 | uint32 | <The total number of IPsec Phase-2 exchanges which were received and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels><br>Общее количество IKE-сессий по созданию IPsec соединений, инициированных партнёрами, которые не состоялись по причине рассогласования политик безопасности. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalOutOctets | 1.3.6.1.4.1.9.9.171.1.2.1.11.0 | uint32 | <The total number of octets sent by all currently and previously active and IPsec Phase-1 IKE Tunnels><br>Количество байт, высланных в течение всех IKE-сессий с момента старта Агента | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalOutPkts | 1.3.6.1.4.1.9.9.171.1.2.1.12.0 | uint32 | <The total number of packets sent by all currently and previously active and IPsec Phase-1 Tunnels><br>Количество ISAKMP-пакетов, высланных в течение всех IKE-сессий с момента старта Агента | CISCO-IPSEC-FLOW-MONITOR-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| cikeGlobalOutDropPkts | 1.3.6.1.4.1.9.9.171.1.2.1.13.0 | uint32 | <The total number of packets which were dropped during send processing by all currently and previously active IPsec Phase-1 IKE Tunnels><br>Количество ISAKMP-пакетов в течение всех IKE-сессий с момента старта Агента, которые были готовы к отсылке, но по каким-то причинам не были отосланы | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalOutP2Exchgs | 1.3.6.1.4.1.9.9.171.1.2.1.15.0 | uint32 | <The total number of IPsec Phase-2 exchanges which were sent by all currently and previously active IPsec Phase-1 IKE Tunnels><br>Количество успешных Quick Modes в качестве инициатора. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalOutP2ExchgInvalids | 1.3.6.1.4.1.9.9.171.1.2.1.16.0 | uint32 | <The total number of IPsec Phase-2 exchanges which were sent and found to be invalid by all currently and previously active IPsec Phase-1 Tunnels><br>Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявшихся по причине ошибки обмена. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalOutP2ExchgRejects | 1.3.6.1.4.1.9.9.171.1.2.1.17.0 | uint32 | <The total number of IPsec Phase-2 exchanges which were sent and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels><br>Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявшихся по причине рассогласования политик безопасности. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalInitTunnels | 1.3.6.1.4.1.9.9.171.1.2.1.19.0 | uint32 | <The total number of IPsec Phase-1 IKE Tunnels which were locally initiated><br>Количество созданных ISAKMP SA в качестве инициатора (т.е. по инициативе локальной стороны). | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalInitTunnelFails | 1.3.6.1.4.1.9.9.171.1.2.1.20.0 | uint32 | <The total number of IPsec Phase-1 IKE Tunnels which were locally initiated and failed to activate><br>Количество инициированных сессий по созданию ISAKMP SA, завершившиеся неудачей | CISCO-IPSEC-FLOW-MONITOR-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| cikeGlobalRespTunnelFails | 1.3.6.1.4.1.9.9.171.1.2.1.21.0 | uint32 | <The total number of IPsec Phase-1 IKE Tunnels which were remotely initiated and failed to activate><br>Количество сессий по созданию ISAKMP SA, инициированных партнёрами, которые завершились неудачей | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalAuthFails | 1.3.6.1.4.1.9.9.171.1.2.1.23.0 | uint32 | <The total number of authentications which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels><br>Количество неудачных сессий по созданию ISAKMP SA, в которых не прошла аутентификация | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalDecryptFails | 1.3.6.1.4.1.9.9.171.1.2.1.24.0 | uint32 | <The total number of decryptions which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels><br>Общее количество IKE-сессий, не состоявшихся по причине ошибки расшифрования пакета. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalHashValidFails | 1.3.6.1.4.1.9.9.171.1.2.1.25.0 | uint32 | <The total number of hash validations which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels><br>Количество неудачных операций по проверке значения хэш-функции во всех IKE сессиях | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeGlobalNoSaFails | 1.3.6.1.4.1.9.9.171.1.2.1.26.0 | uint32 | <The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-1 IKE Tunnels><br>Общее количество IKE-сессий, не состоявшихся по причине отсутствия ISAKMP соединения. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| **Глобальная IPsec-статистика** | | | | |
| cipSecGlobalActiveTunnels | 1.3.6.1.4.1.9.9.171.1.3.1.1.0 | uint32 | <The total number of currently active IPsec Phase-2 Tunnels><br>Количество существующих на данный момент IPsec соединений. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalPreviousTunnels | 1.3.6.1.4.1.9.9.171.1.3.1.2.0 | uint32 | <The total number of previously active IPsec Phase-2 Tunnels><br>Количество IPsec SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены. | CISCO-IPSEC-FLOW-MONITOR-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| cipSecGlobalInOctets | 1.3.6.1.4.1.9.9.171.1.3.1.3.0 | uint32 | <The total number of octets received by all current and previous IPsec Phase-2 Tunnels.<br>This value is accumulated BEFORE determining whether or not the packet should be decompressed. See also cipSecGlobalInOctWraps for the number of times this counter has wrapped><br>Количество байт, принятых под защитой всех IPsec SA с момента старта Агента | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalInOctWraps | 1.3.6.1.4.1.9.9.171.1.3.1.5.0 | uint32 | <The number of times the global octets received counter (cipSecGlobalInOctets) has wrapped><br>Количество переполнений счетчика cipSecGlobalInOctets. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalInPkts | 1.3.6.1.4.1.9.9.171.1.3.1.9.0 | uint32 | <The total number of packets received by all current and previous IPsec Phase-2 Tunnels><br>Количество пакетов, принятых под защитой всех IPsec SA с момента старта Агента | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalInDrops | 1.3.6.1.4.1.9.9.171.1.3.1.10.0 | uint32 | <The total number of packets dropped during receive processing by all current and previous IPsec Phase-2 Tunnels. This count does NOT include packets dropped due to Anti-Replay processing><br>Общее количество всех входящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения (Кроме проигнорированных по Anti-Replay). | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalInReplayDrops | 1.3.6.1.4.1.9.9.171.1.3.1.11.0 | uint32 | <The total number of packets dropped during receive processing due to Anti-Replay processing by all current and previous IPsec Phase-2 Tunnels><br>Общее количество всех входящих пакетов, отвергнутых локальным устройством посредством механизма Anti-Replay, при задействовании<br>IPsec соединения. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalInAuthFails | 1.3.6.1.4.1.9.9.171.1.3.1.13.0 | uint32 | <The total number of inbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels><br>Общее количество всех неудачных входящих аутентификаций по IPsec соединениям. | CISCO-IPSEC-FLOW-MONITOR-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| cipSecGlobalInDecrypts | 1.3.6.1.4.1.9.9.171.1.3.1.14.0 | uint32 | <The total number of inbound decryption's performed by all current and previous IPsec Phase-2 Tunnels><br>То же самое значение, что и cipSecGlobalInPkts. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalInDecryptFails | 1.3.6.1.4.1.9.9.171.1.3.1.15.0 | uint32 | <The total number of inbound decryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels><br>Общее количество входящих пакетов, которые были неудачно расшифрованы IPsec соединениями. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalOutOctets | 1.3.6.1.4.1.9.9.171.1.3.1.16.0 | uint32 | <The total number of octets sent by all current and pre-vious IPsec Phase-2 Tunnels. This value is accumulated AFTER determining whether or not the packet should be compressed. See also cipSecGlobalOutOctWraps for the number of times this counter has wrapped><br>Количество байт, отосланных под защитой всех IPsec SA с момента старта Агента | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalOutOctWraps | 1.3.6.1.4.1.9.9.171.1.3.1.18.0 | uint32 | <The number of times the global octets sent counter (cipSecGlobalOutOctets) has wrapped><br>Количество переполнений счетчика cipSecGlobalOutOctets. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalOutPkts | 1.3.6.1.4.1.9.9.171.1.3.1.22.0 | uint32 | <The total number of packets sent by all current and previous IPsec Phase-2 Tunnels><br>Количество пакетов, отосланных под защитой всех IPsec SA с момента старта Агента | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalOutDrops | 1.3.6.1.4.1.9.9.171.1.3.1.23.0 | uint32 | <The total number of packets dropped during send processing by all current and previous IPsec Phase-2 Tunnels><br>Общее количество всех исходящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalOutAuthFails | 1.3.6.1.4.1.9.9.171.1.3.1.25.0 | uint32 | <The total number of outbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels><br>Общее количество всех неудачных исходящих аутентификаций по IPsec соединениям. | CISCO-IPSEC-FLOW-MONITOR-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| cipSecGlobalOutEncrypts | 1.3.6.1.4.1.9.9.171.1.3.1.26.0 | uint32 | <The total number of outbound encryption's performed by all current and previous IPsec Phase-2 Tunnels><br>Тоже самое значение, что и cipSecGlobalOutPkts. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalOutEncryptFails | 1.3.6.1.4.1.9.9.171.1.3.1.27.0 | uint32 | <The total number of outbound encryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels><br>Общее количество исходящих пакетов, которые были неудачно зашифрованы IPsec соединениями. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecGlobalNoSaFails | 1.3.6.1.4.1.9.9.171.1.3.1.29.0 | uint32 | <The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-2 Tunnels><br>Общее количество обменов, не состоявшихся по причине отсутствия IPsec соединения. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| **Interfaces-статистика** | | | | |
| ifPhysAddress | 1.3.6.1.2.1.2.2.1.6.<ifIndex> | Octet string | <The interface's address at the protocol layer immediately `below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.><br>MAC-адрес данного интерфейса.<br>Индекс для данного значения берется из ipAdEntIfIndex.<ip> | RFC1213-MIB |
| **IP - статистика** | | | | |
| ipAdEntAddr | 1.3.6.1.2.1.4.20.1.1.<ip> | IpAddress | <The IP address to which this entry's addressing information pertains.><br>Собственно сам <ip> (совпадает с индексом значения) | IP-MIB |
| ipAdEntNetMask | 1.3.6.1.2.1.4.20.1.3.<ip> | IpAddress | <The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.><br>Маска адреса. | IP-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| ipAdEntIfIndex | 1.3.6.1.2.1.4.20.1.2.<ip> | int32 | <The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.><br>Индексом переменной является IP-адрес устройства. Значением – индекс интерфейса (в таблице ifTable), который содержит данный адрес. | IP-MIB |
| **CPU, Memory - статистика** | | | | |
| cpmCPUTotal5sec | 1.3.6.1.4.1.9.9.109.1.1.1.1.3.1 | uint32 (1..100) | <The overall CPU busy percentage in the last 5 second period. This object obsoletes the busyPer object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5secRev which has the changed range of value (0..100).><br>Загрузка процессора за последние 5 секунд. | CISCO-PROCESS-MIB |
| cpmCPUTotal5secRev | 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 | uint32 (0..100) | <The overall CPU busy percentage in the last 5 second period. This object deprecates the object cpmCPUTotal5sec and increases the value range to (0..100). This object is deprecated by cpmCPUTotalMonInterval><br>Загрузка процессора за последние 5 секунд. Отличается от cpmCPUTotal5sec допустимыми пределами. | CISCO-PROCESS-MIB |
| cpmCPUTotal1min | 1.3.6.1.4.1.9.9.109.1.1.1.1.4.1 | uint32 (1..100) | <The overall CPU busy percentage in the last 1 minute period. This object obsoletes the avgBusy1 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal1minRev which has the changed range of value (0..100).><br>Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1minRev допустимыми пределами. | CISCO-PROCESS-MIB |

