

УТВЕРЖДЕНО

BY.PTHK.00004-04.1 34 01-8-ЛУ

**Программный комплекс
«Шлюз безопасности виртуальный
Bel VPN Gate-V 4.1»**

Руководство администратора

Специализированные команды

BY.PTHK.00004-04.1 34 01-8

Листов 87

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

Содержание

| | |
|------------------------------------------|----------|
| Содержание | 2 |
| Специализированные команды | 5 |
| Информация о Продукте | 6 |
| ver_show | 6 |
| Проверка целостности | 7 |
| belvpn_verify | 7 |
| avverify | 8 |
| integr_mgr check | 8 |
| integr_mgr calc | 9 |
| Работа с сертификатами | 10 |
| cert_mgr create | 10 |
| cert_mgr import | 11 |
| cert_mgr show | 13 |
| cert_mgr remove | 14 |
| cert_mgr check | 15 |
| Работа с предопределенными ключами | 17 |
| key_mgr show | 17 |
| key_mgr list | 17 |
| key_mgr import | 18 |
| key_mgr remove | 18 |
| Работа с LSP конфигурацией | 20 |
| lsp_mgr show | 20 |
| lsp_mgr show-info | 21 |
| lsp_mgr load | 22 |
| lsp_mgr unload | 22 |
| lsp_mgr reload | 23 |
| lsp_mgr check | 23 |
| Работа с сетевыми интерфейсами | 24 |
| if_show | 24 |
| Работа с DefaultDriverPolicy | 27 |

| | |
|------------------------------------------------------|----|
| dp_mgr show | 27 |
| dp_mgr set | 27 |
| Настройка протоколирования | 29 |
| log_mgr set | 29 |
| log_mgr show | 32 |
| Просмотр и удаление защищенных соединений (SA) | 34 |
| sa_mgr show | 34 |
| sa_mgr clear | 38 |
| Работа с лицензией | 40 |
| lic_mgr show | 40 |
| lic_mgr set | 40 |
| Работа с настройками IPsec драйвера | 42 |
| drv_mgr | 42 |
| drv_mgr show | 48 |
| drv_mgr set | 49 |
| drv_mgr reload | 49 |
| Просмотр TCP-соединений | 50 |
| fwconn_show | 50 |
| Просмотр сообщений IPsec-драйвера | 53 |
| klogview | 53 |
| Работа с криптоконтейнерами | 73 |
| Сообщения об ошибках | 80 |

| | |
|----------------------------------|----|
| cryptocont x | 73 |
| cryptocont e | 73 |
| cryptocont n | 74 |
| cryptocont c | 74 |
| cryptocont r | 75 |
| cryptocont l | 76 |
| cryptocont t | 76 |
| cryptocont i | 77 |
| cryptocont ex | 77 |
| cryptocont im | 78 |
| cryptocont g | 78 |
| Ограничения на имена контейнеров | 79 |

Специализированные команды

В состав ПК Bel VPN Gate-V входит ряд утилит командной строки, предназначенных для управления общими настройками Продукта.

Утилиты находятся в каталоге `/opt/VPNagent/bin` и могут вызываться из shell (без необходимости указывать полный путь к файлу).

Все эти утилиты можно также запускать из CLI консоли с помощью команды `run`.

Запуск утилит командной строки с опцией `-h` вызывает помощь.

Все утилиты, обращающиеся к VPN daemon, имеют опцию `-T <timeout>`, устанавливающую максимальное время ожидания ответа от vpnsvc сервиса. Опция глобальная и должна указываться в начале списка опций, с которыми запускается утилита. Например, команда `sa_mgr -T 0 show` – корректная, а `sa_mgr show -T 0` – нет. Если опция не указана явно, то утилита ожидает ответа от демона в течение времени, установленного по умолчанию для этой утилиты.

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

Информация о Продукте

ver_show

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

Синтаксис

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

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

Пример

```
ver_show
```

```
Build information:
product name:      S-Terra Gate
product release:   4.1
product build number: 4.1.13925
product build date: 2013-09-18 14:25:05
product target CPU: amd64

System information:
OS information:    Linux 2.6.32-5-amd64 #1 SMP Tue May 7 18:21:34
MSK 2013
license information: GATE10000,test,101
crypto provider:   AvC 1.0 (Build 7774)
```

Проверка целостности

`belvpn_verify` – для стартовой и регламентной проверки целостности программной части установленного Продукта.

`avverify` – для проверки целостности заданного файла программной части установленного Продукта.

`integr_mgr check` – для проверки целостности информационной части Продукта.

`integr_mgr calc` – для вычисления хэш-суммы указанного файла.

belvpn_verify

Утилита `belvpn_verify` используется для регламентной проверки целостности программной части ПАК Bel VPN Gate во время его работы. Эта же утилита автоматически запускается при каждом старте программного комплекса, а также после процедуры инициализации ПАК Bel VPN Gate.

Синтаксис

```
/opt/VPNagent/bin/belvpn_verify [-n]
```

`-n` запрет на завершение работы VPN daemon.

Рекомендации по использованию

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

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

где

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

`<full_file_path>` – полный путь к проверяемому файлу.

При запуске утилита проверяет целостность именно этого списка файлов.

Утилита `belvpn_verify` размещена на ПАК в каталоге `/opt/VPNagent/bin` и запускается командой:

```
/opt/VPNagent/bin/belvpn_verify
```

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

Эта же утилита автоматически запускается при каждом старте программного комплекса, а также после процедуры инициализации ПАК Bel VPN Gate.

Если проверка прошла успешно, то никакого сообщения не выдается.

При обнаружении ошибки работа утилиты прекращается с ненулевым кодом возврата и в файл лога `/opt/VPNagent/bin/belvpn_verify_err.log` передается сообщение об ошибке. Затем, в случае запуска утилиты без ключа `-n`, проверяется работа VPN daemon. При его наличии – выполняется аварийное прерывание.

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

При нарушении целостности работающего ПАК Bel VPN Gate восстановите ПАК согласно [«Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Инструкция по восстановлению»](#).

avverify

Утилита `avverify` используется для проверки целостности файлов программной части установленного Продукта.

Синтаксис

```
/opt/VPNagent/bin/avverify [-h|-e] filePath
```

| | |
|-----------------------|----------------------------------------------------|
| <code>-h</code> | проверка будет проводиться по хэш-значению |
| <code>-e</code> | проверка будет проводиться по ЭЦП |
| <code>filePath</code> | имя проверяемого файла, включая полный путь к нему |

Рекомендации по использованию

integr_mgr check

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

Синтаксис

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

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

Рекомендации по использованию

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

```
agent.ini
csp_ipsec_drv.cfg
s_logset.ini
syslog.ini
x509conv.ini
```

Все эти файлы лежат в каталоге `/opt/VPNagent/etc`. Значение контрольной суммы для каждого из этих файлов записано в файл с тем же именем, но с расширением `hash`, например, `/opt/VPNagent/s_logset.ini.hash`.

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

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

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

При проверке списка файлов работа утилиты не прерывается по первому несовпадению хэш-суммы, а также при любых других ошибках контроля целостности – ошибки доступа к файлу, отсутствие предварительно вычисленной хэш-суммы и прочих аналогичных ошибках. При каждой наступившей ошибке (если не указана опция `-q`) об этом выдаётся сообщение: имя обрабатываемого файла, код ошибки, расшифровка распространённых ошибок и проверка продолжается.

Опцию `-q` удобно использовать, если есть необходимость в вызове данной утилиты из какого-либо дополнительного скрипта.

Пример

Проверяется целостность файла `s_logset.ini`:

```
integr_mgr check -f /opt/VPNagent/etc/s_logset.ini
```

integr_mgr calc

Утилита `integr_mgr calc` используется для вычисления хэш-суммы указанного файла по алгоритму СТБ 34.101.31-2011 (п.6.9).

Синтаксис

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

- | | |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-f filePath</code> | имя файла (включая полный путь к нему), для которого будет вычисляться хэш сумма |
| <code>-q</code> | запрет вывода текстовых результатов работы утилиты. Итоговый результат работы утилиты при использовании этой опции возможно узнать только из кода ошибки, возвращаемого утилитой. Допустимо указание ключа <code>-q</code> либо сразу после названия команды, либо в конце командной строки. |

Рекомендации по использованию

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

Пример

Вычисляется хэш-сумма для файла `syslog.ini`. В результате в той же папке появится файл `syslog.ini.hash`.

```
integr_mgr calc -f /opt/VPNagent/etc/syslog.ini
```

Работа с сертификатами

- `cert_mgr create` – создает ключевую пару и запрос на сертификат открытого ключа
- `cert_mgr import` – регистрирует CA, локальные сертификаты, сертификаты партнеров и CRL в базе Продукта
- `cert_mgr show` – для просмотра сертификатов и CRL в файле или базе Продукта
- `cert_mgr remove` – удаляет сертификаты из базы Продукта
- `cert_mgr check` – проверяет сертификаты в базе Продукта.

cert_mgr create

Команда `cert_mgr create` предназначена для генерации ключевой пары и создания запроса на сертификат открытого ключа.

Синтаксис

```
cert_mgr [-T timeout] create -subj CERT_SUBJ [-RSA|-DSA] [-512|-1024] [-mail MAIL] [-ip IP_ADDR] [-dns DNS] [-kc K_CONTAINER_NAME] [-kcp K_CONTAINER_PWD] [-f OUT_FILE_NAME]
```

- `-T timeout` время ожидания ответа от VPN daemon. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд
- `-subj CERT_SUBJ` значение поля Subject Name сертификата
- `-RSA` идентификатор алгоритма RSA, который будет использован для генерации ключевой пары. Затем секретный ключ будет применен для формирования ЭЦП для создаваемого запроса
- `-DSA` идентификатор алгоритма DSA, который будет использован для генерации ключевой пары. Затем секретный ключ будет применен для формирования ЭЦП для создаваемого запроса
- `-512` длина открытого ключа – 512 бит (только для алгоритмов RSA и DSA)
- `-1024` длина открытого ключа – 1024 бита (только для алгоритмов RSA и DSA)
- `-mail MAIL` значение поля Mail для альтернативного имени (Alternative Subject Name) владельца сертификата, которое может использоваться в качестве идентификатора владельца
- `-ip IP_ADDR` значение поля IP Address для альтернативного имени (Alternative Subject Name) владельца сертификата, которое может использоваться в качестве идентификатора владельца
- `-dns DNS` значение поля DNS для альтернативного имени (Alternative Subject Name) владельца сертификата, которое может использоваться в качестве идентификатора владельца
- `-kc K_CONTAINER_NAME` имя контейнера с секретным ключом
- `-kcp K_CONTAINER_PWD` пароль к контейнеру с секретным ключом

`-f OUT_FILE_NAME` имя файла, в который будет помещен запрос на сертификат в формате PKCS#10.

Значение по умолчанию

По умолчанию используется алгоритм RSA и открытый ключ длиной 512 бит.

Рекомендации по использованию

Для проверки подлинности документа и аутентификации партнера используется электронно-цифровая подпись (ЭЦП), которая использует алгоритмы RSA, DSA. Для формирования ЭЦП нужен личный ключ, а для проверки ЭЦП – открытый ключ.

Используйте команду `cert_mgr create` для создания ключевой пары и запроса на сертификат, чтобы не нужно было переносить контейнер с секретным ключом с одного компьютера на другой.

Если при написании команды не указать опцию `-f` с именем файла для размещения запроса на сертификат, то сформированный запрос будет выведен на экран в формате b64.

Можно и другим способом создать ключевую пару. При использовании «AvC ver.1.0» используется утилита `cryptocont`.

Пример

Ниже приведен пример создания запроса на сертификат с использованием алгоритма RSA:

```
cert_mgr create -subj "O=S-Terra-Bel,CN=LocalCert" -RSA -dns s-terra.by -
f /opt/VPNagent/bin/certs/local_cert
```

cert_mgr import

Команда `cert_mgr import` предназначена для регистрации CA, локальных сертификатов, сертификатов партнеров и CRL в базе Продукта.

Синтаксис

```
cert_mgr [-T timeout] import -f C_FILE [-p C_FILE_PWD] [-i OBJ_INDEXN]
[-t | -l | -kc K_CONTAINER_NAME [-kcp K_CONTAINER_PWD]
[-kf K_FILE [-kfp K_FILE_PWD]]]
```

- `-T timeout` время ожидания ответа от VPN daemon. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд
- `-f C_FILE` путь к файлу с сертификатами и/или CRL
- `-p C_FILE_PWD` пароль к файлу с сертификатами или CRL. Необязательный параметр. Используется только для доступа к файлам, защищенным паролем
- `-i OBJ_INDEXN` индекс объекта (сертификата или CRL) в файле, который задает номер искомого сертификата (CRL) в файле. При импорте одного сертификата (CRL) из файла, содержащего один сертификат, данный параметр можно не указывать, он будет равен 1. Индекс задается в виде целого десятичного числа. В качестве индекса нельзя указывать 0
- `-t` используется при регистрации CA сертификата, регистрируемому сертификату присваивается статус `trusted`. При использовании

- этой опции запрещается использование опций `-kc,-kcp`.
Запрещается использовать эту опцию при импорте CRL
- `-l` признак, что сертификат должен быть импортирован как локальный (допустимо только для случая, когда сертификат является ответом на запрос, созданный с помощью `cert_mgr create`; несовместимо с опцией `-kc`).
- `-kc K_CONTAINER_NAME` уникальное имя контейнера с секретным ключом локального сертификата. Не может использоваться, если ранее введена опция `-t` или `-l`.
- См. [Примечание](#) для получения уникального имени контейнера с секретным ключом, а также копирования контейнера с одного ключевого носителя на другой.
- `-kcp K_CONTAINER_PWD` пароль к контейнеру с секретным ключом локального сертификата. Необязательный параметр. Используется тогда, когда контейнер с секретным ключом защищен паролем
- `-kf K_FILE` путь к файлу с секретным ключом регистрируемого сертификата. Необязательный параметр. Не может использоваться, если ранее введена опция `-t` или `-l`. Опция допустима только для RSA или DSA сертификатов
- `-kfp K_FILE_PWD` пароль к файлу с секретным ключом регистрируемого сертификата. Необязательный параметр. Используется, если файл с секретным ключом защищен паролем. Опция допустима только для RSA или DSA сертификатов.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для импорта сертификатов и/или CRL в базу Продукта. При импорте нескольких объектов из одного файла используйте последовательное описание параметров импортируемых объектов.

