УТВЕРЖДЕНО

**BY.PTHK.00001-03.01 34 01-8-ЛУ**

# Программно-аппаратный комплекс

# «Шлюз безопасности Bel VPN Gate 3.0.1»

# РУКОВОДСТВО ОПЕРАТОРА

## Руководство администратора

Специализированные команды

**BY.PTHK.00001-03.01 34 01-8**

Листов 47

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

2012

# Специализированные команды

1 CERT_MGR SHOW ..... 4
2 CERT_MGR IMPORT ..... 5
3 CERT_MGR CREATE ..... 7
4 CERT_MGR REMOVE ..... 8
5 CERT_MGR CHECK ..... 9
6 KEY_MGR SHOW ..... 10
7 KEY_MGR IMPORT ..... 11
8 KEY_MGR REMOVE ..... 12
9 LSP_MGR SHOW ..... 13
10 LSP_MGR LOAD ..... 14
11 LSP_MGR UNLOAD ..... 15
12 LSP_MGR RELOAD ..... 16
13 IF_MGR SHOW ..... 17
14 IF_MGR ADD ..... 18
15 IF_MGR REMOVE ..... 19
16 DP_MGR SHOW ..... 20
17 DP_MGR SET ..... 21
18 LOG_MGR SET ..... 22
19 LOG_MGR SHOW ..... 23
20 SA_SHOW ..... 24
21 LIC_MGR SHOW ..... 26
22 LIC_MGR SET ..... 27
23 DRV_MGR ..... 28
24 DRV_MGR SHOW ..... 32
25 DRV_MGR SET ..... 33
26 DRV_MGR RELOAD ..... 34
27 KLOGVIEW ..... 35
27.1 События группы PASS и DROP ..... 37
27.2 События группы FILT_TRACE ..... 40
27.3 События группы SA_MINOR, SA_MAJOR ..... 40
27.4 События группы SA_TRACE ..... 42
27.5 События группы SA_ERROR ..... 43
28 СООБЩЕНИЯ ОБ ОШИБКАХ ..... 44

  

В состав Bel VPN Gate входит также ряд специализированных команд (или утилит), предназначенных для управления общими настройками Продукта.

Перечень программных утилит, входящих в состав Продукта Bel VPN Gate:

**cert mgr**
**cert mgr check**
**key mgr**
**lsp mgr**
**if mgr**
**dp mgr**
**log mgr**
**sa show**
**lic mgr**
**drv mgr**
**klogview**

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

Все эти команды можно также запускать из CLI консоли с помощью команны **run**.

Запуск утилит с опцией `-h` вызывает помощь.

# 1 cert_mgr show

Команда `cert_mgr show` предназначена для просмотра сертификатов и списков отозванных сертификатов (Certificate Revocation List, CRL), размещенных в файле или базе Продукта. Сертификаты хранятся в файле. Могут также обрабатываться файлы формата PKCS#7 и PKCS#12. Файлы формата PKCS#12 могут быть защищены паролем.

**Синтаксис**

**`cert_mgr show`** `[-f CERT_FILE [-p C_PWD]] [-i OBJ_INDEX_1] ..[-i OBJ_INDEX_N]`

| | |
|---|---|
| `-f CERT_FILE` | Путь к файлу с сертификатами и CRL. Если данная опция не указана, то будут показаны сертификаты из базы Продукта. |
| `-p C_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. |

**Значение по умолчанию** значение по умолчанию отсутствует

**Рекомендации по использованию**

Используйте данную команду для ознакомления с содержимым файла, содержащего сертификаты и CRL, или сертификатами, зарегистрированными в базе Продукта, а также для ознакомления с деталями конкретных сертификатов или CRL.

Для просмотра списка объектов (сертификатов и CRL) в файле или базе Продукта используйте команду `cert_mgr show` без указания индексов. В этом случае будет выведен нумерованный список сертификатов и CRL.

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

**Пример**

Ниже приведен пример просмотра сертификатов, находящихся в базе Продукта (`trusted` – CA сертификат, `local` –локальный сертификат, `remote` – сертификат партнера без контейнера с секретным ключом):

```
cert_mgr show

Found 3 certificates. No CRLs found.
1 Status: trusted C=RU,O=derral, OU=CenterCA,CN=agat
2 Status: local C=RU,O=derral, OU=quality,CN=rubin
3 Status: remote C=RU, O=s-terra, OU=QA,CN=Test
```

  

# 2 cert_mgr import

Команда `cert_mgr import` предназначена для импорта сертификатов и списков отозванных сертификатов (Certificate Revocation List, CRL) из файла в базу Продукта.