  

| Название переменной | OID (идентификатор объекта) | Тип переменной | Значение переменной | MIB |
|---|---|---|---|---|
| cpmCPUTotal1minRev | 1.3.6.1.4.1.9.9.109.1.1.1.1.7.1 | uint32 (0..100) | <The overall CPU busy percentage in the last 1 minute period. This object deprecates the object cpmCPUTotal1min and increases the value range to (0..100).><br>Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1min допустимыми пределами. | CISCO-PROCESS-MIB |
| cpmCPUTotal5min | 1.3.6.1.4.1.9.9.109.1.1.1.1.5.1 | uint32 (1..100) | <The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5minRev which has the changed range of value (0..100).><br>Средняя загрузка процессора за последние 5 минут (в процентах). | CISCO-PROCESS-MIB |
| cpmCPUTotal5minRev | 1.3.6.1.4.1.9.9.109.1.1.1.1.8.1 | uint32 (0..100) | <The overall CPU busy percentage in the last 5 minute period. This object deprecates the object cpmCPUTotal5min and increases the value range to (0..100).><br>Загрузка процессора за последние 5 минут. Отличается от cpmCPUTotal5min допустимыми пределами. | CISCO-PROCESS-MIB |
| ciscoMemoryPoolUsed | 1.3.6.1.4.1.9.9.48.1.1.1.5.1 | uint32 | <Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.><br>Рассматривается как таблица из одного элемента (с индексом 1), которая задает общее количество используемой физической памяти. | CISCO-MEMORY-POOL-MIB |
| ciscoMemoryPoolFree | 1.3.6.1.4.1.9.9.48.1.1.1.6.1 | uint32 | <Indicates the number of bytes from the memory pool that are currently unused on the managed device.<br>Note that the sum of ciscoMemoryPoolUsed and ciscoMemoryPoolFree is the total amount of memory in the pool><br>Общее количество свободной физической памяти. | CISCO-MEMORY-POOL-MIB |

