

Программный продукт
«Клиент безопасности Bel VPN Client-P 4.1»
Руководство администратора
Общее руководство
BY.PTHK.41002-01 34 01-01
Листов 97

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

Содержание

1	Состав программного продукта	4
2	Назначение и функции Продукта	5
3	Требования на базовые платформы и совместимость	7
4	Процесс подготовки персонализированного инсталляционного пакета пользователя	8
5	Подготовка рабочего места администратора безопасности	9
5.1	Инсталляция административного пакета	9
6	Атрибуты аутентификации	13
6.1	Критичные расширения сертификата	13
7	Графический интерфейс	15
7.1	Подготовка инсталляционного пакета с помощью графического интерфейса (GUI)	15
7.2	Режимы графического интерфейса	15
7.3	Описание	16
7.4	Основной режим и режим совместимости с Bel VPN 3.0.1	18
7.5	Режим совместимости с Bel VPN 3.0.1	68
7.6	Формат задания имен алгоритмов в файле admintool.ini	68
8	Интерфейс командной строки	70
8.1	Подготовка инсталляционного пакета с помощью интерфейса командной строки	70
8.2	Режимы	70
8.3	Описание утилиты make_inst	70
8.4	Сообщения об ошибках утилиты make_inst	79
8.5	Создание нескольких инсталляционных пакетов одновременно	83
9	Подготовка к инсталляции персонализированного пакета ПП Bel VPN Client-P	87
10	Сообщения об ошибках при инсталляции административного пакета ПП Bel VPN Client-P	88
11	Настройка нескольких сетевых интерфейсов	Ошибка! Закладка не определена.
12	Работа Bel VPN Client-P с продуктами третьих производителей	89
12.1	Работа с Брандмауэром Windows (ОС Windows 7)	89
12.2	Работа с антивирусом Outpost	91
13	Создание локальной политики безопасности. Конфигурационный файл	92
14	Протоколирование событий безопасности	93
14.1	Настройка Syslog-клиента	93

14.2	Получение журнала сообщений в ОС Windows	93
14.3	Утилиты log_mgr show и log_mgr set	93
14.4	Специальные лог-файлы	94
14.5	Журналы Windows	95
15	Мониторинг	96
15.1	Выдача статистики	96

1 Состав программного продукта

В состав программного продукта «Клиент безопасности Bel VPN Client-P 4.1» входят:

- Комплект исполняемых файлов и документации на машиночитаемом носителе (компакт-диске) «S-Terra Bel. Bel VPN Client-P 4.1»:
- Дистрибутив программного обеспечения программного продукта «Клиент безопасности Bel VPN Client-P 4.1» (BY.ПТНК.41020-01);
- Документация по эксплуатации программного продукта «Клиент безопасности программный Bel VPN Client-P 4.1»:
 - «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1». Руководство администратора» (BY.ПТНК.41002-01 34 01);
 - «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1». Руководство пользователя» (BY.ПТНК.41002-01 34 02);
 - «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1». Подготовительные процедуры» (BY.ПТНК.41002-01 34 03);
- Дистрибутив программного комплекса «Bel VPN КР 4.1» (BY.ПТНК.41005-01);
- Документация по эксплуатации программного комплекса «Bel VPN КР 4.1»:
 - Документ «Программный комплекс «Bel VPN КР 4.1». Руководство администратора» (BY.ПТНК.41005-01 34 01);
 - Документ «Программный комплекс «Bel VPN КР 4.1». Руководство пользователя» (BY.ПТНК.41005-01 34 02).
- Комплект документов в печатном виде:
 - Формуляр на программный программный продукт «Клиент безопасности Bel VPN Client-P 4.1»;
 - Лист лицензии на использование «Программного продукта «Клиент безопасности Bel VPN Client-P 4.1»
либо
 - Лист лицензии на использование «Программного продукта «Клиент безопасности Bel VPN Client-P 4.1». Client-B.

2 Назначение и функции

Программный продукт «Клиент безопасности Bel VPN Client-P 4.1» функционирует на аппаратных платформах в архитектуре Intel x86/x86-64 под управлением операционных систем Microsoft Windows.

Программный продукт «Клиент безопасности Bel VPN Client-P 4.1» (далее ПП Bel VPN Client-P) выполняет роль персонального VPN клиента и персонального межсетевого экрана.

ПП Bel VPN Client-P может устанавливаться на:

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

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

ПП Bel VPN Client-P обеспечивает:

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

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

- Security Architecture for the Internet Protocol – RFC2401.
- IP Authentication Header (AH) – RFC2402.
- IP Encapsulating Security Payload (ESP) – RFC2406.
- Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408.
- The Internet Key Exchange (IKE) – RFC2409.
- The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407.

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

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

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

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

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

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

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

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

3 Требования на базовые платформы и совместимость

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

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

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

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

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

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

4 Процесс подготовки персонализированного инсталляционного пакета пользователя

ВНИМАНИЕ !

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

Администратор безопасности ПП Bel VPN Client-P создает для каждого Пользователя ПП Bel VPN Client-P персонализированный инсталляционный пакет, содержащий локальную политику безопасности, которая описывает правила защиты и пакетной фильтрации трафика.

Подготовка персонализированного пакета Клиента безопасности может производиться двумя способами:

1. С помощью административного пакета Bel VPN Client 4.1 Admin Tool – см. раздел 5 данного документа;
2. С помощью программного комплекса «Bel VPN KP 4.1» –см. документ «Программный комплекс «Bel VPN KP 4.1». Руководство администратора»(BY.ПТНК.41005-01 34 01).

5 Подготовка рабочего места администратора безопасности

Администратор безопасности получает административный пакет в виде отдельного Продукта Bel VPN Client AdminTool, размещенного в каталоге Soft поставляемого диска.

Процесс установки административного пакета описан в разделе “Инсталляция административного пакета”.

Процесс подготовки персонализированного инсталляционного пакета описан в разделе “Подготовка инсталляционного пакета с помощью графического интерфейса”.

5.1 Инсталляция административного пакета

В состав дистрибутива административного пакета ПП Bel VPN Client-P входит:

- hashes – файл с эталонными значениями хэш-сумм для каждого файла дистрибутива;
- setup.exe – утилита запуска Windows Installer;
- setup.ini – настроечный файл, необходимый для setup.exe;
- sysdlls.cab – хранилище системных DLL, необходимых для клиента;
- version.txt – текстовый файл, содержащий версию Продукта;
- VPN_CLIENT_ADMIN.msi – MSI-база инсталлятора (MSI – MicroSoft Installer);
- VPN_CLIENT_ADMIN.cab – хранилище файлов клиента.

Администратор должен установить административный пакет на своем компьютере.

Запуск инсталляции производится командой setup.exe из административного пакета, появляется окно визарда с приглашением к инсталляции:



Рисунок 1

В окне с Лицензионным Соглашением установите переключатель в положение **I accept the license agreement**, кнопка **Next** становится доступной:

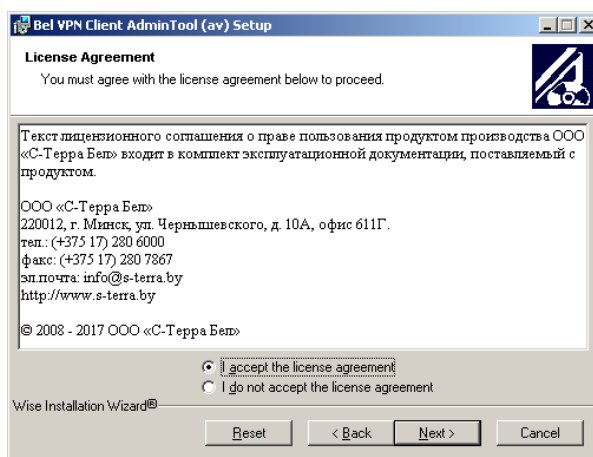


Рисунок 2

Выберите папку, в которую будет установлен административный пакет, нажав на клавишу **Browse**:

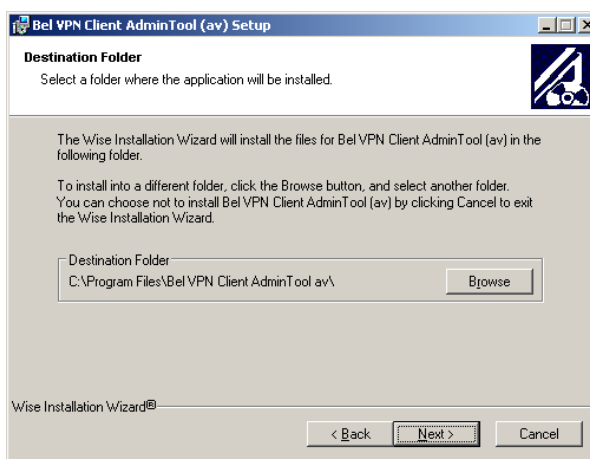


Рисунок 3

Выберите способ инициализации ДСЧ. В случае выбора инициализации с использованием внешнего ключевого носителя введите пин-код от используемого ключевого носителя. Нажмите клавишу **Next**:

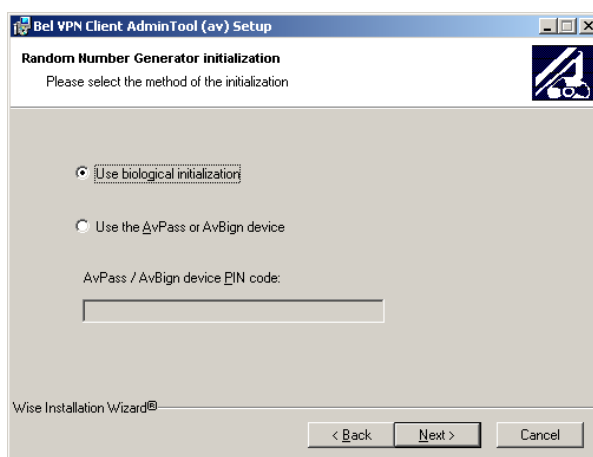


Рисунок 4

Для начала процесса инсталляции нажмите клавишу **Next**:

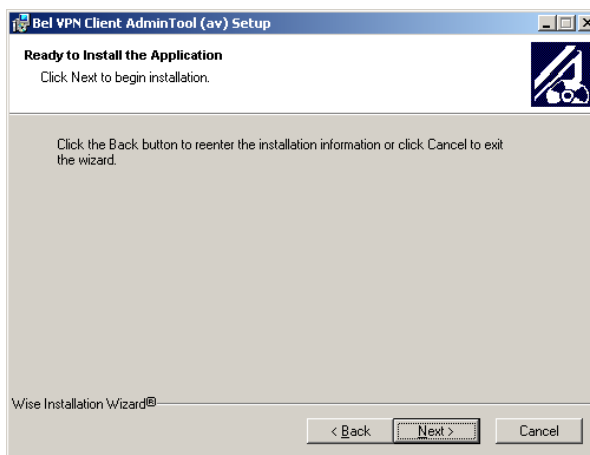


Рисунок 5

Индикатор процесса инсталляции:

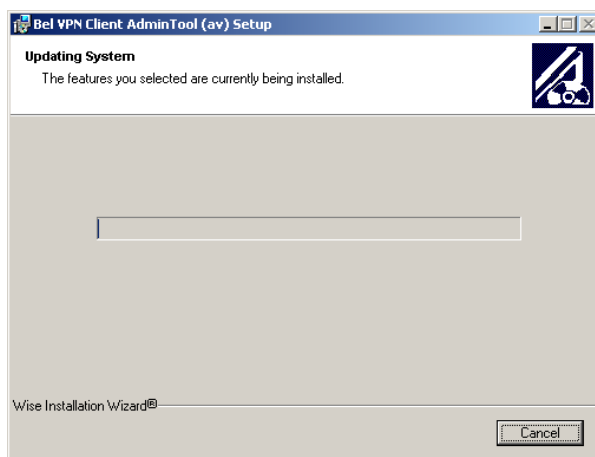


Рисунок 6

В случае, если был выбран биологический тип инициализации ДСЧ, в процессе установки появится окно, представленное на Рисунке 7. Требуется нажимать случайные клавиши до той поры, пока окно не исчезнет.

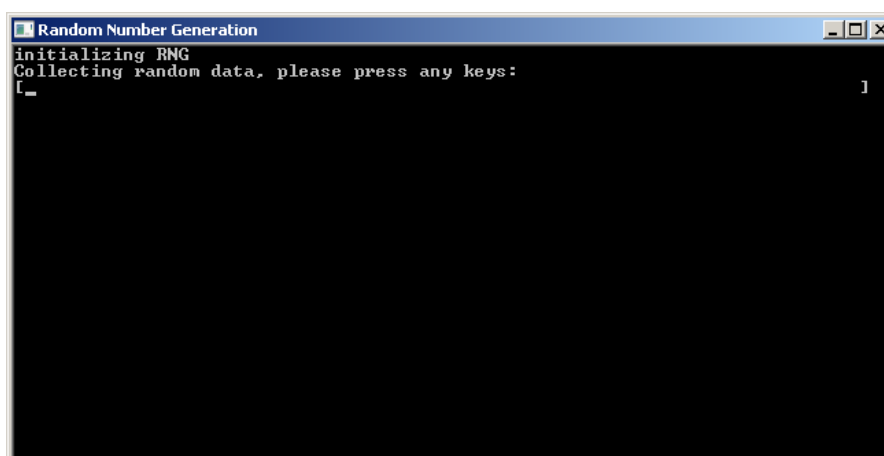


Рисунок 7

Инсталляция завершена, нажмите кнопку **Finish**:

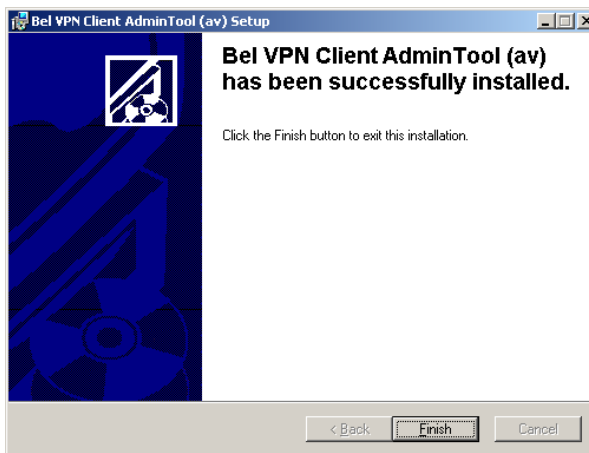


Рисунок 8

При появлении ошибок во время инсталляции административного пакета обращайтесь к разделу «Сообщения об ошибках при инсталляции».

Установленный административный пакет состоит из следующих папок и файлов:

Корневая папка:

- `pkg_maker.exe` – утилита графического интерфейса для создания локальной политики, локальных настроек и инсталляционного файла пользователя;
- `make_inst.exe` – утилита командной строки для создания инсталляционного файла пользователя;
- `integr_mgr.exe` – утилита командной строки для проверки целостности информационной части Продукта;
- `cryptocont.exe` – утилита командной строки для работы с контейнерами ЗАО «Авест»;
- `version.txt` – текстовый файл с версией Продукта;
- `pkg_maker.chm` – файл, содержащий Help;
- вспомогательные файлы (dll, ini) для обеспечения работы утилит.
 - папка Agent содержит основные файлы инсталлятора персонализированного пакета ПП Bel VPN Client-P;
 - папка SFX содержит служебные файлы, необходимые для сборки самораспаковывающегося архива.

6 Атрибуты аутентификации

Для аутентификации взаимодействующих сторон протоколу IKE также необходима некоторая аутентификационная информация. Такой аутентификационной информацией может быть:

- предопределенный (разделяемый) ключ (Preshared Key),
- сертификат открытого ключа стандарта X.509.

Предопределенный ключ – произвольная последовательность байтов, которая может быть записана в файл.

Сертификат открытого ключа – электронный документ, удостоверяющий принадлежность открытого ключа данному устройству/пользователю. Выпускается удостоверяющим центром по запросу на выпуск сертификата.

6.1 Критичные расширения сертификата

Имеются некоторые ограничения при работе с расширениями сертификата (Extensions), которые помечены как критичные. В таблице 1 приведен список расширений сертификата, которые будут распознаваться и обрабатываться Продуктом, если у них установлен признак критичности TRUE. Если в сертификате присутствуют другие расширения, имеющие признак критичности TRUE и не указанные в таблице, такой сертификат не используется. Если же расширение отсутствует в таблице, но является некритичным, то оно игнорируется, а сертификат используется для аутентификации.

Таблица 1

Name	OID value
Subject Key Identifier	2.5.29.14
Key Usage	2.5.29.15
Subject Alternative Name	2.5.29.17
Issuer Alternative Name	2.5.29.18
Basic Constraints	2.5.29.19
Name Constraints	2.5.29.30
CRL Distribution Points	2.5.29.31
Authority Key Identifier	2.5.29.35

Описания значений и полный список Certificate Extensions можно посмотреть в документе RFC 5280 (<http://tools.ietf.org/html/rfc5280#section-4.2>).

Можно изменить реакцию Продукта на отдельные расширения сертификата, помеченные как критичные и отсутствующие в вышеприведенной таблице. Администратор может настроить список расширений сертификата, который будут игнорироваться Продуктом, как если бы эти расширения являлись некритичными. Эти расширения надо описать в файле x509opts.ini, который расположен в корневой папке установленного административного пакета. Расширения описываются в секции IgnoringUnsupportedCriticalExtensions.

Игнорируемое Critical Extension задается в формате **<KEY>=<OID>**, где:

<KEY> – имя расширения, состоящее из букв и цифр и не содержащее разделителей, должно быть уникальным в пределах секции;

<OID> – OID игнорируемого расширения, состоящий из десятичных чисел, разделенных точками. Распознавание расширения происходит по OID.

Пример файла x509opts.ini:

```
[IgnoringUnsupportedCriticalExtensions]
!!
```

```
! Key name is any Alpha-Numerical well-known name of OID
! Key names of different OIDs cannot match
!!
subjectDirectoryAttributes=2.5.29.9
CertificatePolicies=2.5.29.32
QcStatements=1.3.6.1.5.5.7.1.3
HcRole=1.0.21091.2.0.5
```

Примечание 1: следует подчеркнуть, что таким образом нельзя проигнорировать распознаваемые Продуктом Critical Extensions, например BasicConstraints.

Примечание 2: секция IgnoringUnsupportedCriticalExtensions, даже пустая, обязательно должна присутствовать в файле x509opts.ini.

7 Графический интерфейс

7.1 Подготовка инсталляционного пакета с помощью графического интерфейса (GUI)

Утилита **pkg_maker.exe** предоставляет администратору безопасности графический интерфейс (GUI) административного пакета ПП Bel VPN Client-P для создания персонализированного пакета пользователя, включающего локальную политику безопасности и настройки для конкретного пользователя.

При использовании **предопределенного ключа** для аутентификации сторон GUI предоставляет возможность считать созданный ключ либо из файла, либо ввести его с клавиатуры, задать локальную политику безопасности для данного пользователя, персональные настройки и создать персонализированный пакет (инсталляционный файл) Bel VPN Client-P, который и будет передан пользователю. Далее перейдите в раздел [«Аутентификация с использованием Preshared Key»](#).

При использовании **сертификатов открытого ключа** для аутентификации сторон подготовка инсталляционного пакета производится следующим образом:

- Шаг 1:** На компьютере администратора на пользовательском ключевом носителе создается ключевая пара и запрос на сертификат пользователя, который отсылается в Удостоверяющий Центр. Контейнер с секретным ключом размещается на ключевом носителе пользователя. Администратор безопасности получает сертификат Удостоверяющего Центра (Trusted CA Certificate, CA-сертификат) и сертификат пользователя.
- Шаг 2:** Администратор безопасности на своем рабочем месте с помощью GUI задает локальную политику безопасности для данного пользователя, путь к локальному и CA-сертификату, имя контейнера с секретным ключом – где он будет размещен на компьютере пользователя, локальные настройки, создает инсталляционный файл Bel VPN Client-P.
- Шаг 3:** Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из:
- Персонализированного пакета Bel VPN Client-P,
 - контейнера с секретным ключом на внешнем ключевом носителе.

Контейнер должен быть передан пользователю по заслуживающему доверия каналу связи. Персонализированный пакет Bel VPN Client-P содержит базовый инсталляционный файл, локальную политику безопасности, сертификат пользователя и CA-сертификат, персональные настройки.

7.2 Режимы графического интерфейса

Графический интерфейс административного пакета предусматривает три режима работы:

- основной режим (см. раздел ["Графический интерфейс. Основной режим"](#));
- режим совместимости с Bel VPN 3.0.1 (см. раздел ["Графический интерфейс. Режим совместимости с Bel VPN 3.0.1"](#));
- режим международных криптоалгоритмов.

В **основном режиме** при создании инсталляционного пакета Bel VPN Client-P используется следующий набор криптоалгоритмов:

- хэширование – СТБ 34.101.31-2011;
- электронная цифровая подпись – СТБ 34.101.45-2013;
- шифрование и контроль целостности – СТБ 34.101.31-2011;
- генерация случайных данных – СТБ 34.101.47-2012;
- управление ключами – СТБ 34.101.66-2014 (приложение А), управление криптографическими ключами, рекомендованное ОАЦ.

В **режиме совместимости с Bel VPN 3.0.1** при создании инсталляционного пакета Bel VPN Client-P используется следующий набор криптоалгоритмов:

- хэширование – СТБ 1176.1-99;
- электронная цифровая подпись – СТБ 1176.2-99;
- шифрование и контроль целостности – ГОСТ 28147-89;
- генерация случайных данных – СТБ 34.101.47-2012;
- управление ключами – управление криптографическими ключами, рекомендованное ОАЦ.

В **режиме международных криптоалгоритмов** при создании инсталляционного пакета Bel VPN Client-P используется следующий набор криптоалгоритмов:

- хэширование – SHA-1;
- электронная цифровая подпись – RSA, DSA;
- шифрование и контроль целостности – AES-256, SHA-1-HMAC;
- управление ключами – IKE (RFC2409).

7.3 Описание

При запуске утилиты **pkg_maker.exe** (Пуск → Программы → Bel VPN Client AdminTool av → Package Maker) открывается окно главной формы GUI (Рисунок 9).

Главная форма представляет собой диалоговое окно с вкладками.

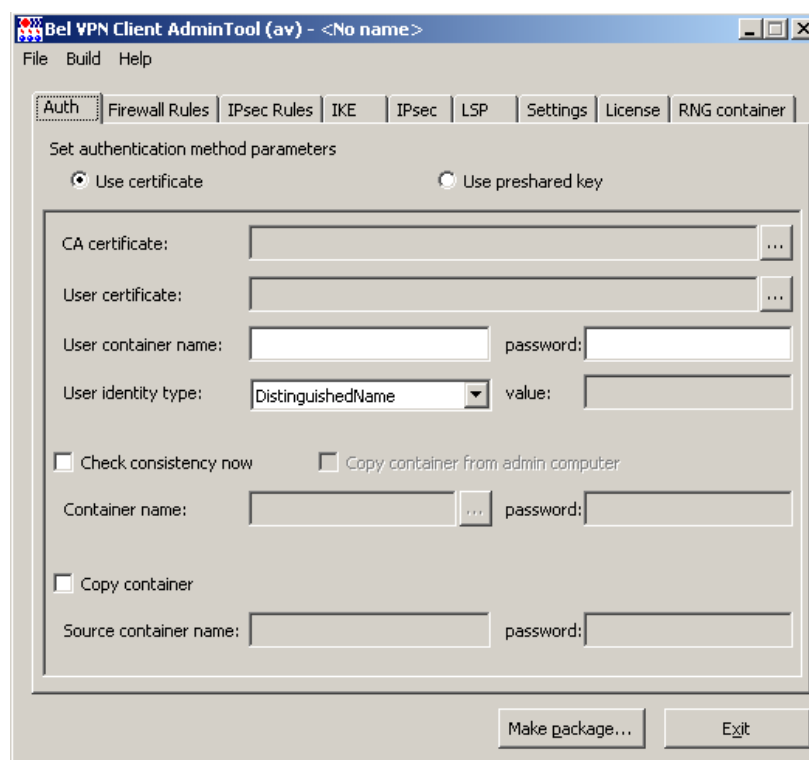


Рисунок 9

Режимы работы главной формы

Режим	Пункт меню
основной режим	Build → Recommended for 4.1 algorithms
режим совместимости с Bel VPN 3.0.1	Build → 3.0.1 compatible algorithms
режим международных криптоалгоритмов	Build → International algorithms

Вкладки главной формы

Наименование вкладки	Назначение
Auth	задание способа аутентификации сторон.
Firewall Rules	задание правил маркирования и фильтрации трафика.
IPsec Rules	задание правил защиты трафика
IKE	задание параметров IKE соединений
IPsec	задание параметров IPsec соединений
LSP	просмотр, редактирование локальной политики безопасности (LSP) и задание дополнительных настроек
Settings	задание локальных настроек и политики по умолчанию
License	задание параметров Лицензии на продукт
RNG container	задание способа инициализации датчика случайных чисел (ДСЧ)

Разделы основного меню главной формы

Наименование раздела / кнопки	Назначение
File	
New Project	открывает новый проект. Проект – это файл в текстовом формате с расширением dsc, в котором будет записана LSP с параметрами, заданными во вкладках, и локальными настройками
Open Project...	открывает существующий (ранее созданный) проект Для работы с проектом, созданным с помощью предыдущей версии AdminTool, воспользуйтесь пунктом меню Import Old Project
Import Old Project	открывает существующий (ранее созданный) проект, созданный с помощью AdminTool предыдущей версии. Во время чтения проекта, созданного с помощью версии 3.0.1, зачитываются партнерские сертификаты, сохраненные отдельно от проекта. Если по какой-либо причине не удастся прочитать какой-то из них, то выдается предупреждение: «Can't read some of partner certificates: <перечисление сертификатов и ошибок> Do you wish to continue?». При отрицательном ответе загрузка прерывается, при положительном – загрузка продолжается, и в списке партнерских сертификатов отображаются только те, которые удалось прочитать
Save Project	сохраняет текущее состояние проекта. При попытке сохранения изменений в проекте, созданном в предыдущих версиях AdminTool, будет выдано предупреждение: «Project file will be saved in new format thus backward compatibility with older versions of tool may be broken. Do you wish to continue?» При отрицательном ответе процесс сохранения изменений будет прерван
Save Project As...	сохраняет текущее состояние проекта в указанный файл
Advanced Project Settings	вызывает окно для задания дополнительных настроек проекта. В данной версии можно указать сертификаты партнеров, CRL при методе аутентификации сторон с использованием сертификатов
Exit	выход из GUI
Build	
Make package...	запускает процесс создания инсталляционного файла Продукта Bel VPN Client-P (аналогично кнопке Make package...)
International algorithms	переключает главную форму в режим международных алгоритмов
3.0.1 compatible algorithms	переключает главную форму в режим совместимости с Bel VPN 3.0.1.
Recommended for 4.1 algorithms	переключает главную форму в основной режим
Help	
Contents	вызывает окно Help-системы с активной вкладкой Содержание.

Наименование раздела / кнопки	Назначение
Index	вызывает окно Help-системы с активной вкладкой Указатель.
About...	открывает окно с названием Продукта, версии, номера сборки, копирайта и логотипом компании.

Функциональные кнопки главной формы

Наименование кнопки	Назначение
Make package	кнопка для запуска процесса создания инсталляционного файла Продукта Bel VPN Client-P.
Exit	выход из GUI.

Формат заполняемых полей

Все поля графического интерфейса, в которые вводится имя папки и файла, могут содержать парные кавычки, пробелы в начале и в конце строки. Все эти символы игнорируются.

Для всех других полей любой введенный символ является значимым.

7.4 Основной режим и режим совместимости с Bel VPN 3.0.1

7.4.1 Вкладка Authentication

Вкладка **Auth** предназначена для задания метода аутентификации и ввода идентификационных данных пользователя. Поддерживаются два метода аутентификации: с использованием сертификата стандарта X.509 или [предопределенного ключа](#).

7.4.1.1 Аутентификация с использованием сертификатов. Задание корневого и локального сертификатов

При аутентификации сторон с использованием сертификатов поставьте переключатель в положение **Use certificate**:

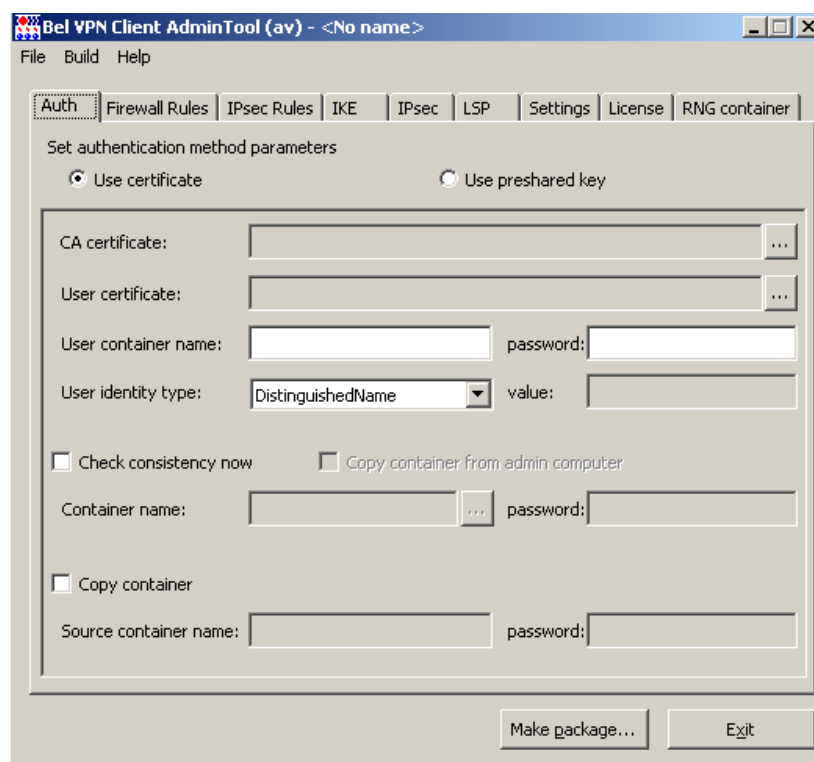


Рисунок 10

При этом становятся доступными для заполнения следующие поля (кнопка с тремя точками в конце поля [...] (Open) означает, что элемент этого поля должен быть доступен (размещен) на компьютере администратора):

- **CA certificate** – здесь отражается поле Subject корневого сертификата Удостоверяющего Центра (Trusted CA Certificate). Для этого разместите на компьютере администратора файл с Trusted CA сертификатом и в конце поля нажмите кнопку [...], в открывшемся окне выберите данный файл с CA сертификатом. Обязательный параметр.
- **User certificate** – здесь отражается поле Subject локального сертификата пользователя. Для этого разместите на компьютере администратора файл с сертификатом пользователя и в конце поля нажмите кнопку [...], в открывшемся окне выберите данный файл с сертификатом. Обязательный параметр.
- **User container name** – уникальное имя контейнера, размещенного на компьютере пользователя, на который будет установлен Продукт Bel VPN Client-P или на ключевом носителе. Контейнер содержит ключевую пару. Обязательный параметр. Имя контейнера должно быть указано в следующем формате:
- **Если носитель ключевой информации не применяется:** имя контейнера
- **Если носитель ключевой информации применяется:**

av:СерийныйНомерНосителя:имя контейнера

Префикс av:СерийныйНомерНосителя: означает, что будет использоваться ключевой контейнер, размещенный на внешнем носителе ключевой информации (AvPass или AvBign, с указанным серийным номером), подключенном по интерфейсу PKCS#11; отсутствие префикса означает что контейнер будет создан на локальной файловой системе (формат контейнера PKCS#15)

- **User container password** – пароль к контейнеру. При использовании AvPass или AvBign в этом поле нужно указать PIN-код к токenu.
- **User identity type** – тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Обязательный параметр. Поле содержит выпадающий список со следующими значениями:
 - **Distinguished Name** – в качестве идентификатора партнеру будет высылаться значение *Subject* из сертификата пользователя, показываемое в поле **User identity value**, если оно там задано. Значение по умолчанию.
 - **Email** – в качестве идентификатора партнеру будет высылаться значение поля *E-mail* расширения сертификата пользователя, показываемое в поле **User identity value**, если оно там задано.
 - **FQDN** – в качестве идентификатора партнеру будет высылаться значение доменного имени хоста, считываемое из поля *DNS* расширения сертификата и показываемое в поле **User identity value**, если оно там задано.
 - **IPV4Addr** – в качестве идентификатора партнеру будет высылаться первый IP-адрес, указанный в расширении сертификата, и показываемый в поле **User identity value**, если он там задан.
 - **Local IP address** – в качестве идентификатора партнеру будет высылаться действительный IP-адрес хоста, на котором будет установлен Bel VPN Client-P.
- **User identity value** – идентификационная информация, пересылаемая партнеру. Поле доступно только для чтения и заполняется автоматически, соответствующим типу идентификатора значением, считываемым из сертификата пользователя. Заполнение происходит в момент выбора типа идентификатора или изменения имени файла с сертификатом пользователя. Параметр обязательный.
- **Check consistency now** – установка этого флажка означает, что при создании инсталляционного файла будет проведена проверка соответствия сертификата пользователя и секретного ключа в контейнере. Для этого внешний носитель с контейнером надо подключить к компьютеру администратора. Имя контейнера указывается в поле **Container name**, а пароль к нему – в поле **Container password**. После установки флажка становятся доступными: **Container name**, **Container password**, **Use container from admin computer**.

