ООО «С-Терра СиЭсПи»
124498, г. Москва, Зеленоград, Георгиевский проспект,
дом 5, помещение I, комната 33
Телефон: +7 (499) 940 9061
Факс: +7 (499) 940 9061
Эл.почта: information@s-terra.com
Сайт: http://www.s-terra.com

Программный комплекс CSP VPN Gate. Версия 3.11

Руководство администратора

Специализированные команды

РЛКЕ.00005-02 90 03

16.04.2015

Содержание

Специализированные команды 4
cspvpn_verify 5
cspvpn_verify_kc3 6
cpverify 7
cert_mgr show 8
cert_mgr import 10
cert_mgr create 12
cert_mgr remove 14
cert_mgr check 15
key_mgr show 16
key_mgr import 17
key_mgr remove 18
lsp_mgr show 19
lsp_mgr load 20
lsp_mgr unload 21
lsp_mgr reload 22
lsp_mgr check 23
if_mgr show 24
if_mgr add 26
if_mgr remove 27
dp_mgr show 28
dp_mgr set 29
log_mgr set 30
log_mgr show 31
sa_mgr show 32
sa_mgr clear 37
lic_mgr show 38
lic_mgr set 39
drv_mgr 40
drv_mgr show 43
drv_mgr set 44
drv_mgr reload 45
klogview 46

 Copyright © S-Terra CSP 2003 -2015

Сообщения об ошибках 55

Специализированные команды

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

Перечень программных утилит, входящих в состав Продукта:

- `cspvpn_verify`
- `cspvpn_verify_kc3`
- `cpverify`
- `cert_mgr`
- `key_mgr`
- `lsp_mgr`
- `if_mgr`
- `dp_mgr`
- `log_mgr`
- `sa_mgr`
- `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 команды `run`.

Запуск утилит с опцией ***–h*** вызывает помощь.

Copyright © S-Terra CSP 2003 -2015

cspvpn_verify

Утилита cspvpn_verify используется для регламентной проверки целостности установленного Продукта CSP VPN Gate, исполнения класса защиты КС1/КС2, во время его работы. Утилита применяется только при использовании СКЗИ "КриптоПро CSP".

Синтаксис

```
/opt/VPNagent/bin/cspvpn_verify
```

Рекомендации по использованию

Используйте утилиту `cspvpn_verify` для проверки целостности всех исполняемых файлов установленного Продукта `CSP VPN Gate`. Утилита `cspvpn_verify` размещена на ПАК в каталоге `/opt/VPNagent/bin` и запускается командой:

```
/opt/VPNagent/bin/cspvpn_verify
```

Эталонные значения хэш-сумм всех проверяемых файлов записаны в файл `/opt/VPNagent/bin/.hashes`, который содержит строки вида:

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

где

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

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

Эта же утилита автоматически запускается при каждом старте программного комплекса, а также после процедуры инициализации CSP 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/cspvpn_verify_err.log` передается сообщение о произошедшей ошибке. Затем проверяется работа сервиса vpnsvc. При его наличии – выполняется аварийное прерывание.

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

При нарушении целостности работающего Продукта CSP VPN Gate восстановите содержимое жесткого диска ПАК из образа жесткого диска, который входит в комплект поставки. Выполните эту процедуру согласно «Инструкции по восстановлению ПАК и замены компакт-флеш карты на модуле».

 Copyright © S-Terra CSP 2003 -2015

cspvpn_verify_kc3

Утилита cspvpn_verify_kc3 используется для регламентной проверки целостности установленного Продукта CSP VPN Gate, исполнения класса защиты КС3, во время его работы. Утилита применяется только при использовании СКЗИ "КриптоПро CSP". Утилита автоматически запускается при каждом старте программного комплекса, а также может быть запущена вручную.