**Синтаксис**

```
cert_mgr import -f CERT_FILE [-p C_PWD]
[-i OBJ_INDEX01] [-t | [-kc CONTAINER_NAME
[-kcp CONTAUNER_PWD]]
```

| | |
|---|---|
| `-f CERT_FILE` | Путь к файлу с сертификатами и/или CRL |
| `-p C_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 или базе Продукта. Если при написании команды указан путь к файлу, то индекс будет определять номер искомого сертификата (CRL) в файле (при импорте одного сертификата (CRL) данный параметр можно не указывать, он будет равен 1). При импорте сертификата из файла, содержащего один сертификат, в качестве индекса следует указывать 1. Индекс задается в виде целого десятичного числа. В качестве индекса нельзя указывать 0. |
| `-t` | импортируемому сертификату присваивается статус `"trusted"` (для CA сертификата). При использовании этой опции запрещается использование опций `-kc,-kcp`. Запрещается использовать эту опцию при импорте CRL |
| `-kc CONTAINER_NAME` | (для "Авест") Имя контейнера с секретным ключом импортируемого сертификата. Не может использоваться, если ранее введена опция `-t`. |
| `-kcp CONTAINER_PWD` | (для "Авест") Пароль к контейнеру с секретным ключом импортируемого сертификата. Необязательный параметр. Используется тогда, когда контейнер с секретным ключом защищен паролем. |

**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.

**Пример**

Ниже приведен пример импорта сертификатов, находящихся в файле, в базу Продукта. Из файла импортируются CA сертификат (его импортируем с присвоением статуса `"trusted"`) и сертификат пользователя:

```
cert_mgr import -f /opt/test.pfx -p password
-t -i 1 -i 2
```

  

```
1 OK O=S-Terra,CN=CA Cert
2 OK O= S-Terra,CN=Technological Cert
```

**Импорт CA сертификата из файла ca.cer в базу Продукта:**

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

**Импорт локального сертификата:**

**Для Авест:**

```
cert_mgr import -f ivanov.cer –kc ivanov –kcp 12345678
```

# 3 cert_mgr create

Команда `cert_mgr create` предназначена для создания запроса на локальный сертификат (Certificate Request), который будет отправляться в Certificate Authority. На основании этого запроса Certificate Authority создаст соответствующий сертификат.

**Синтаксис** **`cert_mgr create`** `-subj CERT_SUBJ [-RSA|-DSA] [-512|-1024](mail MAIL|-ip IP_ADDR|-dns DNS) [-f OUT_FILE]`

| | |
|---|---|
| `-subj CERT_SUB` | значение поля сертификата `"Subject Name"` |
| `-RSA` | алгоритм цифровой подписи. Значение по умолчанию. |
| `-DSA` | алгоритм цифровой подписи. |
| `-512` | длина ключа 512 бит для алгоритма цифровой подписи. Значение по умолчанию. |
| `-1024` | длина ключа 1024 бита Для алгоритма цифровой подписи |
| `-mail MAIL` | значение Mail поля `"Alternative Subject Name"` сертификата. |
| `-ip IP_ADDR` | значение IP Address поля `"Alternative Subject Name"` сертификата. |
| `-dns DNS` | значение DNS поля `"Alternative Subject Name"` сертификата. |
| `-f OUT_FILE` | полное имя файла, в который будет помещен запрос на сертификат. |

**Значение по умолчанию**

По умолчанию используется RSA алгоритм и 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 секретный ключ, а 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, а также запрос на ГОСТ сертификат. При использовании «AvCrypt ver. 5.0» используется утилита `cryptocont`, описанная в документе «Bel VPN Gate 3.0. Приложение».

**Пример**

Ниже приведен пример создания запроса на сертификат:

```
cert_mgr create -subj O=S-Terra,CN=LocalCert -RSA -1024 -dns local.s-terra.com -f /opt/VPNagent/bin/certs/local_cert
```

# 4 cert_mgr remove

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

**Синтаксис** **`cert_mgr remove`** `-i OBJ_INDEX_1..[-i OBJ_INDEX_N]`

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

**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.

Для того, чтобы ознакомиться с сертификатами, хранящимися в базе Продукта и выяснить номера (индексы), под которыми они хранятся в базе, используйте команду **`cert mgr show.`**

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

**Пример**

Ниже приведен 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: Certificate index 3 exceeds number of certificates in
base
```

# 5 cert_mgr check

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

**Синтаксис** **`cert_mgr check`** `[-i OBJ_INDEX01] [-i OBJ_INDEX02] …`

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

  

# 6 key_mgr show

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

**Синтаксис** **`key_mgr show`**

Данная команда не имеет аргументов и ключей.

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

**Рекомендации**

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

Ниже приведен пример выполнения команды `key_mgr show`:

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

# 7 key_mgr import

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

**Синтаксис** **`key_mgr import`** `–n KEY_NAME –f KEY_FILE`

`-n KEY_NAME` имя предопределенного ключа.

`-f KEY_FILE` путь к файлу, содержащему предопределенный ключ.

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

**Рекомендации**

Используйте данную команду для импорта предопределенных ключей из файловой системы в базу Продукта.

**Пример**

Ниже приведен пример импорта предопределенного ключа:

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

OK key1name
OK key2name
OK key3name
```

# 8 key_mgr remove

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

**Синтаксис** **`key_mgr remove`** `-n KEY_NAME`

`-n KEY_NAME` имя предопределенного ключа.

**Значение по умолчанию** Значение по умолчанию отсутствует

**Рекомендации**

Используйте данную команду для удаления предопределенных ключей из базы Продукта.

**Пример**

Ниже приведен пример удаления предопределенного ключа:

```
key_mgr remove -n key1name
OK key1name
```

# 9 lsp_mgr show

Команда `lsp_mgr show` предназначена для просмотра текущей конфигурации.

**Синтаксис** **`lsp_mgr show`**

**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: конфигурация, в которой записана созданная политика безопасности, и `Default Driver Policy`.

Независимо от способа создания конфигурации – в командной строке, графическом интерфейсе, платформе управления CiscoWorks - cisco-like конфигурация конвертируется в native-конфигурацию.