  

# 11.2. Трап-сообщения

SNMP- агент посылает трап-сообщения о возникших событиях SNMP – менеджеру.

Для этого в конфигурационном файле администратор задает IP-адрес и порт, на который отсылаются сообщения SNMP-менеджеру, идентификатор и IP-адрес отправителя трап-сообщения, версию SNMP, в которой создаются трап-сообщения.

В приведенной ниже таблице перечислены реализованные трапы и переменные, которые высылаются SNMP-менеджеру, и описание трапа.

Таблица 11

| Название трапа | SNMPv1 Enterprise and Specific Type; SNMPv2 OID | Список переменных | Значение переменной | MIB |
|---|---|---|---|---|
| cikeSysFailure | 1.3.6.1.4.1.9.9.171.2<br>3<br>1.3.6.1.4.1.9.9.171.2.0.3 | cikePeerLocalAddr – адрес local peer<br>cikePeerRemoteAddr – адрес remote peer<br>Оба значения – табличные. | <This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences an internal or system capacity error.><br>Сигнализация о внутренней ошибке или исчерпании ресурсов при обработке IKE. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeCertCrlFailure | 1.3.6.1.4.1.9.9.171.2<br>4<br>1.3.6.1.4.1.9.9.171.2.0.4 | cikePeerLocalAddr<br>cikePeerRemoteAddr | <This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a Certificate or a Certificate Revoke List (CRL) related error.><br>Ошибка, связанная с сертификатами или CRL. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeProtocolFailure | 1.3.6.1.4.1.9.9.171.2<br>5<br>1.3.6.1.4.1.9.9.171.2.0.5 | cikePeerLocalAddr<br>cikePeerRemoteAddr | <This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a protocol related error.><br>Ошибка, связанная с обработкой протокола IKE:<br>Authentication error (в ситуациях, не попадающих под cikeCertCrlFailure)<br>BlackLog | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cikeNoSa | 1.3.6.1.4.1.9.9.171.2<br>6<br>1.3.6.1.4.1.9.9.171.2.0.6 | cikePeerLocalAddr<br>cikePeerRemoteAddr | <This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a non-existent security association error.><br>Приход IKE-пакетов на несуществующий SA (Invalid cookie). | CISCO-IPSEC-FLOW-MONITOR-MIB |