Синтаксис

```
/opt/VPNagent/bin/cspvpn_verify_ kc3 /opt/VPNagent/bin/.hashes_kc3
```

Рекомендации по использованию

Используйте утилиту `cspvpn_verify_kc3` для проверки целостности всех исполняемых файлов установленного Продукта `CSP VPN Gate`. Утилита `cspvpn_verify_kc3` размещена на ПАК в каталоге `/opt/VPNagent/bin`. Запуск выполняется командой:

```
/opt/VPNagent/bin/cspvpn_verify /opt/VPNagent/bin/.hashes_kc3
```

Эталонные значения хэш-сумм всех проверяемых файлов записаны в файл `/opt/VPNagent/bin/.hashes_kc3`, который содержит строки вида:

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

где

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

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

Утилита выполняет последовательную проверку хэш-сумм по списку, с выдачей сообщений на стандартный вывод: `File '/path/to/file' has been verified`.

В случае несовпадения хэша по файлу работа утилиты завершится с ненулевым кодом ошибки и сообщением: `File '/path/to/file' was corrupted`.

В случае непредвиденных ошибок будет выдана информация об ошибке, утилита завершится с ненулевым кодом ошибки.

При нарушении целостности работающего Продукта CSP VPN Gate восстановите содержимое жесткого диска ПАК из образа жесткого диска, который входит в комплект поставки. Выполните эту процедуру согласно «Инструкции по восстановлению ПАК и замены компакт-флеш карты на модуле».

 Copyright © S-Terra CSP 2003 -2015

cpverify

Утилита cpverify используется для проверки целостности файла дистрибутива CSP VPN Gate с именем `cspvpn.tar`, записанного на поставляемый компакт-диск. Утилита разработана компанией "Крипто-Про" и применяется только при использовании СКЗИ "КриптоПро CSP".

Синтаксис

```
/opt/cprocsp/bin/ia32/cpverify –mk cspvpn.tar
```

Рекомендации по использованию

Утилита `cpverify` размещена на ПАК в каталоге `/opt/cprocsp/bin/ia32`.

Для вычисления хэш-суммы файла дистрибутива и выдачи результата на экран выполните команду:

```
/opt/cprocsp/bin/ia32/cpverify –mk cspvpn.tar
```

Полученное значение сравните со значением хэш-суммы, записанной в файл `hashes`, который размещен на компакт-диске рядом с дистрибутивом.

Файл `hashes` содержит строку вида `<hash> <file_name>`,

где

`<hash>` – эталонное значение хэш-суммы

`<file_name>` – имя файла, для которого подсчитана хэш-сумма.

Для вычисления хэш-суммы и автоматического сравнения с эталонным значением, выполните команду:

```
/opt/cprocsp/bin/ia32/cpverify cspvpn.tar hash_from_file,
```

где

`hash_from_file` – эталонное значение хэш-суммы, скопированное из файла `hashes`.

При нарушении целостности дистрибутива для инсталляции Продукта используйте образ жесткого диска, который входит в комплект поставки для восстановления содержимого жесткого диска ПАК. Выполните эту процедуру согласно «Инструкции по восстановлению ПАК и замены компакт-флеш карты на модуле», описанной в файле документации Restore_image.pdf.

 Copyright © S-Terra CSP 2003 -2015

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 C_FILE [-p C_FILE_PWD]] [-i OBJ_INDEX_1] …
[-i OBJ_INDEX_N] [-expired_remote]
```

`-f C_FILE`	путь к файлу с сертификатами и CRL. Если данная опция не указана, то будут показаны 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 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 всех объектов (сертификатов и CRL) в файле или базе Продукта используйте команду `cert_mgr show` без указания индексов `i` и опции `-expired_remote`. В этом случае будет выведен нумерованный список сертификатов и CRL с указанием поля subject для сертификатов и поля issuer для списка 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 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
```

