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

Программный комплекс С-Терра Шлюз. Версия 4.1

Руководство администратора

Протоколирование событий

РЛКЕ.00009-01 90 03

15.06.2015

Содержание

Протоколирование событий

В Продукте протоколирование событий происходит по протоколу Syslog. Получатель лога может быть только один, в отличие от Cisco IOS. При невозможности использовать Syslog, дополнительно производится запись некоторых сообщений в специальные log-файлы.

Настройка Syslog-клиента

LSP (native) конфигурация

В политике безопасности, созданной в виде текстового файла, настройки протоколирования не задаются. Для этого используйте утилиту ***log_mgr***.

Утилита log_mgr

Утилита ***/opt/VPNagent/bin/log_mgr*** используется для задания и просмотра настроек Syslog-клиента, групп событий и уровней лога для каждой группы.

С целью фильтрации протоколируемых сообщений тем или иным образом устанавливается общий протоколируемый уровень важности LogLevel (или уровень важности по умолчанию). Также, каждое событие имеет свой фиксированный уровень важности Severity, указанный в файле `/opt/VPNagent/etc/s_log.ini` (Таблица 4). Событие, которому соответствует фиксированный уровень важности X, протоколируется только в том случае, если при его совершении общий уровень важности LogLevel не выше данного фиксированного уровня X.

События можно объединять в группы и назначать новый групповой уровень протоколирования.

log_mgr set

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

Синтаксис

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

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 600 секунд
`-l log_level`	общий уровень протоколирования всех событий, не включенных в группы событий. Имеет одно из возможных значений (в порядке уменьшения важности):

`emerg` – аварийные сообщения

`alert` – тревожные сообщения

`crit` – критические сообщения

`err` – сообщения об ошибках

`warning` – предупреждения

`notice` – извещения

`info` – информационные сообщения

`debug` – отладочные сообщения.

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

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

`-y {enable|disable}` включение/выключение протоколирования

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

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

   ```
   log_mgr set –l warning
   ```

2. Продукт поставляется с пятью предустановленными файлами, размещенными в каталоге `/opt/VPNagent/etc`, в которых указаны группы событий и уровень лога для этих событий. Эти файлы созданы для совместимости с продуктом S-Terra Gate версии 3.1:

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

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

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

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

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

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


```
log_mgr save
```

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

```
log_mgr set –e
```

Настройка сохраняется до перезапуска сервиса.

Создание файла с группами событий

Каждый такой файл должен состоять из секций вида:

```
[LOGLEVEL.<LEVEL>]
<MSG_ID1>
<MSG_ID2>
!........
```

где

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

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

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

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

Пример такого файла – “msg_groupDEMO1.ini”:

```
[LOGLEVEL.DEBUG]
! сообщение PRODUCT_START задано его индексом:
03090001
! сообщение PRODUCT_STOP задано его текстовым представлением:
PRODUCT_STOP
```

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

Если необходимо изменить фиксированный уровень аудита, указанный в файле /opt/VPNagent/etc/s_log.ini, для отдельного события, можно создать файл типа msg_XXX.ini и задать в нем нужный уровень протоколирования.

Пример

Например, для изменения фиксированного уровня протоколирования сообщения MSG_ID_AUDIT_SHOW_NEW_LSP с INFO на ERR, создаем в директории /opt/VPNagent/etc файл msg_LSPSHOW.ini, содержащий строки:

```
[LOGLEVEL.ERR]
MSG_ID_AUDIT_SHOW_NEW_LSP
```


Далее выполняем команды:

```
log_mgr set -e msg_LSPSHOW.ini
log_mgr save
```

5. Установка параметров syslog-клиента для сервиса vpnsvc. Для установки настроек Syslog-клиента, которые будут записаны в файл `/opt/VPNagent/etc/syslog.ini`, выполните команду:

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

Например,

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

Неуказанный в команде параметр остается неизменным.

6. Для установки параметров по умолчанию для syslog-клиента выполните:

```
log_mgr reset-syslog
```

при этом действуют следующие настройки:

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

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

Пример

Пример выполнения команды `log_mgr set`:

```
log_mgr set -l warning
```

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

Редактирование файла s_log.ini

Существует группа сообщений, протоколирование которых производит vpnlogsvc. Для таких сообщений описанный выше способ изменения фиксированного уровня протоколирования не работает: внесение изменений происходит непосредственным редактированием файла `s_log.ini`.

Информация, содержащаяся в файле `s_log.ini`, аналогична информации, представленной в Таблица 4, и имеет вид:

```
[ <MSG_ID mnemonic> ]
<Russian(Русские) UTF-8 comment lines for User's Manual>
SEVERITY  = EMERG | ALERT | CRIT | ERR | WARNING | NOTICE | INFO |
DEBUG
INDEX     = 0x<module index><MSG_ID subindex 0001..ffff>
TMPL      = <message template>
NONBLOCKABLE = TRUE | FALSE
```

где

`<MSG_ID mnemonic>`	текстовое представление идентификатора события, состоящее из заглавных латинских букв и знаков «_» и обязательно содержащее префикс "MSG_ID_"

<Russian(Русские) UTF-8 comment lines for User's Manual>	строки, начинающиеся с символов "!!!", содержат описание или комментарии к событию
SEVERITY	уровень важности протоколируемых событий.
INDEX	индекс сообщения, содержащий <module index> = 0001 | 0002 | 0003 | 0010 | 0020 | 0029 | 0032 | 005B | 0065 | 006F | 0072 | 0073 | 007F | 0079 | 0309 | 1000 | 0820..0820 | 0850..085C и <MSG_ID subindex> = 0001..ffff
TMPL	шаблон сообщения
NONBLOCKABLE	опциональный атрибут, установка которого в “TRUE” гарантирует вывод сообщения при любых изменениях уровней важности (LogLevel) протоколируемых событий и изменениях параметров используемого syslog сервера. Т.е., если значение равно “TRUE”, то вывод сообщения не зависит от установленного общего уровня протоколирования. Значение по умолчанию – “FALSE”, т.е. вывод сообщения подчиняется общему установленному уровню аудита.

Примечание: Атрибут NONBLOCKABLE имеет значение TRUE лишь для групп событий, имеющих ID с 08530001 до 0853000A (раздел Installer for Unix) и с 00020001 до 00020005 (раздел Log), согласно Таблица 4. При этом, изменение его на FALSE для событий из раздела Installer for Unix невозможно.

Пример отображения информации о протоколируемом событии в файле s_log.ini:

```
[MSG_ID_LOG_SET_PARTICULAR_LOGLEVELS]
!!! Нефильтруемое сообщение об установке частных уровней логирования
некоторым сообщениям.
!!! Выдается при каждом их изменении и в начале сессии VPN Сервиса.
SEVERITY= INFO
INDEX   = 0x00020003
TMPL    = Some particular log levels are set
NONBLOCKABLE = TRUE
```

Пример редактирования файла s_log.ini:

Например, для изменения уровня протоколирования сообщения, имеющего ID 0029000E, с INFO на DEBUG, необходимо открыть текстовый файл `/opt/VPNagent/etc/s_log.ini` и найти раздел со строкой:

```
INDEX = 0x0029000E
```

В данном разделе нужно изменить значение атрибута SEVERITY на необходимое:

```
SEVERITY = DEBUG
```

Также, если для данного сообщения значение атрибута NONBLOCKABLE равно TRUE, то необходимо выставить его в FALSE:

```
NONBLOCKABLE = FALSE
```

После сохранения файла `s_log.ini` необходимо пересчитать его контрольную сумму, используя утилиту `integr_mgr calc`:

```
integr_mgr calc –f /opt/VPNagent/etc/s_log.ini
```

Перезапустите vpn-демон и log-сервис, последовательно выполнив команды:

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



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

Полный список сообщений, настройка протоколирования которых происходит только путем изменения файла `s_log.ini`, представлен в таблице 1:

Таблица 1

MSG ID	Текстовое представление	Раздел	Уровень
00290001	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_STATS_TRAIL	Firewall	INFO
00290002	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT	Firewall	WARNING
00290003	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT_OFF	Firewall	WARNING
00290004	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_PRIV_PORT	Firewall	WARNING
00290005	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PASV_PRIV_PORT	Firewall	WARNING
00290006	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_NOTAUTH	Firewall	WARNING
00290007	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PASV_NOTAUTH	Firewall	WARNING
00290008	MSG_ID_ON_IPSM_LOG_OTHERS	Firewall	DEBUG
00290009	MSG_ID_KLOGLIB_INIT_NO_MEMORY	Firewall	DEBUG
0029000A	MSG_ID_KLOGLIB_INIT_CANT_ATTACH	Firewall	DEBUG
0029000B	MSG_ID_KLOGLIB_INIT_CANT_SET_FILTER	Firewall	DEBUG
0029000C	MSG_ID_KLOGLIB_INIT_MISSED_ALERT_PACKETS	Firewall	WARNING
0029000D	MSG_ID_KLOGLIB_INIT_MISSED_PACKETS	Firewall	WARNING
0029000E	MSG_ID_KLOGLIB_INIT_PRINT_SUMMARY	Firewall	INFO
03090202	MSG_ID_LOGSRV_SET_SETTINGS_FAIL	<MAIN_APPLICATION>	WARNING
03090203	MSG_ID_LOGSRV_START	<MAIN_APPLICATION>	INFO
03090204	MSG_ID_LOGSRV_STOP	<MAIN_APPLICATION>	INFO

log_mgr show

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

Синтаксис

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

`-T timeout`	время ожидания ответа от vpnsvc сервиса. Допустимые значения – 10..36000 секунд, 0 – бесконечное время ожидания. Значение по умолчанию – 60 секунд
`–e msg_group_file.ini`	имя файла `msg_group_file.ini`, в котором указана группа событий и уровень протоколирования для них
`show-syslog`	вывод настроек syslog-клиента.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