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`.

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

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

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: Thu Feb 19 14:41:08 2008"
   Version = "3.0"
   CRLHandlingMode = DISABLE
)
ESPProposal ESP_ts_m1_sn1(
   Transform* = ESPTransform (
      CipherAlg* = "AES-K192-CBC-12"
      IntegrityAlg* = "MD5-H96-KPDK"
      LifetimeSeconds = 3600
      LifetimeKilobytes = 4608000
   )
)
```

  

# 10 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 load`** `-f LSP_FILE`

`- f LSP_FILE` путь к файлу конфигурации

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

**Рекомендации по использованию**

Используйте данную команду для загрузки конфигурации из файла в базу Продукта.


После загрузки отредактированной конфигурации командой `lsp_mgr load`, внесенные изменения будут присутствовать только в native-конфигурации, 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 «Bel VPN Gate 3.0. Приложение»).

**Пример**

Ниже приведен пример загрузки конфигурации из файла в базу Продукта:

```
lsp_mgr load -f default.txt
LSP successfully loaded from file default.txt
```

# 11 lsp_mgr unload

Команда `lsp_mgr unload` предназначена для загрузки политики Default Driver Policy.

**Синтаксис** **`lsp_mgr unload`**

Команда не имеет аргументов и ключей

**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`**. При этой политике пакеты либо все пропускаются либо пропускаются только по протоколу DHCP.

**Пример**

Ниже приведен пример загрузки политики DDP:

```
lsp_mgr unload
Operation completed successfully
```

# 12 lsp_mgr reload

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

**Синтаксис** **`lsp_mgr reload`**

**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` была 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.
```

# 13 if_mgr show

Команда `if_mgr show` предназначена для просмотра логических, физических имен и других параметров защищаемых сетевых интерфейсов.

**Синтаксис** **`if_mgr show`**

Команда не имеет аргументов и ключей

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

**Рекомендации по умолчанию**

Те интерфейсы, на которые установлен продукт, являются защищаемыми сетевыми интерфейсами. Используйте данную команду для просмотра параметров защищаемых сетевых интерфейсов.

После выполнения этой команды на экран будет выведена следующая информация о защищаемых сетевых интерфейсах:

- логическое имя, под которым сетевой интерфейс зарегистрирован в базе Продукта
- физическое имя интерфейса
- список IP-адресов с масками, приписанных данному интерфейсу.

**Пример**

Ниже приведен пример выполнения команды `if_mgr show`:

```
if_mgr show
1)Network Interface Logical name iprb0
1)Network Interface Physical name iprb0
  IP - 10.10.10.111, Mask 255.0.0.0
```

  

# 14 if_mgr add

Команда `if_mgr add` предназначена для регистрации в базе Продукта новых защищаемых сетевых интерфейсов

**Синтаксис** **`if_mgr add`** `(-a IP_ADDR | -n PHYSICAL_NAME) -l LOGICAL_NAME`

| | |
|---|---|
| `-a IP_ADDR` | IP-адрес защищаемого сетевого интерфейса |
| `-n PHYSICAL_NAME` | физическое имя защищаемого интерфейса |
| `-l LOGICAL_NAME` | логическое имя защищаемого интерфейса |

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

**Рекомендации по использованию**

Используйте данную команду для регистрации в базе Продукта новых защищаемых сетевых интерфейсов.

Занятые логические и физические имена интерфейсов и их IP-адреса можно посмотреть в выводе на экран команды `if_mgr show`.

Имена интерфейсов и их IP-адреса можно взять из выводе на экран системной команды `ifconfig -a`.

Запрещается при регистрации защищаемого сетевого интерфейса указывать уже используемый IP-адрес.


Note

Если командой `if_mgr add` был зарегистрирован новый защищаемый интерфейс после конвертирования cisco-like конфигурации, то для этого интерфейса будет выполняться неяное правило `Drop All`, так как при конвертировании cisco-like конфигурации фильтры для каждого интерфейса прописываются в отдельности При следующем конвертировании cisco-like конфигурации новый интерфейс будет добавлен в эту конфигурацию и для него будут действовать общие правила, как и для остальных интерфейсов.

**Пример**

Ниже приведен пример выполнения команды `if_mgr add`:

```
if_mgr add -a 10.0.19.2 -l iprb1
Saving hardware interface 10.0.19.2 as iprb1
```

# 15 if_mgr remove

Команда `if_mgr remove` предназначена для удаления из базы Продукта записей о защищаемых сетевых интерфейсах.

**Синтаксис** **`if_mgr remove`** `-l LOGICAL_NAME`

`-l LOGICAL_NAME` логическое имя, присвоенное защищаемому интерфейсу.

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

**Рекомендации по использованию**

Используйте данную команду для удаления из базы Продукта записей о защищаемых сетевых интерфейсах. Это может быть полезно если:

- интерфейс не планируется настраивать средствами VPN Gate (например, нет необходимости использовать для него команды **`ip access-group`** или **`crypto map (interface)`**)
- интерфейс не будет использоваться вообще.

**Пример**

Ниже приведен пример выполнения удаления записи о защищаемом сетевом интерфейсе с логическим именем `iprb1`:

```
if_mgr remove -l iprb1
Removing the network interface iprb1
```

# 16 dp_mgr show

Команда `dp_mgr show` предназначена для просмотра установленных настроек политики драйвера по умолчанию - `Default Driver Policy` (DDP). Эта политика имеет одно из двух значений:

| | |
|---|---|
| `passall` | пропускать весь трафик |
| `passdhcp` | пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для конфигурирования TCP/IP стека по протоколу DHCP. |

`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 show`**

Данная команда не имеет аргументов и ключей.