 Copyright © S-Terra CSP 2003 -2015

```
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 2005

  Valid to:   Thu Nov 23 08:06:02 2006

  Version: 3

  Serial number: 04 11 83 A5 00 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\=Publ

ic%20Key%20Services\,CN\=Services\,CN\=Configuration\,DC\=har-test-
dc\,DC\=s-ter

a\,DC\=com?certificateRevocationList?base?objectclass\=cRLDistributionP
oint

  CRLI[0]: 1.2.840.113549.1.9.1=har@s-terra.com,C=RU,L=Moscow,O=S-Terra
CSP,OU=D

evel,CN=Test CA sc-cp

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

sc-cp.crl

  CRLI[1]: 1.2.840.113549.1.9.1=har@s-terra.com,C=RU,L=Moscow,O=S-Terra
CSP,OU=D

evel,CN=Test CA sc-cp

  Private key container name: 'c:\sc_cp\user_sc_cp_01'
```

 Copyright © S-Terra CSP 2003 -2015

cert_mgr import

Команда `cert_mgr import` предназначена для регистрации CA и локальных сертификатов, а также списков отозванных сертификатов (Certificate Revocation List, CRL) в базе Продукта.

При использовании СКЗИ "КриптоПро CSP 3.6"

Синтаксис

```
cert_mgr import -f C_FILE [-p C_FILE_PWD] [-i OBJ_INDEXN]
[-t | -kc K_CONTAINER_NAME [-kcp K_CONTAUNER_PWD]]
```

`-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`	регистрируемому сертификату присваивается статус `"trusted"` (для CA сертификата). При использовании этой опции запрещается использование опций `-kc,-kcp`. Запрещается использовать эту опцию при импорте CRL
`-kc K_CONTAINER_NAME`	имя контейнера с секретным ключом локального сертификата. Не может использоваться, если ранее введена опция `-t`.

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.

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.

Если сертификат был создан на основе запроса, созданного при помощи команды cert_mgr create, то при регистрации такого сертификата нужно указать только файл с сертификатом, не указывая имя контейнера и пароль к нему.

 Copyright © S-Terra CSP 2003 -2015

Примечание:

Для получения уникального имени контейнера , размещенного на каком-либо ключевом носителе, выполните команды:

```
cd /opt/cprocsp/bin/ia32
./csptest -keyset -machinekeyset -verifycontext -enum_containers -
unique
```

Примеры вывода уникальных имен контейнеров:

`'FAT12\\TEST1.000'` – для контейнера на дискете

`'HDIMAGE\\test1'` – для контейнера на жестком диске

Копирование контейнера

Если нужно скопировать контейнер с секретным ключом с одного ключевого носителя на другой, то выполните команды:

```
/opt/cprocsp/bin/ia32/csptest -keycopy -machinekeyset -src
'\\.\media\src_cont' -dest '\\.\media\dst_cont'
```

Тип секретного ключа в контейнере указывать не нужно.

Пример

Ниже приведен пример регистрации сертификатов в базе Продукта.

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

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

Регистрация локального сертификата, размещенного в файле `gate02.cer`, а 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
```

cert_mgr create

Команда `cert_mgr create` предназначена для генерации ключевой пары и создания запроса на сертификат открытого ключа. Полученный запрос нужно будет отправить в Удостоверяющий Центр, где и будет создан соответствующий сертификат открытого ключа.

Синтаксис