- **Copy container from admin computer** – установка этого флажка означает, что контейнер с компьютера администратора будет размещен в инсталляционный файл. При инсталляции Bel VPN Client-P контейнер будет скопирован в контейнер с именем **User container name**. Рекомендуется не устанавливать этот флажок, если канал доставки инсталляционного файла не защищен. Использование контейнера с машины администратора и копирование/импорт контейнера это взаимоисключающие операции, поэтому в окне при выборе одной опции другая отключается автоматически. Переключатели **Copy container** и **Import container from file** будут недоступны.
- **Container name** – уникальное имя контейнера для проведения проверки на компьютере администратора. При нажатии кнопки [...] появится окно **Container list (Ошибка! Источник ссылки не найден.**¹⁾ со списком контейнеров на всех ключевых носителях, подключенных к компьютеру администратора и доступных для всех пользователей. Выберите нужный контейнер для проверки и нажмите **OK**. В поле **Container name** появится уникальное имя контейнера.

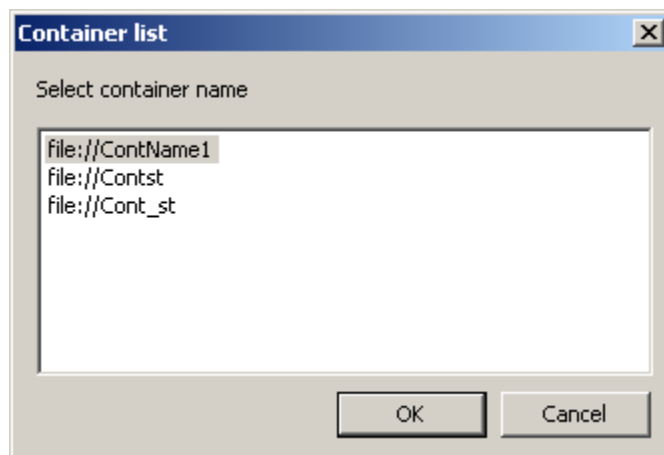


Рисунок 11

- **Container password** – пароль к контейнеру с секретным ключом.
- **Copy container** – установка этого переключателя означает, что во время инсталляции Bel VPN Client-P на компьютере пользователя будет проведено копирование контейнера с именем, указанным в поле **Source container name**, в контейнер с именем, указанным в поле **User container name**.
- **Source container name/file** – имя контейнера на компьютере пользователя, который будет скопирован во время инсталляции, либо полный путь к файлу из которого во время инсталляции будет импортирован контейнер пользователя.
- **Source container password** – пароль (ПИН) к контейнеру с секретным ключом.

7.4.1.2 Аутентификация с использованием Preshared Key

При аутентификации сторон с использованием предопределенного ключа поставьте переключатель в положение **Use preshared key**:

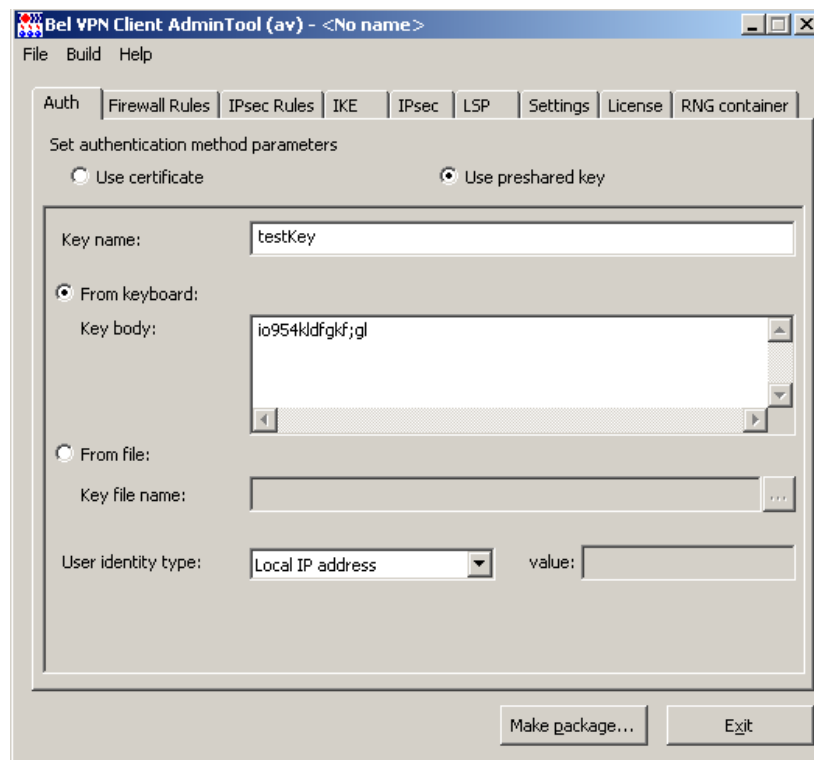


Рисунок 12

Следующие поля доступны для заполнения:

- **Key name** – имя предопределенного ключа. Может состоять из латинских букв, цифр, символов "_" и "-", и должен начинаться с латинской буквы или символа "_". Обязательный параметр.

Для ввода предопределенного ключа имеется переключатель с двумя положениями:

- **From keyboard** – предопределенный ключ нужно ввести с клавиатуры.

Примечание: Если предопределенный ключ задан несколькими строками, то каждый перенос в теле ключа будет представлен двумя символами 0x0D 0x0A (символ возврата и перевода каретки) и тогда при подготовке предопределенного ключа для партнера должны быть использованы эти символы.

- **From file** – предопределенный ключ считывается из файла с именем, указанным в поле **Key file name**.
- **User identity type** – тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Обязательный параметр. Поле содержит выпадающий список со следующими значениями:
 - **IPV4Addr** – в качестве идентификатора партнеру будет высылаться IP-адрес, который нужно задать в поле **User identity value**.
 - **KeyID** – в качестве идентификатора партнеру будут высылаться данные из поля **User identity value**. В это поле нужно ввести любую последовательность символов, которая может включать в себя пробелы и русские буквы. Во вкладке **LSP** атрибуту **KeyID** будет присвоено шестнадцатеричное представление заданной последовательности символов, которое и будет высылаться партнеру в качестве идентификатора.
 - **Local IP address** – в качестве идентификатора партнеру будет высылаться действительный IP-адрес компьютера, на котором будет установлен Bel VPN Client-P. Значение по умолчанию.
- **User identity value** – значение идентификатора, пересылаемое партнеру. Допустимые значения определяются значением поля **User identity type**. Вводится вручную. Параметр обязательный.

7.4.2 Вкладки Firewall Rules и IPsec Rules

7.4.2.1 Порядок обработки пакетов

В следующих вкладках **Firewall Rules** и **IPsec Rules** задаются правила обработки пакетов исходящего и входящего трафиков на интерфейс хоста, на котором установлен Bel VPN Client-P.

Для исходящего трафика порядок обработки следующий – маркирование, защита трафика, пакетная и контекстная фильтрация. Для входящего трафика – пакетная и контекстная фильтрация, декапсуляция, маркирование трафика.

Далее описаны разделы, в которых следует задавать правила для перечисленных этапов обработки пакетов.

Исходящий трафик

1. Сначала для исходящего трафика ищется подходящее правило из набора правил **Outbound classification**, заданного во вкладке **Firewall Rules** (Рисунок 13). В нем задаются правила классификации и маркирования трафика, но могут быть заданы и правила пакетной фильтрации перед инкапсуляцией в IPsec. Если для исходящего пакета не нашлось подходящего правила из набора правил – пакет уничтожается, и дальнейший поиск правил прекращается. Если же подходящее правило найдено и применено, то поиск правил в этом наборе прекращается, и пакет передается на дальнейшую обработку.
2. Далее начинается поиск подходящего правила из набора правил, заданного во вкладке **IPsec Rules**. Это правило IPsec-инкапсуляции трафика. Если подходящее правило из набора **IPsec Rules** найдено – пакет обрабатывается и передается дальше. В противном случае – пакет уничтожается.
3. И наконец, для исходящего пакета осуществляется поиск подходящего правила из набора правил **Outbound Filter**, заданного во вкладке **Firewall Rules**. В нем задаются правила пакетной и контекстной фильтрации, но могут быть заданы и правила классификации и маркирования трафика. Если правило найдено – пакет обрабатывается, в противном случае – уничтожается.

Входящий трафик

1. Сначала для входящего трафика ищется подходящее правило из набора правил **Inbound Filter**, заданного во вкладке **Firewall Rules**. В нем задаются правила пакетной и контекстной фильтрации, но могут быть заданы правила классификации и маркирования трафика.
2. Далее начинается поиск подходящего правила из набора правил, заданного во вкладке **IPsec Rules** – декапсуляция IPsec-трафика.
3. И наконец, осуществляется поиск подходящего правила из набора правил раздела **Outbound classification**, заданного во вкладке **Firewall Rules**. В нем задаются правила классификации и маркирования трафика, но могут быть заданы и правила пакетной фильтрации.

Если для входящего пакета найдено и применено подходящее правило из первого набора правил, то дальнейший поиск правил в этом наборе прекращается, и начинается поиск подходящего правила из следующего набора.

Если для входящего пакета не нашлось подходящего правила из набора правил – пакет уничтожается, и дальнейший поиск правил прекращается.

7.4.2.2 Вкладка Firewall Rules

Во вкладке **Firewall Rules** (Рисунок 13) можно создавать, редактировать, удалять правила пакетной и контекстной фильтрации трафика, а также классификации и маркирования трафика.

Для исходящего и входящего трафиков задаются разные правила.

Правила **классификации и маркирования** исходящего трафика задаются в наборе правил **Outbound classification**, входящего трафика – в **Inbound classification**.

Правила **пакетной и контекстной фильтрации** для исходящего трафика – в наборе правил **Outbound filter**, для входящего трафика – в **Inbound filter**.

В скобках указывается количество правил в каждом наборе.

Правила в списке **Rule list** каждого набора должны быть расположены в порядке убывания приоритета. В списке должно находиться хотя бы одно правило.

При получении TCP/IP пакета правила будут просматриваться в порядке убывания приоритета и сравниваться параметры заголовка пакета с такими же параметрами в правиле до нахождения первого подходящего правила. Если для пакета разрешительное правило не найдено – пакет уничтожается.

Флажок **Refuse inbound TCP connections** – установка этого флажка запрещает создание TCP соединений, инициированных извне, в том числе и из защищенной сети. При формировании LSP добавляются соответствующие правила.

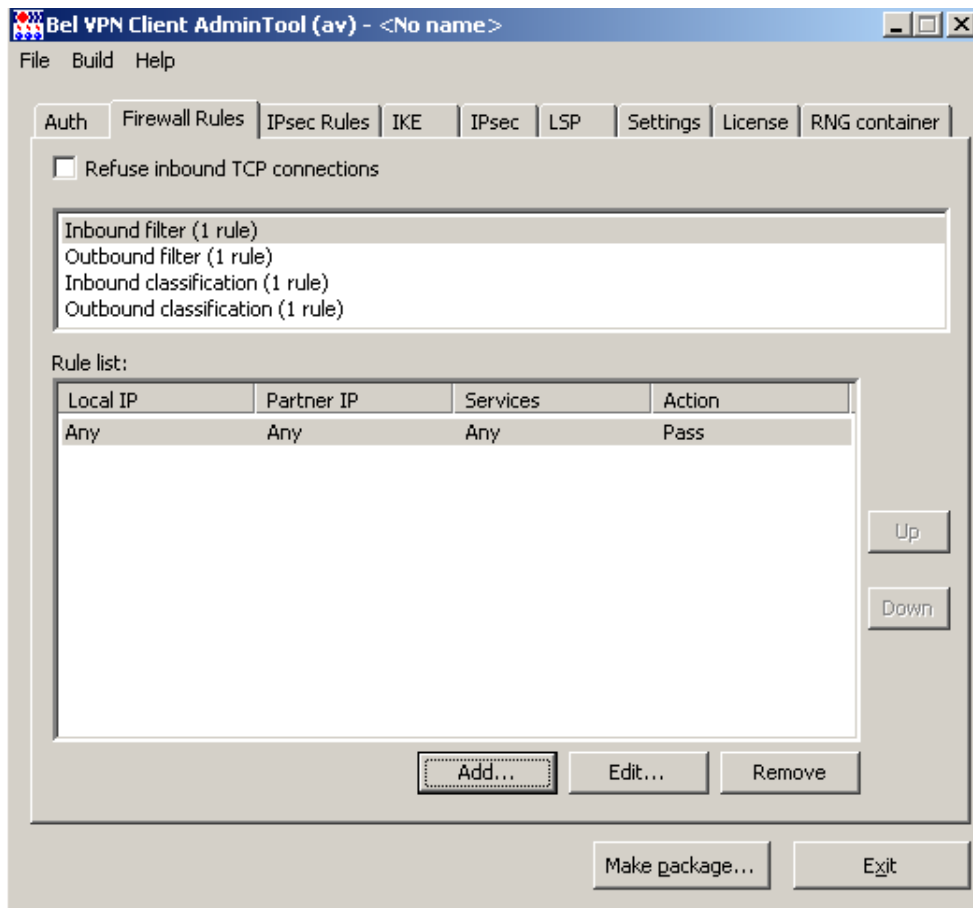


Рисунок 13

Кнопки управления:

- **Add** – вызывает окно для создания нового правила.
- **Edit** – вызывает окно для редактирования выделенного правила.
- **Remove** – удаляет выделенное правило с требованием подтверждения операции удаления. Если в списке только одно правило – оно не удаляется.
- **Up** – при нажатии этой кнопки выделенное правило в списке перемещается на одну строку вверх, увеличивая свой приоритет.
- **Down** – при нажатии этой кнопки выделенное правило в списке перемещается на одну строку вниз, уменьшая свой приоритет.

Маркирование пакетов. Задание правил в Outbound classification и Inbound classification

При выделении одного из наборов правил **Outbound classification** или **Inbound classification** и нажатии кнопки **Add** (Рисунок 13) появляется окно **Add Rule** (Рисунок 14) для создания правила.

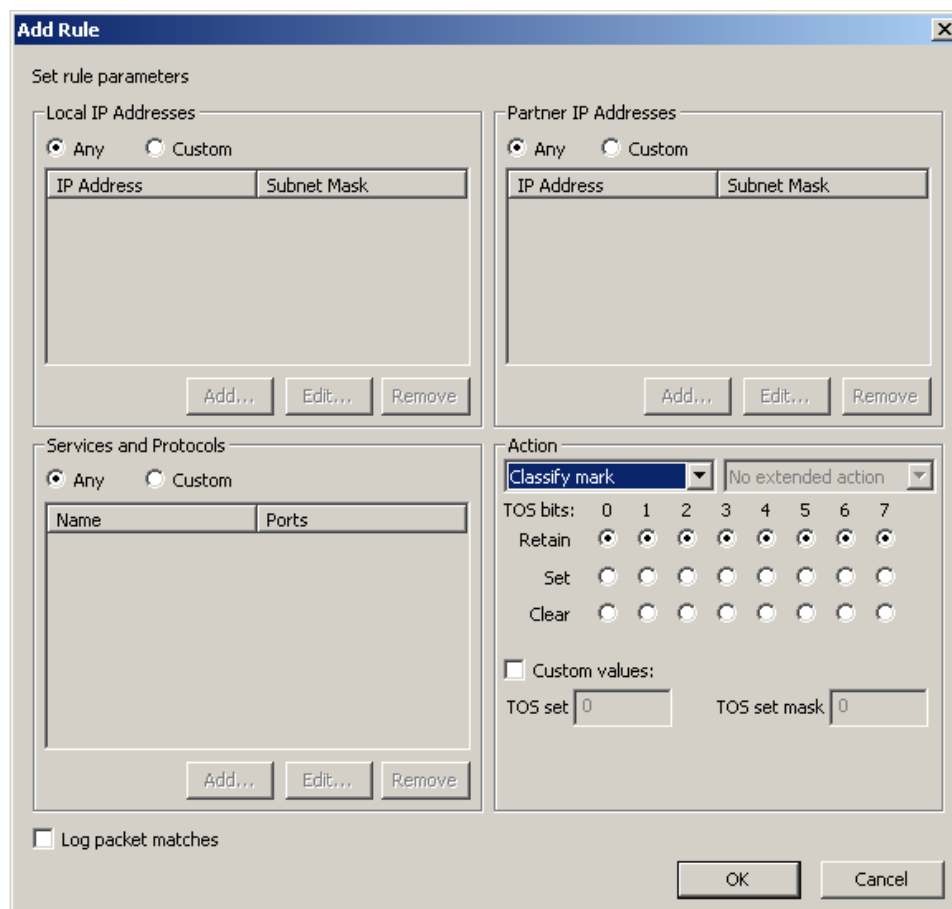


Рисунок 14

Диалоговое окно **Add Rule** имеет 4 области для задания правила:

- **Local IP Addresses** – в этой области задаются IP-адреса локального VPN устройства или подсети, на которые будет распространяться правило. Область имеет переключатель с двумя положениями:
 - *Any* – используется любой IP-адрес.
 - *Custom* – становится доступным окно для ввода IP-адреса и маски подсети.
- **Partner IP Addresses** – в этой области задаются IP-адреса или подсети партнеров, на которые распространяется правило.
- **Services and Protocols** – область для задания сетевых сервисов и протоколов, на которые распространяется правило.
- **Action** – в этой области задается действие, которое будет применено к пакету, если он попадает под данное правило.

Log packet matches – установка флажка задает протоколирование событий обработки пакетов, попадающих под данное правило.

Кнопки управления:

- **Add** – вызывает окно **Add IP Address** (Рисунок 15) для ввода IP-адреса и маски хоста или подсети.
- **Edit** – вызывает окно для редактирования выделенной записи.

- **Remove** – удаляет выделенную запись с требованием подтверждения операции удаления.

Задание IP-адреса и маски подсети в правиле

В областях **Local IP Addresses** и **Partner IP Addresses** для задания/редактирования IP-адреса хоста (подсети) и маски подсети в правиле следует установить переключатель в положение *Custom* и кнопкой **Add** или **Edit** вызвать окно **Add/Edit IP Address** (Рисунок 15). Если задается IP-адрес хоста, то сетевая маска равна 255.255.255.255. Адрес не может быть нулевым.

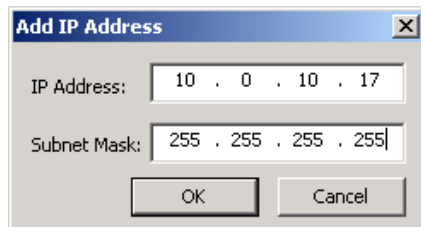


Рисунок 15

Задание сетевого сервиса или протокола в правиле

В области **Services and Protocols** установить переключатель в положение *Custom* и кнопкой **Add** вызвать окно **Add Service** (Рисунок 16):

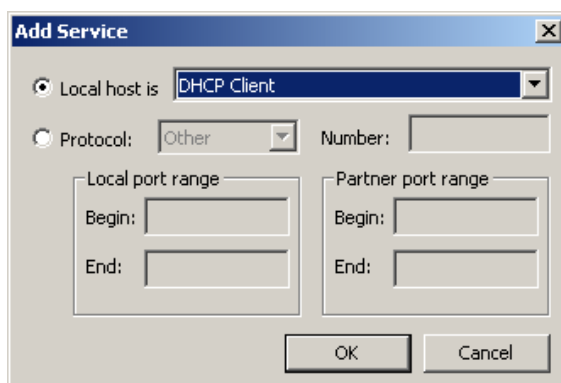


Рисунок 16

Здесь имеется переключатель с двумя положениями:

- **Local host is** – при установке переключателя в это положение выбрать из выпадающего предопределенного списка сервис и в каком качестве выступает локальное устройство – клиент или сервер.

Список предлагаемых сетевых сервисов и протоколов выбран в соответствии с перечнем IANA (<http://www.iana.org/assignments/port-numbers>):

- *DHCP Client* – все пакеты протокола TCP и UDP, идущие на порт 67 компьютера партнера и все пакеты протокола UDP, идущие на порт 68 локального компьютера.
- *DHCP Server* – все пакеты протокола TCP и UDP, идущие на порт 68 компьютера партнера и все пакеты протокола UDP, идущие на порт 67 локального компьютера.
- *HTTP Client* – все пакеты протокола TCP, UDP и SCTP, идущие на(с) порт(порта) 80 компьютера партнера.
- *HTTP Server* – все пакеты протокола TCP, UDP и SCTP, идущие на(с) порт(порта) 80 локального компьютера.
- *LDAP Client* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 389 компьютера партнера.
- *LDAP Server* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 389 локального компьютера.
- *LDAPS Client* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 636 компьютера партнера.

- *LDAP Server* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 636 локального компьютера.
- *RTNET Client* – все пакеты протокола TCP, и UDP идущие на(с) порт(порта) 107 компьютера партнера.
- *RTNET Server* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 107 локального компьютера.
- *SMTP Client* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 25 компьютера партнера.
- *SMTP Server* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 25 локального компьютера.
- *SNMP* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 161 локального компьютера.
- *SNMP Trap* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 162 компьютера партнера.
- *SSH Client* – все пакеты протоколов TCP, UDP и SCTP, идущие на(с) порт(порта) 22 компьютера партнера
- *SSH Server* – все пакеты протоколов TCP, UDP и SCTP, идущие на(с) порт(порта) 22 локального компьютера.
- *TELNET Client* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 23 компьютера партнера.
- *TELNET Server* – все пакеты протокола TCP и UDP, идущие на(с) порт(порта) 23 локального компьютера.
- **Protocol** – при установке переключателя в это положение выбирается протокол из следующего списка: *EGP, GGP, HMP, ICMP, PUP, RDP, RVD, TCP, UDP, SCTP, XNS-IDP* и одновременных перечислений нескольких протоколов: «TCP, UDP» и «TCP, UDP, SCTP» (Рисунок 17). В поле **Number** будет автоматически выводиться номер выбранного протокола. Задать протокол можно и по номеру из зарезервированного пространства (0-255). При указании протокола возможно указание диапазона портов (в тех протоколах, в которых это возможно). Область *Local port range* предназначена для задания портов на локальном устройстве, а область *Partner port range* – для задания портов на компьютере партнера. В полях *Begin* и *End* задается порт или диапазон портов из зарезервированного пространства (0-65535). Значение в поле *Begin* должно быть меньше или равно значению в поле *End*.

Редактирование выделенного сервиса или протокола производится в окне **Edit Service**, совпадающем с окном **Add Service**.

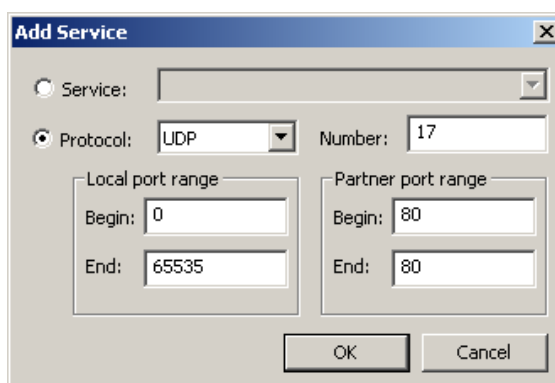


Рисунок 17

Задание действия в правиле

В области **Action** задается действие, которое будет применено к пакету, если пакет попадает под данное правило (Рисунок 255). Из выпадающего списка выбирается одно из действий:

- *Pass* – пропускать пакет.
- *Drop* – не пропускать пакет.

- *Classify mark* – маркировать пакет.

В соседнем поле можно указать дополнительное действие – проверку TCP-флагов.

Действия *Pass* и *Drop* без проверки TCP-флагов используются для создания правил пакетной фильтрации.

Действия *Pass* и *Drop* с проверкой TCP-флагов могут быть использованы для разрешения (запрещения) инициировать TCP-соединение с локального адреса или извне системы (зависит от правила – для исходящего или входящего трафика).

Действие Pass:

- *No extended action* – пропускать пакет без проверок (Рисунок 18)
- *TCP flags* – провести проверку пакета на TCP-флаги (Рисунок 19):
 - *Connection initiate* – пропускать первый пакет для инициации TCP-соединения (разрешается инициировать TCP-соединение).
 - *Connection established* – пропускать пакет, принадлежащий установленному TCP-соединению.

Действие Drop:

- *No extended action* – не пропускать пакет.
- *TCP flags* – провести проверку пакета на TCP-флаги:
 - *Connection initiate* – не пропускать первый пакет для инициации TCP-соединения (запрещается инициировать TCP-соединение).
 - *Connection established* – не пропускать пакет, принадлежащий установленному TCP-соединению.

Действия *Pass* и *Drop* с проверкой TCP-флагов могут быть использованы для разрешения (запрещения) инициировать TCP-соединение с локального адреса или извне системы.

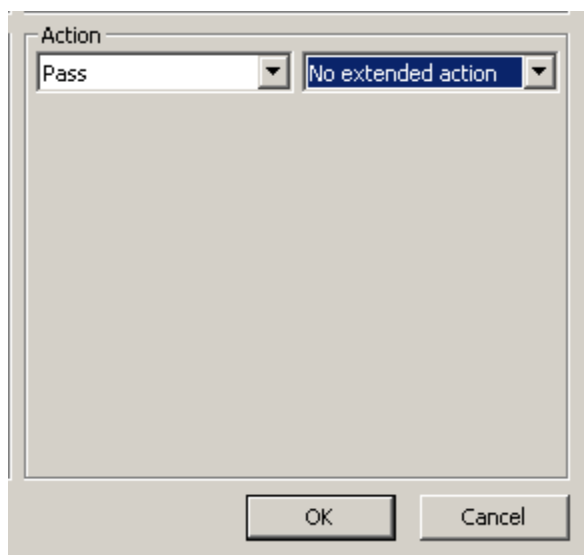


Рисунок 18

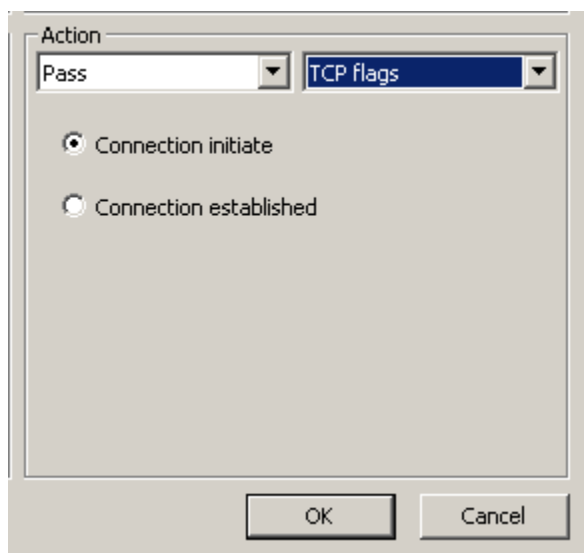


Рисунок 19

Действие Classify mark:

Для указания приоритета обработки пакета и эффективного продвижения пакетов по маршруту от одного узла сети к другому, для обеспечения качества обслуживания (QoS) выполняется маркирование пакетов. Для маркирования используется либо значение *IP Precedence (IPP)*, либо значение *DSCP*.

На (Рисунок 20) показана область *Action* при выборе действия *Classify mark*. Биты ToS-байта пронумерованы так же, как в документе по RFC 2474. Для маркировки следует использовать биты с 0 по 2 (IPP) или с 0 по 5 (DSCP), биты 6 и 7 зарезервированы и используются для специальной сигнализации, и для них переключатель должен стоять в положении «retain». В противном случае, при попытке сохранения правила, выдается предупреждение: «Two less significant bits of TOS byte should be retained unless you know exactly what you are doing. Do you want to proceed?»

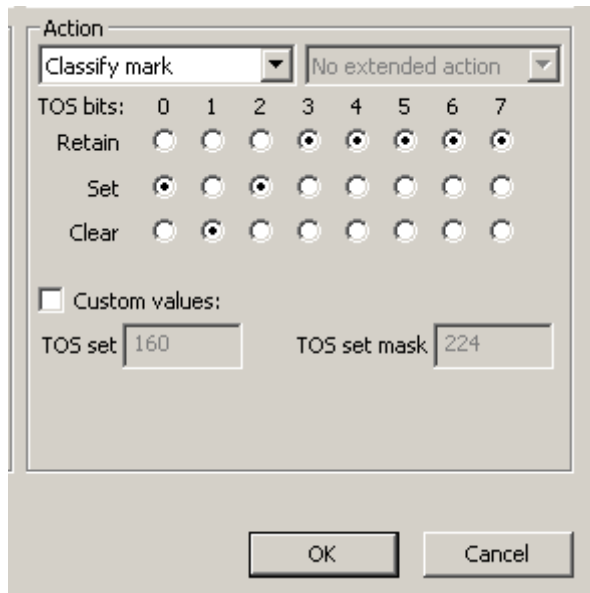


Рисунок 20

Для указания значений битов можно использовать либо переключатель с тремя положениями, либо флажок *Custom values*. Переключатель имеет 3 положения:

- *Retain* – оставить значение бита без изменений, как в пришедшем пакете.
- *Set* – в бите установить значение 1.
- *Clear* – в бите установить значение 0.