Для успешной регистрации CA сертификата в Продукте, в сертификате в поле `Basic Constraints` (Основные ограничения) CA обязательно должен иметь значение `TRUE`. В противном случае, такой CA сертификат зарегистрирован не будет с выдачей сообщения об ошибке.

Работа с ключевым носителем типа AvPass или AvBign

Если контейнер находится на ключевом USB-носителе AvPass или AvBign, то в качестве пароля к контейнеру должен использоваться PIN-код к токenu.

Имя контейнера должно содержать префикс `"av:"`. Может быть вставлен только один токен.

```
cert_mgr import -f har_st_test21.cer -kc av:contname -kcp 1234567890
```

Пример

Регистрация локального сертификата, размещенного в файле `gate02.cer`, секретный ключ к нему размещен в контейнере на жестком диске `HDIMAGE\\GATE02` и защищен паролем `1111`:

```
cert_mgr import -f /opt/certs/gate02.cer -kc 'HDIMAGE\\GATE02' -kcp 1111
```

Регистрация в базе Продукта с присвоением статуса `"trusted"` CA сертификата, размещенного в файле `ca.cer`:

```
cert_mgr import -f /opt/ca.cer -t
```

cert_mgr show

Команда `cert_mgr show` предназначена для просмотра сертификатов и CRL, размещенных в файле или базе Продукта. Могут также обрабатываться файлы формата PKCS#7 и PKCS#12. Файлы формата PKCS#12 могут быть защищены паролем.

Синтаксис

```
cert_mgr [-T timeout] show [-f C_FILE [-p C_FILE_PWD]] [-i OBJ_INDEX_1]
... [-i OBJ_INDEX_N] [-expired_remote]
```

- `-T timeout` время ожидания ответа от VPN daemon. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд
- `-f C_FILE` путь к файлу с сертификатами и CRL. Если данная опция не указана, то будут показаны все сертификаты из базы Продукта
- `-p C_FILE_PWD` пароль к файлу с сертификатами и CRL
- `-i OBJ_INDEX_N` индекс объекта (сертификата и CRL) в файле или в базе Продукта. Если при написании команды указан путь к файлу, то индекс будет определять номер искомого сертификата (CRL) в файле. Если же путь к файлу не указан, то этот индекс будет применяться к базе Продукта сертификатов и CRL
- `-expired_remote` показать все сертификаты партнеров, срок действия которых истек. Сертификаты, не вступившие в силу, не показываются.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра содержимого файла с сертификатами и CRL, или базы Продукта, а также для просмотра деталей конкретных сертификатов или CRL.

Для просмотра всего списка объектов в файле или базе Продукта индекс `i` и опция `expired_remote` не указываются. В этом случае будет выдан нумерованный список сертификатов и CRL с указанием поля `Subject` для сертификатов и поля `Issuer` для списка CRL.

Для просмотра деталей конкретного сертификата или CRL обязательно используйте индекс этого объекта в файле или базе Продукта. В этом случае будет выдана детальная информация о сертификате или CRL. Для просмотра деталей нескольких объектов следует последовательно перечислить индексы этих объектов в опции `-i`.

Пример

Пример детального просмотра локального сертификата, размещенного в базе Продукта под номером 1, и размещение соответствующего ему контейнера с секретным ключом:

```
cert_mgr show -i 1
```

```
1 Status: local
   Subject: 1.2.840.113549.1.9.1=user_sc_cp_01@s-
   terra.com,C=RU,L=Moscow,O=S-Terr
   a CSP,OU=Devel,CN=user_sc_cp_01
   Issuer: 1.2.840.113549.1.9.1=har@s-terra.com,C=RU,L=Moscow,O=S-
   Terra CSP,OU=De
```

```

vel,CN=Test CA sc-cp

Valid from: Wed Nov 23 07:56:02 2012
Valid to:   Thu Nov 23 08:06:02 2013
Version: 3
Serial number: 04 11 83 A5 00 00 00 00 05
Signature algorithm: GOST_R_341001_3411 (Crypto-Pro)
Public key: GOST R 341001(512)
Hash MD5:   68 3B 05 2A E9 5D 11 17 89 64 F2 AB 2D 61 D9 39
Hash SHA1:  D3 82 56 D5 39 A2 69 24 37 46 4C 41 D7 93 A8 C1 C3 02
32 B8

DP[0]:      URI=ldap:///CN=\=Test%20CA%20sc-cp\,CN\=har-test-
w2ks\,CN\=CDP\,CN\=Public%20Key%20Services\,CN\=Services\,CN\=Confi
guration\,DC\=har-test-dc\,DC\=s-
terra\,DC\=com?certificateRevocationList?base?objectclass\=cRLDistr
ibutionPoint

CRLI[0]:    1.2.840.113549.1.9.1=har@s-terra.com,C=RU,L=Moscow,O=S-
Terra CSP,OU=Devel,CN=Test CA sc-cp

DP[1]:      URI=http://har-test-w2ks.har-test-dc.s-
terra.com/CertEnroll/Test%20CA%20sc-cp.crl

CRLI[1]:    1.2.840.113549.1.9.1=har@s-terra.com,C=RU,L=Moscow,O=S-
Terra CSP,OU=Devel,CN=Test CA sc-cp

Private key container name: 'HDIMAGE\user_sc_cp_01'

```

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

```
cert_mgr show -expired_remote
```

```

3 Status: remote

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

```

cert_mgr remove

Команда `cert_mgr remove` предназначена для удаления сертификатов из базы Продукта.

Синтаксис

```
cert_mgr [-T timeout] remove {-i OBJ_INDEX_1 | -expired_remote}..[-i OBJ_INDEX_N]
```

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

-i OBJ_INDEX_N индекс объекта (сертификата) в контейнере или базе Продукта.

-expired_remote сертификаты партнеров, срок действия которых истек (сертификаты, не вступившие в силу, не удаляются).

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для удаления сертификатов из базы Продукта. Удалять можно как один, так и несколько сертификатов.

Для удаления нескольких сертификатов следует последовательно указать номера (индексы) удаляемых сертификатов, под которыми они хранятся в базе Продукта.

Удаление из базы Продукта списка CRL невозможно. Если в команде будет указан номер (индекс) CRL, будет выведено сообщение об ошибке о недопустимом индексе.

Пример

Пример удаления сертификатов из базы Продукта. При написании команды были указаны индексы объектов 1, 2 и 3. Индексы 1 и 2 соответствовали сертификатам, а под индексом 3 в базе хранился список CRL. На попытку удаления CRL программа выдает сообщение об ошибке:

```
cert_mgr remove -i 1 -i 2 -i 3
```

```
1 OK O=S-Terra,CN=Technological Cert
2 OK O=S-Terra,CN=CA Cert
User Error: CRL can not be removed from base
Other operations are cancelled due to error
```

cert_mgr check

Команда `cert_mgr check` предназначена для проверки сертификатов, находящихся в базе Продукта.

Синтаксис

```
cert_mgr [-T timeout] check [-i OBJ_INDEX01] [-i OBJ_INDEX0N]
```

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

-i OBJ_INDEX0N порядковые номера интересующих сертификатов.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Порядковые номера сертификатов совпадают с номерами объектов, находящихся в базе Продукта. При указании номеров сертификатов проверяются только они. При отсутствии номеров сертификатов проверяются все сертификаты, находящиеся в базе Продукта.

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

- `Certificate is invalid` – неверный формат сертификата
- `Certificate is expired` – срок действия сертификата истек
- `Certificate is not valid yet` – время действия сертификата еще не наступило
- `Certificate is revoked` – сертификат отозван
- `Certificate can not be verified` – сертификат не удается проверить:
 - в базе отсутствует сертификат(ы) для построения цепочки сертификатов с корректным конечным СА сертификатом, которому мы доверяем
 - в базе нет необходимого CRL для проверки одного из сертификатов цепочки, подобная ситуация может возникнуть при включении проверки CRLs (загружена DDP или в загруженной конфигурации явно задано `CRLHandlingMode = ENABLE`)
- `Private key container is not accessible` – нет доступа к контейнеру с секретным ключом
- `Private key is not accessible` – нет доступа к секретному ключу
- `Private key is not consistent certificate` – секретный ключ не подходит к сертификату
- `It is certificate request` – данный объект является сертификатным запросом.

Работа с предопределенными ключами

`key_mgr show` – для просмотра предопределенных ключей, зарегистрированных в базе Продукта

`key_mgr list` – для просмотра списка предопределенных ключей, зарегистрированных в базе Продукта

`key_mgr import` – для регистрации предопределенных ключей в базе Продукта

`key_mgr remove` – для удаления предопределенных ключей из базы Продукта.

key_mgr show

Команда `key_mgr show` предназначена для просмотра предопределенных ключей, зарегистрированных в базе Продукта.

Синтаксис

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

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

При выполнении этой команды будут выводиться следующие данные:

- количество предопределенных ключей, обнаруженных в базе Продукта
- имя ключа
- тело ключа в печатном виде или hex-представлении. Если тело ключа содержит непечатные символы, то при выводе в печатном виде они заменяются на ' .' (символ точка).

Пример

Пример выполнения команды `key_mgr show`:

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

key_mgr list

Команда `key_mgr list` предназначена для просмотра списка предопределенных ключей, зарегистрированных в базе Продукта.

Синтаксис

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

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

При выполнении этой команды будут выводиться следующие данные:

- количество предопределенных ключей
- для каждого ключа:
 - имя ключа

key_mgr import

Команда `key_mgr import` предназначена для импорта предопределенных ключей из файловой системы в базу Продукта.

Синтаксис

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

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

-n KEY_NAME имя предопределенного ключа

-f KEY_FILE путь к файлу, содержащему предопределенный ключ.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для регистрации предопределенных ключей в базе Продукта.

Пример

Пример импорта предопределенных ключей из файлов в базу Продукта:

```
key_mgr import -f key1 -n key1name -f key2 -n key2name -f key3 -n key3name
```

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

key_mgr remove

Команда `key_mgr remove` предназначена для удаления предопределенных ключей из базы Продукта.

Синтаксис

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

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

-n KEY_NAME имя предопределенного ключа.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для удаления предопределенных ключей из базы Продукта.

Пример

Пример удаления предопределенного ключа:

```
key_mgr remove -n keylname
```

```
OK keylname
```

Работа с LSP конфигурацией

`lsp_mgr show` – для просмотра текущей конфигурации

`lsp_mgr show-info` – для просмотра информации о текущей конфигурации

`lsp_mgr load` – для загрузки конфигурации из файла в базу Продукта

`lsp_mgr unload` – для загрузки политики Default Driver Policy

`lsp_mgr reload` – для перезагрузки LSP конфигурации

`lsp_mgr check` – для проверки LSP конфигурации.

lsp_mgr show

Команда `lsp_mgr show` предназначена для просмотра текущей конфигурации.

Синтаксис

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

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

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра конфигурации, действующей в данный момент. В базе Продукта присутствует всего две конфигурации: Default Driver Policy и конфигурация, в которой записана созданная политика безопасности.

Поэтому, если текущей является созданная политика безопасности, то по команде `lsp_mgr show` на экран будет выведен весь текст native-конфигурации, а если текущей является политика DDP, то выдается сообщение – Default Driver Policy is loaded.

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

При просмотре native-конфигурацию можно сохранить в файл, например `current.lsp`, командой

```
lsp_mgr show > current.lsp,
```

затем отредактировать в текстовом редакторе, например `vi`, и сохранить.

Пример

Ниже приведен пример вывода текущей конфигурации:

```
lsp_mgr show
```

```
GlobalParameters (
```

```

    Title = "Automatically generated LSP.
Conversion Date/Time: Feb 19 14:41:08 2013"
    Version = "LSP_4_1"
    CRLHandlingMode = DISABLE
)
ESPProposal
    Transform* = ESPTransform
    CipherAlg* = "AES-K192-CBC-12"
    IntegrityAlg* = "GR341194CPR01-H96-HMAC-254"
    LifetimeSeconds = 3600
    LifetimeKilobytes = 4608000 ))

```

lsp_mgr show-info

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

Выводится следующая информация:

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

Source – источник локальной политики безопасности – command line | cs_console

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

Для Source "command line" – значение LABEL в опции -l команды [lsp_mgr load](#).

Для Source "cs_console" – заголовок LSP (значение GlobalSettings.Title).

Синтаксис

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

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

-db показать информацию о конфигурации пользователя, хранящейся в базе локальных настроек продукта.

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

Ниже приведен пример вывода информации о текущей конфигурации:

```
lsp_mgr show-info
```

```

Type: user-defined
Source: cs_console
Source info: This LSP was automatically generated by CSP Converter
at Mon May 06
18:18:37 2013

```

lsp_mgr load

Команда `lsp_mgr load` предназначена для загрузки конфигурации из файла в базу Продукта. При этом загруженная конфигурация становится активной.

Синтаксис

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

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

Значение по умолчанию Значение по умолчанию отсутствует.



Note

После загрузки отредактированной конфигурации командой `lsp_mgr load`, внесенные изменения будут присутствовать только в native-конфигурации (LSP), в cisco-like конфигурации этих изменений не будет. При следующей конвертации cisco-like конфигурации внесенные изменения в native-конфигурации исчезнут. Предыдущая измененная конфигурация будет сохранена в файле `non_cscons.lsp` (см. раздел «Логика запуска конвертора» в документе [«Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Приложение»](#)).