```
cert_mgr create - subj CERT_SUBJ [-RSA|-DSA|-GOST_R3410EL]
[-512|-1024] [-mail MAIL] [-ip IP_ADDR] [-dns DNS]
[-kc K_CONTAINER_NAME] [-kcp K_CONTAINER_PWD] [-f OUT_FILE_NAME]
```

`-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
`-GOST_R3410EL`	идентификатор алгоритма ГОСТ Р 34.10-2001, 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 в бинарной кодировке DER.

Создание ключевой пары и запроса на сертификат с использованием алгоритма ГОСТ можно также выполнить и при помощи утилит, предоставленных криптопровайдерами, и входящими

в состав CSP VPN Gate. Процедуры создания локальных сертификатов с использованием различных криптопровайдеров описаны в документе «Приложение».

Значение по умолчанию

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

Рекомендации по использованию

Используйте данную команду для создания ключевой пары и запроса на сертификат.

Запрос защищается от подмены при помощи ЭЦП, которая формируется с использованием сгенерированного секретного ключа и выбранного алгоритма ЭЦП.

В момент генерации ключевой пары запускается «биологическая» инициализация датчика случайных чисел, поэтому:

- при использовании СКЗИ «КриптоПро CSP» на консоли появляется просьба понажимать любые клавиши или поперемещать указатель мыши.

В случае использования режима КС2 биологическая инициализация ДСЧ не запускается.

Команда `cert_mgr create` позволяет сохранить контейнер с секретным ключом на шлюзе безопасности, избежав ситуации переноса контейнера с одного носителя на другой.

Если при написании команды не указать опцию `-f` с именем файла для размещения запроса, то сформированный запрос будет выведен на экран в кодировке Base64.

Одновременно хранится только один сертификатный запрос. При генерации следующего запроса и незаконченном первом, старый запрос удаляется. При таком удалении неиспользованного запроса будет так же удаляться и контейнер, с ним связанный.

Примечание:

При создании ключевой пары без указания имени контейнера, контейнер будет создан и размещен на жестком диске с именем:

- при использовании СКЗИ «КриптоПро CSP 3.6»:

  `"\\.\HDIMAGE\HDIMAGE\\vpnXXXXXXXX"`

где

`vpnXXXXXXXX` – автоматически сформированное уникальное имя контейнера

Пример

1. Создайте на CSP VPN Gate запрос на сертификат с использованием ГОСТ алгоритма:

```
cert_mgr create -subj O=S-Terra,CN=LocalCert - GOST_R3410EL -f
/opt/VPNagent/bin/local_GW.req
```

2. Полученный бинарный файл сохраните в кодировке Base64, выполнив команду:

```
cat local_GW.req | base64 > local_GW64.req
```

3. Зайдите на шлюз безопасности по протоколу SSH, например, запустив с отдельно стоящего компьютера Putty Configuration, и для вывода запроса на экран выполните команду:

```
cat local_GW64.req
```

4. Выделите мышкой запрос и скопируйте его в файл или буфер, а затем отошлите в Центр Сертификации для создания локального сертификата. Отсылка запроса на сертификат описана в документе «Приложение».

cert_mgr remove

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

Синтаксис

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

`-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.

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: CRL can not be removed from base
Other operations are cancelled due to error
```

 Copyright © S-Terra CSP 2003 -2015

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
- `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 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.

 Copyright © S-Terra CSP 2003 -2015

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 по использованию

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
```

 Copyright © S-Terra CSP 2003 -2015

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 по использованию

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
```

 Copyright © S-Terra CSP 2003 -2015

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 по использованию

Используйте данную команду для удаления предопределенных ключей из базы Продукта.

Пример

Ниже приведен пример удаления предопределенного ключа:

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


Copyright © S-Terra CSP 2003 -2015

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 2004"
   Version = "3.11"
   CRLHandlingMode = DISABLE
)
ESPProposal ESP_ts_m1_sn1(
   Transform* = ESPTransform (
      CipherAlg* = "AES-K192-CBC-12"
      IntegrityAlg* = "GR341194CPRO1-H96-HMAC-254"
      LifetimeSeconds = 3600
      LifetimeKilobytes = 4608000
   )
)
```

 Copyright © S-Terra CSP 2003 -2015

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 «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
```


Copyright © S-Terra CSP 2003 -2015

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
```

 Copyright © S-Terra CSP 2003 -2015

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.
```

 Copyright © S-Terra CSP 2003 -2015

lsp_mgr check

Команда `lsp_mgr check` предназначена для проверки LSP конфигурации.

Синтаксис

```
lsp_mgr check -f LSP_FILE
```

`- f LSP_FILE` путь к файлу конфигурации

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

Copyright © S-Terra CSP 2003 -2015

if_mgr show

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

Синтаксис

```
if_mgr show
```

Команда не имеет аргументов и ключей

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра параметров всех сетевых интерфейсов.