При изменении значений битов с помощью переключателя, в поле *TOS set* отображается значение байта в десятичном виде, а в поле *TOS set mask* – значение маски в десятичном виде. При установке флажка *Custom values* в поля *TOS set* и *TOS set mask* значения нужно ввести вручную в десятичном виде.

Значение IP Precedence

Значение *IP Precedence* (*IPP*) вносится в старшие 3 бита ToS-байта IP-заголовка пакета – в биты с номерами от 0 до 2. В Таблица 2 указаны значения приоритетов.

Таблица 2

Приоритет	Ключевое слово	Рекомендация к использованию	IPP (0-2 бита)
0	Routine – обычный пакет	По умолчанию	000
1	Priority – приоритетный (предпочтительный) пакет	Для приложений данных	001
2	Immediate – немедленный пакет	Для приложений данных	010
3	Flash – мгновенный (срочный) пакет	Для сигнализации вызовов	100
4	Flash-override – быстрее, чем мгновенный (экстренный) пакет	Для видеоконференций и потокового видео	100
5	Critical – критический пакет	Для голосового трафика	101
6	Internet – пакет межсетевого управления	Зарезервирован, не используется	
7	Network – пакет управляющей информации	Зарезервирован, не используется	

Значение DSCP

Значение *DSCP* вносится в старшие 6 битов ToS-байта – в биты с номерами от 0 до 5 (Рисунок 21). В Таблица 3 и Таблица 4 указаны значения *DSCP* для модели дифференцированного обслуживания (DiffServ).

The image shows a configuration window titled 'Action'. At the top, there are two dropdown menus: 'Classify mark' and 'No extended action'. Below these, there is a section for 'TOS bits' with columns for bits 0 through 7. Under each bit, there are three radio buttons labeled 'Retain', 'Set', and 'Clear'. For bit 6, the 'Retain' radio button is selected. Below this section, there is a checkbox labeled 'Custom values:' which is checked. Under this checkbox, there are two input fields: 'TOS set' with the value '148' and 'TOS set mask' with the value '252'. At the bottom of the window, there are 'OK' and 'Cancel' buttons.

Рисунок 21

Дифференцированное обслуживание не гарантирует определенный уровень сервиса, а стремится упорядочить весь трафик по классам таким образом, чтобы каждый класс получил лучший или худший уровень обслуживания по отношению к остальным.

Значение *DSCP* может быть выражено в цифровой форме или с использованием специальных ключевых слов, называемых поведением сетевых участков (PHB – Per-Hop Behavior). Определено три класса *DSCP* маркировки (Таблица 3):

- доставка по возможности (BE – Best Effort или DSCP 0)
- гарантированная доставка (AF – Assured Forwarding) (RFC 2597)
- срочная доставка (EF – Expedited Forwarding) (RFC 2598).

В дополнение к этим трем определенным классам существуют коды селектора классов (CS1-CS7), которые идентичны значениям *IP Precedence* (1-7).

В гарантированной доставке определены еще 4 класса. Обозначение класса начинаются с AF и далее следуют две цифры. Первая цифра определяет AF класс и принимает значения от 1 (низкий приоритет обработки) до 4 (высокий приоритет обработки пакета). Вторая цифра определяет уровень вероятности сброса пакета в пределах каждого класса и принимает значения от 1 (низкая вероятность сброса) до 3 (высокая вероятность сброса) (Таблица 4).

Негарантированная доставка пакетов имеет значение DSCP 0.

Для немедленной передачи пакетов указывается DSCP 101110.

Чем больше значение DSCP, тем больше приоритет обслуживания. Иногда такое количество классов избыточно, и последние 3 бита заполняют нулями.

Таблица 3

Код селектора классов (CS)	Описание		PHB-политика	DSCP
DSCP 0	Best Effort (BE) – default – 000000		PHB-политика негарантированной доставки пакетов, доставка по возможности. Рекомендуется для трафика данных – передача файлов, приложения электронной почты, HTTP и др.	000000
CS1	Class 1	Assured Forwarding (AF)	PHB-политика гарантированной доставки пакетов. Используется для видеотрафика, видеоконференций и рекомендуется значение DSCP 100010 (AF41).	100010 см Таблица 4
CS2	Class 2			
CS3	Class 3			
CS4	Class 4			
CS5	Express Forwarding (EF) – 101110		PHB-политика немедленной передачи пакетов, срочная доставка. Рекомендуется для голосового трафика	101110
CS6	Stays the same (used for IP routing protocols)			
CS7	Stays the same (link layer and routing protocol keep alive)			

Таблица 4 Классы гарантированной доставки пакетов

Приоритет отбрасывания пакета	Приоритет обработки			
	Class 1 (низкий)	Class 2	Class 3	Class 4 (высокий)
Низкий	001010 AF11	010010 AF21	011010 AF31	100010 AF41

Средний	001100 AF12	010100 AF 22	011100 AF32	100100 AF42
Высокий	001110 AF13	010110 AF23	011110 AF33	100110 AF43

Класс 4 обрабатывается более приоритетно, чем класс 3, класс 3 – более приоритетно, чем класс 2 и т.д.

Пакетная и контекстная фильтрация. Задание правил в Outbound filter и Inbound filter

В наборах правил *Outbound filter* или *Inbound filter* вкладки **Firewall Rules** (Ошибка! Источник ссылки не найден.3) задаются правила пакетной и контекстной фильтрации трафика. При нажатии кнопки **Add** появляется окно **Add Rule** (Рисунок 22) для создания правила. Это окно такое же как и для наборов правил *Outbound classification* и *Inbound classification* (Ошибка! Источник ссылки не найден.4), тличается только областью *Action*. Поэтому только область *Action* и опишем далее подробно.

Задание действия в правиле

К трафику, заданному в областях *Local IP Addresses*, *Partner IP Addresses*, *Services and Protocols*, применяется действие из области *Action*. Из выпадающего списка выбирается одно из действий:

- **Pass** – пропускать пакет.
- **Drop** – не пропускать пакет.
- **Classify mark** – маркировать пакет.
- **Inspect TCP** – проверять TCP-трафик.
- **Inspect FTP** – проверять FTP-трафик.

Действия *Pass*, *Drop*, *Classify mark* были ранее описаны в разделе «Задание действия в правиле» в предыдущем параграфе.

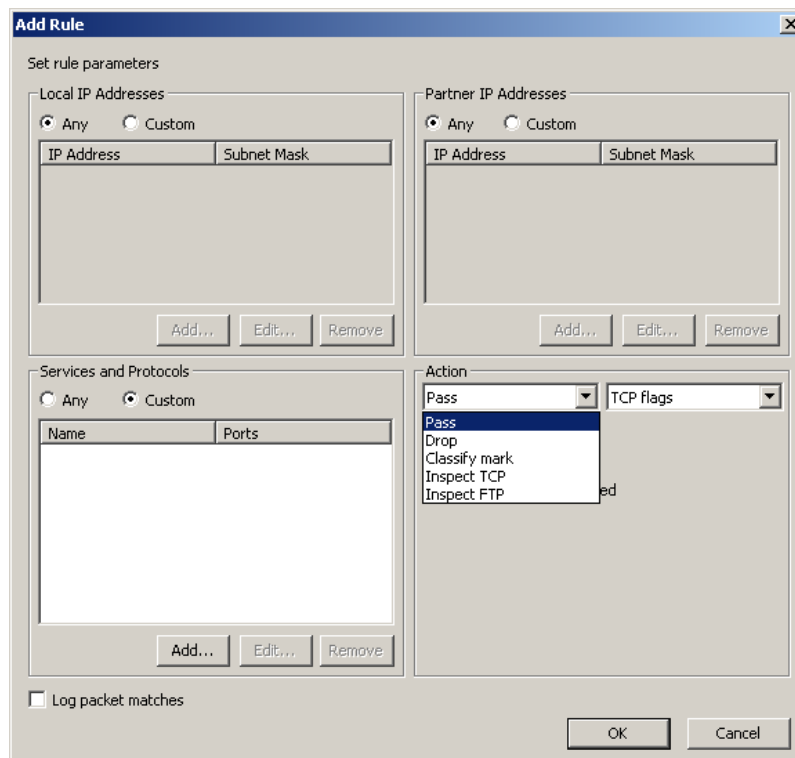


Рисунок 22

Действия *Inspect TCP* и *Inspect FTP* используются для создания правил контекстной фильтрации. Этими правилами будут проверяться только TCP-пакеты и FTP-пакеты.

Действие Inspect TCP:

При выборе этого действия отслеживается состояние TCP-соединения, меняется время жизни записи о соединении в соответствии с текущим состоянием соединения. Для пропуска пакетов в обе стороны, добавляются динамические правила фильтрации для входящего и исходящего трафика. Динамические правила удаляются вместе с записью о соединении.

Действие Inspect FTP:

При выборе этого действия отслеживается состояние FTP-соединения, меняется время жизни записи о соединении в соответствии с текущим состоянием соединения. Для пропуска пакетов в обе стороны, добавляются динамические правила фильтрации для входящего и исходящего трафика. Динамические правила удаляются вместе с записью о соединении. Кроме того, отслеживаются некоторые команды FTP, создаются правила для пропуска соединения для данных FTP, определяются и блокируются некоторые подозрительные команды, которые могут являться атакой на FTP сервер.

Если нужно разрешить только исходящий с клиента TCP-трафик и ответный на него трафик, то разрешительное правило контекстной фильтрации должно быть только в разделе Outbound filter, в разделе Inbound filter такого правила быть не должно. Если разрешительного правила нет, значит трафик запрещен.

При выборе действия *Inspect TCP* (*Inspect FTP*) область *Action* приобретает следующий вид (Рисунок 23). Второй выпадающий список с флагами – не активен.

- *Audit* – при установке этого флажка при закрытии соединения создаются сообщения со статистической информацией, выдаваемые в syslog-файл.
- *No alert* – при установке этого флажка не выдаются сообщения о потенциальных атаках (попытках взлома).
- *Timeout* – переопределяет время жизни в секундах установленного соединения по данному правилу. (Глобальные настройки для всех соединений установлены во вкладке **LSP** – кнопка **Advanced**).

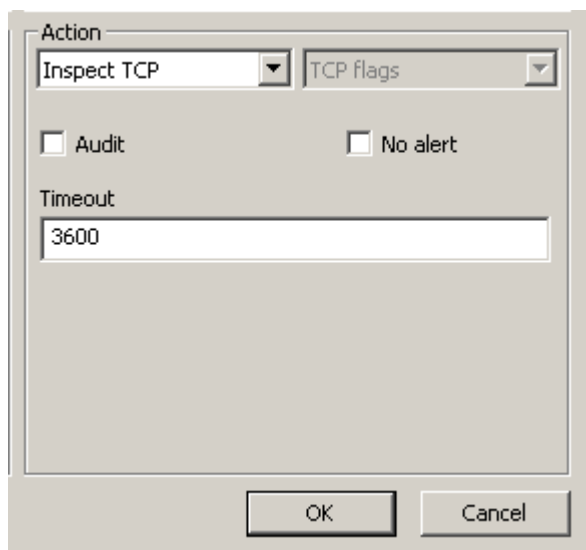


Рисунок 23

7.4.2.3 Вкладка IPsec Rules

Во вкладке **IPsec Rules** задаются правила для защиты трафика с использованием протокола IPsec. Допустимые алгоритмы протоколов AH и ESP задаются во [вкладке IPsec](#).

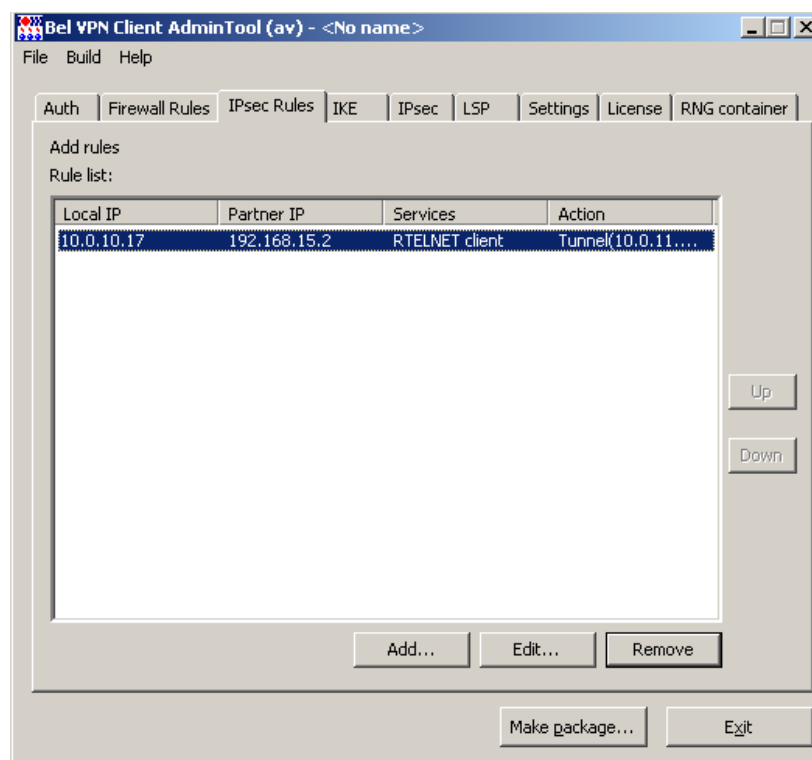


Рисунок 24

Создание и редактирование правила

Создание и редактирование правила производится в окне **Add/Edit Rule**, которое вызывается кнопкой **Add** или **Edit** во вкладке **IPsec Rules**:

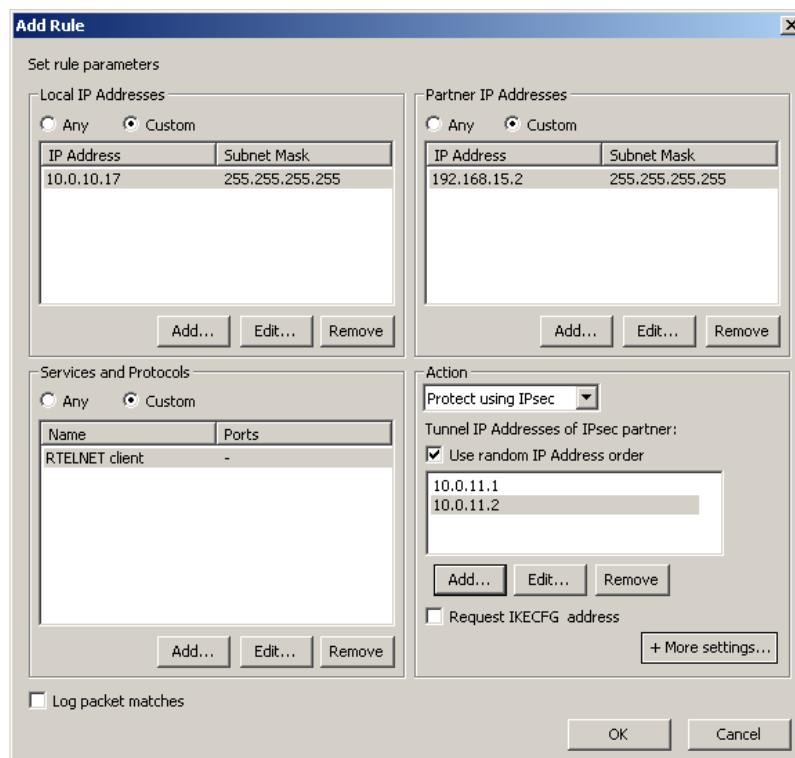


Рисунок 25

Области **Local IP Addresses**, **Partner IP Addresses**, **Services and Protocols** такие же, как во вкладке **Firewall Rules**. Отличается только область **Action**.

Задание действия в правиле

В области **Action** задается действие, которое будет применено к пакету, если пакет подпадает под действие данного правила (Рисунок 25). Из выпадающего списка выбирается одно из действий:

- **Pass** – пропускать трафик без обработки.
- **Drop** – не пропускать трафик.
- **Protect using IPsec** – защищать трафик с использованием протоколов IPsec (алгоритмы протоколов AH и ESP задаются во [вкладке IPsec](#)). Трафик между хостом с локальным IP-адресом и IP-адресом партнера защищается на интервале между локальным IP-адресом и туннельным IPsec адресом партнера (это может быть адрес интерфейса шлюза безопасности, защищающего подсеть, в которой находится партнер). В результате этого строится защищенное IPsec соединение – IPsec SA (туннель) (Рисунок 26).

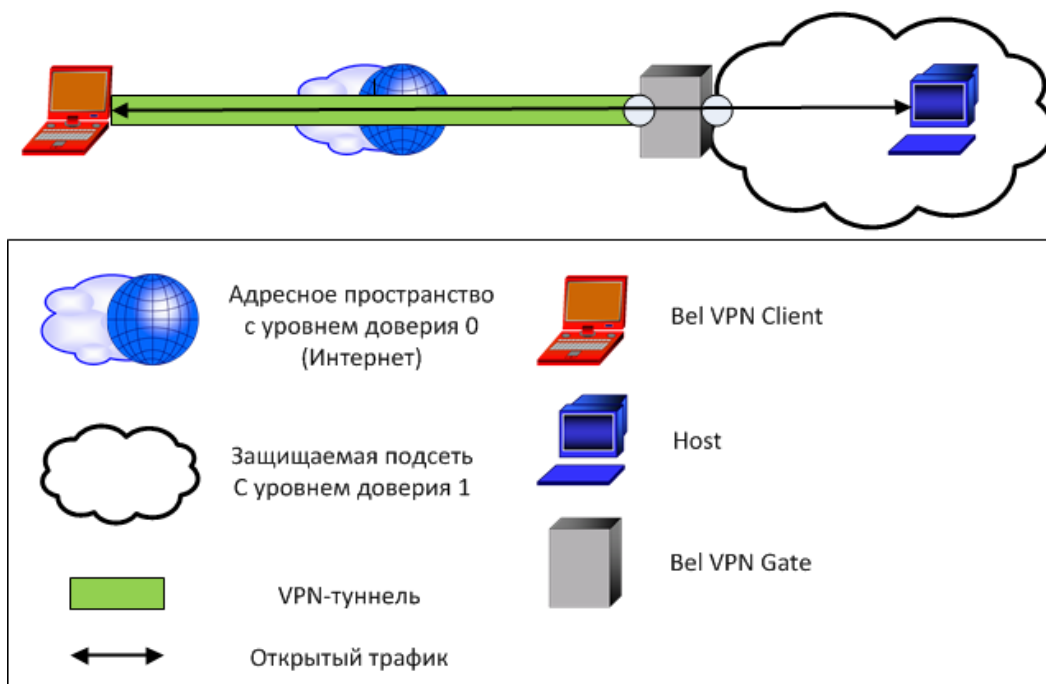


Рисунок 26

Для указания туннельного IPsec адреса партнера нажмите кнопку **Add** в области **Action** и в открывшемся окне **Add IP Address** (Рисунок 27) укажите IP-адрес интерфейса, до которого будет построен туннель от локального IP-адреса клиента. Адрес не может быть нулевым.

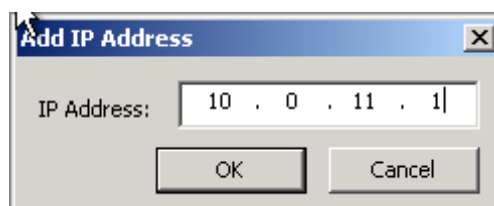


Рисунок 27

Можно указать список IP-адресов, до которых возможно построить туннель. Адреса в списке надо расположить в порядке убывания приоритета – первый в списке имеет самый высокий приоритет. Если не удалось построить туннель до интерфейса с первым указанным адресом, производится попытка построить туннель со вторым IP-адресом и т.д. Кнопки **Up** и **Down** предназначены для изменения приоритета адресов в списке (Рисунок 28).

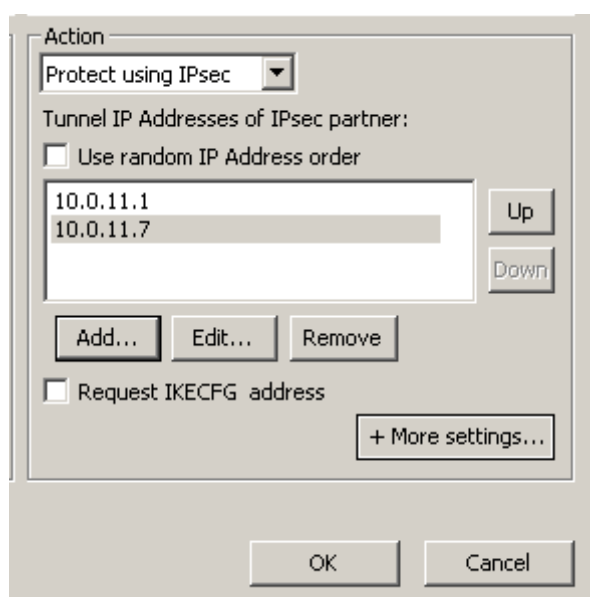


Рисунок 28

Используя кнопки **Add**, **Edit** и **Delete**, можно добавлять, редактировать и удалять адреса из списка.

Use random IP Address order – при установке этого флажка IPsec-адрес партнера будет выбираться из списка случайным образом. При неудачной попытке построить туннель с этим адресом, следующий туннельный адрес будет выбираться также случайным образом.

Request IKECFG address – установка этого флажка позволяет клиенту запрашивать адрес у IKECFG-сервера при построении защищенного соединения по данному правилу. Поэтому в этом правиле обязательно нужно указать туннельный адрес партнера, у которого и будет запрошен IKECFG-адрес (Рисунок 29). Интерфейс, с присвоенным ему IKECFG-адресом, будем называть виртуальным интерфейсом.



Существует ограничение в применении Продукта Bel VPN Client-P, когда запрашивается адрес из IKECFG-пула:

Можно задать только одно правило с запросом IKECFG-адреса, причем в этом правиле нельзя задать фильтрацию по локальным адресам, протоколам и портам (сервисам) (положение переключателя *Custom* недоступно). Это связано с атрибутом **PersistentConnection=TRUE** в структуре *IPsecAction*.

Созданная политика безопасности будет неработоспособна, если весь трафик защищается по протоколу IPsec (трафик между любым локальным IP-адресом и любыми адресами партнеров, указанными в областях *Local IP Addresses* и *Partner IP Addresses*).

Политика безопасности не будет работать, если туннельный IPsec адрес партнера (*Tunnel IP Addresses of IPsec partner*) совпадает с IP-адресом, или подсетью партнера (*Partner IP Addresses*), на которые распространяется правило фильтрации.

Рисунок 29

+More settings – при нажатии на кнопку **+More settings** (Рисунок 29) появляется окно (Ошибка! Источник ссылки не найден.Рисунок 30) для дополнительных настроек.

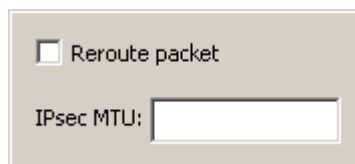


Рисунок 30

- **Reroute packet** – при установке этого флажка пакет будет подвергаться повторной маршрутизации (при создании вложенного туннеля или при отправке пакета с виртуального IKECFG интерфейса после IPsec обработки). При создании вложенного туннеля для исходящего пакета опять выполняется поиск подходящего правила из набора правил *Outbound classification*, а затем из вкладки **IPsecRules**. С виртуального IKECFG интерфейса после IPsec обработки пакет не может быть отправлен в интернет, поэтому он перенаправляется на другой интерфейс.
- **IPsec MTU** – в этом поле можно задать значение MTU для IPsec SA, построенному по данному правилу. Допустимые значения MTU – от 0 до 65535. Значение по умолчанию – 0, при этом MTU будет определяться автоматически, и в LSP в структуре *IPsecAction* значение MTU не указывается.

7.4.3 Вкладка IKE

В этой вкладке определены наборы политик для защиты соединений IKE, которые предлагаются партнеру для согласования при создании ISAKMP SA.

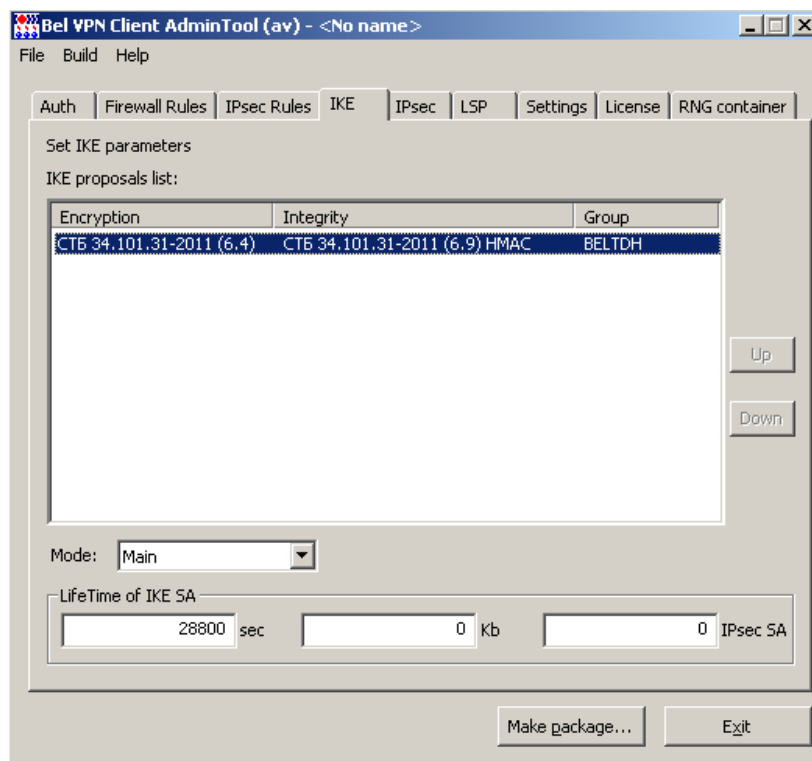


Рисунок 31

IKE proposals list – упорядоченный список IKE предложений по приоритету. В верхней строчке находится предложение с наивысшим приоритетом.

Encryption – алгоритмы шифрования пакетов. Предлагается один криптографический алгоритм:

- **СТБ 34.101.31-2011 (6.4)** – белорусский криптографический алгоритм, представленный в конфигурации (во вкладке LSP) как **STB34101CIPH-K256-CBC-65532**.

Integrity – алгоритмы проверки целостности пакетов. Предлагаются следующие белорусские криптографические алгоритмы:

- **СТБ 34.101.31-2011 (раздел 6.9) HMAC** – белорусский криптографический алгоритм, представленный в конфигурации (во вкладке LSP) как **34101HASH-65532**.

Имена алгоритмов шифрования пакетов и проверки целостности данных считываются из файла admintool.ini, размещенного в папке Продукта Bel VPN Client AdminTool st. Для изменения имен алгоритмов необходимо отредактировать этот файл, описанный в разделе «Формат задания имен алгоритмов в файле admintool.ini», и перезапустить графический интерфейс.

Group – параметры выработки общего сессионного ключа по алгоритму Диффи-Хеллмана:

- BELTDH – протокол формирования общего ключа на основе эллиптических кривых согласно СТБ 34.101.66-2014

Mode – режим обмена информацией о параметрах защиты и установления IKE SA. Имеет два значения:

- *Main* – в этом режиме партнеру высылаются все IKE политики для выбора и согласования.
- *Aggresssive* – в этом режиме партнеру высылается только первая IKE политика из списка, имеющая самый высокий приоритет. При выборе этого режима выдается предупреждение об этом. Если для аутентификации используется предопределенный ключ и выбран тип идентификатора *KeyID*, то должен использоваться только режим *Aggressive*.

LifeTime of IKE SA (sec) – время в секундах, в течение которого ISAKMP SA будет существовать. Возможное значение – целое число из диапазона 0..2147483647. Рекомендуемое значение – 28800, которое выставлено при открытии нового проекта. Значение 0 означает, что время действия SA не ограничено. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

LifeTime of IKE SA (Kb) – указывает объем данных в килобайтах, который могут передать стороны во всех IPsec SA, созданных в рамках одного ISAKMP SA. Возможное значение – целое число из диапазона 0..2147483647. Рекомендуемое значение – 0, которое выставлено при открытии нового проекта. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

IPsec SA – количество IPsec SA, созданных в рамках одного ISAKMP SA. Значение 0 означает, что количество IPsec SA не ограничено.

Кнопки **Up** и **Down** предназначены для упорядочивания списка предложений по приоритету.

7.4.4 Вкладка IPsec

В данной вкладке задаются политики IPsec защиты в виде набора преобразований, каждый из которых есть комбинация AH преобразования и ESP преобразования. Партнеру направляется список наборов преобразований, по протоколу IKE происходит согласование и выбор конкретного набора преобразований, который будет использоваться для защиты трафика для одного SA.

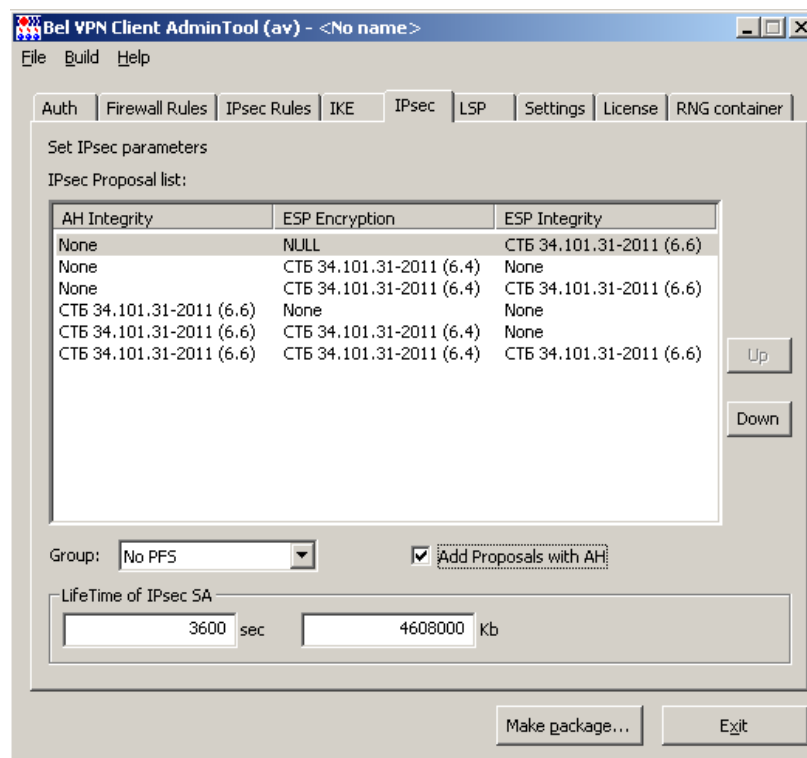


Рисунок 32

IPsec Proposal list – упорядоченный список наборов преобразований, высылаемых партнеру для согласования. При помощи кнопок Up и Down выполняется упорядочивание списка по приоритету. В верхней строчке находится набор преобразований с наивысшим приоритетом.