   ```
   log_mgr show
   ```

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

   ```
   log_mgr show -e
   ```

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

   ```
   log_mgr show –e msg_group_file.ini
   ```

4. Для вывода настроек syslog-клиента используйте команду:

   ```
   log_mgr show-syslog
   ```

Пример

Пример выполнения команды `log_mgr show`:

```
log_mgr show-syslog
syslog parameters: enabled, server_ip=127.0.0.1, facility=local7
log_mgr show –e /opt/VPNagent/etc/msg_grpLDAP.ini
[LEVEL.DEBUG]
MSG_ID_LDAP_REQ_NOT_FOUND
MSG_ID_LDAP_CREATE_REQ_FAILED
MSG_ID_LDAP_PARSE_FAILED
MSG_ID_LDAP_REQ_FAILED_TIMEOUT
MSG_ID_LDAP_REQ_FAILED_NOT_RESPOND
MSG_ID_LDAP_REQ_FAILED_CANCELED
MSG_ID_LDAP_REQ_FAILED_CONNECTION_CLOSED
MSG_ID_LDAP_REQ_FAILED_UNKNOWN
MSG_ID_LDAP_REQ_SUCCESS
MSG_ID_LDAP_REQ_START
```


Cisco-like конфигурация

При старте cs_console настройки Syslog-клиента зачитываются из файла ***syslog.ini***, созданного для сервиса vpnsvc. Изменить настройки Syslog-клиента для консоли можно с использованием следующих команд:

logging on – включение протоколирования событий

logging – задание IP-адреса хоста, на который будут направляться сообщения

logging facility – задание источника сообщений

logging trap – задание текущего уровня важности для всех событий.

Все эти настройки записываются в файл ***/opt/VPNagent/etc/syslog.ini***.

Если данные команды не заданы, то зачитываются настройки из файла syslog.ini.

Настройки по умолчанию для данных команд вступают в действие при задании команд:

```
no logging
no logging facility
no logging trap
```

что эквивалентно настройкам:

```
logging 127.0.0.1
logging facility lopcal7
logging trap informational
```

Подробнее см. описание в разделе «Команды настройки протоколирования событий» документа «Cisco-like команды» (Console_command_reference.pdf).

Файл syslog.ini

Настройки Syslog-клиента будут записываться в файл ***syslog.ini***, поэтому этот файл вручную не редактируется.

Файл ***syslog.ini*** расположен в каталоге ***/opt/VPNagent/etc***. В этом файле задаются только IP-адрес получателя сообщений и источник сообщений. Файл ***syslog.ini*** имеет поля:

- `Enable` (тип boolean) – включение/отключение протоколирования (начальное значение 1):

  0 – протоколирование отключено

  1 – протоколирование включено

- `Destination` (тип IP-address[1]) – IP-адрес получателя сообщений (начальное значение 127.0.0.1)
- `Facility` – источник сообщений (начальное значение: local7). Допустимы следующие значения: kern, user, mail, daemon, auth, syslog, lpr, news, uucp, cron, authpriv, ftp, ntp, audit, alert, cron2, local0, local1, ..., local7.

Для удобства предлагается таблица 2 соответствия значения поля ***Facility*** в файле ***syslog.ini***, числового кода facility протокола Syslog, а также обозначений Facility в иных нотациях:

[1] Для текущей версии поддерживается отсылка протоколируемых сообщений только на один хост.

Таблица 2

Значение Facility в файле syslog.ini	Числовой код протокола Syslog[2]	define из стандартного файла syslog.h	Значение в Cisco-like команде logging facility
kern	0 << 3	LOG_KERN	kern
user	1 << 3	LOG_USER	user
mail	2 << 3	LOG_MAIL	mail
daemon	3 << 3	LOG_DAEMON	daemon
auth	4 << 3	LOG_AUTH	auth
syslog	5 << 3	LOG_SYSLOG	syslog
lpr	6 << 3	LOG_LPR	lpr
news	7 << 3	LOG_NEWS	news
uucp	8 << 3	LOG_UUCP	uucp
cron	9 << 3	LOG_CRON	sys9
authpriv	10 << 3	LOG_AUTHPRIV	sys10
ftp	11 << 3	LOG_FTP	sys11
ntp	12 << 3		sys12
audit	13 << 3		sys13
alert	14 << 3		sys14
cron2	15 << 3		cron
local0	16 << 3	LOG_LOCAL0	local0
local1	17 << 3	LOG_LOCAL1	local1
local2	18 << 3	LOG_LOCAL2	local2
local3	19 << 3	LOG_LOCAL3	local3
local4	20 << 3	LOG_LOCAL4	local4
local5	21 << 3	LOG_LOCAL5	local5
local6	22 << 3	LOG_LOCAL6	local6
local7	23 << 3	LOG_LOCAL7	local7

Настройка локального Syslog-сервера

Локальный Syslog-сервер уже сконфигурирован при подготовке операционной системы к инициализации Продукта следующим образом:

- лог всех уровней важности от источника ***local7*** направляется в файл ***/var/log/cspvpngate.log***
- лог уровня важности ***err и выше*** дополнительно направляется в консоль и файл ***/var/log/error.log***
- Syslog-сервер запускается автоматически при каждом старте ОС с включенной возможностью приёма сообщений по UDP порту 514

[2] << – обозначение операции битового сдвига влево

- при старте ОС, из скрипта ***(/etc/init.d/start_logwatch)*** запускается программа ***logwatch***, которая контролирует размер файла лога. Максимально допустимый размер файла установлен в ***1024 килобайта***. Проверка размера проводится каждые 10 секунд.

  При превышении допустимого размера текущий файл лога сохраняется с суффиксом ***".1"*** после того, как у ранее сохранённых файлов суффиксы меняются с ***".<n>"*** на ***".<n+1>"***. Всего дополнительно к текущему файлу лога сохраняется 2 экземпляра заполненных файлов лога (***cspvpngate.log.1, cspvpngate.log.2***). Если <n+1> больше количества сохраняемых экземпляров, файл с суффиксом ***".<n>"*** удаляется. После переименования файлов Syslog-серверу посылается сигнал SIGHUP для перехода на свежий файл лога.

- программа ***logwatch*** останавливается при остановке системы из скрипта ***/etc/init.d/start_logwatch***.

Перемещать или удалять файл ***start_logwatch*** не следует.

Специальные лог-файлы

В специальные лог-файлы, указанные в таблице 3, производится дополнительно протоколирование некоторых нештатных ситуаций работы Продукта. В эти файлы записывается информация, которая может помочь решить возникшую проблему.

Таблица 3

Имя файла	Путь к файлу	Содержание файла
cspvpn_verify_err.log	/opt/VPNagent/etc	Ошибки утилиты cspvpn_verify для проверки целостности неизменяемых и исполняемых файлов.
cp.log	/tmp	Сообщения криптоподсистемы уровня приложений
failh.log	/tmp	Аварийные события, не связанные с работой vpnsvc и lsp_mgr
error.log	/tmp/vpnsvc	Аварийные события, связанные с работой vpnsvc
error.log	/tmp/vpnlogsvc	Аварийные события, связанные с работой vpnlogsvc
error.log	/tmp/lsp_mgr	Аварийные события, связанные с работой утилиты lsp_mgr
non_cscons.lsp	/var/cspvpn/non_cscons.lsp	Копия LSP, написанной в виде текстового файла и загруженной командой lsp_mgr load (но после этого LSP еще была отредактирована в cs_console и сконвертирована)
erroneous_lsp.txt	/var/cspvpn/erroneous_lsp.txt	Сконвертированная LSP, которую не удалось загрузить

Например,

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

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

   где

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

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

   Пример

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

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

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

   ```
   vpnsvc: forceServiceFini
   ```

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

   ```
   vpnlogsvc: forceServiceFini
   ```

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

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

   или

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

   где

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

   `'%{2}s'` – указание на проблемный файл

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

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

   Пример файла “`/tmp/vpnlogsvc/error.log`” (записан из сервиса vpnlogsvc):

   ```
   1305822677 s_ini FatalError: the integrity check of the "/opt/VPNagent/etc/syslog.ini" failed
   ```

Получение лога в Windows

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

Список протоколируемых событий

Строка протоколируемого события формируется из соответствующего описания сообщения, задаваемого во внешнем текстовом файле ***/opt/VPNagent/etc/s_log.ini***. Каждому протоколируемому событию присвоен фиксированный идентификатор (MSG ID), текстовое представление, уровень важности.