  

| Название трапа | SNMPv1 Enterprise and Specific Type; SNMPv2 OID | Список переменных | Значение переменной | MIB |
|---|---|---|---|---|
| cipSecSetUpFailure | 1.3.6.1.4.1.9.9.171.2<br>10<br>1.3.6.1.4.1.9.9.171.2.0.10 | cikePeerLocalAddr<br>cikePeerRemoteAddr | <This notification is generated when the setup for an IPsec Phase-2 Tunnel fails.><br>По тем или иным причинам не удалось создать IPsec SA (при существующем IKE SA).<br>Примечание: этот трап отсылается только при появлении ошибки во время проведения IKE-сессии и тем партнером, на котором случилась ошибка. Если создание соединения прекращено по другим причинам – остановка сервиса, перезагрузка LSP, delete payload, получение нотификации о том, что партнер по своей инициативе прекратил создание соединения, timeout и др., то локальное устройство трап не отсылает. В этом состоит отличие нашего агента от IOS, где трапы отсылаются с обоих партнеров при любой неуспешной сессии по созданию IPsec соединения. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecTunnelStart | 1.3.6.1.4.1.9.9.171.7<br>7<br>1.3.6.1.4.1.9.9.171.2.0.7 | cipSecTunLifeTime<br>cipSecTunLifeSize<br>Табличные значения. | <This notification is generated when an IPsec Phase-2 Tunnel becomes active.><br>Успешное создание туннеля. | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipSecTunnelStop | 1.3.6.1.4.1.9.9.171.8<br>8<br>1.3.6.1.4.1.9.9.171.2.0.8 | cipSecTunActiveTime<br>Табличное значение | <This notification is generated when an IPsec Phase-2 Tunnel becomes inactive.><br>Уничтожение созданного туннеля (по разным причинам). | CISCO-IPSEC-FLOW-MONITOR-MIB |
| cipsTooManySAs | 1.3.6.1.4.1.9.10.62.2<br>7<br>1.3.6.1.4.1.9.10.62.2.0.7 | cipsMaxSAs – максимальное количество IPsec SAs. Если не существует предела – 0. | <This trap is generated when a new SA is attempted to be setup while the number of currently active SAs equals the maximum configurable. The variables are: cipsMaxSAs><br>Отказ от создания SA по причине достигнутого максимального количества SA, указанного в лицензии. В переменной прописывается максимальное количество SA из лицензии. | CISCO-IPSEC-MIB |

  

| Название трапа | SNMPv1 Enterprise and Specific Type; SNMPv2 OID | Список переменных | Значение переменной | MIB |
|---|---|---|---|---|
| ciscoConfigManEvent | 1.3.6.1.4.1.9.9.43.2<br><br>1<br><br>1.3.6.1.4.1.9.9.43.2.0.1 | ccmHistoryEventCommandSource = { commandLine(1), snmp(2) }<br>ccmHistoryEventConfigSource = { erase(1), commandSource(2), running(3), startup(4), local(5), networkTftp(6), networkRcp(7) }<br><br>ccmHistoryEventConfigDestination = { erase(1), commandSource(2), running(3), startup(4), local(5), networkTftp(6), networkRcp(7) }<br><br>Табличные значения. Индекс – целое число, начинающееся с единицы. Инкрементируется при каждой посылке трапа данного типа. | <Notification of a configuration management event as recorded in ccmHistoryEventTable.><br>Всегда ccmHistoryEventCommandSource=1<br>Несколько вариантов:<br>1 При вызове lsp_mgr show или cs_console show run:<br>ccmHistoryEventConfigSource=2<br>ccmHistoryEventConfigDestination=2<br>Примечание: аналогично реакции Cisco на команду show run<br><br>2 При успешной прогрузке LSP:<br>ccmHistoryEventConfigSource=2<br>ccmHistoryEventConfigDestination=3<br>Примечание: аналогично реакции Cisco на команду configure terminal.<br>Для стартовой загрузки LSP надо задать ccmHistoryEventConfigSource = 4<br><br>3 При отгрузке LSP (по разным причинам):<br>ccmHistoryEventConfigSource=1<br>ccmHistoryEventConfigDestination=3 | CISCO-CONFIG-MAN-MIB |

  