AH Integrity – предлагаемые алгоритмы проверки целостности пакета по протоколу AH: Имеется три значения:

- **None** – алгоритм проверки целостности не применяется.
- **СТБ 34.101.31-2011 (6.6)** – белорусский криптографический алгоритм, представленный в конфигурации (во вкладке LSP) как **STB34101CIPH-K256-MAC-252**.

ESP Integrity – предлагаемые алгоритмы проверки целостности пакета по протоколу ESP:

- **None** – алгоритм проверки целостности не применяется.
- **СТБ 34.101.31 (6.6)** – криптографический алгоритм, представленный в конфигурации (вкладке LSP) как **STB34101CIPH-K256-MAC-65532**.

ESP Encryption – предлагаемые алгоритмы шифрования пакетов по протоколу ESP:

- **None** – алгоритм шифрования ESP не применяется.
- **Null** – алгоритм применять, но не шифровать.
- **СТБ 34.101.31-2011 (6.4)** – белорусский криптографический алгоритм, представленный в конфигурации (во вкладке LSP) как **STB34101CIPH-K256-SVC-252**.

Имена алгоритмов шифрования пакетов и проверки целостности данных считываются из файла `admintool.ini`, размещенного в папке Продукта Bel VPN Client AdminTool. Для изменения имен алгоритмов необходимо отредактировать этот файл, описанный в разделе [«Формат задания имен алгоритмов в файле admintool.ini»](#), и перезапустить графический интерфейс.

Add Proposals with AH – при установке этого флажка выводится сообщение:

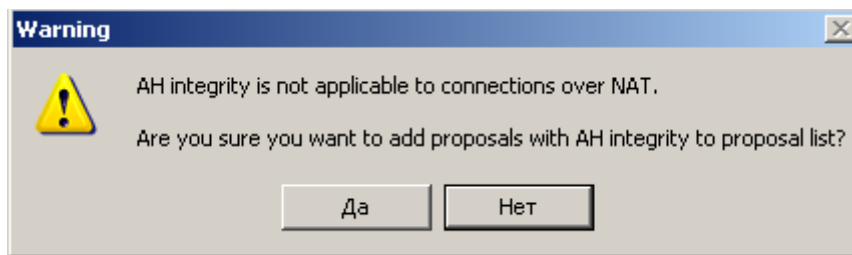


Рисунок 33

Оно означает, что протокол АН несовместим со средствами NAT, так как NAT изменяют IP-адрес в заголовке TCP/IP пакета. Протокол АН обеспечивает проверку аутентичности и целостности пакетов, а NAT нарушает данные аутентификации. После нажатия кнопки Yes добавляется белорусский криптографический алгоритм контроля целостности СТБ 34.101.31-2011 (раздел 6.6).

Group – параметры выработки ключевого материала, высылаемые партнеру для согласования:

- **No PFS** – опция PFS не включена и при согласовании новой SA новый обмен по алгоритму Диффи-Хеллмана для выработки общего сессионного ключа не выполняется. Ключевой материал заимствуется из первой фазы IKE.
- **BELTDH** – протокол формирования общего ключа на основе эллиптических кривых согласно СТБ 34.101.66-2014

LifeTime of IPsec SA (sec) – время в секундах, в течение которого IPsec SA будет существовать. Возможное значение – целое число из диапазона 1..2147483647. Рекомендуемое значение – 3600, которое выставлено при открытии нового проекта. Пустая строка и значение 0, которое означает неограниченное время жизни IPsec SA, – недопустимы, при создании инсталляционного файла будет выдано сообщение об ошибке.

Рекомендуется указывать такое время SA жизни в секундах, что бы в основном удаление IPsec SA происходило по времени, а ограничение на объем трафика выбирать как дополнительную меру.

LifeTime of IPsec SA (Kb) – указывает объем данных в килобайтах, который могут передать стороны в рамках одной IPsec SA. Возможное значение – целое число из диапазона 0..2147483647. Рекомендуемое значение – 4608000, которое выставлено при открытии нового проекта. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

При превышении указанного значения для созданного SA, в журнал протоколирования будет выдано сообщение, что в созданном IPsec SA ограничение по трафику не соответствует допустимому ограничению для используемого криптографического алгоритма:

"SA traffic limit exceeds limitations imposed by the cryptographic algorithm"

Кнопки **Up** и **Down** предназначены для упорядочивания списка предложений по приоритету.

7.4.5 Вкладка LSP

Во вкладке **LSP** (Рисунок 34) просматривается и редактируется локальная политика безопасности для пользователя, заданная в предыдущих вкладках.

Существует два режима работы с LSP:

- режим автоматического формирования LSP
- режим ручного задания LSP.

7.4.5.1 Режим автоматического формирования LSP

В режиме автоматического формирования (флажок "Use custom LSP" не установлен) локальная политика безопасности формируется на основе данных вкладок **Auth**, **Firewall Rules**, **IPsec Rules**, **IKE**, **IPsec** и расширенных параметров, задаваемых в диалоговом окне, вызываемом кнопкой *Advanced*.

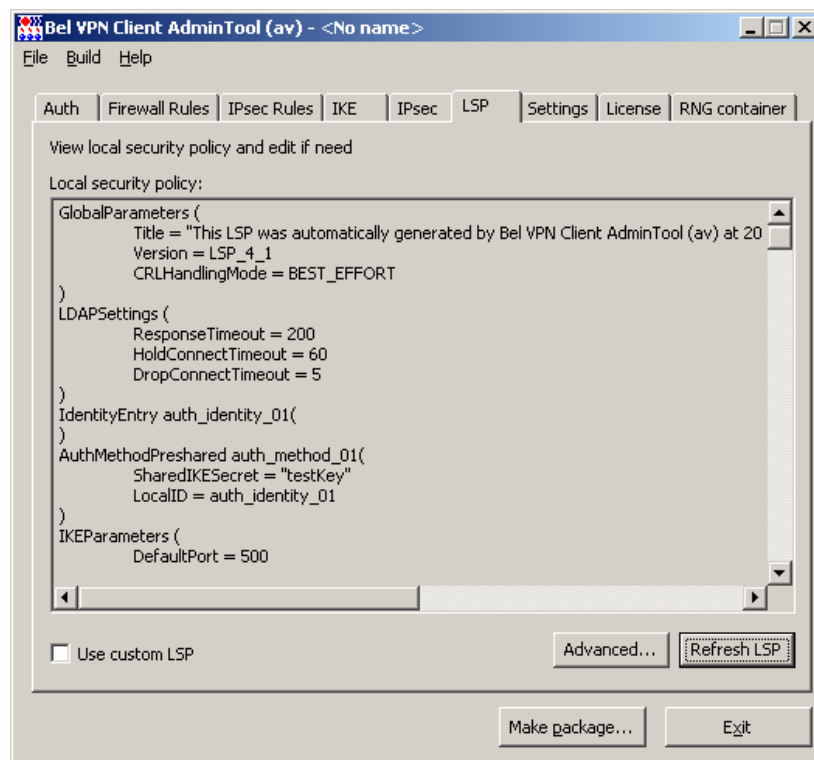


Рисунок 34

Local security policy – поле с LSP в текстовом формате.

Use custom LSP – установка этого флажка переключает в режим ручного формирования LSP.

Refresh LSP – кнопка для обновления LSP в окне **Local security policy** для отображения текущей конфигурации с изменениями.

Advanced – кнопка вызова окна [Advanced LSP Settings](#) для настройки расширенного списка параметров LSP.

7.4.5.2 Окно Advanced LSP Settings

Это окно (Рисунок 35) отображает расширенный список переменных LSP и их текущие значения, которые можно отредактировать и установить значения по умолчанию. Переменные объединены в шесть групп.

Окно содержит 4 функциональные кнопки:

- **Edit** – кнопка вызова окна для редактирования выделенной переменной. Окно редактирования открывается также при двойном клике левой кнопки "мыши" на выделенной строке.
- **Set defaults** – кнопка для установки значений по умолчанию для всех переменных.
- **Accept** – кнопка для закрытия окна с сохранением отредактированных значений переменных.
- **Cancel** – кнопка для закрытия окна без сохранения отредактированных значений переменных.

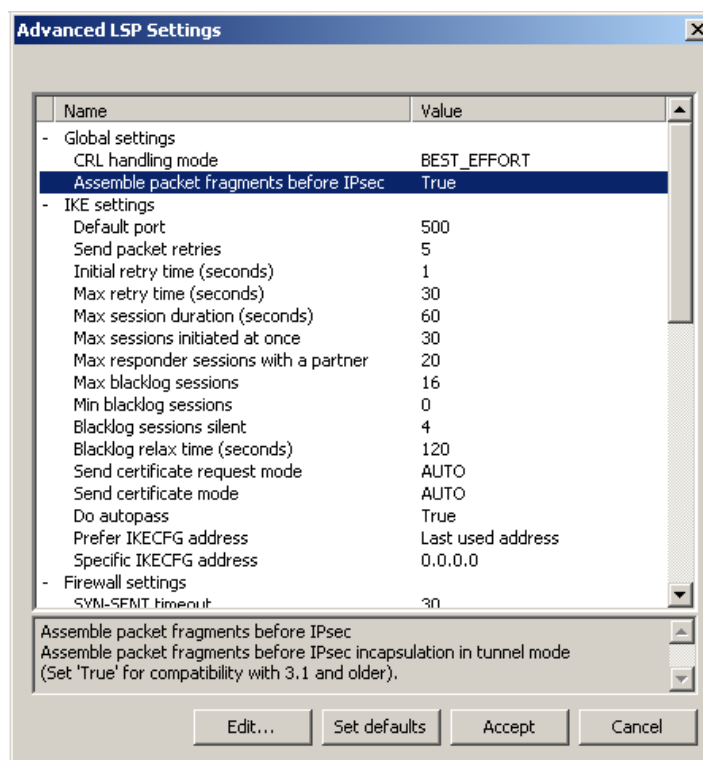


Рисунок 35

Global settings

CRL handling mode

Переменная задает режим использования списков отозванных сертификатов (CRL). При нажатии кнопки Edit появляется окно для выбора значений из выпадающего списка:

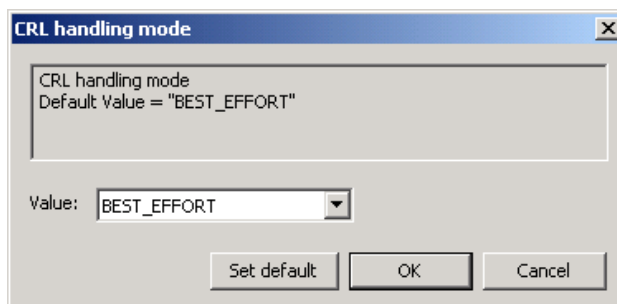


Рисунок 36

Возможные значения:

- **DISABLE** – при проверке сертификата список отозванных сертификатов не обрабатывается.
- **OPTIONAL** – список отозванных сертификатов используется только в случае, если он был предустановлен или получен (и обработан) в процессе IKE обмена и является действующим.
- **BEST_EFFORT** – список отозванных сертификатов используется при проверке сертификата только в том случае, если он является действующим. Этот режим отличается от режима OPTIONAL тем, что CRL может быть получен посредством протокола LDAP (если он настроен). Это значение используется по умолчанию.
- **ENABLE** – для успешной проверки сертификата обрабатывается список отозванных сертификатов.

Значение по умолчанию – **BEST_EFFORT**.

Все окна для редактирования переменных имеют три функциональные кнопки:

- **Set default** – кнопка для установления значения по умолчанию данной переменной;

- **OK** – кнопка для закрытия окна с сохранением выбранного значения переменной;
- **Cancel** – кнопка для закрытия окна без сохранения выбранного значения переменной.

Assemble packet fragments before IPsec

Переменная задает сборку IP-пакетов из фрагментов перед IPsec-инкапсуляцией. При нажатии кнопки **Edit** появляется окно с двумя положениями переключателя:

- *FALSE* – сборка пакета не производится.
- *TRUE* – производится сборка пакета из фрагментов.

Значение по умолчанию – *TRUE*.

Для совместимости с версией клиента 3.0.1 установите значение *TRUE*.

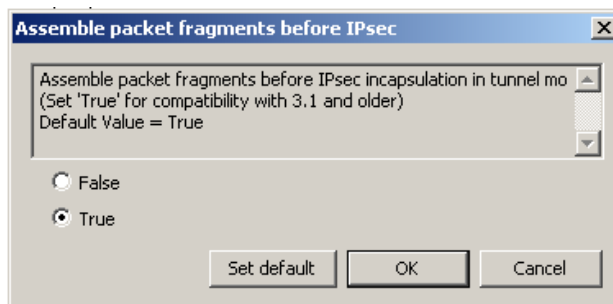


Рисунок 37

IKE settings

Переменные, в названии которых имеется слово *blacklog*, задают поведение механизма так называемого "черного списка". "Черный список" предназначен для защиты от DoS-атак (Denial of Service – отказ от обслуживания). "Черный список" минимизирует обработку IKE-пакетов от партнеров, находящихся в "черном списке".

Default port

Порт для протокола IKE, который будет использован по умолчанию. Возможное значение – целое число из диапазона 1..65535. Значение по умолчанию – 500.

Окно для выбора значения порта:

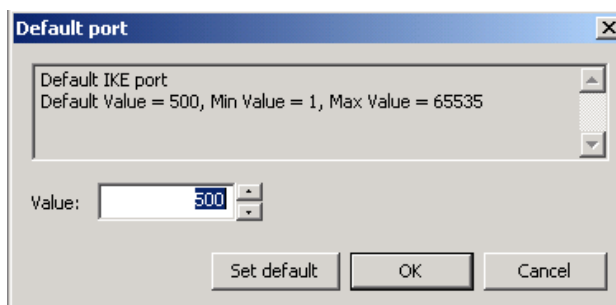


Рисунок 38

Send packet retries

Количество попыток послыки IKE-пакетов партнеру. Возможное значение – целое число из диапазона 1..30. Значение по умолчанию – 5.

Окно для установки значения представлено на рисунке 269:

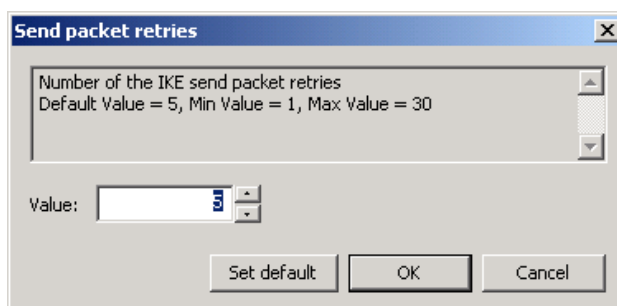


Рисунок 39

Initial retry time (seconds)

Начальный интервал времени между повторными попытками отправки IKE-пакетов партнеру (в секундах). Если ответ не получен в течение начального интервала, то запрос отправляется повторно и интервал между повторными попытками увеличивается в два раза. Этот интервал увеличивается в два раза до тех пор, пока:

- не будет получен ответ или
- значение интервала Initial retry time не достигнет значения *Max retry time*, (повторные попытки будут продолжаться с интервалом *Max retry time*) и количество попыток не достигнет значения *Send packet retries*.

Возможное значение – целое число из диапазона 1..5. Значение по умолчанию – 1.

Окно для установки начального интервала времени:

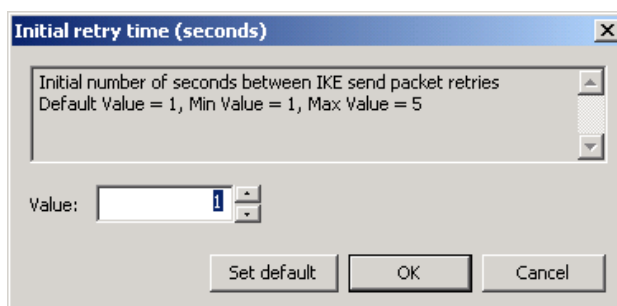


Рисунок 40

Max retry time (seconds)

Максимальный интервал времени между повторными попытками отправки IKE-пакетов партнеру (в секундах). Если выставленное значение *Max retry time* меньше, чем значение *Initial retry time*, то при загрузке конфигурации *Max retry time* присваивается значение *Initial retry time*. Возможное значение – целое число из диапазона 1..60. Значение по умолчанию – 30.

Окно для установки максимального интервала времени:

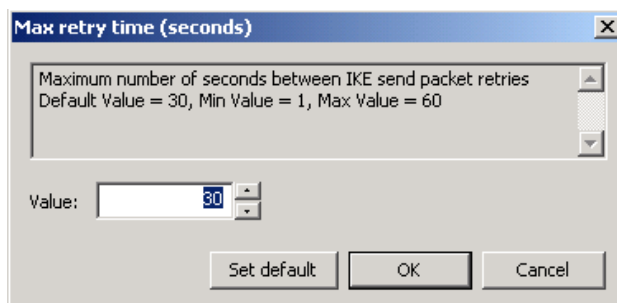


Рисунок 41

Max session duration (seconds)

Максимальный интервал времени на каждую сессию IKE (в секундах). Возможное значение – целое число из диапазона 10..300. Значение по умолчанию – 60. Окно для выбора значения:

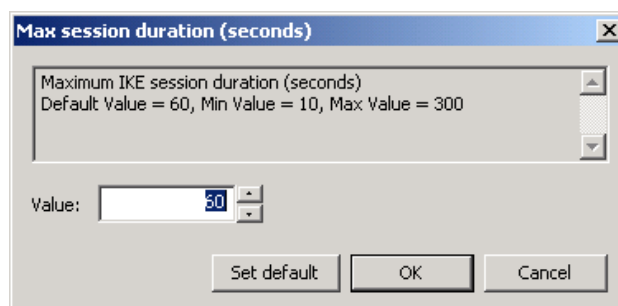


Рисунок 42

Max sessions initiated at once

Максимальное количество одновременно иницируемых IKE-сессий для всех партнёров. Возможное значение – целое число из диапазона 1..10000. Значение по умолчанию – 30. Окно для выбора значения:

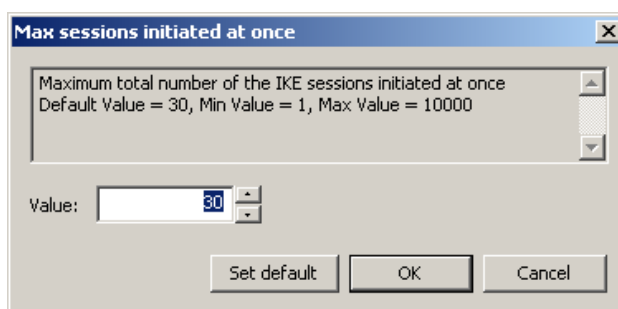


Рисунок 43

Max responder sessions with a partner

Максимально допустимое количество одновременных обменов, проводимых VPN-устройством со всеми партнерами, в качестве ответчика. Если локальное устройство имеет указанное количество незавершенных IKE-обменов в роли ответчика, то все входящие ISAKMP-пакеты, требующие установления новых обменов, игнорируются (без оповещения партнера).

Возможное значение – целое число из диапазона 1..10000. Значение по умолчанию – 20. Окно для установки значения:

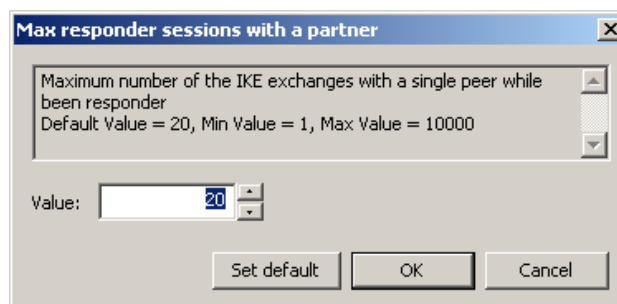


Рисунок 44

Max backlog sessions

Max backlog sessions устанавливает начальное число разрешенных одновременных IKE обменов, иницируемых одним партнером¹. При каждом неудачном завершении IKE обмена число разрешенных одновременных IKE обменов для данного партнера снижается вдвое с округлением в меньшую сторону, вплоть до полного запрещения IKE трафика с данным партнером.

¹В данном случае партнер идентифицируется по паре ip:port. Пока партнер не аутентифицирован (т.е. с таким партнером на данный момент нет ни одного ISAKMP-соединения – SA), допустимое количество IKE-обменов может снижаться в зависимости от того, насколько успешно завершаются IKE-обмены с этим партнером.

Примечание: как только партнер заносится в "черный список", для него текущее значение разрешенных одновременно проводимых IKE обменов не только начинает уменьшаться в два раза после каждого неуспешного завершения обмена, но и увеличиваться на единицу по истечении каждого интервала времени *Blacklog relax time* (описанного далее).

Возможное значение – целое число из диапазона – 0..2147483647.

Если значение равно 0, то "черный список" не используется.

Если значение *Max blacklog sessions* больше или равно значению *Max responder sessions with a partner*, то *Max blacklog sessions* присваивается значение *Max responder sessions with a partner*.

Значение по умолчанию – 16.

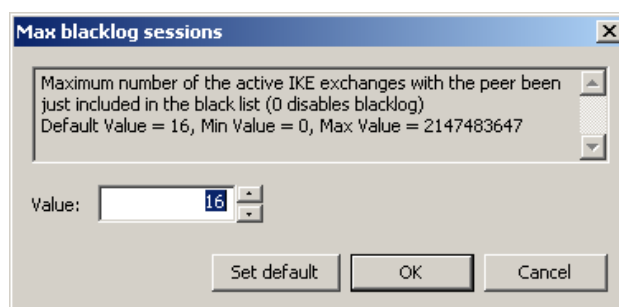


Рисунок 45

Min blacklog sessions

Минимальное число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером.

Возможное значение – целое число из диапазона – 0..2147483647.

Если значение *Min blacklog sessions* равно или больше, чем *Max blacklog sessions*, то число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером, не снижается (т.е. "черный список" отключен)².

Значение по умолчанию – 0 означает, что для партнера, поведение которого привело к понижению числа разрешенных инициируемых им одновременных IKE обменов до значения *Min blacklog sessions*, игнорируется весь IKE-трафик, а все имеющиеся с ним недостроенные IKE-сессии уничтожаются (ситуация "Access denied").

Окно для выбора минимального количества обменов с партнером:

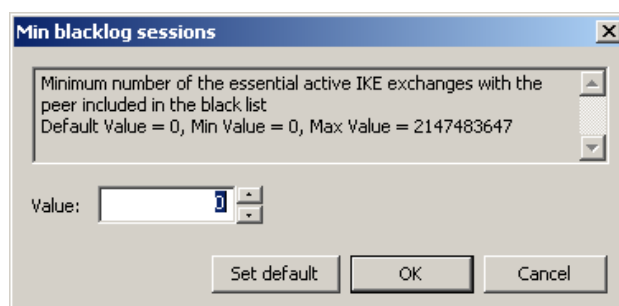


Рисунок 46

Blacklog sessions silent

Число активных обменов, инициированных неаутентифицированным партнером, по достижении которого VPN-устройство перестает информировать партнера о причине неуспешного завершения инициированного им IKE-обмена.

² При загрузке конфигурации с *отключенным* «черным списком» вся статистическая информация о «плохих» партнерах сбрасывается. Если же «черный список» *включен*, то к уже имеющейся накопленной статистике применяются новые параметры настроек «черного списка».

Возможное значение – целое число из диапазона – 0..2147483647.

Если значение *Blacklog sessions silent* больше, чем *Max blacklog sessions*, то *Blacklog sessions silent* присваивается значение *Max blacklog sessions*. Если значение равно 0, то неаутентифицированный партнер никогда не оповещается о причинах ошибки инициированного им обмена.

Значение по умолчанию – 4.

Окно для выбора количества обменов:

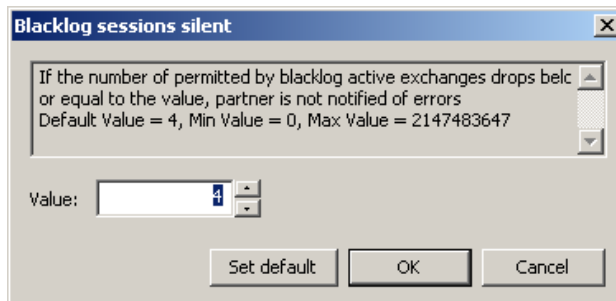


Рисунок 47

Blacklog relax time (seconds)

Устанавливает интервал времени (в секундах) релаксации "черного списка".

За указанный период времени число разрешенных одновременных IKE обменов для каждого партнера, находящегося в "черном списке", увеличивается на единицу. По истечении следующего такого же интервала времени, текущие значения разрешенных одновременно проводимых IKE обменов для каждого партнера опять увеличивается на единицу и т.д. Этот интервал времени отсчитывается с момента последней загрузки конфигурации.

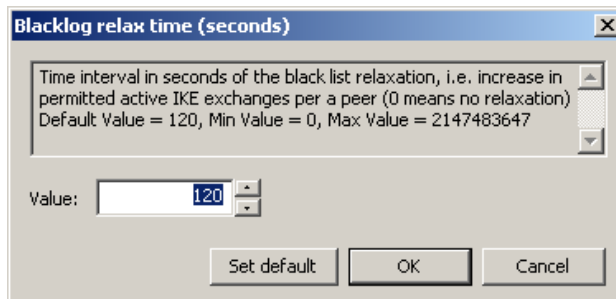
Как только текущее значение разрешенных одновременно проводимых партнером IKE обменов начинает превышать значение *Max blacklog sessions*, такой партнер исключается из "черного списка".

Возможное значение – целое число из диапазона 0..2147483647. Значение 0 означает бесконечное время релаксации "черного списка" (партнер попадает в "черный список" навсегда). Значение по умолчанию – 120 секунд.

Примечание: помимо механизма релаксации, партнер также может быть исключен из "черного списка" в следующих случаях:

- при перезапуске сервиса
- при загрузке конфигурации с отключенным "черным списком"
- при инициации IKE обмена со стороны локального VPN устройства с целью установления ISAKMP (IPsec) соединения³
- если партнеру удалось установить ISAKMP (IPsec) соединение с локальным VPN устройством, и тем самым партнер был успешно аутентифицирован.

Окно для выбора интервала времени:



³ В данном случае считается, что локальное VPN устройство потенциально доверяет партнеру, с которым оно хочет установить соединение, и информация, накопленная в "черном списке", для такого партнера сбрасывается.

Рисунок 48

Send certificate request mode

Определяет логику отсылки запроса на сертификат партнера. Возможные значения:

- *AUTO* – запрос высылается, если возможный сертификат партнера отсутствует
- *NEVER* – запрос не высылается
- *ALWAYS* – запрос высылается всегда.

Значение по умолчанию – *AUTO*.

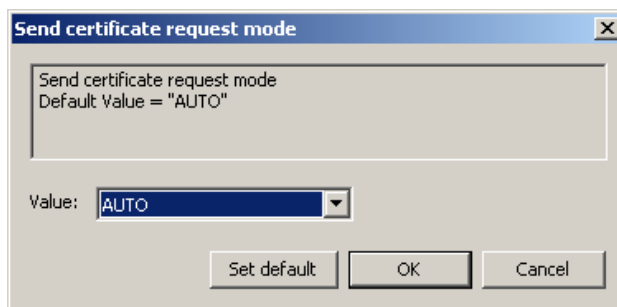


Рисунок 49

Send certificate mode

Определяет логику отсылки локального сертификата в процессе первой фазы IKE на запрос партнера. В своем запросе партнер может указать, какому CA сертификату он доверяет. Если такой сертификат не найден, то он не отправляется. Возможные значения:

- *AUTO* – автоматически определяется, когда необходима отсылка локального сертификата партнеру.
- *NEVER* – сертификат не высылается.
- *ALWAYS* – сертификат высылается всегда.
- *CHAIN* – сертификат высылается всегда, причем в составе с цепочкой доверительных CA. Имеется ввиду цепочка сертификатов, построенная от локального сертификата до CA, который удовлетворяет описанию, присланному партнером в запросе. В общем случае это CA, удовлетворяющий запросу партнера, произвольное количество промежуточных CA и локальный сертификат.

Значение по умолчанию – *AUTO*.

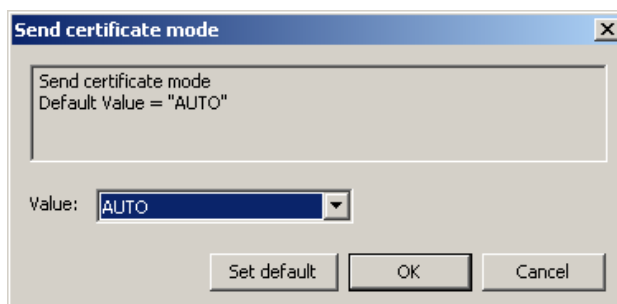


Рисунок 50

Do autopass

Задает режим автоматического пропуска ISAKMP-трафика. Возможные значения:

- *TRUE* – автоматически пропускать ISAKMP-пакеты по всем фильтрам, по которым защищается трафик.
- *FALSE* – не пропускать автоматически ISAKMP-пакеты. Правило фильтрации для пропуска ISAKMP-трафика должно быть задано явно (вручную) с действием PASS.

Значение по умолчанию – *TRUE*.

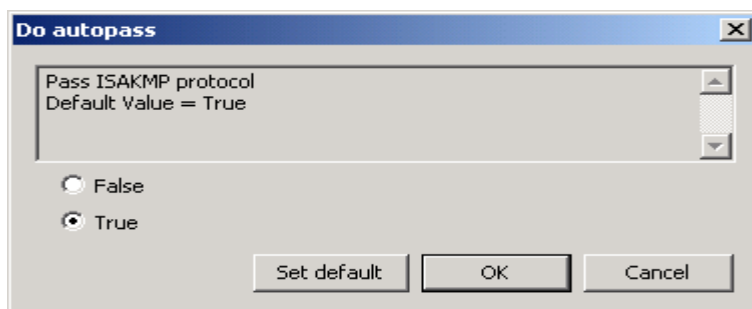


Рисунок 51

Prefer IKECFG address

Задаёт предпочитаемый запрашиваемый адрес по протоколу IKECFG при установлении соединения. Возможные значения:

- *Last used address* – запрашивается адрес, который был получен в предыдущий раз.
- *No preferred address* – предпочтений нет, запрашивается любой адрес.
- *Specific address* – запрашивается адрес, указанный в переменной *Specific IKECFG address*.

Значение по умолчанию – *Last used address*.

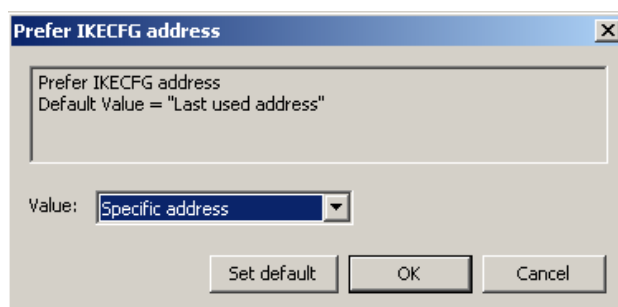


Рисунок 52

Specific IKECFG address

Задаёт адрес, который клиент предпочитает получить по протоколу IKECFG, если в переменной *Prefer IKECFG address* выбрано значение *Specific address*. Значение по умолчанию – 0.0.0.0, означает, что запрашивается произвольный адрес из пула.