Уровни важности (Severity) протоколируемых событий соответствуют уровням Severity для протокола Syslog: EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, DEBUG.

Выдаваемые сообщения и описание событий по этим сообщениям представлены в Таблица 4.

Ведется также протоколирование ошибок криптографической подсистемы, список которых представлен в Таблица 8. Эти ошибки доводятся до сведения пользователя также через Syslog, используя источник сообщений (Facility) `kern`.

Список сообщений об ошибках подсистемы Reverse Route Injection (RRI) приведен в Таблица 9.

Таблица 4

MSG ID	Текстовое представление	Раздел	Уровень	Шаблон сообщения	Описание события
03090001	MSG_ID_PRODUCT_START	<MAIN_APPLICATION>	NOTICE	Service started, version %{1}s	Старт сервиса
03090002	MSG_ID_PRODUCT_STOP	<MAIN_APPLICATION>	NOTICE	Service stopped	Остановка сервиса
03090003	MSG_ID_LOG_SUSPEND_SYSTEM	<MAIN_APPLICATION>	INFO	OS is going to the Suspend or Hibernation mode	Операционная Система переходит в режим сна или гибернации (Suspend or Hibernation)
03090004	MSG_ID_LOG_RESUME_SYSTEM	<MAIN_APPLICATION>	INFO	OS resumed from the Suspend or Hibernation mode %{1}u sec ago	Операционная Система вышла из режима сна или гибернации (Suspend or Hibernation) %(1}s - Время, потраченное сервисом на ожидание восстановления доступности сетевых интерфейсов
03090202	MSG_ID_LOGSRV_SET_SETTINGS_FAIL	<MAIN_APPLICATION>	WARNING	Failed to set VPN log service settings	Неудача изменения параметров установок LOG-сервиса. Возможно, серис не запущен.
03090203	MSG_ID_LOGSRV_START	<MAIN_APPLICATION>	INFO	VPN log service started, version %{1}s	Старт LOG-сервиса
03090204	MSG_ID_LOGSRV_STOP	<MAIN_APPLICATION>	INFO	VPN log service stopped	Остановка LOG-сервиса
005B0001	MSG_ID_EVENT_MGR_PROFILER_QUEUE	Event Manager	INFO	Event Manager profiler: waiting time of task queue is %{1}s sec, queue length is %{2}s tasks	сообщение профайлера менеджера событий сервиса о статистике по очереди событий
005B0002	MSG_ID_EVENT_MGR_PROFILER_TASK	Event Manager	WARNING	Event Manager profiler: task time is %{1}s sec (src=%{2}s dst=%{3}s idx=%{4}s proc=%{5}s)	сообщение профайлера менеджера событий сервиса о чрезмерно долгом времени обработки события

08200001	MSG_ID_ARPM_ERR_WRITE_PARP_FILE	<ARPM>	WARNING	Could not write ProxyARP table in file "%{1}s"	ошибка записи служебного файла протоколирования изменений таблицы Proxy ARP
08200002	MSG_ID_ARPM_ERR_READ_PARP_FILE	<ARPM>	WARNING	Could not read ProxyARP table from file "%{1}s"	ошибка чтения служебного файла протоколирования изменений таблицы Proxy ARP
08200003	MSG_ID_ARPM_IP_ADDED_TO_SYSTEM_PARP	<ARPM>	DEBUG	IP %{1}s%[added to ProxyARP table(s) of "%{10}s";%]%[was not added to ProxyARP table(s) of "%{11}s";%]	Добавление или обновление IP адреса в Proxy ARP таблицы сетевых интерфейсов %(1}s - добавляемый IP адрес %{10}s - список интерфейсов, к которым IP добавлен успешно %{11}s - список интерфейсов, к которым следовало добавить IP, но не удалось
08200004	MSG_ID_ARPM_IP_DELETED_FROM_SYSTEM_PARP	<ARPM>	DEBUG	IP %{1}s%[deleted from ProxyARP table(s) of "%{10}s";%]%[was not deleted from ProxyARP table(s) of "%{11}s";%]	Удаление IP адреса из Proxy ARP таблиц сетевых интерфейсов %(1}s - удаляемый IP адрес %{10}s - список интерфейсов, из которым IP удален успешно %{11}s - список интерфейсов, из которых IP удалить не удалось. Возможно, он был удален ранее
08200005	MSG_ID_ARPM_REFRESH_SYSTEM_PARP	<ARPM>	INFO	In the ProxyARP table(s) of "%{11}s" interface(s) %{2}u IP(s) was(were) not refreshed	Пересоздание Proxy ARP таблиц сетевых интерфейсов. Может происходить при перезагрузке LSP %{11}s - список интерфейсов, к которым следовало добавить IP, но не удалось

00014001	MSG_ID_SNMP_TRAP_RECEIVER_ADD_FAILED	Statistics & SNMP	WARNING	[SNMP] failed to configure SNMP trap receiver %{1}s%[:%{2}u%], community "%{3}s"%[, interface "%{4}s"%]%[, local address %{5}s%]	Не удалось добавить получателя SNMP traps (структура LSP TrapReceiver) %{1} - IP-адрес получателя %{2} - порт получателя %{3} - SNMP trap community %{4} - логическое имя сетевого интерфейса %{5} - локальный IP-адрес
00014002	MSG_ID_SNMP_POLLING_SETUP_LOCAL_ADDR_FAILED	Statistics & SNMP	WARNING	[SNMP] failed to configure SNMP polling agent on address(es) %{1}s%[(port %{2}u)%]	Не удалось настроить прием SNMP-запросов в соответствии со структурой LSP SNMPPollSettings на определенном локальном IP-адресе {1} - локальный IP-адрес {2} - локальный порт
--------	--------	--------	--------	--------	Общие параметры для сообщений: %{8}s IP-адрес партнёра по IKE обмену. %{9}u IP-порт партнёра по IKE обмену. Если не указан, то порт стандартный (500) %{10}s Значение IKE идентификатора для аутентификации партнёра. %{15}u Порог ограничения ресурса %{20}s Причина возникновения события %{32}s Идентификатор сессии IKE обмена. Формат - "<n:m>", где n - номер защищающего ISAKMP соединения, m - номер обмена, защищаемого данным ISAKMP соединением %{40}u Номер ISAKMP соединения
00101011	MSG_ID_LP_ISAKMP_PROPOSALS_SEND	LP	DEBUG	%[%{32}s %]Sending ISAKMP proposals:	Партнёру отсылаются наборы криптопараметров устанавливаемого ISAKMP соединения

00101012	MSG_ID_LP_ISAKMP_PROPOSALS_RECV	LP	DEBUG	%[%{32}s %]Received ISAKMP proposals:	От партнёра получены наборы криптопараметров устанавливаемого ISAKMP соединения
00101013	MSG_ID_LP_ISAKMP_TRANSFORM	LP	DEBUG	%[%{32}s %] Transform #%{1}u: %{2}s	Описание варианта криптопараметров устанавливаемого ISAKMP соединения
00101021	MSG_ID_LP_IPSEC_PROPOSALS_SEND	LP	DEBUG	%[%{32}s %]Sending IPSec proposals:	Партнёру отсылаются наборы криптопараметров устанавливаемого IPSec соединения
00101022	MSG_ID_LP_IPSEC_PROPOSALS_RECV	LP	DEBUG	%[%{32}s %]Received IPSec proposals:	От партнёра получены варианты наборов криптопараметров для устанавливаемого IPSec соединения
00101023	MSG_ID_LP_IPSEC_PROPOSAL	LP	DEBUG	%[%{32}s %] Proposal #%{1}u:	Описание варианта набора криптопараметров устанавливаемого IPSec соединения
00101024	MSG_ID_LP_IPSEC_PROTO	LP	DEBUG	%[%{32}s %] Protocol %{1}s:	Описание вариантов криптопараметров для указанного протокола
00101025	MSG_ID_LP_IPSEC_TRANSFORM	LP	DEBUG	%[%{32}s %] Transform #%{1}u: %{2}s	Описание варианта криптопараметров устанавливаемого IPSec соединения

00101031	MSG_ID_LP_CHECK_PROPOSAL	LP	DEBUG	%[%{32}s %]Checking %[Proposal #%{1}u, Protocol %{2}s, %]Transform #%{3}u for Rule "%{4}s", %[Proposal #%{5}u, Protocol %{6}s, %]Transform #%{7}u: %{8}s %{9}s	Проверка каждого из присланных вариантов наборов криптопараметров на соответствие локальному IKE/IPSec правилу. %{1}u номер присланного варианта набора криптопараметров (для IPSec) %{2}s протокол присланного набора криптопараметров (для IPSec) - ESP либо AH %{3}u номер присланного варианта криптопараметров %{4}s имя локального IKE/IPSec правила %{5}u номер локального варианта набора криптопараметров (для IPSec) %{6}s протокол локального набора криптопараметров (для IPSec) - ESP либо AH %{7}u номер локального варианта криптопараметров %{8}s %{9}s результат проверки
00101032	MSG_ID_LP_CHECK_PROPOSAL_SHORT	LP	DEBUG	%[%{32}s %]Checking proposal #%{1}u for Rule "%{4}s", Proposal #%{5}u: %{8}s %{9}s	Проверка набора криптопараметров на соответствие локальному IPSec правилу. %{1}u номер присланного варианта набора криптопараметров %{4}s имя локального IKE правила %{5}u номер локального варианта набора криптопараметров %{8}s %{9}s результат проверки
00101034	MSG_ID_LP_IKE_RULE_NOT_FOUND	LP	INFO	%[%{32}s %]Unable to choose authentication rule	Невозможно подобрать IKE правило для аутентификации партнёра
00101035	MSG_ID_LP_CHOOSE_IKE_RULE_BY_IP	LP	INFO	%[%{32}s %]Unable to find IKE rule by remote id. Using IP-address as partner's id.	Для присланного ID первой фазы IKE не найдено подходящего IKE правила. В качестве идентификатора будет использован IP-адрес партнёра.