После выполнения этой команды на экран будет выведена информация о логических именах защищаемых интерфейсов и связанных с ними данных по физическим интерфейсам, а также информация по физическим интерфейсам, не защищаемых Продуктом.

Примечание:

В выводе команды параметр State показывает общее состояние интерфейса. Параметр State отображает состояние физического интерфейса, и считается, что оно совпадает с состоянием логических интерфейсов.

Пример

Ниже приведен пример выполнения команды `if_mgr show`:

```
[root@cspgate]# if_mgr show
Logical network interface 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: eth1
        State:         DOWN
        Index:         3
        MTU:           1500
```

 Copyright © S-Terra CSP 2003 -2015

```
        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 ppps:
        Physical name template: ppp*

        Physical name: ppp0
        State:          UP
        Index:          14
        MTU:            1200
        MAC addr:
        IP addr:        1.1.1.2 mask 255.255.255.255 brd 0.0.0.0
```

 Copyright © S-Terra CSP 2003 -2015

if_mgr add

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

Синтаксис

```
if_mgr add {-a IP_ADDR |-i IF_INDEX |-n PHYSICAL_NAME}
-l LOGICAL_NAME
```

`-a IP_ADDR`	IP-адрес защищаемого сетевого интерфейса
`-i IF_INDEX`	индекс 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 вывода на экран системной команды `ifconfig –a`.

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

При регистрации сетевого интерфейса с заданным IP-адресом или индексом, или физическим именем происходит проверка на существование физического интерфейса с заданным параметром. Если такой физический интерфейс существует, то команда завершается успешно.



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
```

 Copyright © S-Terra CSP 2003 -2015

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
```

 Copyright © S-Terra CSP 2003 -2015

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 настройки 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
```

 Copyright © S-Terra CSP 2003 -2015

dp_mgr set

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


Copyright © S-Terra CSP 2003 -2015

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
```

 Copyright © S-Terra CSP 2003 -2015

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
```

 Copyright © S-Terra CSP 2003 -2015

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

`-isakmp`	выводится информацию об ISAKMP соединениях
`-ipsec`	выводится информацию об IPsec соединениях
`-i CONNn_ID`	выводится информация о соединении с указанным идентификатором
`-detail`	выводится детальная информация о соединениях

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

`sa_mgr show`

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

```
ISAKMP sessions: 0 initiated, 0 responded


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



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

В выводе присутствует следующая информация:

- `ISAKMP sessions` – количество незавершенных IKE-обменов:
  - `ni initiated` – в качестве инициатора
  - `nr responded` – в качестве ответчика.

 Copyright © S-Terra CSP 2003 -2015

- `ISAKMP connections` – информация обо всех ISAKMP SA и для каждого соединения:
  - `Num` – порядковый номер ISAKMP соединения
  - `Conn-id` – уникальный идентификатор ISAKMP соединения
  - `Remote Addr,Port` – адрес и порт партнера, если порт любой - *
  - `Local Addr,Port` – локальный адрес и порт, если порт любой - *
  - `State` – состояние SA:
    - `incomplete` – недостроенное соединение
    - `active` – активное соединение
    - `configuration` – для данного SA проводится дополнительная настройка `(IKECFG, XAuth, etc.)`
    - `deleted` – SA не используется, подготовлен к удалению
    - `unknown` – статус соединения неизвестен
  - `Sent` – количество переданной информации (в байтах)
  - `Rcvd` – количество принятой информации (в байтах)
- `IPsec connections` – информация обо всех IPsec SA и для каждого соединения:
  - `Num` – порядковый номер IPsec соединения
  - `Conn-id` – уникальный идентификатор IPsec соединения
  - `Remote Addr,Port` – адрес и порт партнера, если порт любой – *
  - `Local Addr,Port` – локальный адрес и порт, если порт любой –- *
  - `Protocol` – сетевой протокол, если протокол любой – *
  - `Action` – действие – {`AH+ESP|AH|ESP`}
  - Type – тип:
    - `tunn` – туннельный режим
    - `trans` – транспортный режим
    - `nat-t-tunn` – туннельный режим через NAT
    - `nat-t-trans` – транспортный режим через NAT
  - `Sent` – количество переданной информации (в байтах)
  - `Rcvd` – количество принятой информации (в байтах)

`sa_mgr show –ipsec –i 8`

Данная команда выводит информацию о соединении с заданными свойствами.