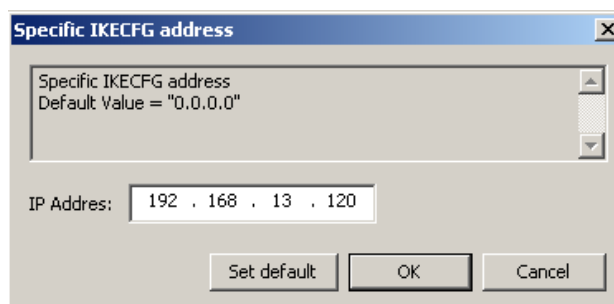


Рисунок 53

Firewall settings

SYN-SENT timeout

SYN-SENT timeout устанавливает период времени в секундах, в течение которого существует запись о TCP-соединении в состоянии SYN-SENT. Возможное значение – целое число из диапазона 1..65535. Значение по умолчанию – 30 секунд.

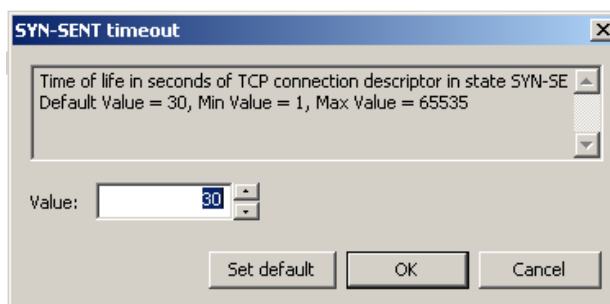


Рисунок 54

SYN-RECEIVED timeout

SYN-RECEIVED timeout устанавливает период времени в секундах, в течение которого существует запись о TCP-соединении в состоянии SYN-RECEIVED. Возможное значение – целое число из диапазона 1..65535. Значение по умолчанию – 30 секунд.

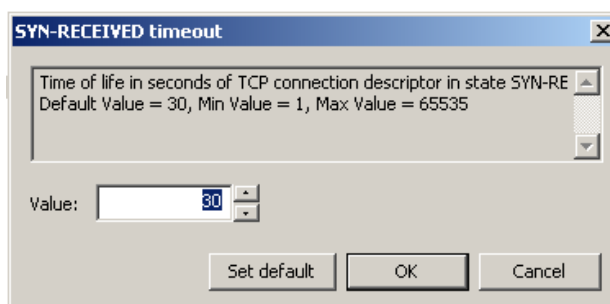


Рисунок 55

FIN timeout

FIN timeout устанавливает период времени в секундах, в течение которого существует запись о TCP-соединении в состоянии FIN-WAIT-1, CLOSE-WAIT, FIN-WAIT-2, LAST-ACK, TIME-WAIT или CLOSING. Возможное значение – целое число из диапазона 1..65535. Значение по умолчанию – 5 секунд.

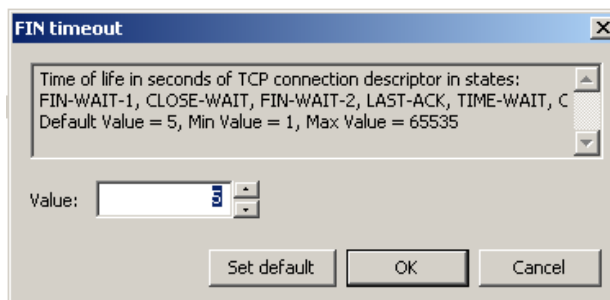


Рисунок 56

CLOSED timeout

CLOSED timeout устанавливает период времени в секундах, в течение которого существует запись о TCP-соединении в состоянии CLOSED или LISTEN. Возможное значение – целое число из диапазона 1..65535. Значение по умолчанию – 30 секунд.

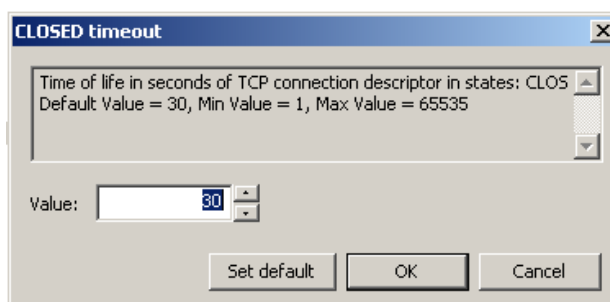


Рисунок 57

ESTABLISHED timeout

ESTABLISHED timeout устанавливает период времени в секундах, в течение которого существует запись о TCP-соединении в состоянии *ESTABLISHED*. Возможное значение – целое число из диапазона 1..65535. Значение по умолчанию – 3600 секунд

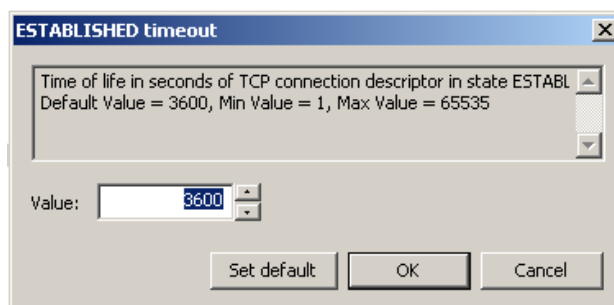


Рисунок 58

Maximum number of half open connections

Maximum number of half open connections устанавливает максимальное количество одновременно существующих полуоткрытых TCP-соединений (запросов соединения, оставшихся без ответов, или недостроенных соединений, не успевших перейти в установленное состояние). Когда количество полуоткрытых соединений превысит максимальное количество и как только появится новый запрос на соединение, одно полуоткрытое соединение будет удалено. Удаление будет происходить до тех пор, пока число полуоткрытых соединений не станет меньше значения *Lower bound of half open connections*. Далее вновь допускается увеличение TCP-соединений.

Возможное значение – целое число из диапазона 0..1000000. Значение по умолчанию – 500 полуоткрытых сеансов.

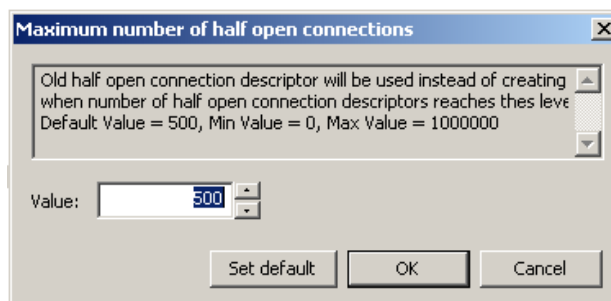


Рисунок 59

Lower bound of half open connections

Lower bound of half open connections устанавливает минимальное количество одновременно существующих полуоткрытых TCP-соединений (запросов соединения, оставшихся без ответов, или недостроенных соединений), по достижении которого прекращается их удаление. Возможное значение – целое число из диапазона 0..1000000. Значение по умолчанию – 400 полуоткрытых сеансов.

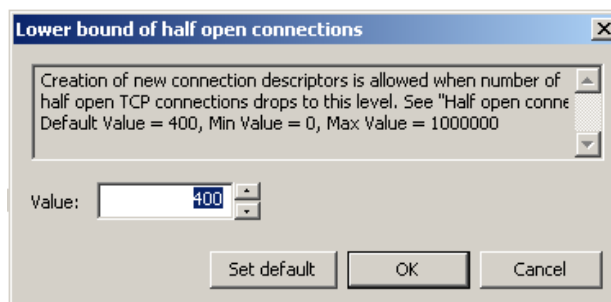


Рисунок 60

Maximum of new TCP connections rate

Maximum of new TCP connections rate устанавливает количество новых контекстов соединений, создаваемых в минуту, по достижении которого начинается их удаление, чтобы принимать новые запросы на соединение. Удаление будет продолжаться до тех пор, пока частота появления не будет совпадать с частотой, установленной переменной *Lower bound of TCP connections rate*. Возможное значение – целое число из диапазона 0..2147483647. Значение по умолчанию – 500 полуоткрытых сеансов в минуту.

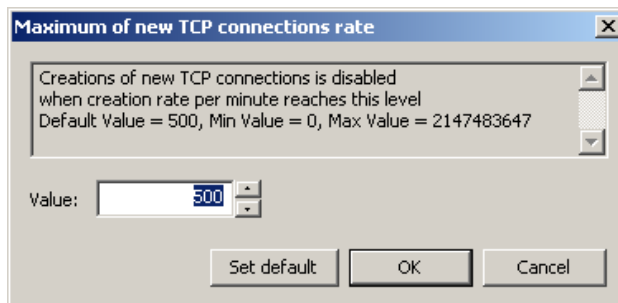


Рисунок 61

Lower bound of TCP connections rate

Lower bound of TCP connections rate устанавливает количество новых контекстов соединений, создаваемых в минуту, по достижении которого прекращается их удаление. Возможное значение – целое число из диапазона 0..2147483647. Значение по умолчанию – 400 полуоткрытых сеансов в минуту.

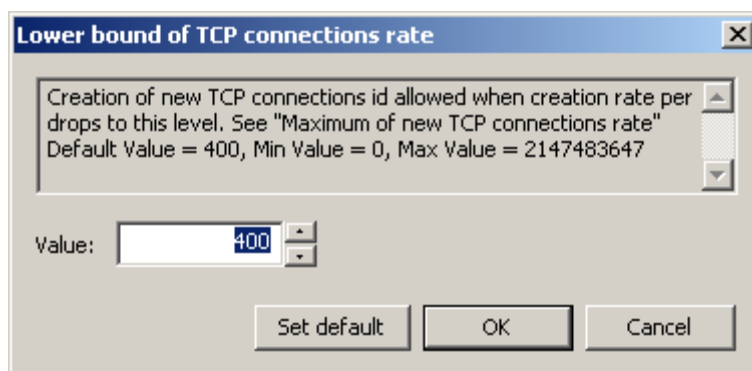


Рисунок 62

Maximum number of TCP connections

Maximum number of TCP connections устанавливает максимальное разрешенное количество TCP-соединений. При превышении данного предела новые TCP-соединения будут отвергаться. Возможное значение – целое число из диапазона 0..1000000. Значение по умолчанию – 65536.

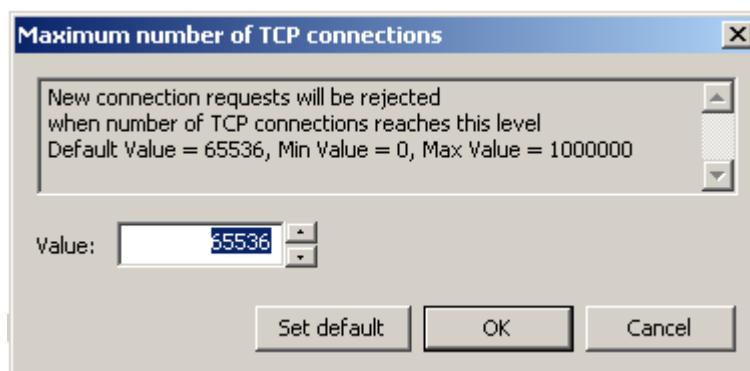


Рисунок 63

Strictness level

Strictness level задает уровень строгости обработки различных ошибочных ситуаций. В Таблица 5 приведены основные отличия в поведении при различных значениях *Strictness Level*. Возможное значение – целое число из диапазона 0..6. Значение по умолчанию – 3.

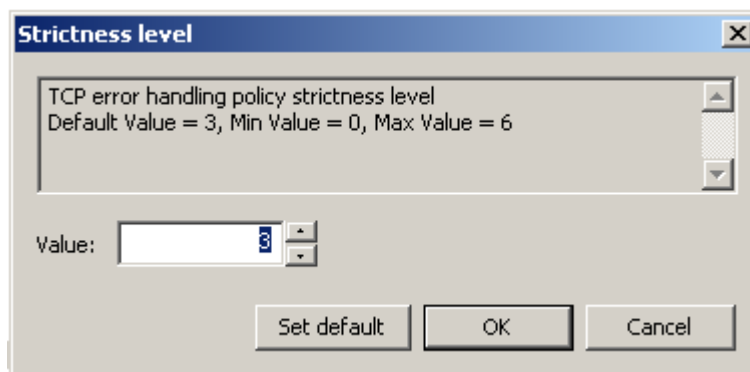


Рисунок 64

Таблица 5

Значение Strictness Level	Условие, при котором пакет уничтожается	Условие, при котором состояние соединения ⁴ не изменяется
0	Пакеты не уничтожаются firewall	При некорректном TCP заголовке (проверяется соответствие длины пакета, TCP заголовка, контрольной суммы)
1	При некорректном TCP заголовке	При некорректном TCP заголовке
2	При некорректном TCP заголовке	При некорректном TCP заголовке или при sequence, несоответствующем состоянию партнера
3	При некорректном TCP заголовке	При некорректном TCP заголовке или при несоответствии флагов заголовка состоянию партнера
4	При некорректном TCP заголовке или при несоответствии флагов заголовка состоянию партнера	При некорректном TCP заголовке или при несоответствии флагов заголовка состоянию партнера

⁴ Например, не пролонгируется существование записи о соединении.

Значение Strictness Level	Условие, при котором пакет уничтожается	Условие, при котором состояние соединения ⁴ не изменяется
5	При некорректном TCP заголовке или при sequence, несоответствующем состоянию партнера	При некорректном TCP заголовке или при несоответствии флагов заголовка состоянию партнера
6	При некорректном TCP заголовке или при приеме SYN для установившегося соединения	При некорректном TCP заголовке или при несоответствии флагов заголовка состоянию партнера, или при получении первым не SYN-пакета, или при приеме SYN-пакета для установившегося соединения.

LDAP settings

Server address

Задаваемые здесь параметры LDAP-сервера используются тогда, когда сертификат, для которого производится проверка подписи, не содержит расширение CDP (CRL Distribution Point) с адресом LDAP-сервера либо в этом поле прописанный путь к LDAP-серверу является неполным, и тогда добавляются данные из этой структуры.

В окне *Server address* задаются параметры LDAP-сервера. Возможные значения:

- LDAP-сервер не используется, когда флажок Use default LDAP Server не установлен.
- LDAP-сервер используется, когда флажок Use default LDAP Server установлен. При необходимости будет производиться поиск сертификатов и CRLs на заданном LDAP сервере. При этом нужно заполнить поля:
 - IP Address – сетевой адрес LDAP-сервера.
 - Port – сетевой порт LDAP-сервера, на который будут посылаться LDAP запросы. Значение по умолчанию – 389.
 - Search base – имя (Distinguished Name, DN) корневого X.500-объекта, в поддереве которого производится поиск сертификатов и CRL на LDAP-сервере. Если DN сертификата и DN X.500-объекта не совпадают, и если DN сертификата является частью имени DN X.500-объекта, то заполняется поле Searchbase, чтобы дополнить запрос, созданный на основе имени из сертификата или CRL, для нахождения соответствующего X.500-объекта. Для запроса на основе URL данное имя не используется. См. Пример в структуре LDAPSettings.
- Pass LDAP protocol with the LDAP Server – при установке этого флажка производится автоматическое создание сетевого фильтра для пропуска пакетов между агентом и LDAP-сервером.

Значение по умолчанию – LDAP-сервер не используется.

Сначала делается попытка установить соединение по LDAP версии 2. Если эта попытка завершается с ошибкой LDAP_PROTOCOL_ERROR (наиболее вероятная причина – не поддерживается версия 2), то повторяется попытка установить соединение по LDAP версии 3.

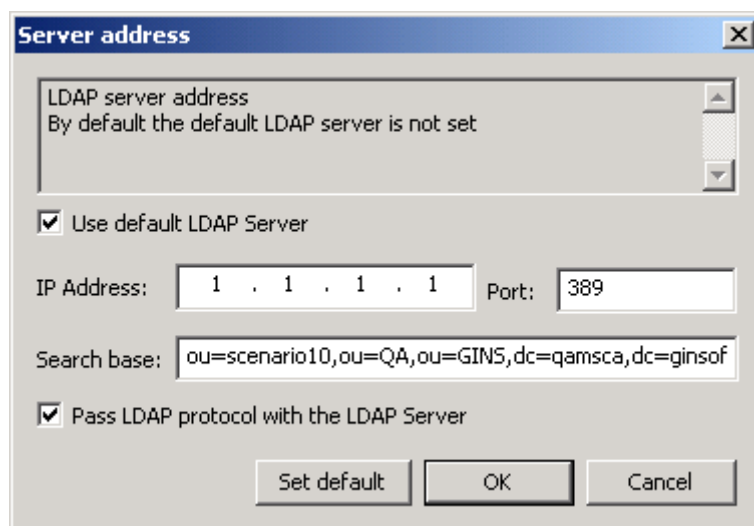


Рисунок 65

Connect timeout

Connect timeout позволяет ограничить время (в секундах) создания TCP-соединения с LDAP-сервером. Возможное значение – целое число из диапазона 1..6000. Значение по умолчанию – 0, которое означает, что время создания TCP-соединения с LDAP-сервером ограничивается установленным для ОС временем создания TCP-соединения.

Примечание: Если в момент обращения к LDAP-серверу устройство, на котором он установлен, недоступно, то процесс создания TCP-соединения может занимать продолжительное время (до 3 минут, зависит от ОС). По этой причине могут наблюдаться внешние признаки зависания агента, и это может служить причиной неудачной попытки создания соединения.

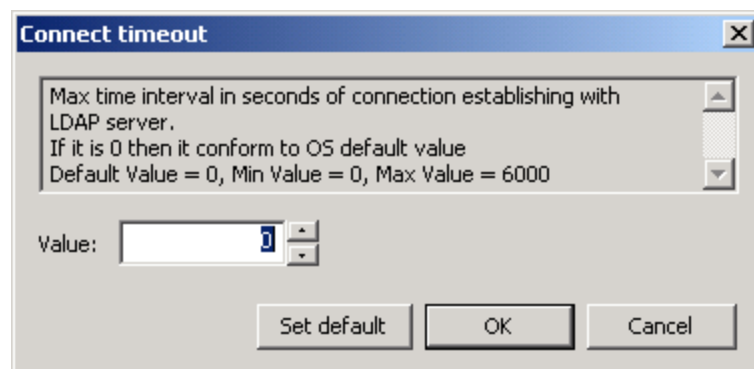


Рисунок 66

Response timeout

Поиск посредством протокола LDAP может занимать достаточно продолжительное время, оно зависит от многих факторов, в том числе от масштаба запроса и характеристик канала передачи данных. Response timeout позволяет ограничить время (в секундах), в течение которого ожидается ответ от LDAP-сервера на единичный запрос. Возможное значение – целое число из диапазона 2..6000. Значение по умолчанию – 200.

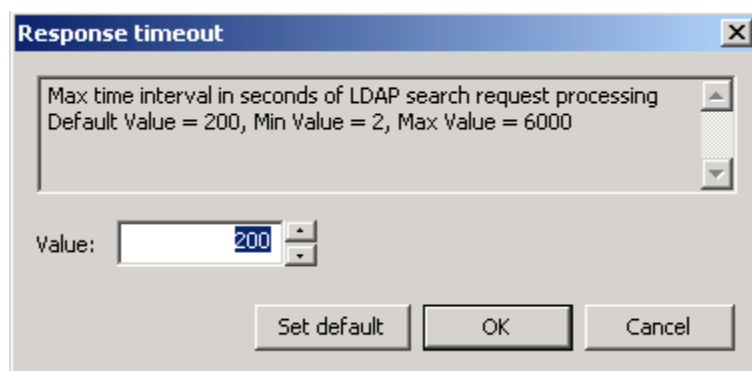


Рисунок 67

Hold connection timeout

Hold connection timeout устанавливает период времени, в течение которого держится установленное соединение к серверу на случай, если придет к нему повторный запрос. Возможное значение – целое число из диапазона 0..6000.

При значении 0 после обмена с LDAP-сервером соединение с ним сразу закрывается.

Не рекомендуется выставлять значение в 1 секунду в виду наличия погрешности в 1 секунду, поскольку это может привести в некоторых случаях к немедленному закрытию соединения и к избыточному открытию нового соединения.

Значение по умолчанию – 60.

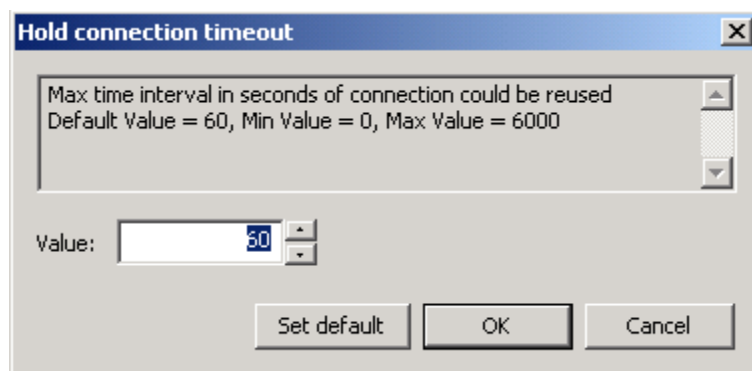


Рисунок 68

Drop connection timeout

Атрибут *Drop connection timeout* устанавливает период времени, начиная с первой неудачной попытки создания соединения с LDAP-сервером, в течение которого новые попытки создания соединения с ним игнорируются. Возможное значение – целое число из диапазона 0..6000.

При значении 0 в случае неудачной попытки установления соединения с LDAP-сервером новые попытки не игнорируются.

Не рекомендуется выставлять значение в 1 секунду в виду наличия погрешности в одну секунду, поскольку это может привести в некоторых случаях к избыточным попыткам создания соединения.

Значение по умолчанию – 5.

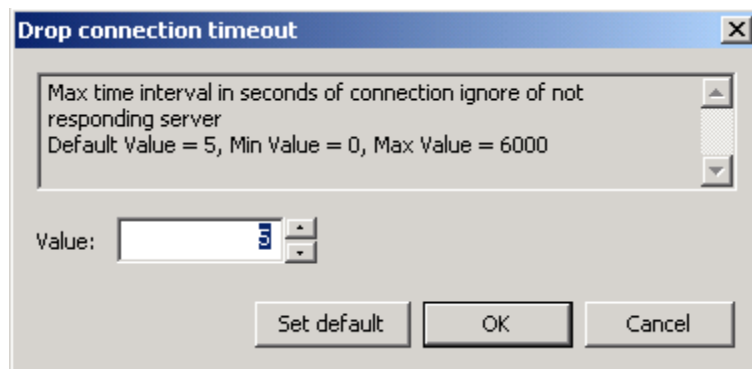


Рисунок 69

SNMP settings

SNMP polling

Задаёт настройки по выдаче информации по запросу SNMP-менеджера. Возможные значения:

- не принимаются и не обрабатываются запросы на выдачу SNMP статистики
- принимаются и обрабатываются запросы на выдачу SNMP статистики.

Значение по умолчанию – SNMP статистика не выдается.

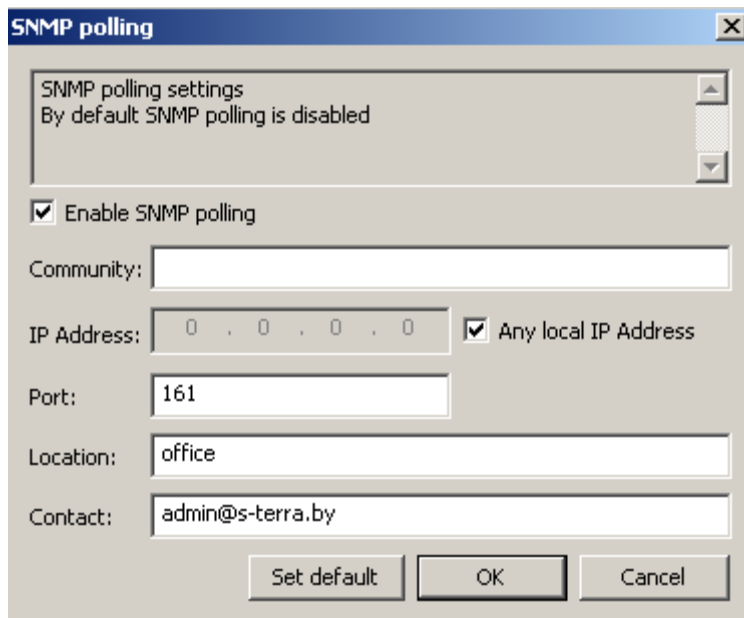


Рисунок 70

- *Enable SNMP polling* – при установке этого флажка задаются настройки для принятия запроса и выдачи статистики.
- *Community* – эта строка действует подобно паролю и разрешает доступ к чтению статистики SNMP-менеджеру.
- *IP Address* – локальный IPv4-адрес, на который можно получать запросы от SNMP-менеджера.
- *Any local IP Address* – установка этого флажка разрешает получение запроса от SNMP-менеджера на любой локальный IP-адрес.
- *Port* – задаёт порт, на который можно получать SNMP-запросы.
- *Location* – информация о физическом расположении SNMP-агента.
- *Contact* – информация о контактном лице, ответственном за работу SNMP-агента.

Trap receiver

Задаёт настройки получателя SNMP-трапов и дополнительные настройки для трапов, отсылаемых на него. Возможные значения:

- получатель SNMP-трапов не задан,
- получатель SNMP-трапов задан.

Значение по умолчанию – получатель SNMP-трапов не задан.

Можно задать до трех получателей SNMP-трапов.

- *Enable the trap receiver* – при установке этого флажка задаются настройки получателя SNMP-трапов.

- *Community* – текстовая строка, играющая роль идентификатора отправителя трап-сообщения.
- *Receiver's IP Address* – IP-адрес получателя SNMP-трапов.
- *Receiver's Port* – UDP-порт, на который менеджеру будут высылаться трап-сообщения.
- *SNMP Version* – версия SNMP, в которой формируются трап-сообщения.
- *Agent's IP Address* – IP-адрес отправителя трап-сообщения. Этот атрибут указывается только для Version = V1.

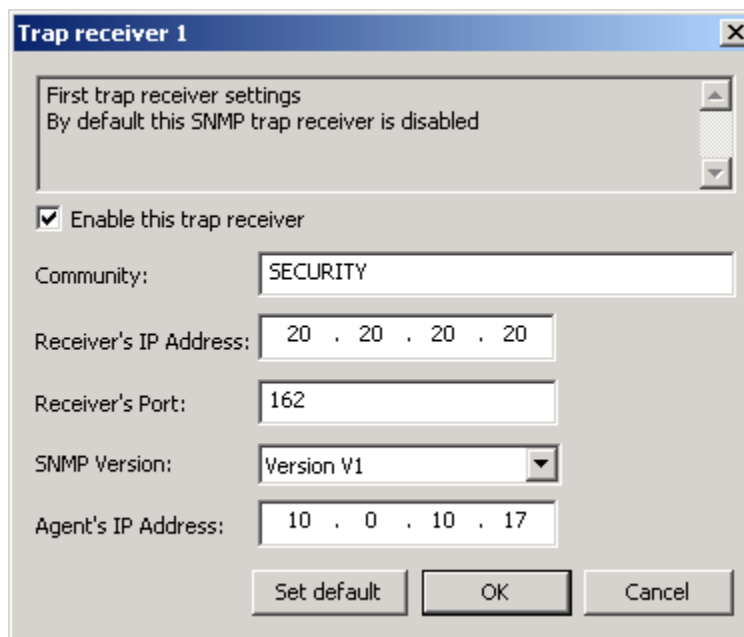


Рисунок 71

DPD settings

Use DPD

Задаёт режим использования протокола DPD (Dead-Peer-Detection). Возможные значения:

- *TRUE* – использовать протокол DPD.
- *FALSE* – не использовать протокол DPD. В этом случае другие переменные этого раздела не появляются.

Значение по умолчанию – *TRUE*.

Окно для установки переключателя:

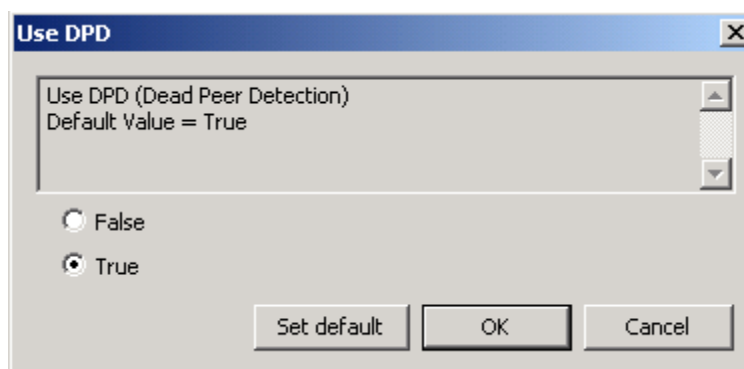


Рисунок 72

Idle duration (seconds)

Интервал времени отсутствия входящего трафика от партнера, по истечению которого, при наличии исходящего трафика, активируется DPD-сессия. Возможные значения – целое число из диапазона 1..32762. Значение по умолчанию – 60. Окно для установки значения:

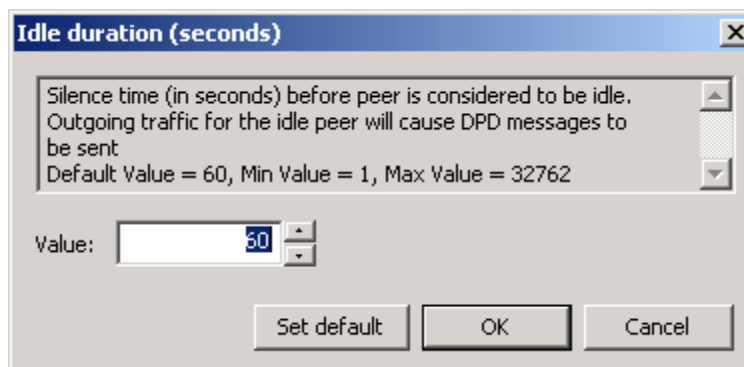


Рисунок 73

Response duration

Время ожидания ответа от партнера на DPD-запрос в секундах. Возможные значения – целое число из диапазона 1..300. Значение по умолчанию – 5. Окно для выбора значения:

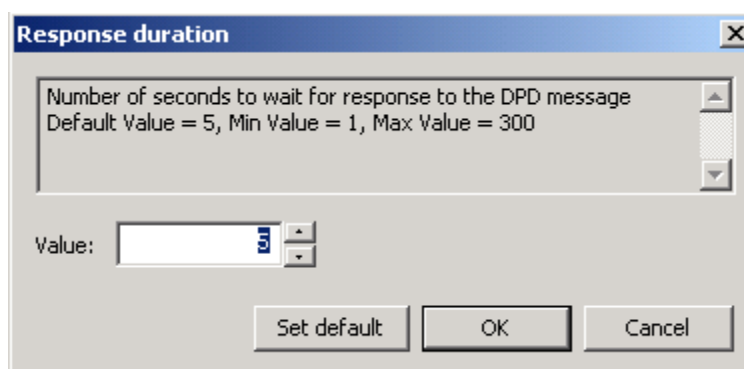


Рисунок 74

Retries

Количество попыток провести DPD-обмен. Если все попытки закончились неудачей, защищенное соединение (IKE-контекст) считается "мертвым", и производится попытка создать его заново. Возможные значения – целое число из диапазона 1..10. Значение по умолчанию – 3. Окно для выбора значения:

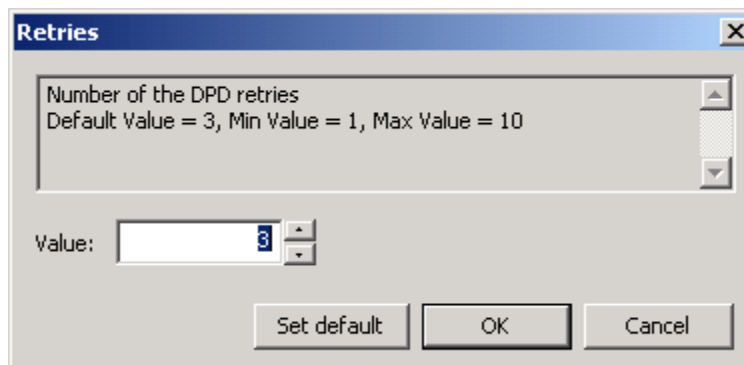


Рисунок 75

7.4.5.3 Режим ручного задания LSP

В режиме ручного задания локальная политика безопасности задается администратором (вкладки **Firewall Rules**, **IPsec Rules**, **IKE** и **IPsec** становятся невидимыми) (Рисунок 76).