00101036	MSG_ID_LP_USE_PRESHARED_KEY	LP	DEBUG	%[%{32}s %]Using preshared key "%{1}s"	Выбран предопределённый ключ для аутентификации %{1}s идентификатор ключа
00101037	MSG_ID_LP_KEY_ABSENT	LP	WARNING	%[%{32}s %]Preshared key "%{1}s" not found, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Не найден предопределённый ключ для аутентификации %{1}u идентификатор ключа
00101038	MSG_ID_LP_IP_DOESNT_MATCH	LP	INFO	%[%{32}s %]IKERule "%{1}s": IP address is not in %{2}s list, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	IKE правило не подходит из-за того, что IP адрес отсутствует в списке разрешенных (IKEPeerIPFilter или IKELocalIPFilter) %{1}s имя локального IKE правила %{2}s IKEPeerIPFilter или IKELocalIPFilter
00100101	MSG_ID_LP_IKECFGIF_ASSIGNED_IP	LP	INFO	%[%{32}s %]Address %{1}s assigned to IKECFG network interface, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Активирован ikecfg-интерфейс с адресом %{1}
00100105	MSG_ID_LP_IKECFGIF_DNS_ADDR_SET	LP	INFO	%[%{32}s %]DNS address(es) %{1}s configured on IKECFG network interface, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Адрес или адреса DNS-серверов получены от партнера и добавлены в системный список. %{1}s - список адресов
00100106	MSG_ID_LP_IKECFGIF_DNS_ADDR_ERROR	LP	WARNING	%[%{32}s %]Failed to configure DNS address(es) %{1}s on IKECFG network interface, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Ошибка при добавлении адресов DNS-серверов в системный список %{1}s - список адресов

00100107	MSG_ID_LP_IKECFGIF_DNS_SUFFIXES_SET	LP	INFO	%[%{32}s %]DNS suffix(es) %{1}s added to the system, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	DNS-суффиксы получены от партнера и добавлены в системный список %{1}s - список суффиксов
00100108	MSG_ID_LP_IKECFGIF_DNS_SUFFIXES_ERROR	LP	WARNING	%[%{32}s %]Failed to add DNS suffix(es) %{1}s to the system, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Ошибка при добавлении DNS-суффиксов в системный список %{1}s - список суффиксов
00100102	MSG_ID_LP_IKECFGIF_BAD_IP	LP	WARNING	%[%{32}s %]IKECFG address %{1}s can't be used in current network configuration. Attempting to get another address. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Присланный по IKECFG IP-адрес конфликтует с существующими в системе адресами или правилами роутинга. %{1}s - полученный адрес
00100103	MSG_ID_LP_IKECFGIF_BAD_PH2ID	LP	ERR	%[%{32}s %]Incorrect IKE traffic request %{1}s for IKECFG interface. Subnet expected. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Присланный во второй фазе IKE ID (селектор SA) не подходит для IKECFG-интерфейса, т.к. содержит протоколы или не является описанем подсети. %{1}s - присланный ID
00100104	MSG_ID_LP_IKECFGIF_RULE_NOT_PERSISTENT	LP	ERR	%[%{32}s %]IKECFG is not supported for non persistent connection, IKERule "%{1}s", peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Работа IKECFG по IPsecAction запрещена т.к. он не имеет флага PersistentConnection. %{1}s - имя IKERule, присоединенного к IPsecAction без флага PersistentConnection

00100111	MSG_ID_LP_VIF_NO_PHY	LP	WARNING	[CFG] no physical interface found for NetworkInterface "%{1}s" pattern "%{2}s"	При загрузке конфигурации не найдено ни одного сетевого интерфейса, соответствующего описанию NetworkInterface. %{1}s - LogicalName этого NetworkInterface %{2}s - шаблон имени, найденный по LogicalName
00100201	MSG_ID_IKECFGIF_SETUP_FAILED	LP	CRIT	[IKECFGIF] can't setup IKECFG interface: see failh log	Ошибка при конфигурации виртуального интерфейса IKECFG. Подробности описаны в файле %TEMP%/vpnsvc/error.log, который необходимо передать разработчикам.
00100202	MSG_ID_IKECFGIF_DIFFERENT_IP	LP	WARNING	[IKECFGIF] changing address of IKECFG interface from %{1}s to %{2}s	Возникла необходимость смены адреса, отключения или изменения состояния IKECFG-интерфейса. Вероятно, изменилась конфигурация IKE-партнера, или адрес IKECFG был занят кем-то другим. Производится перезагрузка конфигурации. %{1} - старый адрес %{2} - новый адрес
00100203	MSG_ID_IKECFGIF_ADD_ROUTE_FAILED	LP	WARNING	[IKECFGIF] can't setup IKECFG interface: can't create route %{1}s/%{2}s via %{3}s: %{4}s	Ошибка создания маршрута в системной таблице роутинга при конфигурации IKECFG-интерфейса {1} - подсеть назначения {2} - маска подсети {3} - gateway {4} - расшифровка ошибки
00100205	MSG_ID_LP_IKECFG_REFUSED_BY_SERVER	LP	WARNING	%[%{32}s %]IKECFG address request rejected by server, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	На запрос адреса по IKECFG IKE партнер ответил отказом.

00100206	MSG_ID_LP_IKECFG_RADIUS_IGNORED	LP	NOTICE	%[%{32}s %]Framed IP address from RADIUS server will be ignored. Using local IKECFG data instead. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Присланный RADIUS-сервером Framed IP address для партнёра не будет использован, так как в LSP задано использование локального IKECFG пула.
00100207	MSG_ID_IKECFGIF_WIN_ENABLE_ROUTER_FAILED	LP	WARNING	[IKECFGIF] can't enable packet forwarding	Не удалось включить пересылку пакетов между сетевыми интерфейсами. Возможно, данная функциональность заблокирована антивирусными приложениями.
00100112	MSG_ID_LP_CONFIGURATION_LOADED	LP	NOTICE	[CFG] %{2}s configuration loaded via %{1}s%[, title "%{4}s"%]	Конфигурация успешно загружена. %{1} - источник конфигурации (cs_console, command line, token и т.п.) %{2} - тип конфигурации (driver default, DHCP only, user-defined) %{4} - название из конфигруации (GlobalParameters.Title)
00100113	MSG_ID_LP_CONFIGURATION_PARTIALLY_LOADED	LP	WARNING	[CFG] %{2}s configuration loaded via %{1}s%[, title "%{4}s"%], %{6}u potential problem(s) found%[: %{5}s%]	Конфигурация успешно загружена, но есть предупреждения, которые направлены в лог. %{1} - источник конфигурации (cs_console, command line, token и т.п.) %{2} - тип конфигурации (driver default, DHCP only, user-defined) %{4} - название из конфигруации (GlobalParameters.Title) %{5} - текст предупреждения %{6} - количество предупреждений
00100114	MSG_ID_LP_CONFIGURATION_LOAD_FAILURE	LP	ERR	[CFG] error in configuration from "%{1}s": %{3}s	Ошибка разбора конфигруации %{1} - источник конфигурации (cs_console, command line, token и т.п.) %{3} - описание ошибки