# 12. Приложение

## 12.1. Создание локального сертификата при использовании "AvCrypt ver. 5.1" (РБ.ЮСКИ.09000-02)

При использовании "AvCrypt ver. 5.1"(РБ.ЮСКИ.09000-02), создание локального сертификата можно осуществить с использованием утилиты `cryptocont`, созданной компанией “АВЕСТ”, и которая входит как в состав дистрибутива Bel VPN Client AdminTool, так и в состав каждого инсталляционного пакета, подготовленного администратором безопасности. Утилита используются для создания ключевой пары, запроса на локальный сертификат, создания контейнера и др.

Создание ключевой пары и формирование запроса на локальный сертификат выполняются с помощью утилиты cryptocont.exe. Все действия необходимо производить в режиме командной строки из каталога, где находится утилита.

**Шаг1:** Создайте контейнер, содержащий личный ключ, используя утилиту `cryptocont.exe`.

Выполните команду:

```
cryptocont n –n=<Container> [-p=<Password>]
[-y=<SysRandomSource>] [-r=<RandomFile>]
[-key_alg=<KeyAlgOid>] [–u]
```

где

`Container` – имя контейнера

`Password` – пароль к контейнеру, может отсутствовать, в этом случае пользователю предлагается дважды ввести пароль с клавиатуры

`SysRandomSource` – системный источник энтропии используемой при генерации случайности. Для Windows параметр указывает код типа используемого криптопровайдера (для криптопровайдера компании «АВЕСТ» указывается код «420» или «421», для криптопровайдеров других производителей – код «1»), для linux и solaris параметр игнорируется.

`RandomFile` – имя файла, используемого при генерации случайности. Файл должен быть не пуст, содержимое файла свыше 64 килобайт игнорируется.

`KeyAlgOid` – OID алгоритма ключа ЭЦП. Возможные значения (без кавычек): `"1.3.6.1.4.1.12656.1.38"` или `"bds"` - ЭЦП согласно СТБ 1176.2-99

`"1.3.6.1.4.1.12656.1.35"` или `"bdspro"` - ЭЦП согласно СТБ 1176.2-99 с предварительным хэшированием

Значение по умолчанию – `"bds"`

`-u` – неинтерактивный режим генерации случайности.

**Шаг2:** Создайте запрос на сертификат, содержащий открытый ключ ЭЦП СТБ 1176.2-99 и экспортируйте запрос в файл используя утилиту `cryptocont`. Открытый ключ вычисляется на основе личного ключа, хранящегося в указанном контейнере.

Выполните команду:

```
cryptocont r {-f=<RequestFileName> -s=<SubjectName> -
c=<Country> [-k=<KeyUsage>] –n=<ContainerName> [-
p=<Password>]} {-i=IniFile}
```

где

  

`ContainerName` – имя контейнера, содержащего личный ключ ЭЦП СТБ 1176.2-99.

`Password` – пароль к контейнеру, может отсутствовать, в этом случае пароль вводится с клавиатуры.

`RequestFileName` – имя создаваемого файла запроса.

`SubjectName` - имя абонента.

`Country` – идентификатор страны абонента, например BY.

`KeyUsage` – область применения ключа согласно X.509, этот параметр рекомендуется не использовать – будет применено значение по умолчанию – “100000000” (ЭЦП).

Если указан параметр `-i`, данные берутся из .ini-файла `IniFile`, раздел request, поля filename, subject, keyusage, country, а также раздел container, поля name, pin.

пример `ini` файла:

```
[container]
name=cont1
pin=12345678

[request]
filename=req.req
subject=test subject
country=BY
keyusage=100010000
```

**Шаг3:** Отправьте созданный запрос доступным вам способом на сервер доверенного Удостоверяющего Центра, где по данному запросу будет создан локальный сертификат.

В качестве УЦ может использоваться программа «Центр цифровых сертификатов Авест».

**Шаг4:** Получите из Удостоверяющего Центра локальный сертификат, цепочку сертификатов издателя и списки отозванных сертификатов в виде файлов.

  