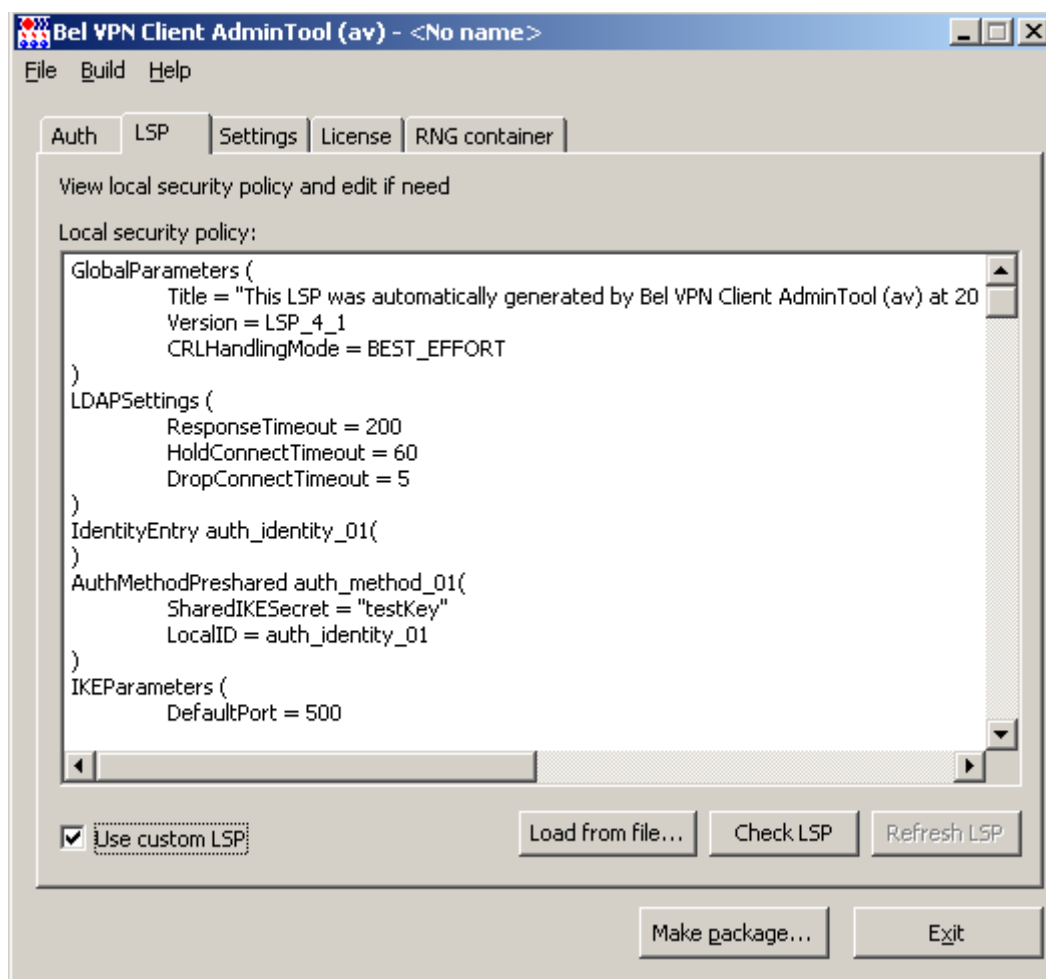


Рисунок 76

Local security policy – поле с текстовым представлением локальной политики безопасности. В этом поле можно создавать и редактировать LSP.

Use custom LSP – снятие этого флажка переводит в режим автоматического формирования LSP.

Load from file – при нажатии этой кнопки происходит загрузка LSP из файла и отображение в поле Local security policy.

Check LSP – при нажатии этой кнопки происходит проверка заданной LSP по выявлению синтаксических ошибок. При обнаружении ошибки выдается сообщение с описанием ошибки (если строка с ошибочными символами определена, то она выделяется и на эту строку автоматически переводится фокус). Если данная LSP не содержит синтаксических ошибок, то выдается сообщение, что синтаксических ошибок не найдено.

7.4.6 Вкладка Settings

Во вкладке **Settings** задаются настройки протоколирования событий, политика по умолчанию и дополнительные параметры инсталляции Продукта Bel VPN Client.

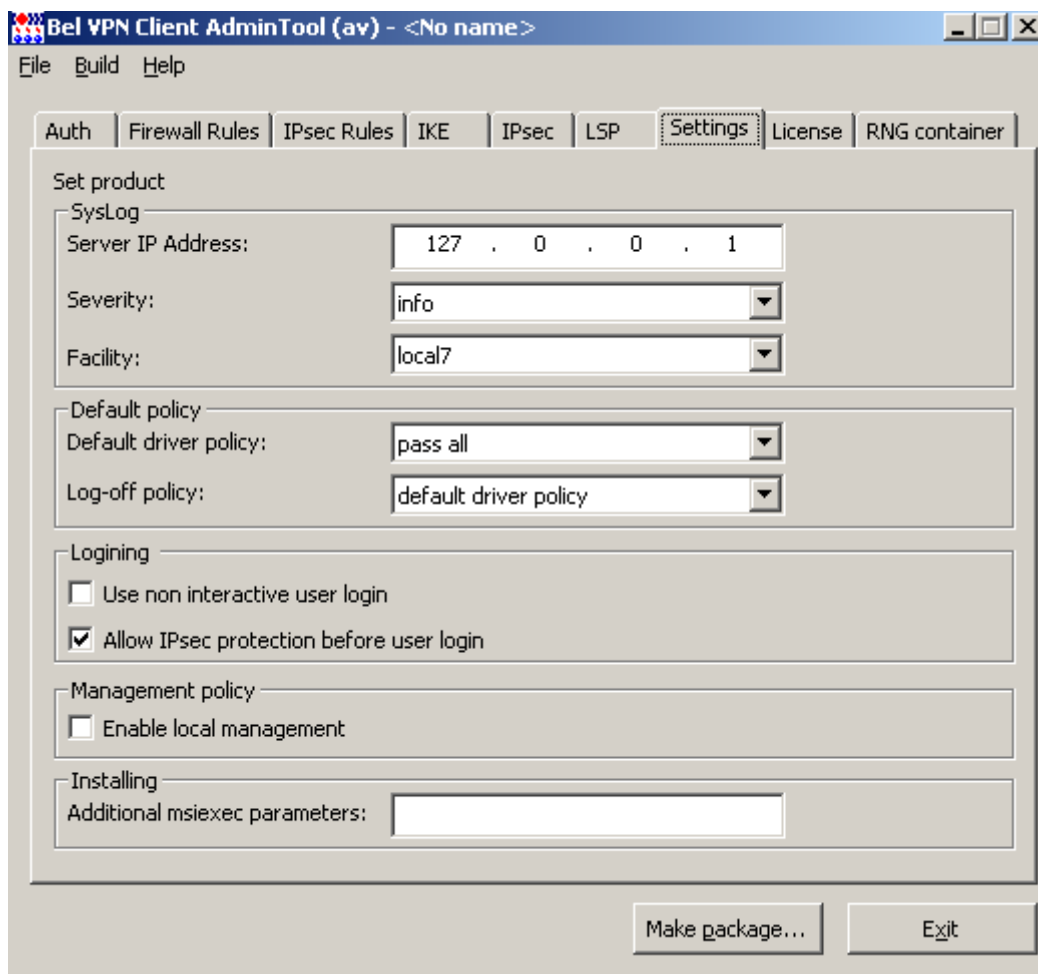


Рисунок 77

Для задания настроек Syslog-клиента заполняются следующие поля:

- **Server IP-Address** – IP-адрес компьютера, на который будут посылаться сообщения о протоколируемых событиях. Значение по умолчанию – *127.0.0.1* означает, что сообщения посылаются на локальный хост.
- **Severity** – задание общего уровня протоколирования. Содержит выпадающий список значений – *emerg, alert, crit, err, warning, notice, info, debug*. Значение по умолчанию – *info*.
- **Facility** – задание источника сообщений. Значение по умолчанию – *local7*.

Default Driver Policy (DDP) – политика драйвера по умолчанию. Выпадающий список содержит значения:

- *pass all* – пропускать все пакеты. Значение по умолчанию.
- *pass dhcp* – пропускать пакеты только по протоколу DHCP. Т.е. будут уничтожаться все пакеты, кроме исходящих UDP-пакетов на порт 67 и входящих UDP-пакетов на порт 68.
- *drop all* – не пропускать трафик.

Политика DDP, которая задается администратором, загружается в следующих случаях:

- при ошибке загрузки конфигурации,
- до старта VPN Service,

- при остановке VPN Service.

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

- *default driver policy (DDP)* – политика драйвера по умолчанию
- *pass dhcp* – пропускать пакеты только по протоколу DHCP. Будут уничтожаться все пакеты, кроме исходящих UDP-пакетов на порт 67 и входящих UDP-пакетов на порт 68.

Политика Log-off policy загружается автоматически в следующих случаях:

- до тех пор, пока пользователь не ввел свой пароль,
- при вводе неверного пароля три раза,
- при отказе от регистрации (login), если нажать кнопку *Cancel*,
- при выходе пользователя из системы,
- при смене пользователя,
- если при загрузке конфигурации обнаружены ошибки (если была ранее загружена Log-off policy).

Use non interactive user login – при установке этого флажка Bel VPN Client-P будет использовать неинтерактивный режим логина, а при снятии – интерактивный режим логина:

- Неинтерактивный режим – при входе пользователя в систему производится попытка логина в продукт Bel VPN Client-P с пустым паролем (в качестве пароля используется пустая строка). При таком успешном логине окно с запросом пароля не выводится. При неуспешном логине – Продукт ведет себя как при интерактивном режиме.
- Интерактивный режим – выдается окно запроса пароля для регистрации в Продукте Bel VPN Client-P. Этот режим используется по умолчанию.

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

Allow IPsec protection before user login – установка флажка включает функциональность по защите до логина в ОС. По умолчанию защита включена. (Включить и отключить эту опцию можно и для установленного Продукта. Для этого в "Установка и удаление программ" для Продукта выбрать "Изменить". Далее "Modify". Затем установить соответствующую функцию для "Login Protection".)

Enable local management – при установке этого флажка включается возможность изменять настройки Продукта конечным пользователем. По умолчанию эта возможность отключена (пользователь может менять только пароль, уровень логирования, добавлять CRL и сертификаты партнеров, перезагружать локальную политику безопасности).

Additional msiexec parameters – в этом поле можно установить дополнительные параметры запуска WinInstaller.

Например, альтернативный каталог, в который будет установлен Продукт, настройки лога Windows Installer и т.п. Эти параметры можно посмотреть по ссылке http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp

/I* C:\Client\install_log_file.txt - протоколирование событий в файл C:\Client\install_log_file.txt при инсталляции Bel VPN Client-P (рекомендуется при режиме silent).

INSTALLDIR=каталог установки продукта – переопределение каталога. Указание каталога, недоступного на компьютере пользователя, приведет к ошибке инсталляции.

Можно часть текста заключить в символы % (процент) и она будет рассматриваться как имя переменной окружения. И эта часть текста будет заменяться на значение переменной окружения (значения переменных окружения можно просмотреть командой set). Если переменная окружения отсутствует, в командке остается исходный текст.

Поддерживается специальная переменная окружения SfxDir – полный путь к папке, в которую распакованы данные. Таким образом, последовательность символов %SfxDir% заменяется на полный путь к папке, в которую распакованы данные.

REBOOT=F – обязательно запрашивать перезагрузку системы в конце инсталляции, даже если он не инициируется инсталлятором.

REBOOT=S – отключить запрос на перезагрузку системы в конце инсталляции. Не блокировать рестарт в случае ForceReboot action.

REBOOT=R – полностью отключить все запросы на перезагрузку системы, включая ForceReboot action. Используется для установки нескольких продуктов и/или выполнения дополнительных действий после инсталляции. После этого перезапустить систему вручную или с помощью сторонних инструментальных средств.

MAX_SERVICE_START_TIMEOUT=... – время (в секундах) ожидания старта VPN сервиса (vpnsvc). Максимальное значение – 600 секунд. Значение по умолчанию – 30. Можно использовать для предотвращения появления сообщений об ошибке связи с сервисом на этапе логина для медленных и/или находящихся под сильной нагрузкой систем

AGENT_DB_REMOVE=1 – автоматически (без дополнительных запросов) будет удаляться база локальных настроек при установке или при удалении продукта. Рекомендуется использовать для режима инсталляции silent

AGENT_DB_REMOVE=0 – база локальных настроек удаляться не будет, запросы пользователю выдаваться не будут. По умолчанию (параметр пустой) - пользователю выдается запрос на удаление базы локальных настроек.

DISABLE_ANTIVIRUS_WARNING=1 – при инсталляции не будет показываться предупреждение [25036](#) (о необходимости отключения антивирусных программ).

Примечание: пользователь должен знать о необходимости отключения антивируса, иначе данный параметр использовать не следует.

REBOOT_REQUIRED=1 – принудительно инициировать запрос на рестарт системы в конце инсталляции. Параметр обычно выставляется автоматически (при необходимости).

DISABLE_CALL_LOGIN=1 – в конце инсталляции логин не запустится. Устанавливать параметр имеет смысл только для интерактивного логина (NON_INTERACTIVE_LOGIN=0) на Windows Vista и более поздних версиях.

7.4.7 Вкладка License

Во вкладке **License** задаются регистрационные данные Лицензии на Продукт Bel VPN Client-P:

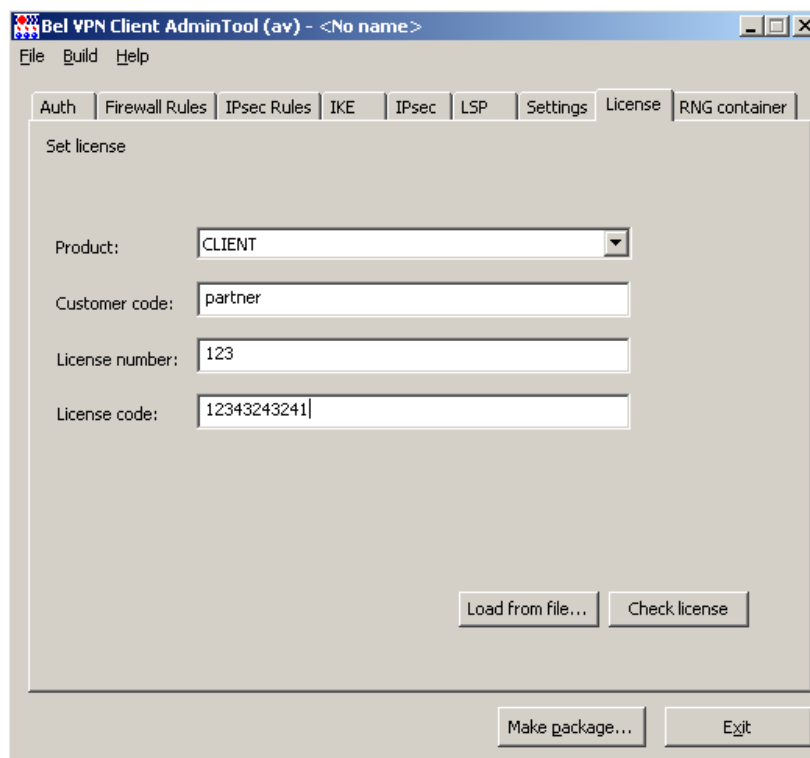


Рисунок 788

Данные Лицензии:

- **Product** – поле для задания типа Продукта
- **Customer code** – код пользователя
- **License number** – номер лицензии
- **License code** – код лицензии.

Кнопки управления:

- **Load from file** – при нажатии этой кнопки происходит загрузка данных Лицензии из указанного текстового файла. В файле данные Лицензии должны быть записаны в виде:

```
[license]
CustomerCode=NNNN
ProductCode=CLIENTB/CLIENT
LicenseNumber=NNNN
LicenseCode=NNNNNNN
```

- **Check License** – проверка правильности введенных данных Лицензии.

7.4.8 Задание сертификатов партнеров

Сертификат партнера можно получить либо по протоколу IKE, либо по протоколу LDAP при создании IKE соединения.

Сначала шлюз безопасности пытается получить сертификат партнера по IKE. Если партнер не прислал сертификат, а прислал свой идентификатор, то шлюз безопасности по этому идентификатору ищет сертификат партнера сначала в своей базе Продукта, если не нашел, то продолжает поиск на LDAP-сервере.

Но не всегда удается получить сертификаты от удаленных партнеров: могут быть проблемы, связанные с фрагментацией UDP пакетов.

Поэтому появилась возможность положить в базу Продукта Bel VPN Client-P имеющиеся сертификаты партнеров.

В меню GUI выберите раздел **File**, а затем предложение **Advanced Project Settings**. В одноименном окне (Рисунок 79) с одной вкладкой *Partner certificates* создайте список сертификатов ваших партнеров. Сертификаты партнеров будут актуальны только при аутентификации с использованием сертификатов.

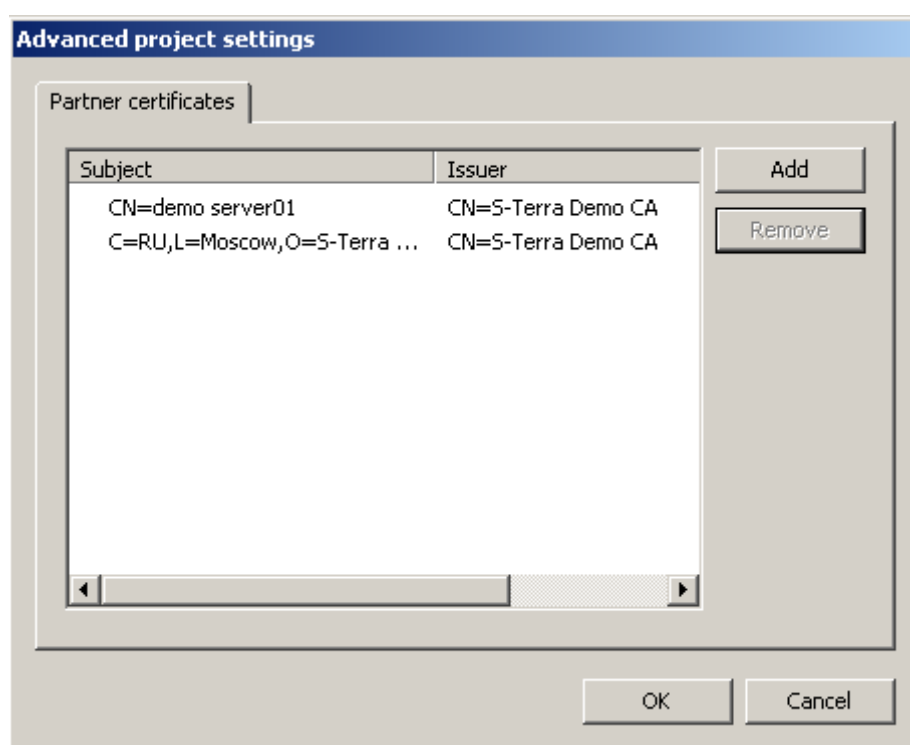


Рисунок 79

Кнопки управления:

- **Add** – добавляет сертификат партнера в список, при этом появляется стандартное окно открытия файла.
- **Remove** – удаляет выделенный сертификат партнера из списка.

Если добавление сертификата происходит из контейнера формата PKCS#12 (.pfx), в котором размещено более одного сертификата, появляется окно для выбора сертификата для добавления в список (**Ошибка! Источник ссылки не найден.**63):

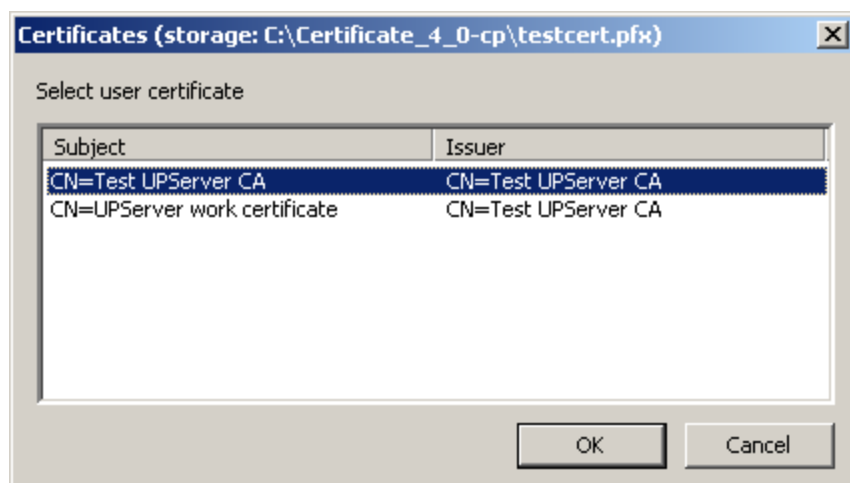


Рисунок 80

Добавление сертификата в список может быть неуспешным с выводом соответствующих сообщений по следующим причинам:

- прочитанные данные не являются корректным сертификатом: «Certificate storage <путь к файлу> is incorrect»;
- список уже содержит такой сертификат, при этом пути к файлам могут быть разными (сравниваются сами сертификаты): «This certificate already in list Subject: <subject сертификата> Issuer: <issuer сертификата>».

В случае, когда некорректные данные прочитаны из файла проекта (созданного в Bel VPN Client Admintool версии 3.0 или 3.0.1 и если были отредактированы вручную ссылки на сертификаты), выполняется проверка дублирования сертификатов в списке, отображаемых в окне (Рисунок 81). Напротив проблемной строки отображается восклицательный знак красного цвета, таким образом помечаются второй и последующие одинаковые сертификаты.

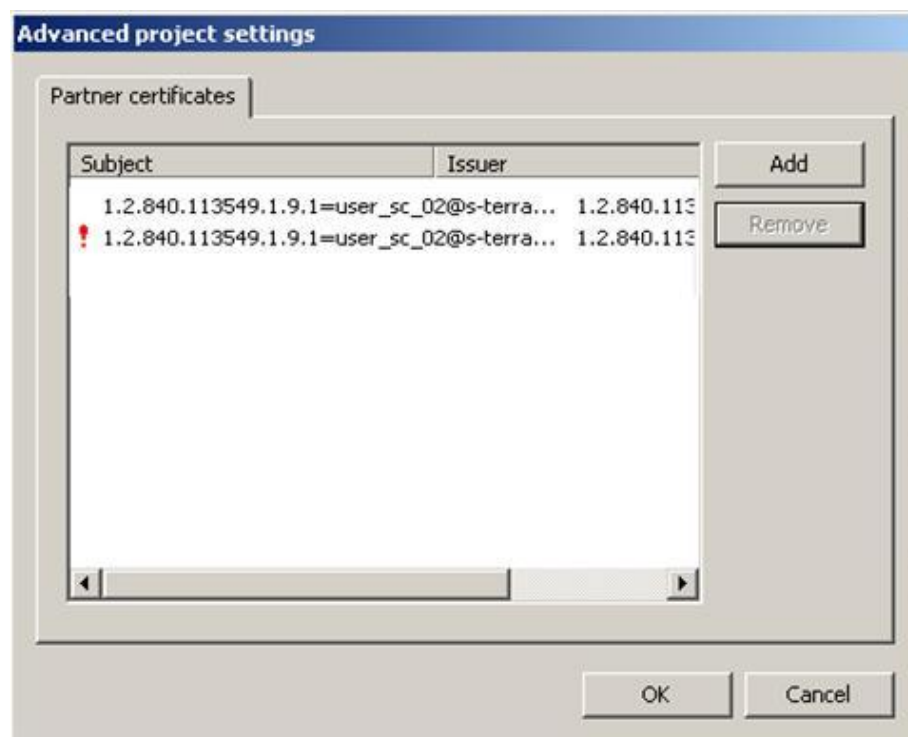


Рисунок 81

7.4.9 Создание инсталляционного файла

Создание инсталляционного файла Bel VPN Client происходит при нажатии кнопки **Make package** в главной форме. При этом происходит проверка корректности введенных данных и при обнаружении ошибки выводится сообщение о возможных причинах, и переключение на вкладку с некорректными данными. Если ошибки не обнаружено, то появляется окно **Package parameters** (Рисунок 82).

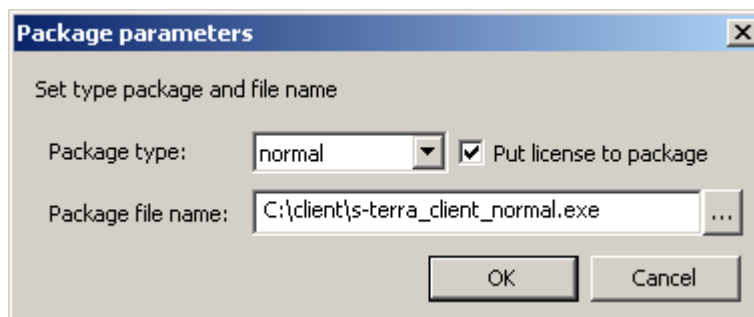


Рисунок 82

В этом окне необходимо задать:

- **Package type** – поле для выбора режима инсталляции. Возможные значения:
 - *basic* – неинтерактивная установка с запросом на инсталляцию. Вариант по умолчанию,
 - *normal* – интерактивная установка (в диалоговом режиме) с демонстрацией Лицензионного Соглашения и другими окнами,
 - *silent* – неинтерактивная установка без запросов.
- **Package file name** – поле для ввода имени инсталляционного файла на компьютере администратора.
- **Put license to package** – при установке этого флажка введенные данные Лицензии будут включены в инсталляционный файл. При этом вкладка **License** должна содержать корректные данные Лицензии.

При нажатии кнопки **OK** вызывается утилита `make_inst.exe` с соответствующими опциями, которая и создает инсталляционный файл. На время работы утилиты появляется окно с просьбой подождать (Рисунок 83):

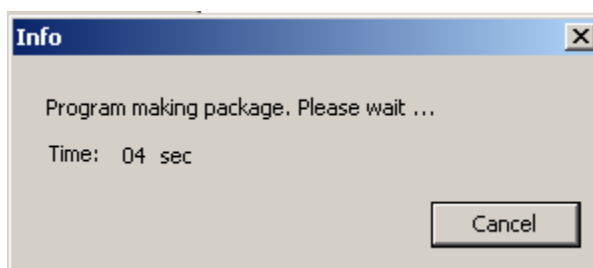


Рисунок 83

В случае выявления ошибки выдается сообщение о коде ошибки.

При нажатии на кнопку **Cancel** работа утилиты `make_inst.exe` прерывается (инсталляционный файл не создается). В случае успешного завершения работы утилиты выдается сообщение о создании инсталляционного файла:

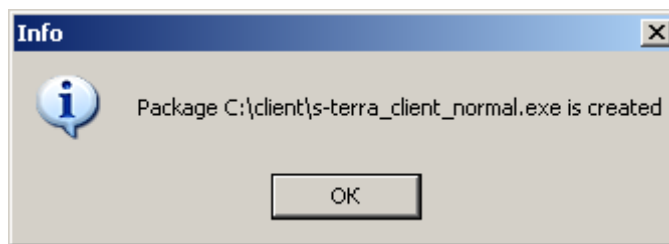


Рисунок 844

Все сообщения, выдаваемые программой утилитой make_inst в процессе ее работы, выводятся в файл make_inst_log.txt (при каждом создании инсталляционного файла make_inst_log.txt переписывается).

7.4.10 Сохранение данных проекта

В процессе сохранения проекта – Save Project as (Save Project) – сохраняются данные тех вкладок, которые на данный момент являются активными. Данные вкладок, которые являются невидимыми, не сохраняются. Исключение составляет ситуация: при переключении на ручное задание LSP (вкладка **LSP**, выставлен флажок *Use custom LSP*) данные вкладок **Firewall Rules**, **IPsec Rules**, **IKE** и **IPsec** сохраняются в проекте, не смотря на то, что после переключения эти вкладки являются неактивными и не показываются пользователю. При повторном открытии сохраненного проекта, при переходе к режиму автоматического формирования LSP (снятие флажка *Use custom LSP*), все введенные ранее пользователем данные во вкладках **Firewall Rules**, **IPsec Rules**, **IKE** и **IPsec** будут доступны для дальнейшего редактирования. Данная особенность реализована для облегчения редактирования LSP при ее автоматическом формировании.