00100115	MSG_ID_LP_CONNECTION_REQUEST	LP	INFO	[IPSEC] connection request #%{1}u, packet %{2}s,%[Filter "%{3}s", %]IPsecAction "%{4}s"	Начало создания IPsec-соединения (обработка bundle request). %{1} - номер запроса %{2} - селектор пакета из запроса %{3} - имя Filter %{4} - имя IPsecAction
00100116	MSG_ID_LP_CONNECTION_REQUEST_INI_FAILED	LP	ERR	[IPSEC] connection request #%{1}u failed,%[Filter "%{2}s", %]packet %{3}s: %{4}s	Ошибка на начальной стадии создания IPsec-соединения (обработка bundle request). %{1} - номер запроса %{2} - селектор пакета из запроса %{3} - описание ошибки
00100117	MSG_ID_LP_CONFIGURATION_SAVE_FAILED	LP	CRIT	[CFG] can't save configuration in db: error "%{1}d"	Ошибка сохранения конфигурации в базе данных продукта. %{1} - код ошибки, который можно передать в службу поддержки для расшифровки
00100119	MSG_ID_LP_HOST_CONNECTED	LP	NOTICE	%[%{32}s %]IPSec connection %{1}u established, traffic selector %{2}s, peer %{8}s%[:%{9}u%], id "%{10}s"%[, Filter %{3}s%], IPsecAction %{4}s, IKERule %{5}s	Создано IPsec-соединения (IKE Quick Mode завершилась успешно). %{1} - номер созданного IPsec-соединения %{2} - IKE traffic request/phase 2id/селектор IPsec SA %{3} - название фильтра %{4} - имя IPsec-правила %{5} - имя IKE-правила

0010011A	MSG_ID_LP_CONNECTION_REQUEST_FAILURE	LP	ERR	%[%{32}s %]IPSec connection request #%{6}u failed%[: %{1}s%]%[: %{2}s%]. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]%[, Filter %{3}s%]%[, IPsecAction %{4}s%]%[, IKERule %{5}s%]	Попытка создания IPsec SA закончилась неудачей. %{1} - стадия ike, где обнаружена ошибка %{2} - причина ошибки %{3} - название фильтра %{4} - имя IPsec-правила %{5} - имя IKE-правила %{6} - порядковый номер запроса на создание IPsec-соединения
0010011B	MSG_ID_LP_CONNECTION_REKEYING_FAILURE	LP	WARNING	%[%{32}s %]Re-keying of IPSec connection %{6}u failed%[: %{1}s%]%[: %{2}s%]. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]%[, Filter %{3}s%]%[, IPsecAction %{4}s%]%[, IKERule %{5}s%]	Попытка пересоздания IPsec SA закончилась неудачей. %{1} - стадия ike, где обнаружена ошибка %{2} - причина ошибки %{3} - название фильтра %{4} - имя IPsec-правила %{5} - имя IKE-правила %{6} - номер IPsec-соединения, которое пытались обновить
0010011C	MSG_ID_LP_INCOMING_CONNECTION_FAILURE	LP	ERR	%[%{32}s %]Incoming connection failed%[: %{1}s%]%[: %{2}s%]. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]%[, Filter %{3}s%]%[, IPsecAction %{4}s%]%[, IKERule %{5}s%]	Обмен IKE, где мы выступаем в качестве респондера, закончился неудачей. %{1} - стадия ike, где обнаружена ошибка %{2} - причина ошибки %{3} - название фильтра %{4} - имя IPsec-правила %{5} - имя IKE-правила
0010011D	MSG_ID_LP_CONNECTION_CLOSED	LP	NOTICE	IPSec connection %{1}u closed: %{3}u bytes sent, %{4}u received: %{2}s%[, matched by license number %{5}u%]	IPsec SA удалены. %{1} - идентификатор IPsec-соединения %{2} - причина удаления SA %{3} - байтов отправлено %{4} - байтов принято

0010011E	MSG_ID_LP_STALE_CONNECTION_BY_LICENSE	LP	WARNING	%[%{32}s %]Stale IPSec connection %{1}u detected with peer %{18}s%[:%{19}u%], id "%{20}s", license number: %{2}s: while processing initial contact from peer %{8}s%[:%{9}u%], id "%{10}s"	По уникальному номеру лицензии партнёра обнаружен старое, неиспользуемое IPSec соединение %{1} - идентификатор старого IPsec-соединения %{2} - номер лицензии партнёра. %{18} - IP-адрес партнёра по IKE обмену для старого соединения. %{19} - IP-порт партнёра по IKE обмену для старого соединения. Если не указан, то порт стандартный (500) %{20} - Значение IKE идентификатора для аутентификации партнёра для старого соединения.
00100124	MSG_ID_LP_LICENSE_CHECKED	LP	INFO	Product license info: product code %{1}s, license number %{2}u	Проверка лицензии прошла успешно %{1} - тип продукта в лицензии %{2} - номер лицензии
00100125	MSG_ID_LP_NO_LICENSE	LP	ALERT	Product license info: no license	Файл лицензии отсутствует или в нем неправильные данные. Продукт будет работать с ограничениями до ввода лицензии и рестарта.
00100129	MSG_ID_LP_SNMP_TRAP_RECV_NO_IP	LP	WARNING	[SNMP] failed to configure SNMP trap destination %{1}s: no IP address found for network interface "%{2}s"	Не удалось найти адрес для сетевого интерфейса, который указан в качестве источника SNMP trap %{1} - адрес получателя SNMP trap %{2} - логическое имя сетевого интерфейса

0010012C	MSG_ID_LP_ID_CONFLICT	LP	WARNING	%[%{32}s %]Traffic request overlaps with other IPsec SA created for peer %{1}s:%{2}d, conflicting address range: %{5}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Селектор создаваемого SA пересекается с селектором ранее созданного SA для одного фильтра. Это признак несогласованности конфигураций парнера, может привести к удалению IPsec-пакетов при обработке из-за несоответствия политике безопасности. Данное сообщение является предупреждением о возможных проблемах и не прерывает процесс создания SA. %{1} - IP адрес партнера, создавшего SA, с которым конфликтует вновь создаваемый %{2} - порт этого партнера
00100130	MSG_ID_LP_SAME_AUTH_METHOD_SPEC	LP	WARNING	[CFG] IKERule "%{2}s", line %{3}d: %{1}s has multiple authentication methods with the same type, only first of them will be used.	Предупреждение возникает, если при загрузке конфигурации обнаружено, что в IKERule присутствует несколько методов аутентификации одного типа. Респондер будет использовать только первый вариант из двух однотипных методов. %{1} - список, где встречен повтор (AggrModeAuthMethod/MainModeAuthMethod) %{2} - имя ike-правила %{3} - номер строки, где это правило описано
00100138	MSG_ID_LP_AGENT_INI_CP_CONTEXTS_PER_SA_INVALID	LP	WARNING	DefaultCryptoContextsPerIPSecSA in "agent.ini" is not valid (should be 1..128), %{1}d will be used instead.	При чтении ini-файла обнаружено неправильное значение для DefaultCryptoContextsPerIPSecSA будет использовано значение по-умолчанию. %{1} - значение по-умолчанию

00100139	MSG_ID_LP_AM_USE_ONE_GROUP	LP	WARNING	[CFG] IKERule "%{2}s", line %{3}d: in Aggressive Mode initiator will use %{1}d only.	Предупреждение возникает, если при загрузке конфигурации обнаружено, что в IKERule затребован aggressive-режим для инициатора, но присутствуют трансформы с различными GroupID. Инициатором будет использоваться только указанный GroupID. %{1} - группа, которая будет использована инициатором %{2} - имя ike-правила %{3} - номер строки, где это правило описано
0010013D	MSG_ID_LP_OLD_SA_DIE_BEFORE_NEW	LP	WARNING	%[%{32}s %]Old IPSec SA had been killed before new IPSec SA was created during rekeying. Please report this to the product support. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	SA, для которого проводился rekeying был удален до загрузки вновь созданного SA. Просьба сообщить в службу поддержки о подобном поведении.
0010013E	MSG_ID_LP_DEL_ROUTE_FAILED	LP	WARNING	[ROUTE] can't delete route %{1}s/%{2}d via %{3}s: %{4}s	Ошибка удаления маршрута, описанного в LSP. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway или имя интерфейса %{4} - пояснение ошибки
0010013F	MSG_ID_LP_ADD_ROUTE_FAILED	LP	WARNING	[ROUTE] can't add route %{1}s/%{2}d via %{3}s: %{4}s	Ошибка добавления маршрута, описанного в LSP. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway или имя интерфейса %{4} - пояснение ошибки

00100140	MSG_ID_LP_IPSEC_HI_TTL_TRAFFIC	LP	WARNING	%[%{32}s %]SA traffic limit (%{1}d) exceeds limitations imposed by the cryptograghic algorithm, peer %{8}s%[:%{9}u%], id "%{10}s"	В созданном IPsec SA ограничение по трафику не соответствует допустимому ограничению для используемого криптографического алгоритма. %{1} - ограничение, которое будет использовано в созданном IPsec SA (0 - без ограничений)
00100151	MSG_ID_AUDIT_LOAD_NEW_LSP	LP	INFO	[CFG] new LSP (%{1}s line(s)) successfully loaded by "%{2}s" user via %{3}s%["%{6}s"%] process%[%{4}s using unrecognized connection%]%[using %{5}s remote connection%]	Конфигурация успешно загружена по инициативе пользователя посредством утилиты (cs_console, lsp_mgr). Предваряет построчную выдачу загруженной LSP по MSG_ID_AUDIT_SHOW_NEW_LSP. %{1} - количество строк в загруженной LSP. %{2} - имя пользователя, инициировавшего загрузку %{3} - PID процесса локальной утилиты, выполнившей запрос на загрузку LSP %{4} - вспомогательный аргумент %{5} - детали remote-connection ("Daemon(<IPs><ports>)") %{6} - имя утилиты, инициировавшей загрузку
00100152	MSG_ID_AUDIT_SHOW_NEW_LSP	LP	INFO	[CFG] new LSP, line %{1}u/%{2}u: %{3}s	Последовательно выдаются "as is" нумерованные строки загруженной LSP сразу после выдачи сообщения MSG_ID_AUDIT_LOAD_NEW_LSP %{1} - номер выдаваемой строки LSP %{2} - всего строк в LSP %{3} - строка LSP