IPsec connections:

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

`sa_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/recv errors: 2/0

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

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

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

 Copyright © S-Terra CSP 2003 -2015

```
    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 SA,

Синтаксис

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

`-isakmp`	удаляет ISAKMP соединения
`-ipsec`	удаляет IPsec соединения
`-i CONNn_ID`	удаляет соединения с указанным идентификатором
`-silent`	удаляет соединения без уведомления партнера
`-all`	удаляет все соединения

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для удаления SA, Для выборочного удаления используются опции `–isakmp, -ipsec, -i`.

Для удаления всех соединений указывается опция `–all`. При использовании этой опции имеется следующая особенность: если сначала удалятся ISAKMP SA, то для удаления IPsec SA может понадобится создание новых ISAKMP SA. Таким образом, команда `sa_mgr clear –all` удаляет все существующие, до начала выполнения команды, ISAKMP SA и IPSec SA, но в процессе ее выполнения могут быть построены новые ISAKMP SA

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

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

 Copyright © S-Terra CSP 2003 -2015

lic_mgr show

Команда `lic_mgr show` предназначена для просмотра текущей Лицензии на продукт CSP 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.

Copyright © S-Terra CSP 2003 -2015

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
```

 Copyright © S-Terra CSP 2003 -2015

drv_mgr

Утилита `drv_mgr` предназначена для решения проблем, возникающих на CSP VPN Gate, если на обработку поступает больший объем трафика, чем может обработать шлюз безопасности. Эту ситуацию будем называть "перегрузка". В связи с перегрузкой на платформе 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_psize          read-write      4                 [1-100000]
pq_tos_mask       read-write      1                 unlimited
pq_do_idle        read-write      1                 [0-2]
pq_busy_interval  read-write      4                 [1-1000000]
pq_drop_low_pri   read-write      1                 [0-1]
pq_drop_thres     read-write      4                 [0-100]
ipsec_breq_max    read-write      4                 unlimited
ipsec_breq_count  read-only       4                 unlimited
```

Рекомендации по использованию

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 = 2`, то производится перемещение нити в конец очереди задач, что теоретически повышает интерактивность операционной системы за счёт некоторого снижения пропускной способности VPN при существенной посторонней нагрузке.

 Copyright © S-Terra CSP 2003 -2015

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	***Тип доступа***	***Размер-ность***	***Рекомен-дуемые значения***	***Значение по умолчанию***	***Описание***
pq_psize	чтение-запись	пакеты	1-1000	100	Максимальное количество пакетов в очереди, при достижении которого пакеты начинают уничтожаться.
pq_do_idle	чтение-запись		0, 1, 2	1	Включение/выключение механизма защиты от перегрузки: 0 – защита от перегрузки выключена 1 – передача управления системному планировщику задач, который выбирает для выполнения задачу с наивысшим приоритетом 2 – передача управления системному планировщику задач с одновременным перемещени- ем задачи обработки пакетов в конец очереди.
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 равно 255, то при любом не равном нулю поле TOS, пакет является приоритетным.
pq_busy_interval	чтение-запись	микро-секунды	0-1000000	20000	Интервал времени, в течение которого происходит обработка пакетов IPsec драйвером. После , при необходимости, делается передача управления системе.
pq_drop_low_pri	чтение-запись		0, 1	0	Включение/выключение механизма уничтожения неприоритетных пакетов: 0 – неприоритетные пакеты явно не уничтожаются, происходит разделение очереди на две части – общую и приоритетную; 1 – неприоритетные пакеты уничтожаются при уровне заполнения очереди pq_drop_thres

 Copyright © S-Terra CSP 2003 -2015

Наименование настройки	*Тип доступа*	*Размер-ность*	*Рекомен-дуемые значения*	*Значение по умолчанию*	*Описание*
					и выше.
pq_drop_thres	чтение-запись	проценты	1-100	90	Процент заполнения очереди пакетов от максимального количества пакетов, при котором неприоритетные пакеты начинают уничтожаться.
ipsec_breq_max	чтение-запись			1000	Максимальное количество одновременно выполняющихся запросов на создание SA bundle.
ipsec_breq_count	чтение			0	Текущее количество одновременно выполняющихся запросов на создание SA bundle.

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_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