7.5 Режим совместимости с Bel VPN 3.0.1

7.6 Формат задания имен алгоритмов в файле admintool.ini

Имена алгоритмов, используемые во вкладках **IKE**, **IPsec** и **LSP**, задаются в файле admintool.ini в секция [algorithm_set ...]:

```
[algorithm_set_0]
region=international
label=International algorithms

ike-hash=SHA1 (SHA1)
ike-cipher=AES-K256-CBC (AES-256)
ah-integrity=SHA1-H96-HMAC (SHA1)
esp-integrity=SHA1-H96-HMAC (SHA1)
esp-cipher=AES-K256-CBC (AES-256)
oakley-group1=MODP_768
oakley-group2=MODP_1024
oakley-group3=MODP_1536

[algorithm_set_1]
region=gost
label=3.0.1 compatible algorithms

ike-hash=STB1176199-65530 (СТБ 1176.1-99)
```

```
ike-cipher=G2814789AV1-K256-CBC-65530 (ГОСТ 28147-89)
ah-integrity1=STB1176199-H96-HMAC-250 (СТБ 1176.1-99)
ah-integrity2=G2814789AV1-K256-MAC-251 (ГОСТ 28147-89)
esp-integrity1=STB1176199-H96-HMAC-65530 (СТБ 1176.1-99)
esp-integrity2=G2814789AV1-K256-MAC-65531 (ГОСТ 28147-89)
esp-cipher1=G2814789AV1-K256-CBC-250 (ГОСТ 28147-89)
oakley-group1=MODP_768
oakley-group2=MODP_1024
oakley-group3=MODP_1536

[algorithm_set_2]
region=gost
label=Recommended for 4.1 algorithms

ike-hash=STB34101HASH-65532 (СТБ 34.101.31-2011 (6.9) HMAC)
ike-cipher=STB34101CIPH-K256-CBC-65532 (СТБ 34.101.31-2011 (6.4))
ah-integrity=STB34101CIPH-K256-MAC-252 (СТБ 34.101.31-2011 (6.6))
esp-integrity=STB34101CIPH-K256-MAC-65532 (СТБ 34.101.31-2011 (6.6))
esp-cipher=STB34101CIPH-K256-CBC-252 (СТБ 34.101.31-2011 (6.4))
oakley-group=BELTDH
```

Для большей наглядности разрешается назначать алгоритмам пользовательские псевдонимы (в этом случае во вкладках **IKE** и **IPsec** будут отображаться не реальные имена, а назначенные псевдонимы). Для задания псевдонима необходимо дополнить строку имени алгоритма именем псевдонима, заключенного в круглые скобки:

Имеется возможность задать список алгоритмов для каждого семейства алгоритмов. При этом к имени семейства алгоритмов добавляется номер, начиная с 1. Порядок строк в файле не важен. Например:

```
ah-integrity1=GR341194CPRO1-H96-HMAC-254 (ГОСТ Р 34.11-94)
ah-integrity2=G2814789CPRO1-K256-MAC-255 (ГОСТ 28147-89)
```

Разрешение спорных ситуаций происходит по следующим правилам:

- если в файле присутствует описание алгоритма без номера в имени семейства, то будет считан только он, даже не смотря на то, что в файле могут быть строки с описанием алгоритмов для этого же семейства с альтернативным синтаксисом для списков. Например, из файла содержащего следующие строки будет прочитана только первая строка:

```
ah-integrity=GR341194CPRO1-H96-HMAC-254 (ГОСТ Р 34.11-94)
ah-integrity1=GR341194CPRO1-H96-HMAC-254 (ГОСТ Р 34.11-94)
ah-integrity2=G2814789CPRO1-K256-MAC-255 (ГОСТ 28147-89)
```

- если при задании списка один или несколько номеров будет пропущен, то описания после пропуска прочитаны не будут. Например, из файла, содержащего следующие строки, будет прочитана только первая строка:

```
ah-integrity1=GR341194CPRO1-H96-HMAC-254 (ГОСТ Р 34.11-94)
ah-integrity3=G2814789CPRO1-K256-MAC-255 (ГОСТ 28147-89)
```

- если в файле присутствует две или более строки с одинаковым именем семейства алгоритмов, включая номер (текст перед знаком «=»), то будет прочитана только последняя.

8 Интерфейс командной строки

8.1 Подготовка инсталляционного пакета с помощью интерфейса командной строки

Утилита **make_inst** предоставляет администратору безопасности интерфейс командной строки для задания локальных настроек Продукта Bel VPN Client-P и создания инсталляционного файла Продукта Bel VPN Client-P для пользователя.

При использовании **предопределенного ключа** для аутентификации сторон предоставляется возможность считывать созданный ключ из файла либо задать его значение в командной строке.

Для подготовки инсталляционного пакета с использованием **сертификатов открытого ключа** для аутентификации сторон необходимо выполнить следующие действия:

- Шаг 1:** На компьютере пользователя либо компьютере администратора создается ключевая пара и запрос на сертификат пользователя, который отсылается в Удостоверяющий Центр. Контейнер с секретным ключом размещается на ключевом носителе пользователя. Администратор безопасности получает сертификат Удостоверяющего Центра (Trusted CA Certificate, CA-сертификат) и сертификат пользователя.
- Шаг 2:** Администратор безопасности задает локальную политику безопасности (LSP) для данного пользователя в виде текстового файла (см. раздел [«Создание локальной политики безопасности. Конфигурационный файл»](#)).
- Шаг 3:** Администратор безопасности на своем рабочем месте запускает команду **make_inst**, в опциях задает файл с LSP для данного пользователя, путь к локальному и CA-сертификату, имя контейнера на ключевом носителе, локальные настройки, и создает инсталляционный файл Bel VPN Client-P.
- Шаг 4:** Администратор безопасности передает пользователю подготовленный инсталляционный пакет, состоящий из:
- инсталляционного файла Bel VPN Client-P
 - пользовательского токена с записанным на нем ключевым контейнером.

8.2 Режимы

Подготовить инсталляционный пакет можно в одном из двух режимов:

- **основной режим**, в котором при создании инсталляционного файла Bel VPN Client-P используются алгоритмы СТБ, ГОСТ при шифровании, проверки целостности пакетов, формировании и проверки ЭЦП.

С помощью утилиты **make_inst** можно создать одновременно инсталляционные файлы Bel VPN Client-P для большого количества пользователей (см. раздел [«Создание нескольких инсталляционных пакетов одновременно»](#)).

Все сообщения, выдаваемые утилитой **make_inst** в процессе ее работы, выводятся в файл **make_inst_log.txt** (при каждом создании инсталляционного файла **make_inst_log.txt** переписывается).

8.3 Описание утилиты make_inst

Вызов утилиты **make_inst.exe** должен происходить из каталога административного пакета. В противном случае будет выдано сообщение об ошибке. Утилита имеет обязательные опции и необязательные, которые заключены в квадратные скобки.

```
make_inst.exe -o SFX_file_path -l LSP_file_path
```

При использовании **Preshared_Key** указываются опции:

```
-kn Preshared_key_name {-kv Preshared_key_val|-kvf file_path_Preshared_key_val}
```

При использовании сертификатов указываются опции:

- для CA сертификата:

```
-c CA_file_path
[-capwd CA_storage_password] | [-capwdf file_path_CA_storage_password]
[-caidx CA_object_index]
```

- для локального сертификата:

```
-u USER_cert_file_path
{ [-certpwd USER_cert_storage_password] | [-certpwndf
file_path_USER_cert_storage_password] }
[-certidx USER_cert_object_index]
[-uc USER_cert_container_name]
{ [-up USER_cert_container_password] | [-ufp file_path_USER_cert_container_password] }
```

- для сертификатов партнеров или CRL:

```
[-p PARTNER_cert_1_file_path [-p PARTNER_cert_2_file_path] ...]
```

- для проверки соответствия сертификата пользователя и секретного ключа на компьютере администратора, для копирования контейнера в инсталляционный файл указываются опции:

```
[-chksecret {on | off}]
[-uac USER_cert_container_name_ADMIN]
{ [-uap USER_cert_container_password_ADMIN] | [-uafp
file_path_USER_cert_container_password_ADMIN] }
[-ucpkgcopy {on | off}]
```

- режим международных сертификатов:

```
[-intern {on | off}] (default: off)
```

Локальные настройки:

```
[-q {basic | normal | silent}] (default: basic)
[-d {passall | passdhcp | dropall}] (default: passall)
[-f {ddp | passdhcp}] (default: ddp)
[-s {emerg | alert | crit | err | warning | notice | info | debug}] (default: notice)
[-t <SYSLOG_server_IP>] (default: 127.0.0.1)
[-y <log_facility>] (default: log_local7)
[-a "<Additional_cmd_msiexec_params>"]
[-lic <license_file_path>]
[-nilogin {on | off}] (default: off)
[-login_protection { on | off }] (default: on)
[-local_mgmt { on | off }] (default: off)
[-token {on | off}] (default: off)
```

где:

-o SFX_file_path

SFX_file_path – имя создаваемого инсталляционного SFX-файла. Обязательная опция. Имя файла подразумевает и путь к этому файлу.

-l LSP_file_path

LSP_file_path – имя файла, содержащего LSP. Имеет текстовый формат. Обязательная опция, если не задан режим логина с использованием пользовательского токена ([-token on](#)).

Использование предопределенного ключа	
-kn Preshared_key_name	
	Preshared_key_name – имя предопределенного ключа. Обязательная опция, если используются предопределенные ключи. Может быть задано несколько таких ключей (см. Примечание 1). Предопределенные ключи или сертификаты обязательно должны быть заданы. Можно задавать и то, и другое.
-kv Preshared_key_val	
	Preshared_key_val – значение предопределенного ключа. Например, -kv 12345 или -kv "Test preshared key" (кавычки в ключ не входят). Может быть задано несколько таких ключей (см. Примечание 1).
-kvf file_path_Preshared_key_val	
	file_path_Preshared_key_val – имя файла, содержащего значение предопределенного ключа на компьютере администратора. Если используется предопределенный ключ, то обязательно должна быть задана опция -kv либо -kvf. Может быть задано несколько таких ключей (см. Примечание 1).
Использование CA сертификата	
-c CA_file_path	
	CA_file_path – имя файла с CA-сертификатом на компьютере администратора. Обязательная опция, если используются сертификаты.
-capwd CA_storage_password	
	CA_storage_password – пароль к хранилищу с CA сертификатом (если требуется, например, для файла в формате PKCS#12). Ситуации – отсутствие пароля (пароль не задан) и пустой пароль ("") – не различаются.
-capwdf file_path_CA_storage_password	
	file_path_CA_storage_password – имя файла, содержащего пароль к хранилищу с CA сертификатом. В этой и других подобных опциях пароль читается из файла как текстовая строка. Если файл содержит несколько строк, читается только первая из них и воспринимается как пароль. Нельзя указывать одновременно с опцией capwd .
-caidx CA_object_index	
	CA_object_index – порядковый номер CA сертификата в данном хранилище. Нумерация начинается с 1. Значение по умолчанию – 1.
Использование локального сертификата	
-u USER_cert_file_path	
	USER_cert_file_path – имя файла с локальным сертификатом пользователя на компьютере администратора. Если опция не задана – берется хранилище с CA сертификатом. В этом случае порядковые номера CA и локального сертификатов в хранилище (caidx и certidx) должны различаться.
-certpwd USER_cert_storage_password	

USER_cert_storage_password – пароль к хранилищу с локальным сертификатом (если требуется, например, для файла в формате PKCS#12). Ситуации - отсутствие пароля (пароль не задан) и пустой пароль ("") – не различаются. Используется, если задана опция -u.

–certpwd file_path_USER_cert_storage_password

file_path_USER_cert_storage_password – имя файла, содержащего пароль к хранилищу с локальным сертификатом. Пароль читается из файла как текстовая строка. Если файл содержит несколько строк, читается только первая из них и воспринимается как пароль. Нельзя указывать одновременно с опцией [certpwd](#).

–certidx USER_cert_object_index

USER_cert_object_index – порядковый номер локального сертификата в хранилище. Нумерация начинается с 1. Значение по умолчанию – 1.

Если не задана опция -u, используется одно и тоже хранилище для СА и локального сертификатов. В этом случае порядковые номера СА и локального сертификатов в хранилище должны различаться.

–uc USER_cert_container_name

USER_cert_container_name – имя контейнера с секретным ключом на ключевом носителе информации, на котором хранится контейнер. Не больше 60 символов (см. [Примечание 2](#) об именах контейнеров).

Опция не указывается, если используется комбинация `intern on` и `usrkgscoru on`. В противном случае, опция является обязательной, если используются сертификаты.

Если задана опция `intern on` и не задана `usrkgscoru on`, то данная опция **–uc** будет указывать на файл в формате PKCS#12 с секретным ключом на компьютере пользователя.

–up USER_cert_container_password

USER_cert_container_password – пароль к контейнеру с секретным ключом. Не больше 40 символов. Параметр актуален, если не задана опция **–ufp**. Пароль (в том числе и пустой) должен быть указан обязательно. В случае если контейнер находится на токене, пароль контейнера и PIN токена совпадают.

–ufp file_path_USER_cert_container_password

file_path_USER_cert_container_password – имя файла, содержащего пароль к контейнеру, на компьютере администратора. Не больше 40 символов. Пароль читается из файла как текстовая строка. Если файл содержит несколько строк, то читается только первая строка и воспринимается как пароль. Нельзя задавать вместе с опцией **-up**.

Указание сертификатов партнеров, промежуточного CA сертификата

–p PARTNER_cert_i_file_path

PARTNER_cert_i_file_path – путь к сертификату партнера или промежуточному CA-сертификату, который будет положен в базу локальных настроек продукта Bel VPN Client-P при инсталляции. Можно задать несколько таких опций (в базу сертификаты будут положены в порядке перечисления данных опций). Необязательный параметр. Рекомендуется использовать в случаях, когда присутствуют проблемы с передачей сертификатов по протоколу IKE и LDAP.

Проверка соответствия сертификата пользователя и секретного ключа на компьютере администратора

–chksecret {on | off}

включение/выключение проверки соответствия сертификата пользователя и секретного ключа. По умолчанию – значение off. Такая проверка осуществляется на компьютере администратора и возможна только при присоединенном к нему контейнеру с секретным ключом. Проверяется контейнер, указанный в опции **-uac**.

–uac USER_cert_container_name_ADMIN

USER_cert_container_name_ADMIN – имя контейнера на компьютере администратора. Эта опция используется только при включенной опции **chksecret**.

В случае указанной опции **–intern on** данный параметр указывает на файл в формате PKCS#12, содержащему секретный ключ, на компьютере администратора.

–uap USER_cert_container_password_ADMIN

USER_cert_container_password_ADMIN – пароль к контейнеру, указанному в опции **–uac**. По умолчанию – пароль пустой.

–uafp file_path_USER_cert_container_password_ADMIN

file_path_USER_cert_container_password_ADMIN – имя файла на компьютере администратора, в котором записан пароль к контейнеру, указанному в опции **–uac**. Нельзя задавать вместе с опцией **–uap**.

Режим международных сертификатов

–intern {on | off}

Включение/выключение режима использования международных (не ГОСТовых) сертификатов. При использовании международных сертификатов логика работы опций, связанных с сертификатами, может существенно меняться (см. описание соответствующих опций).

-ucpkgcopy {on | off}

Включен/выключен режим копирования сертификатного контейнера в инсталляционный файл. Используется только в режиме международных алгоритмов (опция intern on). В этом случае секретный ключ из контейнера, заданного в опции -uac, копируется в инсталляционный файл. При установке на компьютере пользователя данный секретный ключ переносится в базу локальных настроек S-Terra Client. Значение по умолчанию – off.

Копирование контейнера с одного носителя на другой при инсталляции S-Terra Client

-ccop {copy | import} d

выбор операции копирования или импорта сертификатного контейнера. Обязательный параметр, если используется опция -cs.

-cs Source_USER_cert_container_name

при указании этой опции будет произведено копирование контейнера с именем **Source_USER_cert_container_name**, размещенного на компьютере пользователя, в контейнер с именем **USER_cert_container_name**, которое указано в опции -uc, при инсталляции S-Terra Client на компьютере пользователя. Опция -cs задается, если используется сертификат. Обязательно должен быть выставлен вместе с -ccop. В зависимости от этого ключа различается смысл параметра:

- ccop copy – в -cs <Source_USER_cert_container_name> – задается имя исходного контейнера,
- ccop import – в -cs <Source_USER_cert_container_file_path> – задается путь к файлу (на машине пользователя), из которого импортируется контейнер.

Нельзя задавать вместе с -ucpkgcopy on.

-cp Source_USER_cert_container_password

Source_USER_cert_container_password – пароль к контейнеру с именем, указанным в опции -cs, который будет копироваться при инсталляции. Если пароль отсутствует или пустой, то опция -cp не задается. По умолчанию – пароль пустой.

-cfp file_path_Source_USER_cert_container_password

file_path_Source_USER_cert_container_password – имя файла, в котором записан пароль к контейнеру, указанному в опции -cs. Нельзя задавать одновременно с опцией -cp.

Локальные настройки

-q {basic | normal | silent}

тип инсталляции Продукта Bel VPN Client-P:

- **basic** – неинтерактивная установка с запросом на инсталляцию. Вариант по умолчанию.
- **normal** – интерактивная установка (в диалоговом режиме) с демонстрацией Лицензии и другими окнами.
- **silent** – неинтерактивная установка без запросов. Стартует сразу после запуска EXE-файла без дополнительных запросов.

-d {passall | passdhcp}

Default Driver Policy:

- passall. – пропускать все пакеты. Вариант по умолчанию
- passdhcp – ничего не пропускать, кроме DHCP-пакетов
- dropall – не пропускать трафик.

-f {ddp | passdhcp}

Logoff policy – специальная политика:

- ddp – Default Driver Policy. Вариант по умолчанию
- passdhcp – ничего не пропускать, кроме DHCP-пакетов.

-s log_severity

log_severity = {EMERG|ALERT|CRIT|ERR|WARNING|NOTICE|INFO|DEBUG}

По умолчанию – NOTICE. Опция задает общий уровень важности протоколируемых событий, ее использование описано в главе "Протоколирование событий".

-t SYSLOG_server_IP

SYSLOG_server_IP – IP-адрес SYSLOG сервера, на который будут посылаться сообщения о протоколируемых событиях. По умолчанию – 127.0.0.1 (сообщения будут присылаться на локальный хост).

-y log_facility

log_facility = log_local 0-7. По умолчанию – log_local7.

-a "Additional_cmd_msiexec_params"

"Additional_cmd_msiexec_params" – дополнительные параметры запуска WinInstaller. Например, альтернативная инсталляционная папка, настройки лога Windows Installer и т.п. Эти параметры можно посмотреть по ссылке http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp

/I* C:\Client\install_log_file.txt - протоколирование событий в файл C:\Client\install_log_file.txt при инсталляции Bel VPN Client-P (рекомендуется при режиме silent).

INSTALLDIR=каталог установки продукта – переопределение каталога. Указание каталога, недоступного на компьютере пользователя, приведет к ошибке инсталляции.

Можно часть текста заключить в символы % (процент) и она будет рассматриваться как имя переменной окружения. И эта часть текста будет заменяться на значение переменной окружения (значения переменных окружения можно просмотреть командой set). Если переменная окружения отсутствует, в командке остается исходный текст.

Поддерживается специальная переменная окружения SfxDir – полный путь к папке, в которую распакованы данные. Таким образом, последовательность символов %SfxDir% заменяется на полный путь к папке, в которую распакованы данные.

REBOOT=F – обязательно запрашивать перезагрузку системы в конце инсталляции, даже если он не инициируется инсталлятором.

REBOOT=S – отключить запрос на перезагрузку системы в конце инсталляции. Не блокировать рестарт в случае ForceReboot action.

REBOOT=R – полностью отключить все запросы на перезагрузку системы, включая ForceReboot action. Используется для установки нескольких продуктов и/или выполнения дополнительных действий после инсталляции. После этого перезапустить систему вручную или с помощью сторонних инструментальных средств.

MAX_SERVICE_START_TIMEOUT= – время (в секундах) ожидания старта VPN сервиса (vpnsvc). Максимальное значение – 600 секунд. Значение по умолчанию – 30. Можно использовать для предотвращения появления сообщений об ошибке связи с сервисом на этапе логина для медленных и/или находящихся под сильной нагрузкой систем.

AGENT_DB_REMOVE=1 – автоматически (без дополнительных запросов) будет удаляться база локальных настроек при установке или при удалении продукта (рекомендуется использовать для режима инсталляции silent).

AGENT_DB_REMOVE=0 – база локальных настроек удаляться не будет, запросы пользователю выдаваться не будут. По умолчанию (параметр пустой) – пользователю выдается запрос на удаление базы локальных настроек.

DISABLE_ANTIVIRUS_WARNING=1 – при инсталляции не будет показываться предупреждение [25036](#) (о необходимости отключения антивирусных программ).

Примечание: пользователь должен знать о необходимости отключения антивируса, иначе данный параметр использовать не следует.

REBOOT_REQUIRED=1 – принудительно инициировать запрос на рестарт системы в конце инсталляции. Параметр обычно выставляется автоматически (при необходимости).

DISABLE_CALL_LOGIN=1 – в конце инсталляции логин не запустится. Устанавливать параметр имеет смысл только для интерактивного логина (NON_INTERACTIVE_LOGIN=0) на Windows Vista и более поздних версиях.

–lic license_file_path

License_file_path – имя файла с Лицензией на Bel VPN Client-P на компьютере администратора. Эта опция обязательна для режимов инсталляции basic и silent. Для режима normal эта опция необязательна:

- если ее задать, то при установке Продукта вопросы о Лицензии задаваться не будут
- если ее не задать, то при установке Продукта появится стандартное окно для ввода Лицензии.

В текстовом файле данные Лицензии должны быть записаны в виде:

[license]

CustomerCode=NNNN

ProductCode=CLIENT/CLIENTB

LicenseNumber=NNNN

LicenseCode=NNNNNNN

–nilogin {on | off}

Включение/выключение неинтерактивного режима логина пользователя в Продукт Bel VPN Client-P:

- on – включен неинтерактивный режим
- off - выключен неинтерактивный режим логина, работает интерактивный режим.

При неинтерактивном режиме логина при входе пользователя в систему, производится попытка логина пользователя в Продукт с пустым паролем (в качестве пароля используется пустая строка). При таком успешном логине в Продукт окно с запросом пароля не выводится. При неуспешном логине – Продукт ведет себя как при интерактивном логине (будет выдано окно запроса пароля).

–login_protection {on | off}

Включение/выключение функциональности по защите до логина в ОС. Значение по умолчанию – on.

-local_mgmt {on | off}

Включение/выключение возможности изменять настройки Продукта конечным пользователем. Значение по умолчанию – off (пользователь может менять только пароль, уровень логирования, добавлять CRL и сертификаты партнеров, перезагружать локальную политику безопасности).

-token {on | off}

Использование/неиспользование пользовательского токена для логина в Продукт S-Terra Client. Значение по умолчанию – off.

Примечание 1: если задается несколько предопределенных ключей, то опции с именем ключа и самим ключом (-kn и -kv или -kvf) должны следовать одна за другой, т.е. опции -kn и -kv (-kvf), расположенные рядом относятся к одному и тому же предопределенному ключу.

Пример правильного задания ключей:

-kn key1 -kv value1 -kn key2 -kvf file_with_value2

Пример неправильного задания ключей (два имени и два значения расположены подряд):

-kn key1 -kn key2 -kv value1 -kvf value2

Примечание 2: имя контейнера имеет следующий формат

av:<серийный номер ключевого носителя>:имя контейнера

av – ключевое слово, означающее что контейнер будет создан на внешнем носителе, подключенном по интерфейсу PKCS#11

Например: av:AVP2050050125:ContName1

8.4 Сообщения об ошибках утилиты make_inst

№ п/п	Сообщение	Пояснение
1	Error: SFX file path is missing	Не задан путь к SFX-файлу
2	Error: CA file path is missing	Не задан путь к CA-сертификату
3	Error: Local certificate file path is missing	Не задан путь к локальному сертификату
4	Error: Container name is missing	Не задано имя контейнера
5	Error: LSP file path is missing	Не задан путь к LSP
6	Error: Wrong install type	Неправильно задан тип инсталляции
7	Error: Wrong Default Driver Policy	Неправильно задана DDP
8	Error: Wrong Logoff Policy	Неправильно задана Logoff policy
9	Error: Wrong Log Severity	Неправильно задана Log Severity
10	Error: Wrong Log Facility	Неправильно задана Log Facility
11	Error: Wrong parameter: "..."	Неподдерживаемый параметр
12	Error: temporary directory creation failed	Не удалось создать временную директорию для работы утилиты
13	Error: Key creation failed	Не удалось создать описание контейнера ключа (наиболее вероятная причина – не удалось прочитать файл с паролем).
14	Error: installer files copy failed	Не удалось скопировать файлы инсталлятора
15	Error: CA not found	Не удалось найти файл с CA сертификатом
16	Error: Local certificate not found	Не удалось найти файл с локальным сертификатом
17	Error: LSP not found	Не удалось найти файл с LSP
18	Error: User preferences write failed	Не удалось создать пользовательские настройки
19	Error: Log settings write failed	Не удалось создать настройки лога
20	Error: SFX archive creation failed	Не удалось сформировать SFX-архив
21	Error: Preshared key value not found	Не удалось найти файл со значением Preshared ключа
22	Error: Source container is not applicable	Попытка задать исходный контейнер, когда не используются сертификаты или при использовании опции –intern on
23	Error: Partner certificate is not applicable	Партнерский сертификат неприменим (попытка задать опцию –p при отсутствии других опций, связанных с сертификатами)
24	Error: Source and destination containers have the same name	Исходный и рабочий контейнеры имеют одинаковые имена, что недопустимо
25	Error: Certificates or Preshared key should be set	Сертификаты или Preshared ключ должны быть заданы
26	Error: Preshared key name is missing	Не задано имя Preshared ключа
27	Error: Preshared key value is missing	Не задано значение Preshared ключа
28	Error: Preshared key name or value missed	Не задано имя или значение Preshared ключа
29	Error: Preshared key names should be different	Имена Preshared ключей должны различаться
30	Error: Cannot run utility outside product dir	Не удается запустить утилиту вне директории продукта
31	Error: License should be set for non-interactive installation	Лицензия должна быть задана для неинтерактивной инсталляции
32	Error: Product incorrectly installed or damaged	Продукт некорректно установлен или поврежден

№ п/п	Сообщение	Пояснение
33	Error: Container name on the administrator computer is missing	Отсутствует контейнер на компьютере администратора
34	Error: Secret key copy is only usable with the container copy	Задано копирование секретного ключа, но не задано копирование сертификатного контейнера
35	Error: Secret key type should not be set due to secret key check	Тип секретного ключа не должен указываться, если задана проверка секретного ключа
36	Error: Unknown Driver Signing ignore mode	Неизвестный режим отключения Driver Signing сообщений
37	Error: Insertion of certificate container into package failed	Не удалось вставить сертификатный контейнер в инсталляционный пакет
38	Error: Container password reading from file failed	Не удалось прочитать из файла пароль на контейнер
39	Error: Source container password reading from file failed	Не удалось прочитать из файла пароль на исходный контейнер
40	Error: Container on administrator computer password reading from file failed	Не удалось прочитать из файла пароль на контейнер на компьютере администратора
41	Error: Secret key password reading from file failed	Не удалось прочитать из файла пароль на секретный ключ
42	Error: Cannot load CA: Internal error	Не удалось загрузить СА по невыясненной причине
43	Error: Cannot load CA: file not found or access denied	Не удалось загрузить СА: файл не найден или отказ в доступе
44	Error: Cannot load CA: Unknown storage format	Не удалось загрузить СА: неизвестный формат хранилища
45	Error: Password should be set to unlock the CA storage	Для доступа к хранилищу СА требуется пароль
46	Error: Cannot unlock the CA storage: Possibly incorrect password	Не удалось раскрыть хранилище СА: вероятно введен неправильный пароль
47	Error: Cannot get CA from the storage	Не удалось получить СА из хранилища
48	Error: Cannot get CA from the storage: object index exceeds number of objects in the storage	Не удалось извлечь СА из хранилища: порядковый номер объекта больше, чем количество объектов в хранилище
49	Error: Given certificate cannot be used as CA	Данный сертификат не может использоваться в качестве СА
50	Error: Cannot load local certificate: Internal error	Не удалось загрузить локальный сертификат по невыясненной причине
51	Error: Cannot load local certificate: file not found or access denied	Не удалось загрузить локальный сертификат: файл не найден или отказ в доступе
52	Error: Cannot load local certificate: Unknown storage format	Не удалось загрузить локальный сертификат: неизвестный формат хранилища
53	Error: Password should be set to unlock the local certificate storage	Для доступа к хранилищу локального сертификата требуется пароль
54	Error: Cannot unlock the local certificate storage: Possibly incorrect password	Не удалось раскрыть хранилище локального сертификата: вероятно введен неправильный пароль
55	Error: Cannot get local certificate from the storage	Не удалось получить локальный сертификат из хранилища
56	Error: Cannot get local certificate from the storage: object index exceeds number of objects in the storage	Не удалось извлечь локальный сертификат из хранилища: порядковый номер объекта больше, чем количество объектов в хранилище
57	Error: Given certificate cannot be used as local certificate	Данный сертификат не может использоваться в качестве локального

№ п/п	Сообщение	Пояснение
58	Error: CA storage password reading from file failed	Не удалось прочитать из файла пароль на хранилище СА
59	Error: Local certificate storage password reading from file failed	Не удалось прочитать из файла пароль на хранилище локального сертификата
60	Error: Container password is set by two options: file and clear text. It is prohibited.	Пароль на контейнер задан двумя способами: через файл и открытым текстом. Это запрещено.
61	Error: Source container password is set by two options: file and clear text. It is prohibited.	Пароль на исходный контейнер задан двумя способами: через файл и открытым текстом. Это запрещено.
62	Error: Container on administrative computer password is set by two options: file and clear text. It is prohibited.	Пароль на контейнер на машине администратора задан двумя способами: через файл и открытым текстом. Это запрещено.
63	Error: Secret key password is set by two options: file and clear text. It is prohibited.	Пароль на секретный ключ задан двумя способами: через файл и открытым текстом. Это запрещено.
64	Error: CA storage password is set by two options: file and clear text. It is prohibited.	Пароль на хранилище СА задан двумя способами: через файл и открытым текстом. Это запрещено.
65	Error: Local certificate storage password is set by two options: file and clear text. It is prohibited.	Пароль на хранилище локального сертификата задан двумя способами: через файл и открытым текстом. Это запрещено.
66	Error: Wrong CA object index value	Неправильный порядковый номер объекта СА
67	Error: Wrong local certificate object index value	Неправильный порядковый номер объекта локального сертификата
68	Error: Local certificate storage password is set while local certificate storage is not set	Задан пароль хранилища локального сертификата, но хранилище локального сертификата не задано
69	Error: Container name is not applicable with -intern on and -ucpkgcopy on	Имя контейнера на пользовательской машине несовместимо с опциями –intern on и -ucpkgcopy on
70	Error: Partner certificate '<file_path>' load failed	Не удалось загрузить партнерский сертификат <file_path> (наиболее вероятная причина – отсутствие или неправильный формат файла, заданного в опции –p)
71	Error: Partner certificate processing failed	Не удалось обработать партнерский сертификат
72	Error: Cannot load CA: Internal error	Не удалось загрузить СА: внутренняя ошибка
73	Error: Cannot load CA: file not found or access denied	Не удалось загрузить СА: файл не найден или к нему нет доступа
74	Error: Cannot load CA: Unknown storage format	Не удалось загрузить СА: неизвестный формат хранилища
75	Error: Password should be set to unlock the CA storage	Требуется задать пароль для разблокирования хранилища СА
76	Error: Cannot unlock the CA storage: Possibly incorrect password	Не удается разблокировать хранилище СА: возможно задан неверный пароль
77	Error: Cannot get CA from the storage	Не удастся извлечь СА из хранилища
78	Error: Cannot get CA from the storage: object index exceeds number of objects in the storage	Не удастся получить СА из хранилища: индекс объекта превышает количество объектов в хранилище

№ п/п	Сообщение	Пояснение
79	Error: Cannot load local certificate: Internal error	Не удалось загрузить локальный сертификат: внутренняя ошибка
80	Error: Cannot load local certificate: file not found or access denied	Не удалось загрузить локальный сертификат: файл не найден или к нему нет доступа
81	Error: Cannot load local certificate: Unknown storage format	Не удалось загрузить локальный сертификат: неизвестный формат хранилища
82	Error: Password should be set to unlock the local certificate storage	Требуется задать пароль для разблокирования хранилища с локальным сертификатом
83	Error: Cannot unlock the local certificate storage: Possibly incorrect password	Не удается разблокировать хранилище с локальным сертификатом: возможно задан неверный пароль
84	Error: Cannot get local certificate from the storage	Не удается извлечь локальный сертификат из хранилища
85	Error: Cannot get local certificate from the storage: object index exceeds number of objects in the storage	Не удается получить локальный сертификат из хранилища: индекс объекта превышает количество объектов в хранилище
86	Error: Cannot load partner certificate '<cert_file_path>': Internal error	Не удалось загрузить партнерский сертификат '<cert_file_path>': внутренняя ошибка
87	Error: Cannot load partner certificate '<cert_file_path>': file not found or access denied	Не удалось загрузить партнерский сертификат '<cert_file_path>': файл не найден или к нему нет доступа
88	Error: Cannot load partner certificate '<cert_file_path>': Unknown storage format	Не удалось загрузить партнерский сертификат '<cert_file_path>': неизвестный формат хранилища
89	Error: Password should be set to unlock the partner certificate '<cert_file_path>' storage	Требуется задать пароль для разблокирования хранилища с партнерским сертификатом '<cert_file_path>' <u>Примечание:</u> в текущей версии продукта хранилища партнерских сертификатов, защищенные паролем, не поддерживаются.
90	Error: Cannot get partner certificate '<cert_file_path>' from the storage	Не удалось извлечь партнерский сертификат '<cert_file_path>' из хранилища
91	Error: Cannot load private key of the local certificate: Internal error	Не удалось загрузить секретный ключ локального сертификата: внутренняя ошибка
92	Error: Cannot load private key of the local certificate: file not found or access denied	Не удалось загрузить секретный ключ локального сертификата: файл не найден или к нему нет доступа
93	Error: Cannot load private key of the local certificate: Unknown storage format	Не удалось загрузить секретный ключ локального сертификата: неизвестный формат хранилища
94	Error: Password should be set to unlock the private key of the local certificate storage	Требуется задать пароль для разблокирования хранилища секретный ключ локального сертификата
95	Error: Cannot unlock the private key of the local certificate storage: Possibly incorrect password	Не удается разблокировать хранилище секретного ключа локального сертификата: возможно задан неверный пароль

№ п/п	Сообщение	Пояснение
96	Error: Cannot get private key of the local certificate from the storage	Не удается извлечь секретный ключ локального сертификата из хранилища
97	Error: Cannot get private key of the local certificate from the storage: certificate not found	Не удается извлечь секретный ключ локального сертификата из хранилища: не найден сертификат
98	Error: Unknown certificate container operation	Неизвестная операция с сертификатным контейнером
99	Error: Certificate operation ('copy' or 'import') must be set	Должна быть задана операция с сертификатным контейнером ('copy' или 'import')
100	Error: Certificate operation is not applicable	Операция с сертификатным контейнером неприменима
101	Error: CA certificate processing failed	Не удалось обработать CA
102	Error: Secret key processing failed	Не удалось обработать секретный ключ
103	Error: Local certificate processing failed	Не удалось обработать локальный сертификат
104	Error: LSP processing failed	Не удалось обработать LSP

8.5 Создание нескольких инсталляционных пакетов одновременно

Для создания инсталляционных пакетов для большого числа пользователей одновременно предлагается использовать BAT-файлы, вызывающие в цикле утилиту make_inst.exe. Далее описаны несколько BAT-файлов типичных сценариев. На компьютере администратора должна быть создана специальная папка для файлов пользователей. В этой папке создаются подпапки, которые называются по имени пользователей. Например, папка c:\vpn_client, в ней подпапки c:\vpn_client\alice и c:\vpn_client\bob (важно, чтобы не было посторонних подпапок). В этих подпапках лежит файл localcert.crt, а также для некоторых сценариев могут лежать файлы ca.crt, lsp.txt и pwd.txt (пароль на контейнер).