Пример

Пример загрузки конфигурации из файла в базу Продукта:

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

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

lsp_mgr unload

Команда `lsp_mgr unload` предназначена для выгрузки LSP конфигурации и загрузки политики Default Driver Policy.

Синтаксис

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

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для загрузки конфигурации DDP, которая и будет являться текущей. По команде `lsp_mgr show` будет выдано сообщение – Default Driver Policy is loaded.

Политика драйвера по умолчанию (DDP) задается командой `dp_mgr set`.

Пример

Ниже приведен пример загрузки политики DDP:

```
lsp_mgr unload
```

```
Operation completed successfully
```

lsp_mgr reload

Команда `lsp_mgr reload` предназначена для перезагрузки LSP конфигурации. В этом случае LSP конфигурация будет являться текущей.

Синтаксис

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

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте команду `lsp_mgr reload` в следующих случаях:

- для загрузки LSP конфигурации, если перед этим командой `lsp_mgr unload` эта LSP конфигурация была выгружена и загружена политика DDP
- для устранения всех установленных соединений с партнерами
- во внештатных ситуациях – зависание Продукта и др.

Пример

Ниже приведен пример загрузки LSP конфигурации из базы Продукта:

```
lsp_mgr reload
```

```
LSP is reloaded successfully.
```

lsp_mgr check

Команда `lsp_mgr check` предназначена для проверки синтаксиса файла с LSP конфигурацией.

Синтаксис

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

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

`-f LSP_FILE` путь к файлу конфигурации.

Значение по умолчанию Значение по умолчанию отсутствует.

Работа с сетевыми интерфейсами

if_show

Команда `if_show` предназначена для просмотра логических, физических имен и других параметров сетевых интерфейсов, как защищаемых, так и не контролируемых Продуктом.

Синтаксис

```
if_show [-all]
```

`-all` на экран будут выданы все логические имена интерфейсов, записанные в файле `ifaliases.cf`.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра параметров всех сетевых интерфейсов.

Без указания опции `-all` на экран будут выданы только актуальные логические имена интерфейсов, читаемые из драйвера.

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

При задании опции `-all` на экран будут выданы все логические имена интерфейсов, записанные в специальном файле `/etc/ifaliases.cf`, созданном при настройке ОС. Эта команда полезна для получения логического имени интерфейса перед редактированием атрибута `LogicalName` в структуре `NetworkInterface` в LSP (см. документ «[Программно-аппаратный комплекс Bel VPN Gate 4.1. Создание конфигурационного файла](#)»).

Примечание 1

В файле `/etc/ifaliases.cf` отражено соответствие логического имени, и имени интерфейса в системе посредством структуры `"interface"` с двумя обязательными полями `name` и `pattern`,

где

`name` – логическое имя интерфейса, которое задается в LSP (в атрибуте `LogicalName` структуры `NetworkInterface`) и в `cs-console`

`pattern` – шаблон для имени интерфейса в системе.

Пример:

```
interface (name="FastEthernet0/0" pattern="eth0")
interface (name="FastEthernet0/1" pattern="eth1")
interface (name="default" pattern="*")1
```

¹ Имя "default" имеет специальное значение для LSP - подставляется по умолчанию (если имя интерфейса (`NetworkInterface.LogicalName`) не задано).

Примечание 2

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

Примечание 3

LSP загружена не будет, если для логического имени интерфейса в структуре `NetworkInterface` не найдена соответствующая запись с тем же именем в файле `ifaliases.cf`, и при этом в файл лога будет выдано предупреждение:

```
(00100111) «[CFG] no physical interface found for NetworkInterface "%{1}s" pattern "%{2}s"»
```

где

`%{1}s` – LogicalName этого `NetworkInterface`

`%{2}s` – шаблон имени, найденный по LogicalName»

При загрузке конфигурации не найдено ни одного сетевого интерфейса, соответствующего описанию `NetworkInterface`.

Примечание 4

Присутствовавшие в предыдущей версии Шлюза безопасности Bel VPN Gate 3.0.1 утилиты `if_mgr add` и `if_mgr remove` в данной версии Шлюза безопасности Bel VPN Gate 4.1 отсутствуют, добавлять и удалять интерфейсы из базы Продукта и задавать для них политику следует в атрибуте `LogicalName` структуры `NetworkInterface` в LSP или в `cs_console`.

Пример

Ниже приведен пример выполнения команды `if_show`:

```
[root@cspgate]# if_show
```

```
Logical network interface "eth0":
    Physical name exact template: "eth0"

    Physical name: eth0
    State:         UP
    Index:         2
    MTU:           1500
    MAC addr:      00:0C:29:16:DE:8A
    IP addr:       10.0.10.106 mask 255.255.0.0 brd 10.0.255.255

Logical network interface "eth1":
    Physical name exact template: "eth1"

    Physical name: eth1
    State:         DOWN
    Index:         3
    MTU:           1500
    MAC addr:      00:0C:29:16:DE:94
    IP addr:       192.168.15.106 mask 255.255.255.0 brd 192.168.15.255
```

```
IP addr:      192.168.15.108 mask 255.255.255.255 brd 0.0.0.0
```

Logical network interface "pps":

Physical name template: "pp*"

Physical name: pp0

State: UP

Index: 14

MTU: 1200

MAC addr:

```
IP addr:      1.1.1.2 mask 255.255.255.255 brd 0.0.0.0
```

Работа с DefaultDriverPolicy

`dp_mgr show` – для просмотра настроек DDP

`dp_mgr set` – для настройки параметров DDP.

dp_mgr show

Команда `dp_mgr show` предназначена для просмотра установленных настроек политики драйвера по умолчанию – Default Driver Policy (DDP). Эта политика может принимать следующие значения:

| | |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>passall</code> | пропускать весь трафик. |
| <code>passdhcp</code> | 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. |
| <code>dropall</code> | ничего не пропускать (для релиза 14101 это значение недоступно). |

Default Driver Policy действует в следующих случаях:

- при старте Продукта до загрузки локальной политики безопасности (LSP)
- при незагрузке LSP из-за какой-либо ошибки
- при отсутствии LSP в базе Продукта
- при загрузке DDP командой `lsp_mgr unload`.

Синтаксис

```
dp_mgr [-T timeout] show
```

| | |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-T timeout</code> | время ожидания ответа от VPN daemon. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд. |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

Пример выполнения команды `dp_mgr show`:

```
dp_mgr show
```

```
Default driver policy : passall
```

dp_mgr set

Команда `dp_mgr set` предназначена для настройки параметров DDP.

Синтаксис

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

```
dp_mgr [-T timeout] set [-ddp {passall|passdhcp}] (синтаксис команды для релиза 14101)
```

- T timeout время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд
- ddp {passall|passdhcp|dropall} устанавливает Default Driver Policy в один из режимов: passall (пропускать весь трафик), passdhcp (пропускать только DHCP пакеты), dropall (не пропускать трафик (для релиза 14101 этот режим недоступен)).

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

Ниже приведен пример выполнения команды dp_mgr set:

```
dp_mgr set -ddp passall
```

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

Настройка протоколирования

`log_mgr set` – для настройки syslog-клиента и создания групп событий со своим уровнем протоколирования каждой.

`log_mgr show` – для просмотра уровня протоколирования всех событий, групп событий и настроек syslog-клиента.

log_mgr set

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

Синтаксис

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

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

-l log_level уровень протоколирования всех событий, не включенных в группы событий. Имеет одно из возможных значений:

- emerg – аварийные сообщения
- alert – тревожные сообщения
- crit – критические сообщения
- err – сообщения об ошибках
- warning – предупреждения
- notice – извещения
- info – информационные сообщения
- debug – отладочные сообщения.

-e msg_group_file имя файла msg_grpXXX.ini, в котором можно задать группу событий и уровень протоколирования для нее

-f (force) указание этой опции разрешает изменять файл с группой событий. По умолчанию опция не задана и изменение файла не допускается

-y {enable|disable} включение/выключение протоколирования

-a syslog_ip IP-адрес хоста, на который будут отправляться сообщения (syslog-клиент)

`-f facility` источник сообщений (начальное значение: local7). Возможные значения: kern, user, mail, daemon, auth, syslog, lpr, news, uucp, cron, authpriv, ftp, ntp, audit, alert, cron2, local0, local1, local2, local3, local4, local5, local6, local7.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

```
log_mgr set -l warning
```

2. Продукт поставляется с пятью предустановленными файлами, размещенными в каталоге /opt/VPNagent/etc, в которых указаны группы событий и уровень лога для этих событий. Эти файлы созданы для совместимости с продуктом Шлюза безопасности Bel VPN Gate 3.0.1:

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

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

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

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

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

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

```
log_mgr save
```

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

```
log_mgr set -e
```

Настройка сохраняется до перезапуска сервиса.

Создание файла с группами событий

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

Каждый такой файл должен состоять из секций вида:

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

```
<MSG_ID2>
!.....
```

где

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

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

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

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

Пример такого файла – “msg_groupDEMO1.ini”:

```
[LOGLEVEL.DEBUG]

!сообщение PRODUCT_START задано его индексом:
03090001

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

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

5. Установка параметров syslog-клиента для VPN daemon. Установленные настройки Syslog-клиента будут записаны в файл /opt/VPNagent/etc/syslog.ini.

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

Например,

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

Неуказанный в команде параметр остается неизменным.

6. Установка параметров по умолчанию для syslog-клиента:

```
log_mgr reset-syslog
```

при этом действуют следующие настройки:

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

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

Пример

Пример выполнения команды `log_mgr set`:

```
log_mgr set -l warning
```

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

log_mgr show

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

Синтаксис

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

```
log_mgr [-T timeout] show-syslog
```

`-T timeout` время ожидания ответа от VPN daemon. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд

`-e msg_group_file.ini` имя файла `msg_group_file.ini`, в котором указана группа событий и уровень протоколирования для них

`show-syslog` вывод настроек syslog-клиента.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

1. Для вывода значения общего уровня протоколирования всех событий, не включенных в группы, используйте команду:

```
log_mgr show
```

2. Вывод уровня протоколирования групп событий и идентификаторов этих событий осуществляется только после их редактирования, для вывода используйте команду:

```
log_mgr show -e
```

3. Вывод уровня протоколирования группы событий, указанных в файле, и идентификаторов этих событий, осуществляется только после редактирования этого файла, для вывода используйте команду:

```
log_mgr show -e msg_group_file.ini
```

4. Для вывода настроек syslog-клиента используйте команду:

```
log_mgr show-syslog
```

Пример

Пример выполнения команды `log_mgr show`:

```
log_mgr show-syslog
```

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

```
log_mgr show -e /opt/VPNagent/etc/msg_grpLDAP.ini
```

```
[LEVEL.DEBUG]
```

```
MSG_ID_LDAP_REQ_NOT_FOUND
```

```
MSG_ID_LDAP_CREATE_REQ_FAILED
```

```
MSG_ID_LDAP_PARSE_FAILED
```

```
MSG_ID_LDAP_REQ_FAILED_TIMEOUT
```



```
MSG_ID_LDAP_REQ_FAILED_NOT_RESPOND  
MSG_ID_LDAP_REQ_FAILED_CANCELED  
MSG_ID_LDAP_REQ_FAILED_CONNECTION_CLOSED  
MSG_ID_LDAP_REQ_FAILED_UNKNOWN  
MSG_ID_LDAP_REQ_SUCCESS  
MSG_ID_LDAP_REQ_START
```

Просмотр и удаление защищенных соединений (SA)

`sa_mgr show` – для получения информации обо всех IPsec SA и ISAKMP SA

`sa_mgr clear` – для удаления ISAKMP и IPsec соединений.

sa_mgr show

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

Синтаксис

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

`-T timeout` время ожидания ответа от VPN daemon. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд

`-isakmp` выводится информация об ISAKMP соединениях

`-ipsec` выводится информация об IPsec соединениях

`-i CONNn_ID` выводится информация о соединении с указанным идентификатором

`-detail` выводится детальная информация о соединениях.

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

```
ISAKMP sessions: 0 initiated, 0 responded

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

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

В выводе присутствует следующая информация:

ISAKMP sessions – количество незавершенных IKE-обменов:

- `ni initiated` – в качестве инициатора

- `nr responded` – в качестве ответчика.

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

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

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

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

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

Данная команда выводит информацию о соединении с заданными свойствами.