```
pq_size             100
pq_tos_mask         255
pq_do_idle          0
q_busy_interval     20000
pq_drop_low_pri     0
pq_drop_thres       90
ipsec_breq_max      1000
ipsec_breq_count    0
```

 Copyright © S-Terra CSP 2003 -2015

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_NAMEn`	имена настроек, значения которых нужно изменить
`VALUEn`	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.
```

 Copyright © S-Terra CSP 2003 -2015

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 `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

Copyright © S-Terra CSP 2003 -2015

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.

 Copyright © S-Terra CSP 2003 -2015

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:

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

 Copyright © S-Terra CSP 2003 -2015

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

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

События группы pass и drop

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

Формат сообщения (в порядке следования):

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

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

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

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

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

Примеры сообщений группы drop

Сообщения, связанные с некорректными данными заголовков пакета:

IP-заголовок испорчен:

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

TCP/UDP заголовок испорчен:

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

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

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

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

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

Испорчен ESP или AH заголовок:

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

Может выводиться при внутренних ошибках работы клиентской стороны IKEcfg:

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

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

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

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

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

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

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

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

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

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

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

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

 Copyright © S-Terra CSP 2003 -2015

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

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

Ошибки IPsec:

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

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

Возможны следующие ошибки

Код	***Название***	***Описание проблемы***
1	replay packet detected	обнаружен повторный пакет
2	call to crypto subsystem failed	ошибка крипто-подсистемы
3	last sequence number	последний номер пакета
4	sequence number wrapped	переполнение счетчика пакетов
5	integrity verification failed	проверка целостности не прошла
6	corrupted protocol headers	испорченный протокольный заголовок
7	corrupted headers after decapsulation	испорченный протокольный заголовок после декапсуляции
8	memory allocation failed	невозможно выделить память
9	IP ttl expired	счетчик IP ttl истек
10	buffer is too small[4]	буфер слишком мал
11	can't parse IP options	невозможно разобрать опции IP
12	padding check failed	ошибка в заполнителе
13	incorrect SA parameters (from pmod_init_sa)[5]	неправильные параметры SA
14	encapsulation mode (tunnel/transport) doesn't match the SA	режим инкапсуляции (туннельный или транспортный) не соответствует SA
15	traffic limit exceeded[6]	превышено ограничение на количество обработанного трафика

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

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

[6] SA удалится, и потом должна произойти смена ключей.

 Copyright © S-Terra CSP 2003 -2015

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
```

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
```

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)
```

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

 Copyright © S-Terra CSP 2003 -2015

- 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[7] 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
```

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

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

```
disabled SA 33
```

Удаление SA:

```
removed SA 33
```

Удаление ранее заблокированного SA:

```
removed dead SA 33
```

Другие сообщения:

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

Сообщения, возникающие при ошибочном/странном[8] 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 [9]:

```
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

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

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

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
```