8.5.1 Сценарий 1

В этом сценарии контейнеры с секретными ключами пользователей имеют пустой пароль. Получаемые SFX-файлы кладутся в папки пользователей под именем vpnclient.exe. В папках пользователей лежат локальные сертификаты. Используется один CA сертификат и одна LSP для всех пользователей:

```
@echo off

SET TEMPLATE_DIR=c:\vpn_client
SET MAKE_INST_PATH=D:\S-Terra Client\make_inst.exe
SET CONTAINER_NAME=REGISTRY\container
SET LSP_PATH=c:\vpn_client\lsp.txt
SET CA_PATH=c:\vpn_client\ca.crt

for /r %TEMPLATE_DIR% /d %%i in (*) do (%MAKE_INST_PATH% -o %%i\vpnclient.exe -c %CA_PATH% -u
%%i\localcert.crt -uc %CONTAINER_NAME% -l %LSP_PATH%) & (if errorlevel 1 goto err)

goto :end

:err

echo An error occurred
```

```
exit
```

```
:end
```

```
echo Make installations complete
```

Используются следующие настройки:

`TEMPLATE_DIR` – папка, в которой лежат подпапки пользователей. Путь должен быть без пробелов.

`MAKE_INST_PATH` – путь к утилите `make_inst.exe`.

`CONTAINER_NAME` – имя контейнера.

`LSP_PATH` – путь к общей LSP.

`CA_PATH` – путь к общему CA сертификату.

Здесь и далее фраза в конце "Make installations complete" обозначает успешное завершение, а "An error occurred" – что произошла ошибка.

8.5.2 Сценарий 2

Используется общий пароль для всех контейнеров с секретными ключами всех пользователей. Получаемые SFX-файлы кладутся в папки пользователей под именем `vpnclient.exe`. Каждый пользователь имеет свой CA сертификат и свою LSP:

```
@echo off
```

```
SET TEMPLATE_DIR=c:\vpn_client
```

```
SET MAKE_INST_PATH=D:\S-Terra Client\make_inst.exe
```

```
SET CONTAINER_NAME=REGISTRY\container
```

```
SET CONTAINER_PASSWORD=somepwd
```

```
for /r %TEMPLATE_DIR% /d %%i in (*) do (%MAKE_INST_PATH% -o %%i\vpnclient.exe -c  
%%i\ca.crt -u %%i\localcert.crt -uc %CONTAINER_NAME% -up %CONTAINER_PASSWORD% -l  
%%i\lsp.txt) & (if errorlevel 1 goto err)
```

```
goto :end
```

```
:err
```

```
echo An error occurred
```

```
exit
```

```
:end
```

```
echo Make installations complete
```

Новые настройки:

`CONTAINER_PASSWORD` – общий пароль.

8.5.3 Сценарий 3

Все условия аналогичны сценарию 2, но получаемые файлы кладутся в одну папку с именами username.exe (где username совпадает с именем пользовательской подпапки, например alice.exe или bob.exe):

```
@echo off

SET TEMPLATE_DIR=c:\vpn_client
SET MAKE_INST_PATH=D:\S-Terra Client\make_inst.exe
SET CONTAINER_NAME=REGISTRY\container
SET CONTAINER_PASSWORD=somepwd
SET SFX_DIR=c:\sfx

cd %TEMPLATE_DIR%

for /d %%i in (*) do (%MAKE_INST_PATH% -o %SFX_DIR%\%%i.exe -c %%~fi\ca.crt -u
%%~fi\localcert.crt -uc %CONTAINER_NAME% -up %CONTAINER_PASSWORD% -l %%~fi\lsp.txt)
& (if errorlevel 1 goto err)

goto :end

:err

echo An error occurred
exit

:end

echo Make installations complete
```

где:

SFX_DIR – папка, в которую размещаются получаемые файлы.

8.5.4 Сценарий 4

Выполняется при тех же условиях, что и в сценарии 2, но в каждой папке пользователя дополнительно лежит файл pwd.txt, содержащий пароль контейнера для данного пользователя. Кроме того, когда каждый пользователь будет устанавливать Продукт S-Terra Client из подготовленного для него инсталляционного файла, то он будет ставиться не в папку по умолчанию, а в папку c:\my vpn (с пробелом):

```
@echo off

SET TEMPLATE_DIR=c:\vpn_client
SET MAKE_INST_PATH=D:\S-Terra Client\make_inst.exe
SET CONTAINER_NAME=REGISTRY\container
SET SFX_DIR=c:\sfx

cd %TEMPLATE_DIR%
```

```
for /d %%i in (*) do (%MAKE_INST_PATH% -o %SFX_DIR%\%%i.exe -c %%~fi\ca.crt -u  
%%~fi\localcert.crt -uc %CONTAINER_NAME% -ufp %%~fi\pwd.txt -l %%~fi\lsp.txt -a  
"INSTALLDIR=\"%c:\my vpn\"" & (if errorlevel 1 goto err)  
  
goto :end  
  
:err  
  
echo An error occurred  
exit  
:end  
echo Make installations complete
```

9 Подготовка к инсталляции персонализированного пакета ПП Bel VPN Client-P

Действия, которые необходимо выполнить перед установкой персонализированного пакета ПП Bel VPN Client-P описаны в документе «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1». Подготовительные процедуры».

10 Сообщения об ошибках при инсталляции административного пакета ПП Bel VPN Client-P

Ниже приведены тексты сообщений об ошибках, которые могут появляться при инсталляции административного пакета ПП Bel VPN Client-P (Таблица 6).

Таблица 6

Код ошибки	Текст сообщения	Примечание
1330	A file that is required cannot be installed because the cabinet file <file> has an invalid digital signature. This may indicate that the cabinet file is corrupt	Перед установкой Продукта должны быть установлены корневые сертификаты от Digicert, выпущенные не позднее 01.01.2017, которые удостоверяют сертификат LLC «S-Terra Bel», который в свою очередь подписывает драйвера, MSI и CAB. С сайта microsoft.com получите обновление "Update for Root Certificates" (ключевое слово – KB931125).
25006	RNG initialization failed. Installation aborted. {RNG container path: <path>}	Не удалось создать RNG контейнер.
25018	Product "<Product_name version>" was detected. You should uninstall it first before the installation.	Был обнаружен Продукт "<Product_name version>". Вам необходимо сначала деинсталлировать его.
	This product needs Windows 2000 or higher	Для Продукта необходима Windows 2000 или выше
25026	You must have administrator privileges.	Вам необходимы администраторские привилегии.
25033	The Visual C++ Redistributable Package is absent or damaged	Visual C++ Redistributable Package отсутствует или поврежден
25036	Please disable any anti-virus software during the installation Press "OK" if anti-virus is disabled or not installed Press "Cancel" to cancel the installation	Пожалуйста, отключите антивирусную программу на время инсталляции Нажмите "OK" если антивирус отключен или не установлен Нажмите "Cancel" для отмены инсталляции Примечание: появление данного сообщения может быть отключено с помощью параметра инсталляции DISABLE_ANTIVIRUS_WARNING

11 Работа Bel VPN Client-P с продуктами третьих производителей

11.1 Работа с Брандмауэром Windows (ОС Windows 7)

При работе продукта Bel VPN Client-P под управлением ОС Windows 7 могут появляться проблемы, связанные с пропуском исходящих и входящих пакетов.

Было установлено, что это связано с настройкой Брандмауэр Windows на устройстве.

Если Брандмауэр Windows выключен – проблем с пропуском пакетов нет.

Если Брандмауэр Windows включен – он автоматически определяет типы сетей, к которым подключены интерфейсы, – «Домашние сети», «Рабочие (частные) сети» и «Общественные сети» (Рисунок 85).

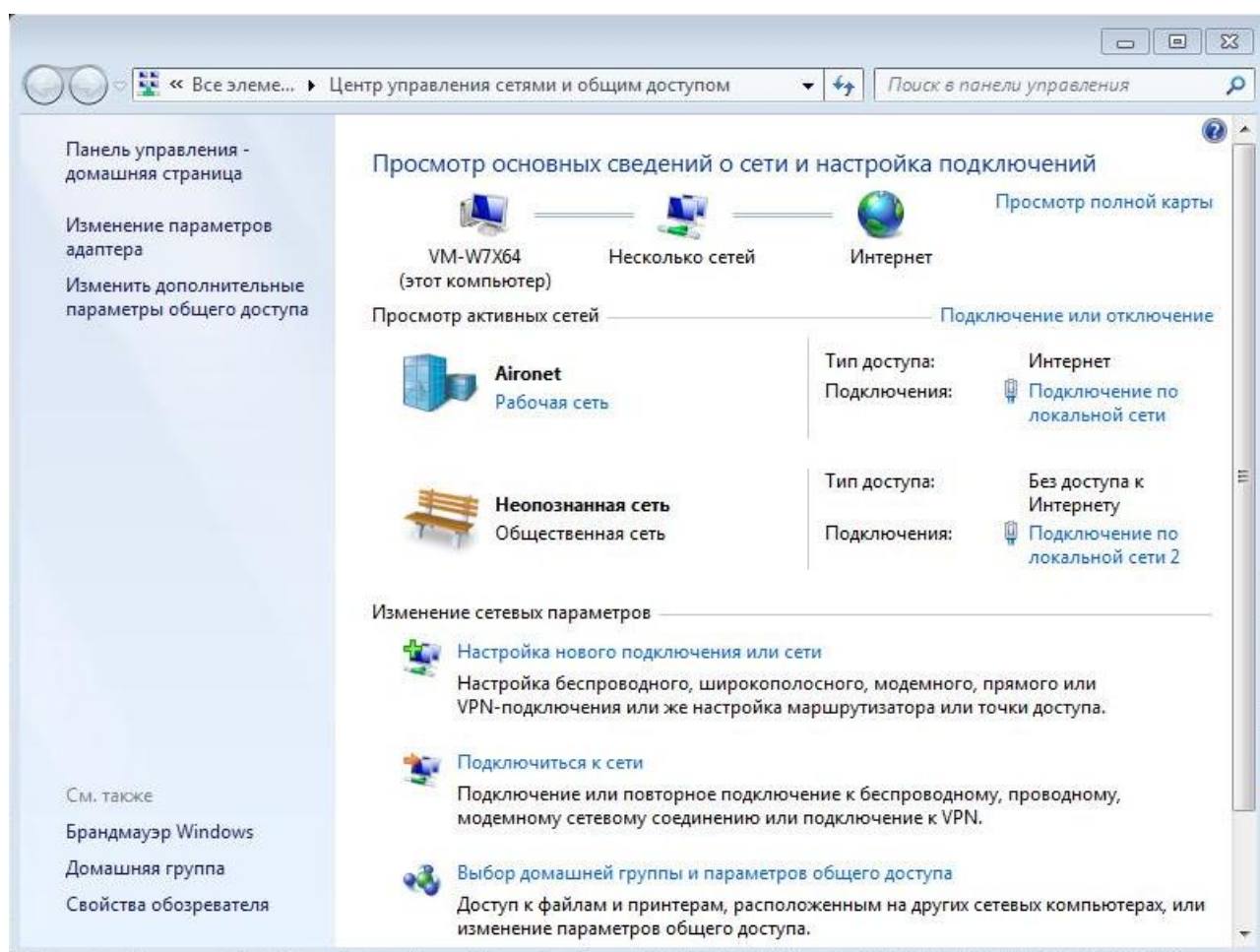


Рисунок 85

Для «Домашних сетей» и «Рабочих (частных) сетей» применяются предопределенные правила, которые пользователь не может увидеть и не может изменить. А для «Общественных сетей» имеется возможность изменять настройки брандмауэра и создавать новые правила. Изменять настройки можно по-разному, например, в окне Брандмауэр Windows выберите предложение «Дополнительные параметры» (Рисунок 86).

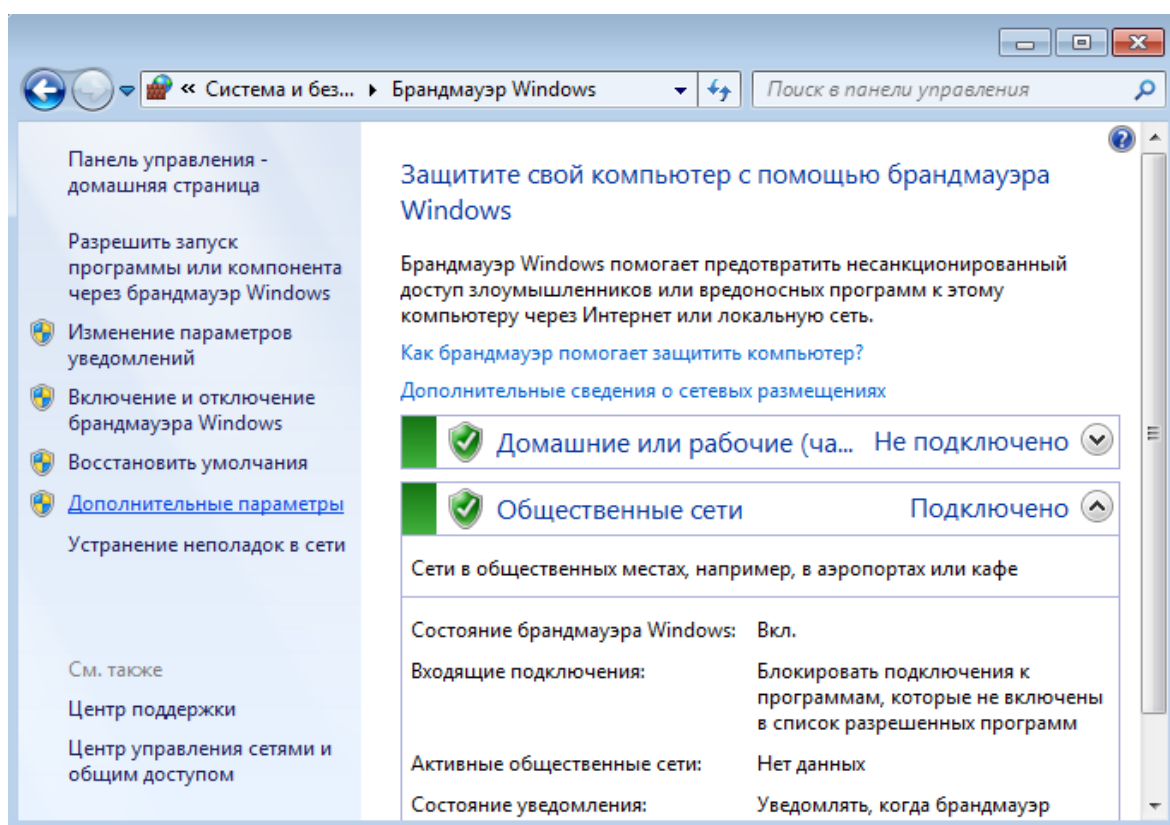


Рисунок 86

В появившемся окне (Рисунок 87) в разделах Правила для входящих и исходящих подключений создайте правила для прохождения нужного трафика.

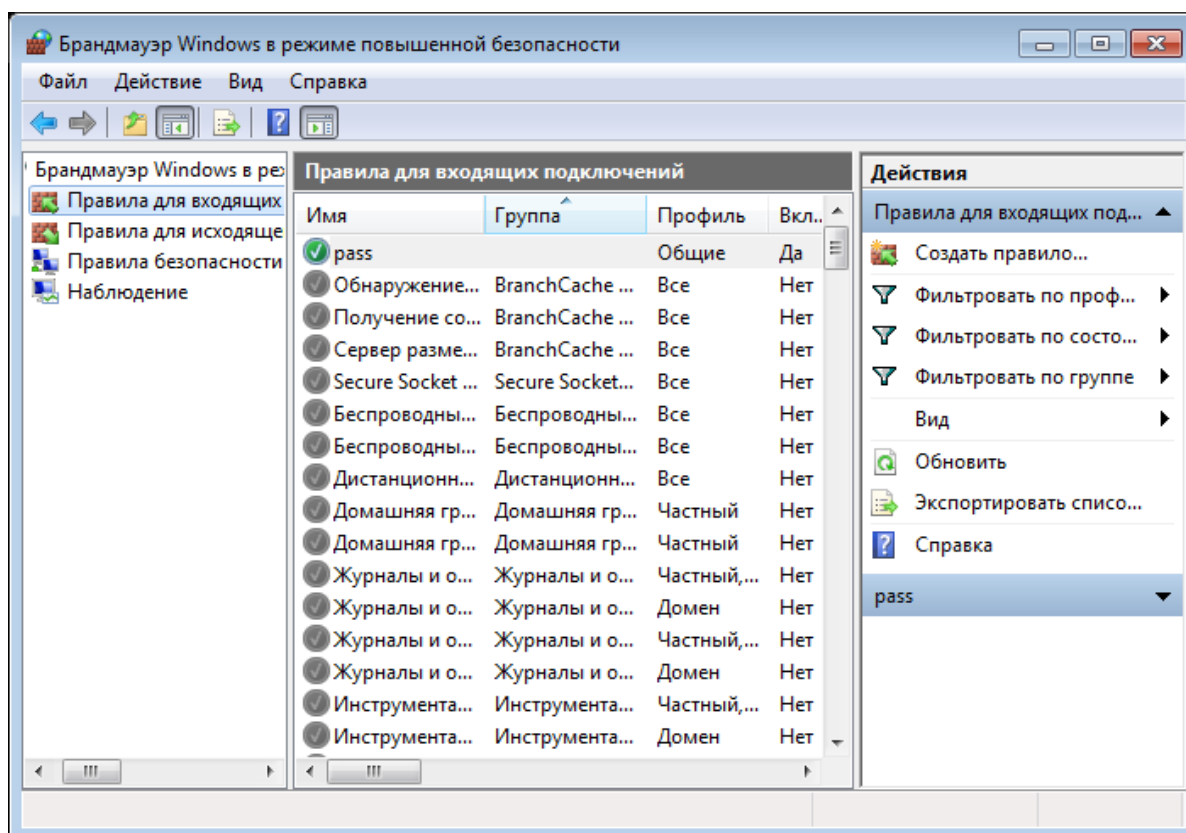


Рисунок 87

11.2 Работа с антивирусом Outpost

При работе Bel VPN Client-P под управлением ОС Windows Vista, Windows 7 (x32), Windows 8(x32), на которых установлен антивирус Outpost, возможны проблемы с созданием соединений, использующих ikcfg-адреса. При этом в syslog появляются сообщения "[IKECFGIF] can't enable packet forwarding".

В этом случае необходимо выполнить следующие действия:

1. В реестре, в разделе:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters`

для `IPEnableRouter` установить значение `1`.

2. Перезагрузить ОС.

12 Создание локальной политики безопасности. Конфигурационный файл

Под политикой безопасности понимается совокупность правил, по которым обрабатываются пакеты входящего и исходящего трафика. Пакеты могут проходить как пакетную фильтрацию, так и обработку с использованием криптографических алгоритмов – построение защищенных (VPN) туннелей между партнерами.

Создание локальной политики безопасности (LSP – Local Security Policy) Bel VPN Client-P осуществляется путем написания конфигурационного файла в текстовом формате для VPN устройства.

Описание грамматики LSP приведено в документе «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1». Руководство администратора. Описание грамматики LSP».

13 Протоколирование событий безопасности

В ПП Bel VPN Client-P регистрация событий безопасности происходит по протоколу Syslog.

При невозможности использовать Syslog и дополнительно сохранить некоторые сообщения, производится запись в [специальные log-файлы](#) или в [журналы Windows](#) раздел «Система».

13.1 Настройка Syslog-клиента

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.

Все настройки syslog-клиента записываются в файл **syslog.ini** каталога продукта, который вручную не редактируется.

13.1.1 Настройка при использовании графического интерфейса

В Графическом интерфейсе административного пакета настройка syslog-клиента производится во вкладке **Settings**.

Подробнее см. раздел «Графический интерфейс. Вкладка Settings».

13.1.2 Настройка при использовании командной строки

В утилите **make_inst** административного пакета для настройки syslog-клиента используются следующие опции:

-t <SYSLOG_server_IP> (по умолчанию: 127.0.0.1) - IP-адрес компьютера, на который будут посылаться сообщения о событиях

-s {emerg|alert|crit|err|warning|notice|info|debug} (по умолчанию: notice) – общий уровень для всех протоколируемых событий

-y <log_facility> (по умолчанию: log_local7) – источник сообщений.

-a /l* C:\Client\install_log_file.txt – протоколирование событий при инсталляции Bel VPN Client-P в указанный файл.

Подробнее см. раздел «Утилита make_inst».

13.2 Получение журнала сообщений в ОС Windows

Для получения журнала сообщений syslog в ОС Windows можно использовать любой syslog-сервер с следующими настройками:

Адрес – **localhost** либо **127.0.0.1**;

Порт – **UDP514**.

13.3 Утилиты log_mgr show и log_mgr set

В состав продукта Bel VPN Client-P входит утилита log_mgr, позволяющая просматривать и управлять уровнем логирования:

- **log_mgr show** – просмотр настройки syslog-клиента и общий уровень лога для всех сообщений.
- **log_mgr set** – изменение настройки уровня протоколирования всех событий, не включенных в группы, уровня протоколирования группы событий, настройки syslog-клиента, задания группы событий и др.

Эти утилиты описаны в документе «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1». Руководство пользователя»(BY.ПТНК.41002-01 34 02), в разделе «Специализированные команды».

13.4 Специальные лог-файлы

В специальные лог-файлы, указанные в Таблице 7, производится дополнительно протоколирование некоторых нештатных ситуаций работы Продукта. В эти файлы записывается информация, которая может помочь решить возникшую проблему.

Таблица 7 Специальные лог-файлы

Имя файла	Путь к файлу	Содержание файла
cspvpn_verify_err.log	Каталог установки продукта (по умолчанию – Bel VPN Client)	Ошибки утилиты cspvpn_verify для проверки целостности неизменяемых и исполняемых файлов.
cp.log	Каталог %USER_TMP% ⁵	Сообщения криптоподсистемы уровня приложений
failh.log	Каталог %USER_TMP%	Аварийные события, не связанные с работой vpnsvc и lsp_show
error.log	Каталог %USER_TMP%\lsp_mgr	Аварийные события, связанные с работой утилиты lsp_mgr
error.log	Каталог %SYS_TMP%\vpnsvc ⁶	Аварийные события, связанные с работой vpnsvc
error.log	Каталог %SYS_TMP%\vpnlogsvc	Аварийные события, связанные с работой vpnlogsvc
SetupAPI.log	%Windir% ⁷	Сообщения инсталлятора ОС Windows XP
SetupAPI.app.log SetupAPI.dev.log	%Windir%\Inf	Сообщения инсталлятора ОС Windows Vista, ОС Windows 7
Имя и путь к файлу указываются администратором в дополнительных параметрах запуска WinInstaller: во вкладке Settings в GUI опция -a утилиты make_inst		Сообщения инсталлятора ОС Windows

Например:

- при неудачном старте vpn-демона (vpnsvc или vpnlogsvc) в файл error.log записывается сообщение следующего вида:

```
initialization of module '%{1}s' failed with code %{2}x
```

где

'%{1}s' – имя модуля при инициализации которого произошла ошибка

'%{2}s' – код ошибки при инициализации модуля

Пример

```
1313076721 initialization of module "hashes checker" failed with code 0xff
```

Модуль hashes checker появляется при проверке целостности неизменяемых файлов продукта при использовании утилиты cspvpn_verify

- при форсированном завершении работы сервиса vpnsvc в файл error.log записывается последнее осмысленное сообщение вида:

```
vpnsvc: forceServiceFini
```

⁵ %USER_TMP% - переменная среды пользователя

⁶ %SYS_TMP% - системная переменная среды, по умолчанию SYS_TMP=C:\Windows\Temp

⁷ %Windir% - каталог установки ОС, по умолчанию Windir=C:\Windows\

- при форсированном завершении работы сервиса vpnlogsvc в его файл error.log записывается последнее осмысленное сообщение вида:

vpnlogsvc: forceServiceFini

- при нарушении контроля целостности ini-файла или базы данных выдается сообщение вида:

'%{1}s' Error: the integrity check of the '%{2}s' failed

или

'%{1}s' FatalError: the integrity check of the '%{2}s' failed

где

'%{1}s' – имя модуля ("s_filestore" или "s_ini"), обнаружившего нарушение

'%{2}s' – указание на проблемный файл

ключ Error означает, что из данного модуля будут выданы дополнительные сообщения, и последним будет сообщение о форсированном завершении сервиса

ключ FatalError означает, что это последнее осмысленное сообщение данного модуля (vpnsvc или vpnlogsvc).

Пример файла "%WINDIR%\temp\vpnsvc\error.log" (записан из сервиса vpnsvc):

1305822135 s_filestore Error: the integrity check of the body-file ".\db\lps\00000002" of the DSC-file "00000002.dsc" failed

1305822135 vpnsvc: forceServiceFini

13.5 Журналы Windows

Для ОС Windows Vista и более новых версий ОС Windows в журнал «Система» протоколируются сообщения от источника **st_ipsm**. Список возможных сообщений приведен в Таблица 8.

Таблица 8

Текст сообщение	Описание
Driver loaded	Драйвер-перехватчик st_ipsm.sys загружен
Driver unloaded	Драйвер-перехватчик st_ipsm.sys выгружен
Filter attach to adapter %2 failed	Не удалось присоединиться к сетевому интерфейсу <имя сетевого интерфейса>
NdisFRegisterFilterDriver failed	Не удалось зарегистрировать драйвер-перехватчик. Загрузка драйвера невозможна
FilterRegisterDevice failed	Не удалось зарегистрировать виртуальное устройство. Загрузка драйвера невозможна
Can't get MTU of adapter %2. Using 1500	Не удалось определить MTU сетевого интерфейса <имя сетевого интерфейса>

Полный список протоколируемых событий приведен в документе «Программный продукт «Клиент безопасности Bel VPN 4.1». Руководство администратора. Протоколирование и мониторинг» (BY.ПТНК.41002-01 34 01-03).

14 Мониторинг

Мониторинг в ПП Bel VPN Client-P осуществляется по протоколу обмена SNMPv1 или SNMPv2c.

SNMP-менеджер имеет возможность запрашивать содержимое базы данных агента.

SNMP-агент может посылать SNMP-менеджеру сообщение о возникшем прерывании в виде трап-сообщения. Список этих сообщений приведен в документе «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1». Руководство администратора. Протоколирование и мониторинг» (BY.ПТНК.41002-01 34 01-03) в разделе «Трап-сообщения».

Настройка SNMP-агента производится администратором при подготовке инсталляционного пакета пользователя:

- В GUI административного пакета настройка SNMP производится во вкладке **LSP**, в окне Advanced LSP Settings, в разделе SNMP settings.
- В конфигурационном файле задание настроек SNMP-агента осуществляется:
 - структурой SNMPPollSettings – для выдачи статистики SNMP-менеджеру. В этой структуре указывается IP-адрес и порт, на который можно получать запросы от SNMP-менеджера, строку, играющую роль пароля при аутентификации сообщений, размещение SNMP-агента и контактное лицо.
 - структурами SNMPTrapSettings и TrapReceiver – для отправки трап-сообщений. В этих структурах указывается IP-адрес и порт, на который отсылаются сообщения SNMP-менеджеру, идентификатор и IP-адрес отправителя трап-сообщения, версия SNMP, в которой создаются трап-сообщения.

14.1 Выдача статистики

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.

База данных MIB, поддерживаемая SNMP-агентом, приведена в документе «Программный продукт «Клиент безопасности Bel VPN Client-P 4.1». Руководство администратора. Протоколирование и мониторинг» (BY.ПТНК.41002-01 34 01-03).