IPsec connections:

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

```
sa_mgr show -detail
```

Команда с опцией detail выводит полную информацию обо всех соединениях.

```
ISAKMP sessions: 0 initiated, 0 responded

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

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

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

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

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

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

  remote identity (IPV4_ADDR): 10.0.10.16
  IPsecAction name: ipsec_action_01
  Filter LogEventID: filter_rule_00_00
  PFS: none

  inbound esp sa:
    spi: 0x94857A70(2491775600)
    transform: esp-gost2814789cp-cbc esp-gostr341194cp-hmac
    in use settings ={Tunnel, }
```

```
sa limits: key lifetime (k/sec): 4608000/3600
sa timing: remaining key lifetime (k/sec): 4607998/1426

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

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

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

В выводе присутствует следующая информация:

ISAKMP sessions – количество незавершенных IKE-обменов:

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

ISAKMP connection – в выводе будет присутствовать:

- поле IKECFG address, если был получен IKECFG адрес:

```
ISAKMP connection id: 1
cookies: F86F80B571D2240F.C177F15CAEA71B4A
local peer (addr/port): 10.0.10.193/500
remote peer (addr/port): 10.0.10.178/500
IKECFG address: 192.168.15.193
```

- поле Status может принимать следующие значения:
 - incomplete – недостроенное соединение
 - active – активное соединение
 - configuration – для данного SA проводится дополнительная настройка (IKECFG, XAuth, etc.)

- `deleted` – SA не используется, подготовлен к удалению
- `unknown` – статус соединения неизвестен

IPsec connection:

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

sa_mgr clear

Команда `sa_mgr clear` предназначена для удаления ISAKMP и IPsec соединений.

Синтаксис

```
sa_mgr [-T timeout] clear {-isakmp|-ipsec} [-i CONN1_ID]..[-i CONNn_ID]
[-silent]
```

```
sa_mgr [-T timeout] clear -all [-silent]
```

| | |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-T timeout</code> | время ожидания ответа от VPN daemon. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд |
| <code>-isakmp</code> | удаляет ISAKMP соединения |
| <code>-ipsec</code> | удаляет IPsec соединения |
| <code>-i CONNn_ID</code> | удаляет соединения с указанным идентификатором |
| <code>-silent</code> | удаляет соединения без уведомления партнера |
| <code>-all</code> | удаляет все IPsec и ISAKMP соединения во всех состояниях, прекращаются все ранее начатые IKE-обмены. |

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

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

При выполнении команды может появиться сообщение:

Timeout expired. Please ensure that all chosen SAs are cleared –Закончилось время ожидания завершения удаления соединений. Убедитесь, что все выбранные соединения удалены».

Пример

Удаление ISAKMP соединений с идентификаторами 1 и 4:

```
sa_mgr clear -isakmp -i 1 -i 4
ISAKMP connection 1 is removed
ISAKMP connection 4 is not found
```

Удаление всех IPsec соединений:

```
sa_mgr clear -ipsec
IPsec connection 1 is removed
IPsec connection 3 is removed
```

Удаление всех соединений:

```
sa_mgr clear -all
All connections are removed
или
Not all connections are removed
```

Работа с лицензией

`lic_mgr show` – показывает текущую лицензию на Продукт

`lic_mgr set` – устанавливает текущую Лицензию.

lic_mgr show

Команда `lic_mgr show` предназначена для просмотра текущей Лицензии на продукт Шлюз безопасности Bel VPN Gate 4.1.

Синтаксис

```
lic_mgr show
```

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

lic_mgr set

Команда `lic_mgr set` предназначена для установки текущей Лицензии. После установки Лицензии необходимо перезапустить VPN демона командами:

```
/etc/init.d/vpngate stop
/etc/init.d/vpngate start
```

Синтаксис

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

`-p PRODUCT_CODE` код Продукта, возможные коды:

```
GATE100
GATE100B
GATE100V
GATE1000
GATE1000V
GATE3000
GATE7000
GATE10000
RVPN
RVPNV
UVPN
UVPNv
KZVPN
KZVPNv
BELVPN
BELVPNv
```

`-c CUSTOMER_CODE` код заказчика

`-n LICENSE_NUMBER` номер лицензии

`-l LICENSE_CODE` код лицензии

Значение по умолчанию Значение по умолчанию отсутствует.

Пример

```
lic_mgr set -p GATE100 -c test -n 1 -l 5B271A01DF5D143A
```

Active license:

CustomerCode=test

ProductCode=GATE100

LicenseNumber=1

LicenseCode=5B271A01DF5D143A

Работа с настройками IPsec драйвера

`drv_mgr` – показывает список всех поддерживаемых настроек

`drv_mgr show` – для просмотра настроек IPsec-драйвера

`drv_mgr set` – изменения настроек IPsec-драйвера

`drv_mgr reload` – не предназначена для пользователя, загружает все настройки.

Утилиты предназначены для работы с настройками IPsec драйвера и помогают в решении проблем, возникающих на Шлюзе безопасности Bel VPN Gate 4.1, если на обработку поступает большой объем трафика, чем может обработать шлюз безопасности. Эту ситуацию будем называть "перегрузка". В связи с перегрузкой возникает следующая проблема: при перегрузке уничтожаются пакеты, которые не успевают обрабатываться, при этом приоритет пакетов (поле TOS IP-заголовка) не учитывается. Качественное решение данной проблемы может быть реализовано только в рамках всего IP-стека. Здесь рассматриваются решения только в рамках IPsec драйвера, поэтому учитываются только те ситуации, где узким местом для трафика является IPsec драйвер.

Для IPsec драйвера вводятся некоторые настройки. Так введена граница, после которой в очередь может попасть только высокоприоритетный пакет. В ОС Linux очередь ограничена максимальным количеством пакетов, при достижении которого пакет не будет обработан вне зависимости от приоритета. Для управления таким поведением могут быть использованы следующие параметры, настраиваемые через утилиту `drv_mgr`: `pq_thread_q_size`, `pq_send_q_size`, `pq_force_ordering`, `pq_tos_mask`, `pq_drop_low_pri_ifs`, `pq_drop_thres`.

Примечание

Описание настройки параметров с целью оптимизации IPsec обработки сетевого трафика на многопроцессорных системах приведено в документе «Настройка шлюза», в разделе «Настройка параметров параллельной обработки сетевого трафика».

drv_mgr

Команда `drv_mgr` показывает список всех поддерживаемых настроек, режим доступа к ним, размер в байтах и диапазон допустимых значений:

Синтаксис

`drv_mgr`

Список выводимых настроек:

| List of properties: | | | |
|----------------------------------|-------------|-----------------|-----------------|
| name | access type | size (in bytes) | range [min-max] |
| <code>pq_tos_mask</code> | read-write | 1 | unlimited |
| <code>pq_drop_low_pri_ifs</code> | read-write | variable | unlimited |
| <code>pq_drop_thres</code> | read-write | 4 | [0-100] |
| <code>pq_thread_q_size</code> | read-write | 4 | [0-16383] |
| <code>pq_send_q_size</code> | read-write | 4 | [0-2047] |
| <code>pq_force_ordering</code> | read-write | 1 | [0-1] |
| <code>fw_tcp_closed_ttl</code> | lsp-managed | 4 | [1-65535] |
| <code>fw_tcp_synsent_ttl</code> | lsp-managed | 4 | [1-65535] |

| | | | |
|--------------------------|-------------|---|-------------|
| fw_tcp_synrcvd_ttl | lsp-managed | 4 | [1-65535] |
| fw_tcp_estab_ttl | lsp-managed | 4 | [1-65535] |
| fw_tcp_fin_ttl | lsp-managed | 4 | [1-65535] |
| fw_tcp_strictness | lsp-managed | 4 | [0-6] |
| fw_tcp_open_max | lsp-managed | 4 | [0-1000000] |
| fw_tcp_half_open_max | lsp-managed | 4 | [0-1000000] |
| fw_tcp_half_open_low | lsp-managed | 4 | [0-1000000] |
| fw_tcp_conn_rate_max | lsp-managed | 4 | unlimited |
| fw_tcp_conn_rate_low | lsp-managed | 4 | unlimited |
| frag_dont_grow_fragments | read-write | 1 | [0-1] |
| frag_minimize_size | read-write | 1 | [0-1] |
| frag_df_options | read-write | 1 | [0-3] |
| qos_preclassify | read-write | 1 | [0-1] |
| ipsec_breq_max | read-write | 4 | unlimited |
| ipsec_breq_count | read-only | 4 | unlimited |
| ipsec_recursive_policy | read-write | 1 | [0-1] |

Описание настроек IPsec драйвера

Таблица 1

| Наименование настройки | Тип доступа | Размерность | Рекомендуемые значения | Значение по умолчанию | Описание |
|------------------------|------------------|---------------|-----------------------------------------------------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pq_tos_mask | чтение запись | битовая маска | 1-255 | 255 | Битовая маска (1 байт), на которую умножается побитно поле TOS (Type of Service – 1 байт) IP-заголовка пакета для определения приоритетных пакетов. Если результат умножения не равен нулю, пакет – приоритетный. Если значение pq_tos_mask=255, то при любом не равном нулю значении поля TOS, пакет является приоритетным. |
| pq_drop_low_pri_ifs | чтение запись | | список физических имен интерфейсов через запятую (без пробелов) | | Включение/выключение механизма уничтожения неприоритетных пакетов, поступающих на интерфейс: если имя интерфейса есть в списке – неприоритетные пакеты уничтожаются при уровне заполнения очереди pq_drop_thres и выше; если имени интерфейса нет в списке – уровень заполнения очереди pq_drop_thres не учитывается, и считается, что поступающие пакеты имеют одинаковый приоритет. |

| Наименование настройки | Тип доступа | Размерность | Рекомендуемые значения | Значение по умолчанию | Описание |
|--------------------------|------------------|----------------|------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | | | Допускается указание интерфейсов, которые в данный момент в системе отсутствуют, но при появлении такого интерфейса он будет учитываться в списке. |
| pq_drop_thres | чтение запись | проценты | 1-100 | 90 | Процент заполнения очереди пакетов от максимального количества пакетов, при котором неприоритетные пакеты начинают уничтожаться. Приоритетные пакеты будут приниматься, пока не будет достигнута граница pq_thread_q_size или pq_send_q_size. Для пакетов низкого приоритета аналогичная граница – $pq_thread_q_size * pq_drop_thres / 100$ или $pq_send_q_size * pq_drop_thres / 100$ (pq_drop_thres влияет на очередь отправки только если pq_force_ordering=1). |
| pq_thread_q_size | чтение запись | кол-во пакетов | 0-16383 | 2000 | Максимальное число пакетов в очереди, ожидающих обработки нитками драйвера. При достижении этого значения пакеты начинают уничтожаться вне зависимости от приоритета. |
| pq_send_q_size | чтение запись | кол-во пакетов | 0-2047 | 2032 | Максимальное число пакетов в очереди отправки (очередь отправки предназначена для восстановления порядка пакетов после параллельной обработки трафика). |
| pq_force_ordering | чтение запись | | 0-1 | 1 | Если выставлено значение 1, то по достижении границы pq_send_q_size пакеты начинают удаляться. Если значение 0, то при заполненной очереди отправки пакеты отправляются минуя эту очередь. |
| frag_dont_grow_fragments | чтение запись | | 0-1 | 0 | Чтобы избежать повторной перефрагментации пакетов промежуточными маршрутизаторами, предусмотрены значения: 1 – размер фрагментов не будет превышать максимальный размер оригинальных фрагментов; 0 – пакет фрагментируется без учета размера оригинальных фрагментов. |

| Наименование настройки | Тип доступа | Размерность | Рекомендуемые значения | Значение по умолчанию | Описание |
|------------------------|------------------|-------------|------------------------|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| frag_minimize_size | чтение запись | | 0-1 | 0 | <p>Чтобы избежать повторной перефрагментации пакетов промежуточными маршрутизаторами предусмотрены значения:</p> <p>1 – размер фрагментов усредняется, т.е. минимизируется максимальный размер фрагмента при сохранении минимального количества фрагментов;</p> <p>0 – все фрагменты делаются максимального размера, кроме последнего.</p> <p><u>Пример:</u> MTU – 270, пакет – 276 байтов, заголовок – 20 байт.</p> <p>Если значение 1, то фрагменты 148 и 148 байтов.</p> <p>Если значение 0 – фрагменты 268 и 28 байтов.</p> |
| frag_df_options | чтение запись | | 0-3 | 0 | <p>Чтобы избежать повторной перефрагментации пакетов промежуточными маршрутизаторами, предусмотрены значения, которые определяют выставлять ли DF-бит на фрагментах:</p> <p>0 – на фрагментах DF-бит всегда сбрасывается</p> <p>1 – выставлять DF-бит у фрагментов, если оригинальный пакет был фрагментирован, не инкапсулирован в IPsec, и на фрагментах был выставлен DF-бит. Этот флаг позволяет восстанавливать DF-флаг для открытого трафика, таким образом хост, отправивший пакет может проводить MTU discovery для фрагментированных пакетов.</p> <p>2 – выставлять DF-бит для фрагментированных IPsec-пакетов, если на соответствующем IPsec SA включено MTU discovery. Этот флаг позволяет проводить MTU discovery для фрагментированных пакетов драйверу и избавиться от повторной фрагментации IPsec пакетов:</p> <p>- IPsec-пакет может быть фрагментирован, если в SA установлен режим сброса или копирования DF-бита (DFHandling в LSP). При этом если установлен режим копирования, в</p> |

| Наименование настройки | Тип доступа | Размер ность | Рекомен дуемые значе ния | Значе ние по умол чанию | Описание |
|----------------------------|------------------|-----------------|-----------------------------------|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | | | <p>исходном пакете DF-бит должен быть сброшен.</p> <p>- сочетание когда включено MTU discovery и DFHandling = CLEAR имеет смысл только при frag_df_options ≥ 2, т.к. нет смысла проводить MTU discovery, когда DF-бит всегда сброшен.</p> <p>3 – комбинация 1 и 2.</p> |
| qos_preclassi fy | чтение запись | | 0-1 | 0 | <p>Использование предварительной классификации пакетов:</p> <p>1 — предварительная классификация включена;</p> <p>0 — предварительная классификация выключена</p> |
| ipsec_breq_ma x | чтение запись | | unlimited | 1000 | Максимальное количество одновременно выполняющихся запросов на создание SA bundle. В LSP можно задать отдельные ограничения для каждого правила. |
| ipsec_breq_co unt | чтение | | unlimited | 0 | Текущее количество одновременно выполняющихся запросов на создание SA bundle. |
| ipsec_recur sive_policy | чтение запись | | | 0 | Включение/выключение рекурсивного режима поиска правил IPsec для обработки пакетов. Настраивается в LSP через атрибут AllowNestedIPsec |
| fw_tcp_closed _ttl | чтение | секунды | | 5 | <p>Время жизни записи о соединении.</p> <p>Шлюз безопасности Bel VPN Gate 4.1 сначала определяет состояние TCP соединения для каждого из партнеров, которые создают TCP соединение через шлюз безопасности. А в LSP в зависимости от этих состояний задано время жизни записи о соединении (см.таблицу соответствий). Настраиваются в LSP</p> |
| fw_tcp_synsen t_ttl | чтение | секунды | | 30 | |
| fw_tcp_synrcv d_ttl | чтение | секунды | | 60 | |
| fw_tcp_estab _ttl | чтение | секунды | | 3600 | |
| fw_tcp_fin_tt l | чтение | секунды | | 30 | |

| Наименование настройки | Тип доступа | Размерность | Рекомендуемые значения | Значение по умолчанию | Описание |
|------------------------|-------------|-------------|------------------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fw_tcp_strictness | чтение | | 0-6 | 3 | Уровень "жесткости" к различным ситуациям, которые воспринимаются шлюзом как ошибочные. Настраивается в LSP атрибуте TCPStrictnessLevel. |
| fw_tcp_open_max | чтение | | | 65536 | Максимальное количество разрешенных TCP-соединений. При превышении данного предела новые TCP-соединения будут отвергаться. Настраивается в LSP. |
| fw_tcp_half_open_max | чтение | | 1-1000000 | 500 | Максимальное количество одновременно существующих полукрытых сеансов TCP, при достижении которого начинается их удаление при появлении нового запроса на соединение. Настраивается в LSP. |
| fw_tcp_half_open_low | чтение | | 1-1000000 | 400 | Минимальное количество одновременно существующих полукрытых сеансов TCP, при достижении которого прекращается их удаление. Настраивается в LSP. |
| fw_tcp_conn_rate_max | чтение | | unlimited | 500 | Максимальная частота появления полукрытых сеансов TCP в минуту, по достижении которой начинается их удаление. Настраивается в LSP. |
| fw_tcp_conn_rate_low | чтение | | unlimited | 400 | Минимальная частота появления полукрытых сеансов TCP в минуту, по достижении которой прекращается их удаление. Настраивается в LSP. |

Таблица состояний TCP и параметров, задающих время жизни соединения

| Состояние | Параметр в LSP | Параметр в drv_mgr (только для просмотра) |
|----------------------------------------------------------|-----------------------|-------------------------------------------|
| CLOSED, LISTEN | TCPClosedTimeout | fw_tcp_closed_ttl |
| SYNSENT | TCPSynSentTimeout | fw_tcp_synsent_ttl |
| SYNRCVD | TCPSynRcvdTimeout | fw_tcp_synrcvd_ttl |
| ESTAB | TCPEstablishedTimeout | fw_tcp_estab_ttl |
| FINWAIT-1, FINWAIT-2, CLOSING, TIMEWAIT, LASTACK, CLOSED | TCPFinTimeout | fw_tcp_fin_ttl |

drv_mgr show

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

Синтаксис

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

`PROPERTY_NAMEn` — имена настроек, значения которых должны быть показаны. Если ни одно имя не задано — будут показаны значения всех поддерживаемых настроек.

Имена настроек указаны в таблице описания утилиты `drv_mgr`.

Пример