08500001	MSG_ID_RRI_NOT_CREATED	RRI	WARNING	[RRI] %{1}s, route not created: destination %{2}s, traffic selector %{10}s%[..%{11}s%]%[:%{12}d%] - >%{13}s%[..%{14}d%]%[:%{15}d%]%[proto %{16}s%]	Ошибка формирования маршрута RRI. То есть проблема обнаружена до попытки добавить маршрут в системную таблицу. %{1} - пояснение ошибки %{2} - туннельный адрес %{10}-%{16} - селектор SA
08500002	MSG_ID_RRI_DEL_ROUTE_FAILED	RRI	WARNING	[RRI] can't delete route %{1}s/%{2}d via %{3}s: %{4}s	Ошибка удаления маршрута, созданного RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway %{4} - пояснение ошибки
08500003	MSG_ID_RRI_ADD_ROUTE_FAILED	RRI	WARNING	[RRI] can't add route %{1}s/%{2}d via %{3}s: %{4}s	Ошибка добавления маршрута RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway %{4} - пояснение ошибки
08500004	MSG_ID_RRI_UPDATED	RRI	INFO	[RRI] updated route to %{1}s/%{2}d: new gw %{3}s, old gw %{4}s	Обнавлен маршрут RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - новый gateway %{4} - предыдущий gateway
08500005	MSG_ID_RRI_CREATED	RRI	INFO	[RRI] created route %{1}s/%{2}d via %{3}s for destination %{4}s, traffic selector %{10}s%[..%{11}s%]%[:%{12}d%] - >%{13}s%[..%{14}d%]%[:%{15}d%]%[proto %{16}s%]	Создан маршрут RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway %{4} - туннельный адрес %{10}-%{16} - селектор SA

08500006	MSG_ID_RRI_REMOVED	RRI	INFO	[RRI] removed route %{1}s/%{2}d via %{3}s for destination %{4}s	Удален маршрут RRI. %{1} - подсеть назначения %{2} - маска подсети %{3} - gateway %{4} - туннельный адрес
10002001	MSG_ID_IKE_IKECFG_ASSIGNED	IKE	INFO	%[%{32}s %]IKECFG address %{1}s assigned to peer %{8}s%[:%{9}u%], id "%{10}s", %{2}s%[, dns server(s): %{11}s%[%{12}s%]%[%{13}s%]%[%{14}s%]%[%{15}s(...)%]%]%[, domain suffix(es): %{21}s%[%{22}s%]%[%{23}s%]%[%{24}s%]%[%{25}s(...)%]%]	Партнёру выдан внутренний адрес из IKECFG пула %{1} - выданный адрес %{2} - статус проксирования ARP-запросов: proxy ARP enabled - проксирование включено для всех интерфейсов с подсетями, включающими выданный адрес; partial proxy ARP - проксирование включено не для всех интерфейсов с подсетями, включающими выданный адрес; no proxy ARP - ARP-запросы не проксируются.
10002003	MSG_ID_IKE_IKECFG_REFUSED_BY_CLIENT	IKE	INFO	%[%{32}s %]IKECFG address rejected by partner. Assigning another address. Peer %{8}s%[:%{9}u%], id "%{10}s"	Партнёр отказался от ранее выданного адреса из IKECFG пула. Делается попытка выдать партёру другой адрес.
10002004	MSG_ID_IKE_IKECFG_POOL_CONFLICT	IKE	INFO	%[%{32}s %]IKECFG address %{1}s is already bound to another partner. Clearing old IKECFG data to resolve address conflict. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Выдаваемый партнёру внутренний адрес из IKECFG пула уже занят другим партнёром со сходными параметрами. Соединения со старым партнёром будут уничтожены.

00102005	MSG_ID_IKE_IKECFG_ADDRESS_ASSIGNMENT_FAILED	LP	INFO	%[%{32}s %]Cannot assign IKECFG address%[%{1}s%] to partner%[: %{2}s%], peer %{8}s%[:%{9}u%], id "%{10}s"	Ошибка при попытке выдачи внутреннего адреса партнёру. %{1}s - выбранный IKECFG адрес для партнёра (если есть) %{2}s - возможные причины: pool is not configured - пул не задан; pool is over - пул исчерпан; proxy ARP failed - ошибка задания проксирования ARP-запросов
10002006	MSG_ID_IKE_IKECFG_ADDRESS_INCOMPATIBLE	IKE	INFO	%[%{32}s %]IKECFG address %{1}s was previously bound to current partner. Clearing old IKECFG data to assign new address. Peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Ранее выданный партнёру внутренний адрес из IKECFG пула несовместим с текущей политикой безопасности, либо партнёр запросил другой IKECFG адрес. Имеющиеся соединения со старым партнёром будут уничтожены.
--------	--------	--------	--------	--------	Общие параметры для сообщений: %{8}s IP-адрес партнёра по IKE обмену. %{9}u IP-порт партнёра по IKE обмену. Если не указан, то порт стандартный (500) %{10}s Значение IKE идентификатора для аутентификации партнёра. %{15}u Порог ограничения ресурса %{20}s Причина возникновения события %{32}s Идентификатор сессии IKE обмена. Формат - "<n:m>", где n - номер защищающего ISAKMP соединения, m - номер обмена, защищаемого данным ISAKMP соединением %{40}u Номер ISAKMP соединения

10000001	MSG_ID_IKE_START_SESSION	IKE	DEBUG	%{32}s Start IKE session, Request: %{1}s, type %{2}s, peer %{8}s%[:%{9}u%]%[, sessionId %{4}s.%{5}s%]	Начат новый IKE обмен. %{1}s Причина, вызвавшая обмен %{2}s Тип обмена (Exchange Type по RFC2408) %{4}s Идентификатор обмена (Initiator Cookie по RFC2408) %{5}s Идентификатор обмена (Message ID по RFC2408)
10000002	MSG_ID_IKE_END_SESSION	IKE	DEBUG	%[%{32}s %]Session completed	IKE обмен завершён
10000003	MSG_ID_IKE_PARTNER_AGENT_INFO	IKE	DEBUG	%[%{32}s %]Partner's VPN Agent info: product:%{1}s%[, build:%{2}s.%{3}s.%{4}s%]%[, OS:%{5}s%]%[, CPU:%{6}s%]%[, features:%{7}s%]%[, product code:%{101}s%]%[, license number:%{103}s%]	Партнёр прислал информацию об используемом CSP VPN Агенте %{1}s Наименование продукта %{2}s Старший номер версии продукта %{3}s Младший номер версии продукта %{4}s Номер сборки продукта %{5}s Операционная система, для которой собран продукт %{6}s Платформа, для которой собран продукт %{7}s Дополнительные опции, включённые в сборку (если имеются) %{101}s Код продукта, указанный в лицензии %{103}s Номер лицензии
10000005	MSG_ID_IKE_SA_CREATED	IKE	INFO	%[%{32}s %]ISAKMP connection %{40}u created, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Создано ISAKMP соединение

10000006	MSG_ID_IKE_SA_CLOSED	IKE	INFO	ISAKMP connection %{40}u closed, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]%>INFO[, bytes sent/received: %{3}u/%{4}u, exchanges passed: %{5}u%]%[, Reason: %{20}s%]%[, matched by license number %{1}u%]	Уничтожено ISAKMP соединение
10000007	MSG_ID_IKE_ID_RECEIVED_FROM	IKE	DEBUG	%[%{32}s %]Receive identity "%{1}s", peer %{8}s%[:%{9}u%]	Партнёр прислал свою идентификационную информацию
10000008	MSG_ID_IKE_ID_SENT_TO	IKE	DEBUG	%[%{32}s %]Send identity "%{1}s", peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Партнёру отослана локальная идентификационная информация
10000009	MSG_ID_IKE_FLOAT_PARTNER	IKE	DEBUG	%[%{32}s %]Float partner to %{8}s%[:%{9}u%]	Изменение сетевых параметров партнёра
1000000A	MSG_ID_IKE_PH2_ID_SEND	IKE	DEBUG	%[%{32}s %]Send traffic request: %{1}s->%{2}s	Партнёру отосланы параметры защищаемого трафика создаваемого IPSec соединения
1000000B	MSG_ID_IKE_PH2_ID_RECV	IKE	DEBUG	%[%{32}s %]Receive traffic request: %{1}s->%{2}s	Партнёр прислал параметры защищаемого трафика создаваемого IPSec соединения
1000000C	MSG_ID_IKE_INITIATE_SESSIONS_LIMIT	IKE	WARNING	[ISAKMP] Exchange pended. Limit of %{15}u initiated sessions achieved. Request: %{1}s, peer %{8}s%[:%{9}u%]	IKE обмен отложен из-за ограниченности ресурсов. %{1}s Причина, вызвавшая отложенный обмен
1000000E	MSG_ID_IKE_ACCESS_RESTRICTED	IKE	INFO	[ISAKMP] Peer %{8}s%[:%{9}u%] has limit of %{15}u responding IKE-sessions. New session requests were rejected %{3}u times	IKE обмен отменён из-за ограничения активности для указанного партнёра. %{3}u Количество отменённых обменов, инициированных партнёром, с момента предыдущего вывода данного сообщения