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

**Рекомендации по использованию**

Используйте данную команду для просмотра настроек политики DDP.

**Пример**

Ниже приведен пример выполнения команды `dp_mgr show`:

```
dp_mgr show
Default driver policy : passall
```

# 17 dp_mgr set

Команда `dp_mgr set` предназначена для настройки параметров `Default Driver Policy` (DDP) – политики по умолчанию.

`Default Driver Policy` (DDP)– политика драйвера по умолчанию, описана в команде **`dp_mgr show`**.

**Синтаксис** **`dp_mgr set`** `[-ddp (passall|passdchp)]`

`-ddp (passall|passdhcp)` устанавливает `Default Driver Policy` в режим `passall` (пропускать весь трафик) или `passdhcp` (пропускать только `DHCP` пакеты).

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

**Рекомендации по использованию**

Используйте данную команду для настройки параметров политики по умолчанию.

**Пример**

Ниже приведен пример выполнения команды `dp_mgr set`:

```
dp_mgr set –ddp passall
Default driver policy is set successfully
```

# 18 log_mgr set

Команда `log_mgr set` предназначена для настройки уровня протоколирования событий по умолчанию.

**Синтаксис** **`log_mgr set`** `-l SEVERITY_LEVEL`

`-l SEVERITY_LEVEL` уровень протоколирования событий. Устанавливается 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.`

**Значение по умолчанию** `debug.`

**Рекомендации по использованию**

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

Уровень лога, установленный данной командой, действует только в двух случаях:

- когда не загружена LSP
- когда в LSP не задан уровень лога для какого-либо события (**Атрибут SystemLogMessageLevel**, **PolicyLogMessageLevel** , **CertificatesLogMessageLevel** , **LDAPLogMessageLevel** ).

На команды `cs_console` уровень лога, установленный этой утилитой, никак не влияет.

**Пример**

Ниже приведен пример выполнения команды `log_mgr set`:

```
log_mgr set -l warning
Severity level set to db successfully
```

# 19 log_mgr show

Команда `log_mgr show` предназначена для просмотра уровня протоколирования событий по умолчанию, установленного командой **`log_mgr set`**.

**Синтаксис** **`log_mgr show`**

Данная команда не имеет аргументов и ключей.

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

**Рекомендации по использованию**

Используйте данную команду для ознакомления с настройкой уровня протоколирования событий.

**Пример**

Ниже приведен пример выполнения команды `log_mgr show`:

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

# 20 sa_show

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

**Синтаксис** **`sa_show`** `[-e]`

Команда `sa_show` (без указания опции) позволяет просмотреть действующие в данный момент `IPsec SA`.

Команда `sa_show -e` выводит полную информацию– `IKE info, ISAKMP SA, IPsec SA`.

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

**Рекомендации по использованию**

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

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

При указании ключа `-e` выводится полная информация:

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

  

**Пример**

Ниже приведен пример выполнения команды `sa_show -e`:

```
IKE sessions: 0 initiated, 0 responded

ISAKMP SA Num (Remote Addr,Port)-(Local Addr,Potr) State Sent Rec
(заголовок вывода)
ISAKMP SA 1 (10.0.10.193,500)-(10.0.10.17,500) deletion 1062 1090
ISAKMP SA 2 (10.0.10.16,500)-(10.0.10.17,500) ready 1246 2602

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

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

# 21 lic_mgr show

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

**Синтаксис** **`lic_mgr show`**

Данная команда не имеет аргументов и ключей.

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

**Рекомендации по использованию**

Используйте данную команду для просмотра текущей лицензии.

# 22 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
GATE1000
GATE3000
GATE7000
AXP BEL VPN
NME BEL VPNV
```

`-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 –c test –n 1 –l 5B271A01DF5D143A
Active license:
CustomerCode=test
ProductCode=GATE3000
LicenseNumber=1
LicenseCode=5B271A01DF5D143A
```

# 23 drv_mgr

Утилита `drv_mgr` предназначена для решения проблем, возникающих на Bel VPN Gate, если на обработку поступает больший объем трафика, чем может обработать шлюз безопасности. Эту ситуацию будем называть "перегрузка". В связи с перегрузкой на платформах Solaris и Linux возникают следующие проблемы:

- поскольку обработка сетевого трафика выполняется в приоритетных нитях ядра ОС, нитям "пользовательских" процессов не отдается управление. Результатом является "подвисание" – невозможность управления компьютером во время перегрузки
- при перегрузке уничтожаются пакеты, которые не успевают обрабатываться, при этом приоритет пакетов (поле TOS IP-заголовка) не учитывается.

Качественное решение данных проблем может быть реализовано только в рамках всего IP стека. Здесь рассмотрим 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. Команда `drv_mgr` предназначена для просмотра настроек работы IPsec драйвера - имен поддерживаемых настроек, режима доступа к ним, размера и диапазона допустимых значений.

**Синтаксис** **`drv_mgr`**

Эта команда показывает список всех поддерживаемых настроек, режим доступа к ним, размер в байтах и диапазон допустимых значений:

Список выводимых настроек:

```
List of properties:

Name              access type size (in bytes) range [min-max]

pq_size            read-write      4          [1-1000000000]
pq_low_water       read-write      4          [0-1000000000]
pq_tos_mask        read-write      1             unlimited
pq_do_idle         read-write      1               [0-1]
pq_busy_interval   read-write      4            [1-4000000]
pq_idle_ratio      read-write      4            [0-999999]
pq_drop_low_pri    read-write      1               [0-1]
pq_drop_thres      read-write      4              [0-100]
```

**Рекомендации по использованию**

**ОС Solaris**

Для решения первой проблемы, чтобы менее приоритетные нити получали управление, делается остановка сервис-процедур STREAMS, и возобновление их работы через некоторое время. Для определения необходимости и времени остановки введены следующие настройки: pq_do_idle, pq_busy_interval, pq_idle_ratio.

Решение второй проблемы. Стандартными параметрами очередей STREAMS является уровень заполнения и максимальная вместимость очереди. Эти параметры задаются при регистрации драйверов и модулей STREAMS. При переполнении очереди пакеты могут уничтожаться. Для защиты от уничтожения приоритетного трафика введены настройки: pq_size, pq_low_water, pq_tos_mask, pq_drop_thres, pq_drop_low_pri.

  

**Описание настроек IPsec драйвера для ОС Solaris:**

| Наименование настройки | Размер-ность | Рекомен-дуемые значения | Значение по умолчанию | Описание |
|---|---|---|---|---|
| pq_size | байты | 1-1000000000 | | Максимальный объем данных, который разрешается помещать во входную и выходную очереди пакетов. |
| pq_low_water | байты | 0-1000000000 | | Минимальный объем данных, который помещается во входную и выходную очереди пакетов. Если уровень заполнения очереди равен значению pq_size, то добавление пакетов в очередь блокируется до тех пор, пока уровень заполнения не станет равен pq_low_water. |
| pq_tos_mask | 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 равно 255, то при любом не равном нулю поле TOS, пакет является приоритетным. |
| pq_do_idle | | 0, 1 | 1 | Включение/выключение механизма защиты от перегрузки: 0 – защита от перегрузки выключена, 1 – защита от перегрузки включена. |
| pq_busy_interval | микро-секунды | 1-4000000 | 100 | Интервал времени, в течение которого измеряется степень загрузки системы, занятой обработкой пакетов IPsec драйвером. Малые значения интервала времени, например 0, ограничат работу сервис-процедуры обработкой пакета за запуск. На основании степени загрузки рассчитывается время, когда система не занята обработкой пакетов IPsec драйвером и сравнивается со значением pq_idle_ratio. Если рассчитанное значение меньше, чем pq_idle_ratio, обработка пакетов будет приостановлена и передано управление системе. |
| pq_idle_ratio | миллионные доли в процентах | 0 - 999999 | 100000 (10%) | Процент времени, который система должна проводить вне обработки пакетов IPsec драйвером. |
| pq_drop_low_pri | | 0, 1 | 0 | Включение/выключение механизма уничтожения неприоритетных пакетов: 0 – пакеты обрабатываются стандартным образом, 1 - неприоритетные пакеты уничтожаются при уровне заполнения очереди pq_drop_thres и выше. |
| pq_drop_thres | проценты | 0-100 | | Процент заполнения очереди пакетов от суммарного размера пакетов, при |

  

| | | | | |
|---|---|---|---|---|
| | | | | котором неприоритетные пакеты начинают уничтожаться. |

**ОС Linux**

Для того чтобы менее приоритетные нити получали управление, нить обработчика пакетов контролирует время своей непрерывной деятельности. Когда время "сессии" превышает порог - pq_busy_interval, нить обработчика отдаёт управление системному планировщику задач - pq_do_idle. Если значение настройки pq_do_idle равно "2", то производится перемещение нити в конец очереди задач.

Как и для Solaris, введена граница, после которой в очередь может попасть только высокоприоритетный пакет. Но в Linux очередь ограничена максимальным количеством пакетов, при достижении которого пакет не будет обработан вне зависимости от приоритета.

**Описание настроек IPsec драйвера для ОС Linux:**

| Наименование настройки | Размер-ность | Рекомен-дуемые значения | Значение по умолчанию | Описание |
|---|---|---|---|---|
| pq_psize | пакеты | 1-1000 | 100 | Максимальное количество пакетов в очереди, при достижении которого пакеты начинают уничтожаться. |
| pq_do_idle | | 0, 1, 2 | 1 | Включение/выключение механизма защиты от перегрузки: 0 – защита от перегрузки выключена, 1 – передача управления системному планировщику задач, 2 – меняется способ передачи управления |
| pq_tos_mask | 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 равно 255, то при любом не равном нулю поле TOS, пакет является приоритетным. |
| pq_busy_interval | милли-секунды | 1-1000 | 20 | Интервал времени, в течение которого измеряется степень загрузки системы, занятой обработкой пакетов IPsec драйвером. Малые значения интервала времени, например 0, ограничат работу сервис-процедуры обработкой пакета за запуск. На основании степени загрузки рассчитывается время, когда система не занята обработкой пакетов IPsec драйвером и сравнивается со значением pq_idle_ratio. Если рассчитанное значение меньше, чем pq_idle_ratio, обработка пакетов будет приостановлена и передано управление системе. |

  

| | | | | |
|---|---|---|---|---|
| pq_drop_low_pri | | 0, 1 | 1 | Включение/выключение механизма уничтожения неприоритетных пакетов: 0 – неприоритетные пакеты явно не уничтожа-ются, происходит разделение очереди на две части - общую и приоритетную; 1 – непри-оритетные пакеты уничтожаются при уровне заполнения очереди pq_drop_thres и выше. |
| pq_drop_thres | проценты | 1-100 | 80 | Процент заполнения очереди пакетов от максимального количества пакетов, при котором неприоритетные пакеты начинают уничтожаться. |

# 24 drv_mgr show

Команда `drv_mgr show` предназначена для просмотра значений настроек работы IPsec-драйвера. Выводятся имена поддерживаемых настроек, режим доступа к ним, их размер и диапазон допустимых значений.

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

| | |
|---|---|
| `PROPERTY_NAME1, PROPERTY_NAME2` | 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**