```
drv_mgr show
```

```

pq_tos_mask          255
pq_drop_low_pri_ifs
pq_drop_thres        90
pq_thread_q_size     2000
pq_send_q_size       2032
pq_force_ordering     1
fw_tcp_closed_ttl    5
fw_tcp_synsent_ttl   30
fw_tcp_synrcvd_ttl   60
fw_tcp_estab_ttl     3600
fw_tcp_fin_ttl       30
fw_tcp_strictness     3
fw_tcp_open_max      65536
fw_tcp_half_open_max 500
fw_tcp_half_open_low 400
fw_tcp_conn_rate_max 500
fw_tcp_conn_rate_low 400
frag_dont_grow_fragments 0
frag_minimize_size   0
frag_df_options      0
qos_preclassify      0
ipsec_breq_max       1000
ipsec_breq_count     0
ipsec_recursive_policy 0

```


drv_mgr set

Команда `drv_mgr set` предназначена для редактирования настроек работы IPsec-драйвера. С помощью этой команды можно изменять значения только тех настроек, которые имеют атрибуты `read-write`.

Синтаксис

```
drv_mgr set PROPERTY_NAME1 VALUE1 [PROPERTY_NAME2 VALUE2]
PROPERTY_NAMEn      имена настроек, значения которых нужно изменить
VALUEn              значения соответствующих настроек.
```

Рекомендации по использованию

Имена настроек указаны в Таблица 1.

При успешной установке значения настройки будет выведено сообщение:

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

При неуспешной установке значения настройки выводится сообщение:

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

Значение настройки также записывается в конфигурационный файл `/opt/VPNagent/etc/csp_ipsec_drv.cfg`, чтобы при запуске демона автоматически выставить его в IPsec-драйвере.

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

drv_mgr reload

Команда `drv_mgr reload` загружает значения всех настроек работы IPsec-драйвера из конфигурационного файла `/opt/VPNagent/etc/csp_ipsec_drv.cfg`. Эта команда имеет технологическое применение и используется для автоматической загрузки настроек IPsec-драйвера при запуске демона. Команда не предназначена для применения пользователем.

Синтаксис

```
drv_mgr reload
```

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

При успешном завершении утилиты возвращает значение 0.

При возникновении ошибки утилиты возвращает следующие значения:

- 1 – Ошибка в синтаксисе команды
- 2 – Не хватает памяти
- 3 – Другая ошибка

Просмотр TCP-соединений

fwconn_show

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

В конфигурационном файле (LSP) `stateful firewall` настраивается с помощью фильтров с `ExtendedAction = inspect_tcp` или `inspect_ftp`. Если политика безопасности создается с помощью Cisco-like команд, то используются команды настройки Firewall.

Синтаксис

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

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

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

Пример

```
fwconn_show
```

```
Connection ID      Protected IP:port  Unprotected IP:port  State
0xd3e38180/0xd3e380c0 10.0.16.103:32779 -> 10.0.131.1:21      ESTAB/ESTAB
Number of TCP connections: 1
Number of established TCP connections: 1
```

где

Connection ID (0xd3e38180/0xd3e380c0) – идентификатор соединения (используется в `fwconn_show` и выводе [klogview](#))

Protected IP:port (10.0.16.103:32779) – IP-адрес и порт, защищаемые firewall (обычно инициатор соединения)

-> – направление открытия соединения

State (ESTAB/ESTAB) – состояние TCP соединения для каждого из партнеров

Number of TCP connections (1) – общее число отслеживаемых TCP-соединений

Number of established TCP connections (1) – общее число отслеживаемых установившихся TCP-соединений.

```
fwconn_show -detail
```

```
Connection ID: 0xd3e38300/0xd3e38480
Reverse connection: yes
```

```

Protected side: 10.0.16.103:32780
    State: CLOSING
    Sequence number: 141965198
    Acknowledgement number: 1585098758
    Window size: 49232
    TTL left / TTL for current state: 27/30
Unprotected side: 10.0.131.1:20
    State: CLOSING
    Sequence number: 1585098758
    Acknowledgement number: 141965198
    Window size: 5840
    TTL left / TTL for current state: 27/30

```

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

Reverse connection (yes) – направление установления соединения – в данном случае соединения от 10.0.131.1:20 к 10.0.16.103:32780

Sequence number (141965198, 1585098758) – TCP sequence number для каждого из партнеров

Acknowledgement number (1585098758, 141965198) – TCP acknowledgement number для каждого из партнеров

Window size (49232, 5840) – размер TCP-окна для каждого из партнеров с учетом TCP window scaling²

TTL left³ (27, 27) – время, через которое будет уничтожена запись о соединении, если не будет нового корректного пакета

TTL for current state (30, 30) – максимальное время хранения записи о соединении при отсутствии активности.

```
fwconn_show -detail -i 0xffff88003f99a100
```

```

Connection ID: 0xffff88003f99a100/0xffff88003f99a800
Reverse connection: no
Protected side: 5.5.5.5:35382
    State: CLOSING
    Sequence number: 3253957880
    Acknowledgement number: 2429155619
    Window size: 92
    TTL left / TTL for current state: 536/600

```

² Возможна ситуация, когда firewall начинает отслеживать уже открытое соединение, не получая первых пакетов. В этом случае window scaling не учитывается.

³ Запись о соединении уничтожается, если для любого из партнеров TTL Left достигает 0.

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

Просмотр сообщений IPsec-драйвера

klogview

Утилита `klogview` предназначена для просмотра сообщений по конкретным событиям, создаваемым системой протоколирования IPsec-драйвера.

Синтаксис

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

- `-l` ожидать сообщения из ядра и выводить их по мере поступления. Эта опция принимается по-умолчанию, если не задана опция `-m`
- `-t` печатать дату и время вывода сообщения
- `-T` печатать относительное время, когда произошло событие. Время выводится в секундах относительно последнего произошедшего события (а не по времени вывода), показанного данным экземпляром утилиты. Например, значение 10.353245 – это 10 секунд и 353245 микросекунд. Максимальная точность – наносекунды, но реальная погрешность зависит от аппаратной платформы и операционной системы. Значение, выдаваемое с первым сообщением, отображает абсолютное значение часов, которые используются для вычисления относительного времени. Это либо время со старта системы либо время относительно какой-то даты, принятой в данной системе за точку отсчета. Возможны отрицательные значения. Время, указанное в событии, относится к началу формирования сообщения, а при параллельном формировании сообщений порядок их отправки не определен
- `-g` печатать перед сообщением в квадратных скобках идентификатор группы событий. Идентификатор группы поясняет к какому разделу относится данное событие. При выборе фильтра, когда выводится множество сообщений различных разделов, без идентификатора трудно соотнести раздел и сообщение.
- `-p ts_precision` количество знаков долей секунд, используемых при печати относительного времени события (`-T`)
- `-f event_mask` задать фильтр событий для данного экземпляра утилиты. Возможные события описаны в таблице
- `-m event_mask` задать фильтр событий по-умолчанию. Заданное значение используется, если не указана опция `-f`
- `-h` вывести краткую информацию об использовании утилиты.

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

- группировка событий по маске – позволяет выбирать сообщения более детально. Подсистема может использовать несколько масок событий. Например, РКТ включает маски `pass` и `drop`

- группировка событий по подсистеме – сообщения, относящиеся к одной подсистеме. Например, RKT – события, относящиеся к подсистеме, реализующей логику обработки пакетов.

Группировка событий по маске

| <i>Имя группы событий</i> | <i>Код</i> | <i>Описание</i> |
|---------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| drop | 0x2 | Уничтожение пакета. Сообщение выводится непосредственно перед уничтожением какого-либо пакета и содержит краткий текст, поясняющий причину уничтожения и информацию из IP-заголовка пакета. В некоторых случаях IP-заголовок может быть испорчен к моменту вывода сообщения, тогда в сообщении допускаются нулевые или любые другие случайные адреса. |
| pass | 0x1 | Пропуск пакета. Сообщение выводится непосредственно перед отсылкой какого-либо пакета и содержит краткий текст, поясняющий действия, которые были произведены над пакетом. |
| sa_minor | 0x8 | Некоторые внутренние события, происходящие с IPsec - контекстом. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста. |
| sa_major | 0x4 | Взаимодействия между IPsec-драйвером и приложением, касающиеся изменения состояния IPsec-контекстов. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста. |
| sa_trace | 0x10 | Сообщения выводятся перед попыткой применения к пакету IPsec-контекста. |
| sa_errors | 0x20 | Ошибки, связанные с неуспешным применением IPsec-контекста к пакету. |
| fw_trace | 0x80 | Результат поиска правил firewall для пакета (если поиск производился). Сообщения, выбираемые fw_trace, включают все сообщения fw_notif. |
| fw_notif | 0x100 | Выводятся при применении правила firewall к пакету, если правило помечено в LSP. |
| fw_obj | 0x200 | Действия, производимые над правилами firewall (добавление, удаление). Идентификаторами правил являются числа двух типов. В десятичном виде выводятся идентификаторы, загружаемые из VPN daemon. В шестнадцатеричном виде (с префиксом 0x) выводятся идентификаторы динамических правил контекстной фильтрации. |
| vif_obj | 0x400 | Изменения конфигурации сетевого интерфейса (vif). |

| Имя группы событий | Код | Описание |
|---------------------------|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| fw_tcpst | 0x800 | Изменения записи о состоянии TCP соединения (tcp state), ошибки и другие события контекстной фильтрации TCP. Включает все сообщения fw_tcpstat и fw_tcperr. Для идентификации сессий используются два числа (0x....), каждое из которых соответствует записи о состоянии партнера по TCP-соединению. Эти же числа являются идентификаторами соответствующих правил фильтрации в сообщениях групп fw_obj, fw_trace. |
| fw_tcpstat | 0x1000 | Вывод статистики после закрытия TCP сессии, если правило помечено в LSP. |
| fw_tcperr | 0x2000 | Вывод ошибок, связанных с контекстной фильтрацией TCP-соединения, если правило помечено в LSP. |
| mtud | 0x4000 | Действия, связанные с path mtu discovery (отсылка и обработка ICMP сообщений, ошибки). В сообщениях выводятся оригинальные заголовки пакетов, даже если к пакету применялся IPsec. Внешний заголовок можно увидеть в соответствующих сообщениях pass/drop. |

Группировка событий по подсистемам

| Обозначение подсистемы | Описание⁴ |
|-------------------------------|-----------------------------------------------------------------------------------------|
| LOG | Сервисные сообщения подсистемы протоколирования. Их прием нельзя включить или отключить |
| SA | Работа с IPsec SA в ядре |
| IPSEC | Работа протоколов IPsec |
| PKT | Основная логика обработки пакетов |
| FW | Фильтрация трафика |
| FR | Действия над правилами фильтрации трафика |
| FWTCP | Контекстная фильтрация TCP |
| MTUD | Работа path mtu discovery |
| VIF | Действия над описаниями виртуальных сетевых интерфейсов. |

Нужный набор событий (`event_mask`) можно указать перечислением масок событий через запятую (пробелы при перечислении не допускаются). Маска может быть задана числовым

⁴ Соответствие масок подсистемам можно увидеть в подсказке утилиты klogview.

значением, именем (из таблицы «Группировка событий по маске») или именем подсистемы (из таблица «Группировка событий по подсистемам»).

Примеры (все перечисленные команды эквивалентны):

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра сообщений, выдаваемых системой протоколирования.

Сообщения, выводимые утилитой

Сообщения, выводимые утилитой, формируются на основе данных, присылаемых из IPsec-драйвера. Структура большинства сообщений определяется строкой формата⁵, получаемой из IPsec-драйвера (см. [Примеры сообщений](#)).

Сервисные сообщения, выводимые утилитой:

| | |
|-------------------------|-----------------------------------------------------------------------------------------|
| *** N messages lost *** | выводится, если утилита не успевает обрабатывать сообщения и N сообщений поретяны |
| no format string | в сообщении отсутствует строка формата ⁶ |
| <error: .. | в выводимом сообщении несоответствие строки формата параметрам сообщения ⁷ . |

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

События группы pass и drop

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

Формат сообщения (в порядке следования):

- входящий или исходящий пакет
- IP-адрес источника
- порт источника
- IP-адрес получателя

⁵ Строка формата по смыслу и стилю похожа на форматную строку в printf

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

⁷ Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.

- порт получателя
- номер IP-протокола
- длина IP-пакета
- логическое имя интерфейса или код интерфейса, если имя неизвестно
- действие "passed" или "dropped"
- строка, описывающая причину уничтожения или отправки пакета.

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

Примеры сообщений группы pass

Пакет обработан по правилу фильтрации с действием PASS:

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

Пакет был обработан по IPsec-правилу:

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

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

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

Пакет был отправлен в IP-стек для маршрутизации:

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

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

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

Примеры сообщений группы drop

Сообщения, связанные с некорректными данными заголовков пакета:

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

TCP/UDP заголовок испорчен:

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

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

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

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

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

Испорчен ESP или AH заголовок:

```
dropped in packet 2.3.4.5->3.4.3.3, proto 50, len 140, if eth0:  
unable to fetch SPI
```

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

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

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

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

Сообщения о подпадании пакета под правило с действием DROP:

Пакет уничтожен на этапе фильтрации.

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

Пакет уничтожен на этапе проверки IPsec-фильтров.

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

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

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

Пакет уничтожен на этапе классификации.

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

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

- несогласованные конфигурации⁸ партнеров по IKE/IPsec соединению
- попытка атаки на защищенную сеть.

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

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

Открытый пакет подпадает под правило фильтрации с IPsec-действием:

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

⁸ Рассогласование может произойти "в динамике" - то есть когда один из партнеров находится в процессе конфигурирования, или параметры, которые должны согласовываться автоматически (например IPsec SA), были рассинхронизированы из-за потерь пакетов или обрыва сетевого соединения.

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

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

Туннельный (внешний) заголовок не соответствует параметрам SA.

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

Пакет пришел не с того сетевого интерфейса.

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

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

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

При вложенном IPsec пакет порядок применения слоев IPsec некорректный.

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

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

После декапсуляции заголовок пакета не соответствует селектору SA.

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

Неизвестный SPI (IPsec SA не найден).

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

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

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

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

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

Ошибки IPsec:

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

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

Возможные ошибки представлены в Таблица 2.

Таблица 2

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

⁹ Это является внутренней ошибкой, просьба сообщать разработчикам.

¹⁰ Тоже внутренняя ошибка, просьба сообщать разработчикам.

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

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

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

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

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

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

Превышено общее количество одновременно выполняющихся запросов¹¹ на создание SA (размер очереди задается в drv_mgr, по умолчанию 1000):

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

Превышено количество одновременно выполняющихся запросов¹² на создание SA по одному фильтру (размер очереди задается в LSP, по умолчанию 8):

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

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

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

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

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

Внутренние ошибки, о возникновении которых необходимо сообщать разработчикам:

```
dropped in packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:
ip data is not 4-byte aligned

dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
unknown network interface

dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:
unknown physical network interface
```

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

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

¹¹ Ограничение касается только запросов, инициатором которых является драйвер.

¹² Ограничение касается только запросов, инициатором которых является драйвер.

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

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

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

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

IPsec-фильтр был уничтожен в процессе обработки пакета.

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

Сообщения о нехватке ресурсов.

```
dropped out packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:  
filter 12: failed to send SA request: out of memory  
  
dropped in packet 10.12.33.4->11.8.3.4, proto 50, len 80, if eth0:  
can't allocate packet buffer  
  
dropped out packet 2.3.4.5:12->3.4.3.3:14, proto 6, len 140, if eth0:  
can't prepare SA list: out of memory
```

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

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

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

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

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

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

Ошибка при попытке фрагментировать пакет.

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

События группы fw_trace, fw_notif

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

Примеры сообщений:

Найден фильтр, результат фильтрации в конце сообщения. Возможны следующие результаты фильтрации: PASS – пропустить пакет, ASSEMBLE – необходима сборка пакетов из фрагментов, DROP – уничтожить пакет, ERROR – ошибка обработки пакета

(испорченный пакет, или нехватка ресурсов для обработки), MATCH – промежуточное состояние при фильтрации (фильтр подобран, но действие еще не определено).

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

Отсутствие подходящего фильтра в цепочке.

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

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

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

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

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

События группы sa_minor, sa_major

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

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

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

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

Примеры сообщений группы sa_major

Превышено ограничение SA по трафику:

```
SA 55 expired
```

Пора начинать rekeying SA (пройден барьер по трафику):

```
requesting rekeying for SA 33
```

Сообщения о загрузке новых SA:

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

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

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

Расшифровка type:

- 51 – AH
- 50 – ESP

Расшифровка некоторых¹³ битов flags:

- 0x1 – входящий
- 0x100 - включен path MTU discovery
- 0x200 - включена повторная маршрутизация (reroute)
- 0x400 -необходима сборка IP-пакетов из фрагментов перед инкапсуляцией

Расшифровка битов ipsec flags:

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

Загрузка связки SA (SA bundle):

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

Расшифровка битов flags:

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

Сообщение о загрузке SA bundle, не содержащее списка SA, означает ошибку создания SA bundle приложением (демоном).

Запрос SA bundle (обычно для его обработки требуется IKE-обмен):

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

Пакет ожидает SA bundle.

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

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

```
disabled SA 33
```

Удаление SA:

```
removed SA 33
```

Пришло подтверждение загрузки SA у партнера, SA активируется:

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

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

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

¹³ Остальные значения флагов не предназначены для интерпретации пользователями.

Сообщения, возникающие при ошибочном/странном¹⁴ поведении Продукта:

```
can't add bundle: filter id 299 is not found in chain 11
can't add bundle: SA id 33 not found
can't load SA: unable to unpack
can't load replacement for SA 33: SA not found
can't load replacement for SA 33: can't unpack
can't remove SA 33: sa not found
can't disable SA 33: sa not found
can't enable SA 33: sa not found
rekey trigger: can't find SA 33
can't add bundle: non-empty "drop" response
can't add bundle: illegal request size 11
can't add bundle: filter id 2 in chain 2 is not an IPsec filter
can't add bundle: filter chain id 22 is empty
can't add bundle: filter chain id 22 not found
can't add bundle: filter id 23, chain 18: request 1.2.3.4->4.3.2.1
not found
can't add bundle: filter 80 is dead
can't add bundle: SA 24 is already in a bundle
```

Примеры сообщений группы **sa_minor**¹⁵:

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

События группы **sa_trace**

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

¹⁴ Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

¹⁵ Сообщения данного раздела предназначены для внутреннего использования. Расшифровка пользователям Продукта не предоставляется.

Примеры сообщений:

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

События группы sa_errors

Сообщения этой группы выводят дополнительную информацию о специфических ошибках IPsec.

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

Пример сообщения:

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

События группы fw_tcpst, fw_tcperr, fw_tcpstat

Сообщения группы fw_tcperr

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

Примеры сообщений:

```
half open session count and creation rate are ok, stopped deleting
connections: count 2 (< 10), 1-minute rate 9 (< 10)
half open sessions limit triggered by 1.1.1.2:23->1.1.1.3:1045, starting to
delete connections: count/max 22/33, 1-minute rate/max 42/42
sessions limit triggered by 1.1.1.2:23->1.1.1.3:1045, dropping packet:
session count/max 4000/4000
blocked attempt to initiate FTP passive-mode data connection 0x%#5x
(%#1,a:%,2u->%,a:%,2u) from server side
blocked attempt to initiate FTP data connection 0x%#5x (%#1,a:%,2u->
%,a:%,2u) from client side
blocked FTP PASV response for 0x%#5x (%#1,a:%,2u->%,a:%,2u): user not
authenticated
blocked attempt to use priveleged port %#6d in FTP PASV response for 0x%#5x
(%#1,a:%,2u->%,a:%,2u)
blocked FTP PORT command for 0x%#5x (%#1,a:%,2u->%,a:%,2u): user not
authenticated
blocked attempt to use priveleged port %#6d in FTP PORT command for 0x%#5x
(%#1,a:%,2u->%,a:%,2u)
```

Дополнительные сообщения от stateful firewall:

TCP sequence number не попадает в TCP window (см. [«Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Создание конфигурационного файла»](#) описание TCPStrictnessLevel). Сообщение может быть связано как с намеренным искажением TCP заголовка так и с ограниченными возможностями по отслеживанию соединений в firewall.

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

TCP флаги не соответствуют состоянию соединения (см. [«Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Создание конфигурационного файла»](#) описание TCPStrictnessLevel). Сообщение может быть связано как с намеренным искажением TCP заголовка так и с ограниченными возможностями по отслеживанию соединений в firewall.

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

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

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

В соответствии с LSP запрещено открытие TCP-стейтов, для соединений, которые открылись раньше сброса конфигурации firewall (см. [«Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Создание конфигурационного файла»](#) описание TCPStrictnessLevel).

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

Открытие новой записи о TCP соединении.

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

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

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

События группы fw_tcpstat

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

Пример сообщения:

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

События группы fw_obj

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

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

Примеры сообщений:

Создание цепочки правил фильтрации:

```
created filter chain 18
```

Удаление цепочки правил фильтрации:

```
destroyed filter chain 18
```

Удаление фильтра из цепочки по инициативе приложения:

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

Групповое удаление фильтров из цепочки по инициативе приложения:

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

Включение фильтра или фильтров (в соответствии с графиком, см. [«Программно-аппаратный комплекс Bel VPN Gate 4.1. Создание конфигурационного файла»](#) описание Schedule):

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

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

Выключение фильтра или фильтров (в соответствии с графиком, см. [«Программно-аппаратный комплекс «Шлюз безопасности Bel VPN Gate 4.1». Создание конфигурационного файла»](#) описание Schedule):

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

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

Уничтожение фильтра:

```
destroyed filter 19
```

Создание фильтра:

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

Селектор (selector) фильтра определяет адресную информацию пакетов, к которым будет применяться действие данного фильтра. Селектор содержит IP-адреса и порты в формате source -> destination, номера IP-протоколов – эти значения всегда выдаются в виде перечисления диапазонов. Так значение 1.2.3.8 1.2.3.11 1.3.3.3 1.3.3.3 – это диапазон 1.2.3.8..1.2.3.11 и единичный адрес 1.3.3.3

pktttype – битовая маска из следующих значений (описание значений есть в LSP, PacketType): 1 – LOCAL_UNICAST, 2 – LOCAL_BROADCAST, 4 – LOCAL_MISDIRECTED, 8 – TRANSIT

nextid – переход к другому фильтру, если произошло совпадение с данным фильтром

position – место в цепочке, в которое фильтр будет вставлен

action – битовая маска действий, которые связаны с совпадением данного фильтра: 2 – уничтожить пакет, 4 – пакет помечен для получения сообщений группы fw_notif, 32 – фильтр загружен в отключенном состоянии в соответствии с графиком (Schedule). Остальные значения для внутреннего использования, пользователю описание не предоставляется.

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

Удаление пары цепочек правил фильтрации:

```
destroyed filter chain pair 18
```

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

```
deregistered filter chain pair 18
```

Создание пары цепочек правил фильтрации.

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

Значения visibility: 1 – объект доступен для изменения из приложений, 0 – внутренний объект драйвера.
Значения type: 1 – зависимые цепочки (для контекстной фильтрации), 2 – независимые цепочки (простая пакетная фильтрация), 3 – симметричная фильтрация (используется одна цепочка, адресная информация в пакете переворачивается в зависимости от направления)

Сообщения, возникающие при ошибочном/странном¹⁶ поведении продукта:

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

¹⁶ Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

События группы vif_obj

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

Примеры сообщений об изменении состояния сетевого интерфейса ОС:

Параметр `flags` отображает следующие состояния:

- I – для данного интерфейса имеется информация о конфигурации IP (IP адрес, маска, MTU)
- P – интерфейс доступен для перехвата пакетов
- V – интерфейс подключен к соответствующему виртуальному интерфейсу.

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

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

Получение IP-информации:

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

Подключение к виртуальному интерфейсу:

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

Появление информации об интерфейсе в перехватчике пакетов:

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

Создание записи о сетевом интерфейсе:

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

Уничтожение записи о сетевом интерфейсе:

```
destroyed phy "eth0"
```

Создание записи о виртуальном интерфейсе по инициативе приложения:

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

Подключение цепочки фильтрации:

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

Расшифровка `type`:

- 0 – firewall, исходящие пакеты
- 1 – firewall, входящие
- 2 – классификация, исходящие
- 3 – классификация, входящие
- 4 – IPsec

Включение виртуального интерфейса в общий список (после этого действия к виртуальному интерфейсу подключаются сетевые интерфейсы ОС):

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

`pname` – шаблон имен сетевых интерфейсов ОС

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

Уничтожение записи о виртуальном интерфейсе.

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

Отключение цепочки фильтрации:

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

Отключение виртуального интерфейса:

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

Сообщения, возникающие при ошибочном/странном¹⁷ поведении продукта:

```
can't attach filter chain pair 2 to vif 3: vif is not found
can't attach filter chain pair 2 to vif 3: chain pair is not found
can't attach filter chain pair 2 to vif 3: unknown chain type 100
can't attach filter chain pair 2 to vif 3, chain type 1: vif is dead
can't attach filter chain pair 2 to vif 3: chain type 1 is occupied
can't detach filter chain pair type 1 from vif 2: vif is not found
can't detach filter chain pair type 120 from vif 2: unknown chain type
can't detach filter chain pair type 1 from vif 2: chain pair is not attached
update phy info: can't find phy "eth140"
update phy: can't unpack
can't create vif: unable to unpack
can't deregister vif 9: not found"
```

События группы mtud

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

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

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

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

Отослано ICMP сообщение о необходимости снижения MTU трассы:

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

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

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

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

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

¹⁷ Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

ICMP сообщение обработано, MTU трассы выставлено в соответствии:

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

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

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

Сообщение об утере данных

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

```
*** 1080 messages lost18 ***
```

¹⁸ Сообщение имеет id IPSPM_LOG_MID_LOST и параметр с индексом 0 типа I32, содержащий количество потерянных сообщений.

Работа с криптоконтейнерами

`cryptocont x` – проверка существования контейнера и корректность пароля

`cryptocont e` – удаление существующего контейнера

`cryptocont n` – создание нового контейнера

`cryptocont c` – копирование контейнера

`cryptocont r` – создание запроса на сертификат

`cryptocont l` – получение списка контейнеров

`cryptocont t` – получение списка ключевых носителей

`cryptocont i` – инициализация датчика случайных чисел

`cryptocont ex` – экспорт контейнера в файл

`cryptocont im` – импорт контейнера из файла

`cryptocont g` – генерация случайной последовательности

cryptocont x

Команда `cryptocont x` предназначена для проверки существования криптоконтейнера и соответствия указанного пароля контейнеру.

Синтаксис

```
cryptocont x -n=<Container> [-p=<Password>]
```

`-n=Container` имя контейнера

`-p=Password` пароль к контейнеру; может отсутствовать, в этом случае проверка пароля не производится

Значение по умолчанию

Нет.

cryptocont e

Команда `cryptocont e` предназначена для удаления указанного криптоконтейнера.

Синтаксис

```
cryptocont e -n=<Container> [-p=<Password>]
```

`-n=Container` имя удаляемого контейнера

`-p=Password` пароль к контейнеру; может отсутствовать, в этом случае удаление производится без проверки пароля

Значение по умолчанию

Нет.

cryptocont n

Команда `cryptocont n` предназначена для создания криптоконтейнера с заданными параметрами.

Синтаксис

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

`-n=Container` имя удаляемого контейнера

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

`SysRandomSource` системный источник энтропии используемой при генерации случайности

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

`KeyAlgOid` – OID алгоритма ключа ЭЦП

Возможные значения (без кавычек):

"1.2.112.0.2.0.34.101.45.2.1" или "bign" - ЭЦП согласно СТБ 34.101.45-2013

"1.3.6.1.4.1.12656.1.38" или "bds" - ЭЦП согласно СТБ 1176.2-99

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

`-u` – неинтерактивный режим генерации случайности.

Создаваемый контейнер содержит личный ключ ЭЦП СТБ 1176.99-2 и параметры ДСЧП на основе функции хэширования СТБ 117.99-1. Для генерации случайности используются:

- системные источники энтропии.
- содержимое файла, указанного параметром `-r` (опционально).

если не указан параметр `-u`, пользователю предлагается произвольным образом нажимать на клавиши до тех пор, пока не будет собрано достаточное количество случайных данных

Значение по умолчанию

Для параметра `key_alg` значение по умолчанию `bign`.

cryptocont c

Команда `cryptocont c` предназначена для копирования контейнеров.

Примечание по использованию:

Только для контейнеров на файловой системе и на ключевых носителях типа AvPass.

Синтаксис

```
cryptocont c -n=<Container1> [-p=<Password1>] -d=<Container2>
[-q=<Password2>]
```

`Container1` имя контейнера-источника

| | |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| Password1 | пароль к контейнеру-источнику, может отсутствовать, в этом случае пароль вводится с клавиатуры. |
| Container2 | имя контейнера-приёмника |
| Password2 | пароль к создаваемому контейнеру-приёмнику, может отсутствовать, в этом случае пользователю предлагается дважды ввести пароль с клавиатуры. |

Значение по умолчанию

Нет.

cryptocont r

Команда `cryptocont r` предназначена для генерации запроса на сертификат для указанного контейнера.

Синтаксис

```
cryptocont r {-f=<RequestFileName> -n=<Container> [-p=<Password>] [-cn=<CommonName>] [-c=<Country>] [-o=<Organization>] [-g=<StateOrProvince>] [-a=<StretAddress>] [-t=<OrganizationalUnit>] [-e=<EmailAddress>] [-k=<KeyUsage>] } | {-i=<IniFile>}
```

| | |
|--------------------|---------------------------------------------------------------------------------------|
| ContainerName | имя контейнера, содержащего личный ключ ЭЦП СТБ 1176.99-2. |
| Password | пароль к контейнеру, может отсутствовать, в этом случае пароль вводится с клавиатуры. |
| RequestFileName | имя создаваемого файла запроса. |
| CommonName | имя абонента. |
| Country | идентификатор страны абонента, например BY. |
| Organization | название организации |
| OrganizationalUnit | название подразделения |
| StateOrProvince | название области |
| StretAddress | городской адрес |
| EmailAddress | адрес электронной почты |
| KeyUsage | область применения ключа согласно X.509, комбинация битов: |
| | 100000000 digitalSignature |
| | 010000000 nonRepudiation |
| | 001000000 keyEncipherment |
| | 000100000 dataEncipherment |
| | 000010000 keyAgreement |
| | 000001000 keyCertSign |
| | 000000100 CRLSign |
| | 000000010 encipherOnly |
| | 000000001 decipherOnly |

Параметр `KeyUsage` может отсутствовать, значение по умолчанию – “1000000000” (ЭЦП).

`-i=<IniFile>` использовать .ini-файл `IniFile`, раздел `request`, поля `filename`, `commonname`, `keyusage`, `country`, `organization`, `stateorprovince`, `address`, `organizationalUnit`, `email` а также раздел `container`, поля `name`, `pin`.

пример ini файла:

```
[container]
name=Container1
pin=12345678

[request]
country=BY
organization=Avest
stateorprovince=Minskaya
address=PravdaStreet5
organizationalUnit=Avest1
commonname=ivanov
email=ivanov@avest.by
keyusage=100010000
```

Значение по умолчанию

Нет.

cryptocont l

Команда `cryptocont l` предназначена для вывода перечня криптоконтейнеров, имеющих в системе.

Синтаксис

```
cryptocont l
```

Формат вывода:

```
имя_контейнера1
имя_контейнера2
...
```

Контейнер, содержащий ДПСЧП по умолчанию, в списке не отображается.

cryptocont t

Команда `cryptocont t` предназначена для вывода перечня носителей ключевой информации, присутствующих в системе..

Синтаксис

```
cryptocont t
```

Формат вывода:

```
имя_носителя1
```

```
имя_носителя2
```

cryptocont i

Команда `cryptocont i` предназначена для инициализации и проверки датчика случайных чисел.

Синтаксис

```
cryptocont i [-n=<Container>] [-p=<Password>] [-y=<SysRandomSource>] [-r=<RandomFile>] [-k]
```

| | |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|
| Container | имя контейнера, используемого для генерации параметров датчика случайных чисел по умолчанию. |
| Password | пароль контейнера. |
| SysRandomSource | системный источник энтропии используемой при генерации случайности. |
| RandomFile | имя файла, используемого при генерации случайности. Файл должен быть не пуст, содержимое файла свыше 64 килобайт игнорируется. |
| -k | производится проверка существования контейнера ДПСЧП по умолчанию. |

Если не указан параметр “-k”, команда создаёт контейнер с именем `prdrparams` и паролем `prdrparams`, содержащий ДПСЧП, используемый по умолчанию. Если указано имя и пароль контейнера, его содержимое используется для генерации параметров ДПСЧП, иначе пользователю предлагается произвольным образом нажимать на клавиши до тех пор, пока не будет собрано достаточное количество случайных данных.

При инициализации создаваемого контейнера для генерации случайности также используются:

- системные источники энтропии;
- содержимое файла, указанного параметром `-r` (опционально).

Значение по умолчанию

Нет.

cryptocont ex

Команда `cryptocont i` предназначена для экспорта криптоконтейнера в файл.

Синтаксис

```
cryptocont ex -n=<Container> [-p=<Password1>] -f=<FileName> [-q=<Password2>]
```

| | |
|-----------|--------------------------------|
| Container | имя экспортируемого контейнера |
|-----------|--------------------------------|

| | |
|-----------|---------------------------------------------------------------------------------------|
| Password1 | пароль к контейнеру, может отсутствовать, в этом случае пароль вводится с клавиатуры. |
| FileName | имя файла экспорта |
| Password2 | пароль к экспортируемому файлу |

Значение по умолчанию

Нет.

cryptocont im

Команда cryptocont i предназначена для импорта ключевого контейнера из файла.

Синтаксис

```
cryptocont im -f=<FileName> [-p=<Password1>] -n=<Container> [-q=<Password2>] [-y=<SysRandomSource>] [-r=<RandomFile>] [-u]
```

| | |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------|
| FileName | имя файла импорта |
| Password1 | пароль к файлу, указанный при экспорте |
| Container | имя создаваемого контейнера |
| Password2 | пароль к контейнеру, может отсутствовать, в этом случае пароль дважды вводится с клавиатуры. |
| SysRandomSource | системный источник энтропии используемой при генерации случайности. |
| RandomFile | имя файла, используемого при генерации случайности. Файл должен быть не пуст, содержимое файла свыше 64 килобайт игнорируется. |
| -u | неинтерактивный режим генерации случайности. |

Команда создаёт новый контейнер и импортирует в него ключи, сохранённые в файле `FileName` при экспорте. При создании контейнера производится инициализация ДПСЧП. Для генерации случайности используются:

- системные источники энтропии.
- содержимое файла, указанного параметром `-r` (опционально).

если не указан параметр `-u`, пользователю предлагается произвольным образом нажимать на клавиши до тех пор, пока не будет собрано достаточное количество случайных данных.

cryptocont g

Команда cryptocont i предназначена для генерации последовательности случайных данных.

Синтаксис