1000000F	MSG_ID_IKE_ACCESS_DENIED	IKE	WARNING	[ISAKMP] Access denied for peer %{8}s%[:%{9}u%]. %{3}u IKE-packet(s) dropped	IKE трафик от указанного партнёра полностью игнорируется. %{3}u Количество сброшенных IKE пакетов от указанного партнёра с момента предыдущего вывода данного сообщения
10000011	MSG_ID_IKE_NO_PEER_CERT	IKE	INFO	%[%{32}s %]Searching peer certificate failed, Reason: not found, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Сертификат партёра не найден
10000012	MSG_ID_IKE_PEER_CERT_INVALID	IKE	INFO	%[%{32}s %]Searching peer certificate failed. Reason: %{20}s.%{1}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Сертификат партёра не пригоден для использования %{1}s Описание сертификата
10000013	MSG_ID_IKE_PEER_CERT_FOUND	IKE	INFO	%[%{32}s %]Using peer certificate:%{1}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Использование сертификата партнёра для проверки подписи %{1}s Описание сертификата
10000014	MSG_ID_IKE_NO_LOCAL_CERT	IKE	WARNING	%[%{32}s %]Searching local certificate failed, Reason: not found, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Не найден локальный сертификат для создания подписи
10000015	MSG_ID_IKE_LOCAL_CERT_INVALID	IKE	WARNING	%[%{32}s %]Searching local certificate failed. Reason: %{20}s.%{1}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Локальный сертификат не пригоден для использования %{1}s Описание сертификата
10000016	MSG_ID_IKE_LOCAL_CERT_FOUND	IKE	DEBUG	%[%{32}s %]Using local certificate:%{1}s, peer %{8}s%[:%{9}u%]%[, id "%{10}s"%]	Использование локального сертификата для создания подписи %{1}s Описание сертификата

10000018	MSG_ID_IKE_EXCHANGE_FAILED	IKE	DEBUG	%[%{32}s %]IKE session stopped%[at %{1}s%]%<DEBUG[, type %{2}s, peer %{8}s%[:%{9}u%]%[, sessionId %{4}s.%{5}s%]%]%[, Reason: %{20}s%]	Неуспешное завершение IKE обмена %{1}s Список (стек) операций, при выполнении которых произошла ошибка. %{2}s Тип обмена (Exchange Type по RFC2408) %{4}s Идентификатор обмена (Initiator Cookie по RFC2408) %{5}s Идентификатор обмена (Message ID по RFC2408)
10000019	MSG_ID_IKE_DELETION_SEND	IKE	INFO	%[%{32}s %]Sending deletion for%[ISAKMP connection %{40}n%]%[IPSec connection %{2}u -%]%[%{3}s%>INFO[, spi:%{4}s%]%]	Отсылка партнёру сообщения об удалении соединения. %{40}s Номер удаляемого ISAKMP соединения. %{2}u Номер удаляемого IPSec соединения. %{3}u Сетевой протокол IPSec соединения. %{4}s Идентификатор spi удаляемого IPSec соединения.
1000001A	MSG_ID_IKE_DELETION_RECV	IKE	INFO	%[%{32}s %]Received deletion for%[ISAKMP connection %{40}n%]%[IPSec connection %{2}u -%]%[%{3}s%>INFO[, spi:%{4}s%]%]	Получено сообщение об удалении соединения партнёром. %{40}s Номер удаляемого ISAKMP соединения. %{2}u Номер удаляемого IPSec соединения. %{3}u Сетевой протокол удаляемого IPSec соединения. %{4}s Идентификатор spi удаляемого IPSec соединения.

1000001B	MSG_ID_IKE_NOTIFICATION_SEND	IKE	DEBUG	%[%{32}s %]Sending notification [%{1}s]%[for %{33}s%]%[for ISAKMP connection %{40}s%]%[, LifeTime:%{4}u%]%[, LifeTraffic:%{5}u%]	Отсылка партнёру информационного сообщения. %{1}u Тип информационного сообщения (Notification) по RFC2407, RFC2408. %{4}u Новое значение ограничения жизни соединения в секундах (для нотификации RESPONDER-LIFETIME). %{5}u Новое значение ограничения жизни соединения в килобайтах (для нотификации RESPONDER-LIFETIME). %{33}s Идентификатор адресуемой сессии IKE обмена. %{40}s Номер адресуемого ISAKMP соединения.
1000001C	MSG_ID_IKE_NOTIFICATION_RECV	IKE	DEBUG	%[%{32}s %]Received notification [%{1}s]%[for %{33}s%]%[for ISAKMP connection %{40}s%]%[: %{3}s%]%[, LifeTime:%{4}u%]%[, LifeTraffic:%{5}u%]	Получено информационное сообщение. %{1}u Тип информационного сообщения (Notification) по RFC2407, RFC2408. %{3}s Реакция на полученное сообщение. %{4}u Новое значение ограничения жизни соединения в секундах (для нотификации RESPONDER-LIFETIME). %{5}u Новое значение ограничения жизни соединения в килобайтах (для нотификации RESPONDER-LIFETIME). %{33}s Идентификатор адресуемой сессии IKE обмена. %{40}s Номер адресуемого ISAKMP соединения.

1000001D	MSG_ID_IKE_UNPROTECTED_NOTIFICATION_RECV	IKE	DEBUG	%[%{32}s %]Received unprotected notification [%{1}s]%[for %{33}s%]%[for ISAKMP connection %{40}s%]: Ignore	Получено незащищённое (недоверяемое) информационное сообщение. %{1}u Тип информационного сообщения (Notification) по RFC2407, RFC2408. %{33}s Идентификатор адресуемой сессии IKE обмена. %{40}s Номер адресуемого ISAKMP соединения.
1000001E	MSG_ID_IKE_SA_DEACTIVATED	IKE	DEBUG	%[%{32}s %]ISAKMP connection %{40}u deactivated%[, Reason: %{20}s%]%[, matched by license number %{1}u%]	ISAKMP соединение закрыто для использования в новых IKE-обменах. Некоторое время соединение может быть использовано для защиты ранее созданных и информационных обменов.
10000020	MSG_ID_IKE_REDUCE_LIFE_TIME	IKE	INFO	%[%{32}s %]Reducing life time%[for ISAKMP connection %{40}s%] to %{1}u seconds	Изменено ограничение жизни устанавливаемого соединения по времени. %{1}u Новое значение ограничения жизни соединения в секундах.
10000021	MSG_ID_IKE_REDUCE_LIFE_TRAFFIC	IKE	INFO	%[%{32}s %]Reducing life traffic%[for ISAKMP connection %{40}s%] to %{1}u kilobytes	Изменено ограничение жизни устанавливаемого соединения по трафику. %{1}u Новое значение ограничения жизни соединения в килобайтах.
10000050	MSG_ID_IKE_RESPOND_PH1_REJECT	IKE	WARNING	[ISAKMP] Limit of %{1}u responding Phase-1 sessions is achieved. Starting to reject new sessions.	Достигнуто ограничение по общему количеству выполняемых IKE обменов в роли респондера. Все новые обмены певой фазы, предлагаемые партнёрами, будут отвергаться до момента снижения нагрузки (см. MSG_ID_IKE_RESPOND_PH1_ACCEPT). %{1}u Достигнутый порог огранчения.