```
pq_size             100000
pq_low_water        70000
pq_tos_mask         255
pq_do_idle          0
pq_busy_interval    100000
pq_idle_ratio       100000
pq_drop_low_pri     0
pq_drop_thres       90
```

# 25 drv_mgr set

Команда `drv_mgr set` предназначена для редактирования установленных значений 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_NAME1, PROPERTY_NAME2 | имена настроек, значения которых нужно изменить |
| VALUE1, VALUE2 - | значения соответствующих настроек. |

Имена настроек указаны в таблице описания утилиты `drv_mgr`.

При успешной установке значения настройки будет выведено сообщение:

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

Значение настройки также записывается в конфигурационный файл, чтобы при запуске демона автоматически выставить его в IPsec-драйвере.

Имя конфигурационного файла, в который записываются значения:

```
%PROD_DIR%/etc/csp_ipsec_drv.cfg
```

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

При неуспешной установке значения настройки выводится сообщение:

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

  

# 26 drv_mgr reload

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

**Синтаксис** **`drv_mgr reload`**

Редактировать конфигурационный файл нельзя. Установить новые значения настроек драйвера, записываемые в конфигурационный файл, можно только командой й **`drv mgr set.`**

При успешном завершении утилита возвращает значение 0.

При возникновении ошибки утилита возвращает следующие значения:

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

# 27 klogview

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

**Синтаксис** **`klogview`** `[-ltT] [-p ts_precision][-m event_mask] [-f event_mask]`

`-l` ожидать сообщения из ядра и выводить их по мере поступления. Эта опция принимается по-умолчанию, если не задана опция –m.

`-t` печатать дату и время вывода сообщения

`-T` печатать относительное время, когда произошло событие. Время выводится в секундах относительно предыдущего события, показанного данным экземпляром утилиты. Например, значение 10.353245 – это 10 секунд и 353245 микросекунд. Максимальная точность – наносекунды, но реальная погрешность зависит от аппаратной плаформы 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.

`-p ts_precision` количество знаков долей секунд, используемых при печати относительного времени события (-T).

`-f event_mask` задать фильтр событий для данного экземпляра утилиты. Возможные события описаны в таблице.

`-m event_mask` задать фильтр событий по-умолчанию. Заданное значение используется, если не указана опция `-f`.

`-h` вывести краткую информацию об использовании утилиты.

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

| Имя группы событий | Код | Описание |
|---|---|---|
| `drop` | 2 | 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` | 1 | Пропуск пакета. Сообщение выводится непосредственно перед отсылкой какого-либо пакета и содержит краткий текст, поясняющий действия, которые были произведены над пакетом. |

  

| Имя группы событий | Код | Описание |
|---|---|---|
| sa_minor | 8 | Некоторые внутренние события, происходящие с IPsec - контекстом. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста. |
| sa_major | 4 | Взаимодействия между IPsec-драйвером и приложением, касающиеся изменения состояния IPsec-контекстов. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста. |
| sa_trace | 16 | Сообщения выводятся перед попыткой применения к пакету IPsec-контекста. |
| sa_errors | 32 | Ошибки, связанные с неуспешным применением IPsec-контекста к пакету. |
| filt_trace | 64 | В сообщении выводится имя и индекс правила фильтрации, если такое для пакета найдено. |

Нужный набор событий (event_mask) можно указать двумя способами:

- сложением кодов групп событий (см. в таблице)
  **Пример:**

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

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

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

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

**Рекомендации по использованию**

Используйте данную команду для просмотра сообщений, выдаваемых системой протоколирования.

## Сообщения, выводимые утилитой

Сообщения, выводимые утилитой, формируются на основе данных, присылаемых из IPsec-драйвера. Структура большинства сообщений определяется строкой формата[1], получаемой из IPsec-драйвера (см. Примеры сообщений).

Специальные сообщения, выводимые утилитой:

| | |
|---|---|
| *** N messages lost *** | выводится, если утилита не успевает обрабатывать сообщения и N сообщений поретяны. |
| no format string | в сообщении отсутствует строка формата[2]. |
| <error: .. | в выводимом сообщении несоответствие строки формата параметрам сообщения[3]. |

[1] Строка формата по смыслу и стилю похожа на форматную строку в printf

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

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

# 27.1 События группы pass и drop

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

Формат сообщения (в порядке следования):

- входящий или выходящий пакет
- IP-адрес источника
- порт источника
- IP-адрес получателя
- порт получателя
- номер IP-протокола
- логическое имя интерфейса или код интерфейса, если имя неизвестно
- действие "`passed`" или "`dropped`"
- строка, описывающая причину уничтожения или отправки пакета.

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

### Примеры сообщений группы pass

Пакет обработан по правилу фильтрации с действием `PASS`:

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

Пакет был обработан по `IPsec`-правилу:

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

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

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

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

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

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

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

## Примеры сообщений группы drop

Сообщения, связанные с некорректными данными заголовков пакета:

IP-заголовок испорчен:

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

TCP/UDP заголовок испорчен:

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

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

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

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

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

Испорчен ESP или AH заголовок:

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

Может выводиться при внутренних ошибках работы клиентской стороны IKEcfg:

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

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

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

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

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

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

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

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

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

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

Открытый пакет подпадает под правило фильтрации с IPsec-действием:

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

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

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

Ошибки IPsec:

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

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

**Возможны следующие ошибки:**

| Код | Название |
|---|---|
| 1 | replay packet detected |
| 2 | call to crypto subsystem failed |
| 3 | last sequence number |
| 4 | sequence number wrapped |
| 5 | integrity verification failed |
| 6 | corrupted protocol headers |
| 7 | corrupted headers after decapsulation |
| 8 | memory allocation failed |
| 9 | IP ttl expired |
| 10 | buffer is too small[4] |
| 11 | can't parse IP options |
| 12 | padding check failed |
| 13 | wrong encapsulation mode for the SA |

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

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

Очередь пакетов, ожидающая создания IPsec SA bundle переполнена:

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

[4] Это является внутренней ошибкой, просьба сообщать разработчикам.

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

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

Внутренние ошибки, о которых просьба сообщать разработчикам:

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

Другие сообщения:

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

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

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

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

## 27.2 События группы filt_trace

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

Пример сообщения:

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

## 27.3 События группы sa_minor, sa_major

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

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

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

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

## Примеры сообщений группы sa_major

Превышено ограничение SA по трафику:

```
SA 55 expired
```

Пора начинать rekeying SA (пройден барьер по трафику):

```
requesting rekeying for SA 33
```

SA нигде не используются и должны быть удалены:

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

Сообщения о загрузке новых SA:

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

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

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

  ```
  51 – AH
  50 - ESP
  ```
- Расшифровка некоторых[5] битов flags:

  ```
  0x1 – входящий
  ```
- Расшифровка битов `ipsec flags`:

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

Загрузка связки SA (SA bundle):

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

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

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

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

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

```
disabled SA 33
```

[5] Остальные значения флагов не предназначены для интерпретации пользователями.

  

Удаление SA:

```
removed SA 33
```

Удаление ранее заблокированного SA:

```
removed dead SA 33
```

Другие сообщения:

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

Сообщения, возникающие при ошибочном/странном[6] поведении Продукта:

```
can't add bundle: filter id 299 not found
can't add bundle: SA id 33 not found
can't add bundle: SA id 33 is unusable
can't load SA: unable to unpack
can't load replacement for SA 33: SA not found
can't load replacement for SA 33: can't unpack
can't load replacement for SA 33: race condition - SA is dead
can't remove SA 33: sa not found
can't disable SA 33: sa not found
can't enable SA 33: sa not found
rekey trigger: can't find SA 33
```

### Примеры сообщений группы sa_minor [7]:

```
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
```

## 27.4 События группы sa_trace

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

Примеры сообщений:

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

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

[7] Сообщения данного раздела предназначены для внутреннего использования. Расшифровка пользователям Продукта не предоставляется.

## 27.5 События группы sa_error

Сообщения этой группы выводят дополнительную информацию о специфических ошибках IPsec.

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

Пример сообщения:

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

# 28 Сообщения об ошибках

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

## Утилита cert_mgr

| | Текст сообщения | Описание проблемы |
|---|---|---|
| 1 | User error: no source file specified | Не указан путь к файлу (cert_mgr … -f) |
| 2 | FILENAME unable to open file | Проблемы с загрузкой 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 | 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 удается получить сертификаты из базы данных |
| 8 | User error: no number specified\n | Не указан номер сертификата (cert_mgr –i) |
| 9 | User error: NUMBER exceeds number of objects | Указанный индекс превышает количество объектов в базе данных. |
| 10 | User error. No subject | Не заполнено поле Subject Name |
| 11 | User error: Key KEY1 is not compatible with key KEY2 | Несовместимость ключей |
| 12 | User error: Key KEY is useless | Задан бесполезный ключ |
| 13 | User error: Key KEY is used twice | Повторное использование ключа |
| 14 | User error: Unable remove. Base is empty | Попытка удаления сертификата из пустой базы данных. |
| 15 | Internal error:Unable remove object from base | Невозможно удалить объект из базы данных. |
| 16 | User Error. Missing parameter | Пропущен параметр |
| 17 | User Error.  No file name specified | Не указано имя файла |
| 18 | Internal error. Storage error. | Ошибка при открытии хранилища |
| 19 | User error: INDEX exceeds number of objects in NAME | Ошибка указания индекса объекта |
| 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 |
| 22 | User error: Object index INDEX exceeds number of certificates and CRLs in base | Неверное указание индекса объекта |
| 23 | User Error. Missing index of object to be removed from base. Specify 'i' key and index | Не указан индекс объекта |

  

| | Текст сообщения | Описание проблемы |
|---|---|---|
| 24 | User error. Specify certificate request subject | Ошибка задания Subject сертификатного запроса |
| 25 | Internal error. Unable to create certificate request ERRCODE | Ошибка при создании сертификатного запроса |
| 26 | Unable to put certificate request into base ERRCODE | Ошибка при сохранении сертификатного запроса |
| 27 | User Error. Missing index of object to be imported from <FILENAME>. Specify i\|t key and index | Нет индекса и ключа при импорте объекта в базу (cert_mgr import –f file) |
| 28 | User Error. Missing index of object to be removed from base. Specify 'i' key and index | Нет индекса объекта при попытке удаления из базы |
| 29 | Container 'CONTAINER_NAME' is not exists or access denied | Не удалось получить доступ к контейнеру |
| 30 | Failed to read private key: ERROR_DESCRIPTION | Не удалось получить секретный ключ |
| 31 | Cannot connect to the IPsec service: service is not running. | Не удалось соединиться с демоном |
| 32 | Unable to set trusted status to certificate CERT_DSC | Не удалось выставить сертификату статус TRUSTED |
| 33 | Key is not consistent to cert CERT_DSC | Секретный ключ не подходит к сертификату или проверка закончилась неудачей |
| 34 | Unable to associate key and crt CERT_DSC | Не удалось прикрепить секретный ключ к сертификату |

## Утилита key_mgr

| | Текст сообщения | Описание проблемы |
|---|---|---|
| 1 | Internal error: No memory to open file FILENAME | Нет свободной оперативной памяти, необходимой для открытия файла |
| 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 данных. |
| 5 | Error: unable to remove key from db | Ошибка при попытке удалить ключ из базы данных. |

## Утилита lsp_mgr

| | Текст сообщения | Описание проблемы |
|---|---|---|
| 1 | FILENAME unable to open file | Ошибка при попытке открыть файл. |
| 2 | Internal error: Unable to set LSP as active | Ошибка активации конфигурации. |
| 3 | Internal error: No memory to open file FILENAME | Нет свободной оперативной памяти, необходимой для открытия файла |

| | | |
|---|---|---|
| 4 | Internal error: unrecognized error | Внутренняя ошибка. |
| 5 | Internal error: Unable to load lsp from base | Ошибка при попытке прочитать активную конфигурацию. |
| 6 | LSP loading error | Ошибка при попытке загрузить конфигурацию |

## Утилита lf_mgr

| | Текст сообщения | Описание проблемы |
|---|---|---|
| 1 | User error. Specify Physical Name | Не указано физическое имя сетевого интерфейса. |
| 2 | User error. Specify Logical name and key | Не указано логическое имя сетевого интерфейса. |
| 3 | User error. Unable to detect Network Interface NAME | Не найден сетевой интерфейс с указанным именем. |
| 4 | User error. Logical name NAME already occupied | Сетевой интерфейс с указанным логическим именем уже существует. |
| 5 | User error. Invalid logical name | Неправильный формат ввода логического имени. |
| 6 | User error. Specify IP-address | Не указан IP адрес сетевого интерфейса. |
| 7 | User error. Specify logical name | Не указано логическое имя сетевого интерфейса. |
| 8 | User error. Bad IP-address format | Неправильный формат IP адреса. |
| 9 | Internal error. Network interface initialization failure | Ошибка инициализации сетевого интерфейса. |
| 10 | Error. Network Interface with IP-address IP already registered by logical name NAME | Ошибка при попытке описать сетевой интерфейс с IP адресом, который принадлежит другому сетевому интерфейсу. |
| 11 | Error. Selected IP-address IP is not corresponds to any hardware interface | Ошибка при попытке описать сетевого интерфейса с IP адресом, которого нет ни у одного из сетевых интерфейсов. |
| 12 | User error. Specify IP-address or physical name and corresponding key | Не задан критерий поиска добавляемого сетевого интерфейса. |
| 13 | User error. Simultaneous definition of IP-address and physical name is prohibited | Ошибка при попытке описать сетевой интерфейс с указанием физического имени и IP адреса одновременно. |
| 14 | Internal error. Saving interface CODE | Ошибка при сохранении описания сетевого интерфейса. |
| 15 | User error. Undefined Network Interface logical name NAME | При удалении сетевого интерфейса не указано его логическое имя. |
| 16 | Can't find the network interface NAME | Не найдено интерфейса с указанным логическим именем. |

  

## Утилита dp_mgr

| | Текст сообщения | Описание проблемы |
|---|---|---|
| 1 | "ddd" is unknown parameter | Введен неизвестный параметр. |
| 2 | Error %d: VPN demon is not started | Проблема со стартом демона. |
| 3 | Error %d: Default driver policy is not wrote to db | Ошибка при записи Default Driver Policy в базу данных. |
| 4 | Error %d: Default driver policy is not read from db | Ошибка при чтении Default Driver Policy из базы данных. |

## Утилита log_mgr

| | Текст сообщения | Описание проблемы |
|---|---|---|
| 1 | "ddd" is unknown parameter | Введен неизвестный параметр. |
| 2 | Error %d: VPN demon is not started | Проблема со стартом демона. |
| 3 | Error %d: Severity level is not wrote to db | Ошибка при записи уровня протоколирования |
| 4 | Error %d: Severity level is not read from db | Ошибка при чтении уровня протоколирования |

## Утилита lic_mgr

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

## Утилита drv_mgr

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

-