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.
```

 Copyright © S-Terra CSP 2003 -2015

Сообщения об ошибках

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

Утилиты cspvpn_verify, cpverify

	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 cpverify 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 cpverify эти ситуации не различает)).

Утилита cert_mgr

	Текст сообщения	*Описание проблемы*
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	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)

 Copyright © S-Terra CSP 2003 -2015

	Текст сообщения	*Описание проблемы*
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 при удалении из базы продукта
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	Internal error. 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' key and index	Нет индекса и ключа при импорте объекта в базу (cert_mgr import –f file)
28	User error. Container 'CONTAINER_NAME' is not exists or access denied	Не удалось получить доступ к контейнеру
29	User error. Failed to read private key: ERROR_DESCRIPTION	Не удалось получить секретный ключ
30	User error. Cannot connect to the IPsec service: service is not running.	Не удалось соединиться с демоном

 Copyright © S-Terra CSP 2003 -2015

	Текст сообщения	*Описание проблемы*
31	User error. Unable to set trusted status to certificate CERT_DSC	Не удалось выставить сертификату статус TRUSTED
32	User error. Key is not consistent to cert CERT_DSC	Секретный ключ не подходит к сертификату или проверка закончилась неудачей
33	User error. Unable to associate key and crt CERT_DSC	Не удалось прикрепить секретный ключ к сертификату
34	User Error: This certificate can not be imported into DB with specified parameters.	Не удалось импортировать в базу продукта сертификат с заданными параметрами
35	Crypto error. Unable to create key container.	Не удается создать контайнер ключа (проверить правильность имени контайнера)
36	Crypto error. Unable to create certificate request. Error code: CRYPTO PROVIDER ERROR	Не удалось создать запрос на сертификат (проверить отсутствие символов '_' в имени контайнера CryptoPro)

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	User error. 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	Internal error: Unable to set LSP as active.	Не может загрузить конфигурацию. Указанный

 Copyright © S-Terra CSP 2003 -2015

	Algorithm “Algorithm” not supported. Other operations are cancelled due to error	алгоритм не поддерживается.

Утилита lf_mgr

	Текст сообщения	*Описание проблемы*
1	User error. Specify physical name	Не указано физическое имя сетевого интерфейса.
2	User error. Specify interface index	Не указан индекс сетевого интерфейса.
3	User error. Logical name NAME already occupied	Сетевой интерфейс с указанным логическим именем уже существует.
4	User error. Invalid logical name	Неправильный формат ввода логического имени.
5	User error. Specify IP-address	Не указан IP адрес сетевого интерфейса.
6	User error. Specify logical name	Не указано логическое имя сетевого интерфейса.
7	User error. Bad IP-address format	Неправильный формат IP адреса.
8	User error. Bad interface index format	Неправильный формат индекса интерфейса
9	Internal error. Network interface initialization failure	Ошибка инициализации сетевого интерфейса.
10	Internal error. Local network interfaces list initialization failure	Не удалось получить информацию об именах логических интерфейсов
11	User error. Network Interface with IP-address IP already registered by logical name NAME	Указанный IP адрес принадлежит сетевому интерфесу уже зарегистрированному в базе продукта
12	User Error. Network Interface with name NAME already registered by logical name NAME	Указанный сетевой интерфейс с именем NAME уже зарегистрирован в базе продукта с логическим именем NAME
13	User Error. Network Interface with interface index IF_INDEX already registered by logical name NAME	Указанный сетевой интерфейс с индексом IF_INDEX уже зарегистрирован в базе продукта с логическим именем NAME
14	User Error. Selected IP-address IP is not corresponds to any hardware interface	Указанный IP адрес не соответствует никакому физическому интерфейсу
15	User Error. Selected interface index INDEX is not corresponds to any hardware interface	Указанный индекс сетевого интерфейса не соответствует никакому физическому интерфейсу
16	User error. Specify IP-address or physical name or index and corresponding key	Не задан критерий поиска добавляемого сетевого интерфейса.

	Текст сообщения	*Описание проблемы*
17	User error. Only one of IP-address, physical name or index must be set	Ошибка при попытке описать сетевой интерфейс, указывая одновременно несовместные параметры: Физическое Имя, IP-адрес, индекс интерфейса
18	Internal error. Logical interface NAME is not added. Error code: CODE	Ошибка при сохранении описания сетевого интерфейса.
19	User error. Undefined Network Interface logical name NAME	При удалении сетевого интерфейса не указано его логическое имя.
20	User error. 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.

 Copyright © S-Terra CSP 2003 -2015