```
cryptocont g -f=<FileName> -l=<RandomSize> [-n=<Container>] [-p=<Password>]
```

| | |
|------------|--------------------------------------------------------------|
| FileName | имя файла для сохранения сгенерированной последовательности. |
| RandomSize | длина генерируемой последовательности в байтах. |

| | |
|-----------|-----------------------------------------------------------------------------------------------------------------|
| Container | имя контейнера, используемого для генерации. Если параметр не задан, используется контейнер ДПСЧП по умолчанию. |
| Password | пароль к контейнеру. |

Ограничения на имена контейнеров

Ключевой контейнер может располагаться либо на локальном жестком диске, либо на отчуждаемом ключевом носителе типа AvPass или AvBign.

Для контейнеров, расположенных на ключевых носителях AvPass и AvBign имя контейнера должно иметь префикс «**av:**».

Пример: `av:container1.cont`

Для контейнеров, расположенных на локальном жестком диске, имя носителя не указывается, полное имя контейнера имеет вид: **имя_контейнера**.

Пример: `container1.cont`

Имя контейнера не должно содержать пробелы и символ "/".

Сообщения об ошибках

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

При появлении сообщения, начинающегося с фразы «Internal Error:...», обращайтесь в службу поддержки по адресу: support@s-terra.by.

Утилита cert_mgr

| | <i>Текст сообщения</i> | <i>Описание проблемы</i> |
|----|------------------------------------------------------|----------------------------------------------------------------|
| 1 | User Error: no source file specified | Не указан путь к файлу (cert_mgr ... -f) |
| 2 | User Error: FILENAME unable to open file | Ошибка при открытии файла |
| 3 | Internal Error: No memory | Нет свободной оперативной памяти |
| 4 | User Error: No password specified to open FILENAME | Не задан пароль доступа к файлу. |
| 5 | User Error: FILENAME wrong password PASSWORD | Неправильное значение пароля. |
| 6 | User Error. No password specified | Не указан пароль (cert_mgr-p) |
| 7 | Internal Error. Unable obtain certs from DB | Не удастся получить сертификаты из базы Продукта |
| 8 | User Error: no number specified\n | Не указан индекс сертификата (cert_mgr -i) |
| 9 | User Error: NUMBER exceeds number of objects | Указанный индекс превышает количество объектов в базе Продукта |
| 10 | User Error. No subject | Не заполнено поле Subject Name |
| 11 | User Error: Key KEY1 is not compatible with key KEY2 | Несовместимость заданных параметров (ключей) |
| 12 | User Error: Key KEY is useless | Задан лишний параметр |
| 13 | User Error: Key KEY is used twice | Повторное задание параметра (ключа) |
| 14 | User Error: Unable remove. Base is empty | Попытка удаления сертификата из пустой базы Продукта |
| 15 | Internal Error:Unable remove object from base | Неудачная попытка удаления объекта из базы Продукта. |
| 16 | User Error. Missing parameter | Отсутствует параметр |
| 17 | User Error. No file name specified | Не указано имя файла |

| | Текст сообщения | Описание проблемы |
|----|-----------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| 18 | Internal Error. Storage error | Ошибка при открытии хранилища |
| 19 | User Error: NUMBER exceeds number of objects in NAME | Значение индекса превышает количество объектов в хранилище NAME |
| 20 | User Error: Container name is not specified | Не указано имя контейнера |
| 21 | User Error: CRL can not be removed from base | CRL не может быть удален из базы Продукта |
| 22 | User Error: Object index INDEX exceeds number of certificates and CRLs in base | Индекс объекта превышает количество сертификатов и CRL в базе продукта |
| 23 | User Error. Missing index of object to be removed from base. Specify 'i' key and index | Не указан индекс объекта для удаления из базы продукта |
| 24 | User Error. Specify certificate request subject | Ошибка задания поля Subject в запросе на сертификат |
| 25 | Internal Error. Unable to create certificate request ERRCODE | Ошибка при создании запроса на сертификат |
| 26 | Internal Error. Unable to put certificate request into base ERRCODE | Ошибка при сохранении запроса на сертификат |
| 27 | User Error. Missing index of object to be imported from <FILENAME>. Specify 'i' key and index | Не указан индекс объекта для регистрации в базе продукта |
| 28 | User Error. Container 'CONTAINER_NAME' is not exists or access denied | Не удалось получить доступ к контейнеру (убедиться в наличии и доступности контейнера) |
| 29 | User Error. Failed to read private key: ERROR_DESCRIPTION | Не удалось получить секретный ключ (убедиться в доступности ключа в контейнере) |
| 30 | User Error. Cannot connect to the IPsec service: service is not running. | Не удалось соединиться с демоном (убедиться, что демон запущен) |
| 31 | User Error. Unable to set trusted status to certificate CERT_DSC | Не удалось выставить сертификату статус TRUSTED (убедиться, что сертификат CA) |
| 32 | User Error. Key is not consistent to cert CERT_DSC | Секретный ключ не подходит к сертификату или проверка закончилась неудачей (убедиться, что задан верный контейнер) |
| 33 | User Error. Unable to associate key and crt CERT_DSC | Не удалось ассоциировать секретный ключ и сертификат (убедиться, что сертификат не CA) |
| 34 | User Error: Key -l is not compatible with key -t -kf -kfp -kc -kcp. | Задан недопустимый ключ “-kf -kfp -kc -kcp” при импорте сертификата, полученного из ранее созданного запроса на сертификат |

| | Текст сообщения | Описание проблемы |
|----|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| 35 | User Error: attempt to import a CRL as certificate | Задан недопустимый ключ "-t -l -kf -kfp -kc -kcp" при импорте CRL |
| 36 | User Error: Key -t is not compatible with key -l -kf -kfp -kc -kcp | Задан недопустимый ключ "-l -kf -kfp -kc -kcp" при импорте Trusted CA сертификата |
| 37 | Crypto error. Unable to create key container. | Не удастся создать контейнер ключа (проверить правильность имени контейнера) |
| 38 | Crypto error. Unable to create certificate request. | Не удалось создать запрос на сертификат (проверить отсутствие символов '_' в имени контейнера). |

Утилиты avverify, belvpn_verify

| | Текст сообщения | Описание проблемы |
|---|--------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1 | Integrity verification tool not found | Отсутствует продукт, используемый непосредственно для подсчета контрольных сумм. |
| 2 | Integrity verification list "file_.hashes_full_path" not found | Отсутствует файл .hashes. |
| 3 | Integrity verification list "file_.hashes_full_path" is corrupted | Проблемы с чтением файла .hashes (например, ошибочный синтаксис файла). |
| 4 | Integrity verification tool call failed on file "product_file_full_path" | Запуск avverify по каким-либо причинам не произошел (какая-то системная ошибка; например, нехватка ресурсов, проблемы с правами доступа и т.п.) или вернул неожиданный код возврата (прерывание по сигналу, необработанный exception и т.п.). |
| 5 | File "product_file_full_path" is corrupted | Один или больше файлов продукта повреждены (хэш-сумма не соответствует эталонной; также возможны и другие ситуации, например, отсутствует файл (утилита avverify эти ситуации не различает)). |

Утилита dp_mgr

| | Текст сообщения | Описание проблемы |
|---|-------------------------------------------------------------|----------------------------------------|
| 1 | User Error. "ddd" is unknown parameter | Введен неизвестный параметр. |
| 2 | User Error %d: VPN demon is not started | Проблема со стартом демона. |
| 3 | Internal Error %d: Default driver policy is not wrote to db | Ошибка при записи DDP в базу продукта. |

| | Текст сообщения | Описание проблемы |
|---|--------------------------------------------------------------|-----------------------------------------|
| 4 | Internal Error %d: Default driver policy is not read from db | Ошибка при чтении DDP из базы продукта. |

Утилита drv_mgr

| | Текст сообщения | Описание проблемы |
|---|--------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
| 1 | User Error: Value for "NAME" is missing | Не задано значение настройки |
| 2 | User Error: Property name "NAME " is unknown | Имя настройки введено не верно |
| 3 | User Error: Required parameters are missing | Не задан обязательный параметр |
| 4 | User Error: command "NAME" is unknown | Введена неизвестная команда |
| 5 | Internal Error: Value of "NAME" cannot be read. Error: DESC | Не удалось получить значение настройки из драйвера |
| 6 | User Error: Value of "NAME" is not set to VALUE. Error: DESC | Не удалось выставить значение настройки в драйвер |
| 7 | User Error: Value of "NAME" is not saved to file.\n | Не удалось сохранить значение настройки в cfg файл (убедиться, что файл доступен на запись) |
| 8 | User Error: Values are not saved to file NAME.Error:DESC. | Не удалось сохранить cfg файл |
| 9 | User Error: File NAME cannot be loaded | Не удалось загрузить значения настроек из cfg файла (убедиться, что файл доступен на чтение). |

Утилита if_show

| | Текст сообщения | Описание проблемы |
|---|----------------------------------------------------------------------|--------------------------------------------------------------------|
| 1 | Internal error. Couldn't initialize local network interface list | Не удастся получить информацию о сетевых интерфейсах |
| 2 | Internal error. Couldn't receive local network interface information | Не удастся получить информацию об именах логических интерфейсов |
| 3 | User Error. Couldn't load network interface aliases file | Невозможно загрузить файл "ifaliases.cf", хотя пакет установлен |
| 4 | User Error. Couldn't access PRODUCT driver | Драйвер пакета недоступен, хотя пакет установлен |
| 5 | Warning: PRODUCT is not located | Предупреждение. Установленный пакет не найден. Не является ошибкой |

Утилита `integr_mgr`

| <i>Код ошибки</i> | <i>Текст сообщения</i> | <i>Описание проблемы</i> |
|-------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0 | SUCCESS: Operation was finished successfully. | Успешное окончание. |
| 9 | ERROR: Missing required command or parameters. (Try 'integr_mgr -h' for help) | Недостаточное количество параметров в командной строке. |
| 9 | ERROR: Invalid command 'имя_команды'. (Try 'integr_mgr -h' for help) | Введено имя операции, которое утилита распознать не может. Допустимы операции 'calc' и 'check'. |
| 9 | ERROR: Missing or invalid target file definition. (Try 'integr_mgr -h' for help) | В командной строке отсутствует имя файла для выполнения операции с единственным файлом.. |
| 9 | ERROR: Missing target file name. (Try 'integr_mgr -h' for help) | В командной строке отсутствует имя файла со списком объектов для выполнения операции. |
| 9 | ERROR: Too long target file name 'имя файла'. (Try 'integr_mgr -h' for help) | Указанное имя файла превышает в длину 500 символов. |
| 9 | ERROR: Hash library initialization error. | Внутренняя ошибка инициализации системы вычисления хеша. |
| 50 | ERROR:: Missing file '<имя_файла>' or missing access to this file. | Указано имя несуществующего файла либо отсутствуют права на чтение содержимого этого файла. Данная ошибка может возникнуть как при обработке списка, так и при обработке единичного файла. |
| 50 | ERROR:: Missing file '<имя_файла_с_расширением_hash>'. | При попытке операции проверки выявлено отсутствие файла с контрольной информацией. |
| 54 | ERROR: Read file is fault. | Ошибка чтения содержимого проверяемого файла. |
| 54 | ERROR: Invalid hash calculation. | Внутренняя ошибка вычисления контрольной информации. |
| 54 | ERROR: Invalid contents file '<имя_файла_с_расширением_hash>'. | Файл с контрольной информацией поврежден. |
| 54 | ERROR: Corrupted file '<имя_проверяемого_файла>' | Проверяемый файл поврежден. |
| 54 | ERROR: Invalid format of list file. | Формат файла списка проверяемых файлов нарушен. |
| 54 | ERROR: File '<имя_файла_из_списка>' was corrupted. | Поврежден проверяемый файл из списка. |

| Код ошибки | Текст сообщения | Описание проблемы |
|-------------------|---------------------------------------------------------------|----------------------------------------------------|
| 75 | ERROR: Can't create file '<имя_файла_с_расширением_hash>'. | Невозможно создать файл с контрольной информацией. |
| 75 | ERROR: Can't write file '<имя_файла_с_расширением_hash>' | Невозможно записать файл с контрольной информацией |

Утилита key_mgr

| | Текст сообщения | Описание проблемы |
|---|-----------------------------------------------------------|-----------------------------------------------------|
| 1 | Internal Error: No memory to open file FILENAME | Недостаточно памяти, чтобы открыть файл |
| 2 | User Error: Key file no specified | Не указан файл с ключом |
| 3 | User Error: Key name no specified | Не указано имя ключа |
| 4 | Internal Error. Unable to append key into base KEYNAME | Ошибка при попытке импорта ключа в базу Продукта |

Утилита lic_mgr

| | Текст сообщения | Описание проблемы |
|---|------------------------------------------|------------------------------|
| 1 | User Error: <parameter> undefined | Не указан один из параметров |
| 2 | User Error: Wrong license | Неверная лицензия |
| 3 | Internal Error: Can't write license file | Ошибка при записи лицензии |

Утилита log_mgr

| | Текст сообщения | Описание проблемы |
|---|-----------------------------------------------------------|----------------------------------------------|
| 1 | User Error: "ddd" is unknown parameter | Введен неизвестный параметр |
| 2 | User Error: %d: VPN demon is not started | Проблема со стартом демона |
| 3 | Internal Error %d: Failed to set default log level | Ошибка при установке уровня протоколирования |
| 4 | Internal Error %d: Failed to get default log level | Ошибка при получении уровня протоколирования |
| 5 | User Error: Parameter is missing | Пропущен параметр команды |
| 6 | User Error: Too many parameters | Слишком много параметров команды |
| 7 | Internal Error: Failed to set log levels for msg group | Ошибка установки уровня для группы |
| 8 | Internal Error: Failed to load the msg group file | Ошибка загрузки файла группы |

| | | |
|----|---------------------------------------------|------------------------------------|
| 9 | Internal Error: Failed to get the msg group | Ошибка получения группы log levels |
| 10 | Internal Error: Failed to save log levels | Ошибка сохранения log levels |

Утилита lsp_mgr

| | <i>Текст сообщения</i> | <i>Описание проблемы</i> |
|---|-------------------------------------------------|------------------------------------------------------------------|
| 1 | User Error. FILENAME unable to open file | Ошибка при попытке открыть файл (убедиться в доступности файла). |
| 2 | Internal Error: Unable to set LSP as active | Не удалось загрузить LSP из файла в базу продукта |
| 3 | Internal Error: No memory to open file FILENAME | Недостаточно памяти для открытия файла |
| 4 | Internal Error: unrecognized error | Внутренняя ошибка. |
| 5 | Internal Error: Unable to reload lsp from base | Не удалось перезагрузить LSP из базы продукта. |

Утилита sa_mgr

| | <i>Текст сообщения</i> | <i>Описание проблемы</i> |
|---|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|
| 1 | Internal Error: SAs' clearing failed. Error: %s | Не удалось удалить ISAKMP или IPsec соединения |
| 2 | Internal Error: ISAKMP info not available. Error: %s | Не удастся получить информацию об ISAKMP |
| 3 | Internal Error: Connections info not available.. Error: %s | Не удастся получить информацию об IPsec соединениях |
| 4 | Timeout expired. Please ensure that all chosen SAs are cleared. | Закончилось время ожидания завершения удаления соединений. Убедитесь, что все выбранные соединения удалены. |

Утилита cryptocont

| | <i>Код ошибки</i> | <i>Описание проблемы</i> |
|---|--------------------------|---------------------------------------------|
| 1 | AVCN_BAD_CMDLINE | Неверные параметры командной строки |
| 2 | AVCN_CONTAINER_NOT_FOUND | Контейнер с указанным именем не существует. |
| 3 | AVCN_INVALID_PASSWORD | Указан неверный пароль |
| 4 | AVCN_ALREADY_EXIST | Контейнер с указанным именем уже существует |
| 5 | AVCN_BAD_VERSION | Неверная версия структуры данных контейнера |
| 6 | AVCN_READ_ERROR | Ошибка чтения |

| | <i>Код ошибки</i> | <i>Описание проблемы</i> |
|----|--------------------------|-------------------------------------------|
| 7 | AVCN_WRITE_ERROR | Ошибка записи |
| 8 | AVCN_IO_ERROR | Общая ошибка ввода-вывода |
| 9 | AVCN_SHORT_PASSWORD | Длина пароля меньше 8 символов |
| 10 | AVCN_DATA_ERROR | Нарушена структура данных контейнера |
| 11 | AVCN_ACCESS_DENIED | Ошибка доступа при операциях ввода-вывода |
| 12 | AVCN_BAD_KEYUSAGE | Указано неверное значение KeyUsage |
| 13 | AVCN_FILE_NOT_FOUND | Файл не найден |