10000051	MSG_ID_IKE_RESPOND_PH1_ACCEPT	IKE	WARNING	[ISAKMP] %{1}u packets for new Phase-1 sessions were dropped. Starting to accept new sessions.	Возобновление проведения новых IKE обменов певой фазы, предлагаемых партнёрами. (см. MSG_ID_IKE_RESPOND_PH1_REJECT) %{1}u Количество отвергнутых пакетов новых обменов первой фазы за время действия ограничения.
10000070	MSG_ID_IKE_WRONG_PADDING	IKE	DEBUG	%[%{32}s %]Wrong padding in partner's encrypted packet	Партнёр прислал зашифрованный пакет с неправильным форматом padding'a.
10000071	MSG_ID_IKE_SEND_PACKET_FAILED	IKE	DEBUG	%[%{32}s %]Unable to send IKE packet%[to %{8}s%[:%{9}u%]%]	Произошла ошибка при отсылке IKE-пакета. Пакет может быть послан позднее при ретрансмиссии.
10000101	MSG_ID_IKE_NAT_REMOTE_DETECTED	IKE	DEBUG	%[%{32}s %]NAT detected on remote side	Обнаружено NAT-устройство на стороне партнёра
10000102	MSG_ID_IKE_NAT_LOCAL_DETECTED	IKE	DEBUG	%[%{32}s %]NAT detected on local side	Обнаружено NAT-устройство на локальной стороне
10000103	MSG_ID_IKE_NAT_T_WRONG_PORT	IKE	DEBUG	%[%{32}s %]Packet to incompatible port received while using NAT-Traversal	При использовании NAT-Traversal от партнёра получен IKE пакет на UDP порт 500
10000104	MSG_ID_IKE_NAT_T_UNABLE_USE_PORT	IKE	ERR	%[%{32}s %]Unable to use port 4500 for NAT-Traversal, peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	Невозможно задействовать NAT-Traversal так как не был открыт сокет на UDP порт 4500

10000201	MSG_ID_IKE_STALE_CONNECTION_BY_LICENSE	IKE	WARNING	%[%{32}s %]Stale ISAKMP connection %{40}u detected with peer %{18}s%[:%{19}u%], id "%{20}s", license number %{2}u: while processing initial contact from peer %{8}s%[:%{9}u%], id "%{10}s"	По уникальному номеру лицензии партнёра обнаружен старое, неиспользуемое ISAKMP соединение %{2}u Номер лицензии партнёра. %{18}s IP-адрес партнёра по IKE обмену для старого соединения. %{19}u IP-порт партнёра по IKE обмену для старого соединения. Если не указан, то порт стандартный (500) %{20}s Значение IKE идентификатора для аутентификации партнёра для старого соединения.
10000202	MSG_ID_IKE_LOCAL_LICENSE_DUPLICATION_DETECTED	IKE	DEBUG	%[%{32}s %]Duplicate of local license detected	Партнёр использует ту же лицензию, что и на локальном устройстве
10008001	MSG_ID_IKE_UDP_SOCKET_FAILED	IKE	WARNING	[ISAKMP] Failed to open UDP socket for %{8}s:%{9}u. Please send this message to support.	Ошибка открытия сокета для поддержки протокола ISAKMP Начиная с Windows Vista может изредка возникать после выхода Windows из режима Гибернации (Hibernation) или Сна (Suspend). В этом случае следует перезагрузить LSP для восстановления работоспособности Агента.
10000401	MSG_ID_IKE_RADIUS_REQUEST_USER	IKE	DEBUG	%[%{32}s %]RADIUS: Sending request to Access Server for user "%{1}s", peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	Отсылка запроса на аутентификацию Access серверу для указанного username
10000410	MSG_ID_IKE_RADIUS_ACCESS_GRANTED	IKE	DEBUG	%[%{32}s %]RADIUS: Access granted.%[Additional attributes received: %{1}s.%] Peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	От Access сервера получено разрешение на создание соединения с партнёром %{1} - Присланные дополнительные атрибуты. Формируются из сообщения MSG_ID_IKE_RADIUS_IKECFG_DATA

10000411	MSG_ID_IKE_RADIUS_IKECFG_DATA	IKE	DEBUG	Framed-IP-Address:%{1}s%[, cisco-av-pair:"dns-servers=%{10}s%[%{11}s%]"%]%[, cisco-av-pair:"default-domain=%{20}s%[%{21}s%]"%]%[: (%{3}s)%]	Дополнительные атрибуты, присланные RADIUS-сервером, формируемые для сообщения MSG_ID_IKE_RADIUS_ACCESS_GRANTED (Не является самостоятельным сообщением) %{1},%{10},%{11},%{20},%{21} - значения соответствующих атрибутов %{3} - дальнейшие действия по использованию атрибутов: sending received attributes to peer as IKECFG data - значения будут переданы партнёру в качестве IKECFG параметров ignored due to intersection with local AddressPool - значения будут игнорированы, так как присланный ip-адрес попадает в пул, который контролирует локальный IKECFG сервер ignored: IKERule has IKECFGPool, using local IKECFG data instead - значения будут игнорированы, так как в сработавшем IKE-правиле задействована выдача IKECFG параметров из локального пула

10000420	MSG_ID_IKE_RADIUS_ACCESS_FAILED	IKE	DEBUG	%[%{32}s %]RADIUS: %{1}s. Peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	Неуспешное завершение запроса к RADIUS-серверу %{1} - Причина отказа: Access Server timeout - нет отклика от RADIUS-сервера Access Server is not authenticated - неуспешная аутентификация RADIUS-сервера (неверное значение secret) Rejected by Access Server - RADIUS-сервер отказал в доступе партнёру (неверная пара user-password) Request to Access Server failed - прочие ошибки
00880001	MSG_ID_RADIUS_LOAD_SETTINGS	RADIUS Client	WARNING	[RADIUS] AAA Settings are not properly activated: %{1}s	Не удалось настроить клиент RADIUS (структура LSP AAASettings).
00880002	MSG_ID_RADIUS_NO_KEY	RADIUS Client	WARNING	[RADIUS] Can't retrieve key "%{1}s" from DB	Не удалось обнаружить ключ в базе данных продукта
007F0001	MSG_ID_IKECFGSRV_DUMMY_OBJECT	IKECFG Server	WARNING	[IKECFGSRV] There is no pool in new configuration for remaining address %{1}s, peer: %{8}s%[:%{9}u%]%[, id: "%{10}s"%]	В загружаемой новой LSP отсутствуют IKECFG пулы, которые соответствуют сохранённым ранее выданным IKECFG адресам. IKECFG адрес продолжает удерживаться, хотя он не соответствует ни одному из пулов в новой LSP. Примечание: Данное сообщение может не выводиться при логировании на внешний syslog сервер.
00324001	MSG_ID_LDAP_REQ_NOT_FOUND	LDAP	INFO	%[%{32}s %]LDAP request result: NOT FOUND. Query: "%{1}s".	Результат LDAP запроса – объекты не найдены {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена

00324101	MSG_ID_LDAP_CREATE_REQ_FAILED	LDAP	WARNING	%[%{32}s %]Failed to create LDAP request. Query: "%{1}s".	Не удалось сформировать корректный LDAP запрос. {1} - LDAP запрос (URL) Здесь и далее: данный запрос может отличаться от URL, указанного в сообщении о формировании LDAP-запроса (случай "CRL by URL"), если исходный URL не содержал адреса LDAP-сервера. {32} - идентификатор сессии IKE обмена
00324102	MSG_ID_LDAP_PARSE_FAILED	LDAP	WARNING	%[%{32}s %]Failed to parse LDAP message. Query: "%{1}s".	Ошибка разбора сообщения от LDAP сервера. {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена
00324103	MSG_ID_LDAP_REQ_FAILED_TIMEOUT	LDAP	WARNING	%[%{32}s %]LDAP request cancelled by timeout. Query: "%{1}s".	LDAP запрос завершен по таймауту. {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена
00324104	MSG_ID_LDAP_REQ_FAILED_NOT_RESPOND	LDAP	WARNING	%[%{32}s %]LDAP server is not responding. Query: "%{1}s".	LDAP сервер не отвечает. {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена
00324105	MSG_ID_LDAP_REQ_FAILED_CANCELED	LDAP	DEBUG	%[%{32}s %]LDAP request cancelled.	LDAP запрос отменен (например при остановке сервиса vpnsvc) {32} - идентификатор сессии IKE обмена
00324106	MSG_ID_LDAP_REQ_FAILED_CONNECTION_CLOSED	LDAP	DEBUG	%[%{32}s %]LDAP connection was closed by LSP unload.	Соединение LDAP было закрыто при выгрузке LSP. {32} - идентификатор сессии IKE обмена
003241FF	MSG_ID_LDAP_REQ_FAILED_UNKNOWN	LDAP	DEBUG	%[%{32}s %]LDAP internal error.	Внутренняя ошибка модуля LDAP. {32} - идентификатор сессии IKE обмена

00325001	MSG_ID_LDAP_REQ_SUCCESS	LDAP	INFO	%[%{32}s %]LDAP request result: %{2}u object(s) found. Query: "%{1}s".	Результат LDAP запроса - найдено {2} объектов {1} - LDAP запрос (URL) {32} - идентификатор сессии IKE обмена
00327001	MSG_ID_LDAP_REQ_START	LDAP	DEBUG	%[%{32}s %]LDAP request: "%{1}s".	Сформирован LDAP запрос {1} где {1} – запрос в одном из следующих видов: "CRL by DN: <Printable_DN>" – запрос CRL производится по DN. "Certificate by DN: <Printable_DN>" – запрос сертификата производится в виде DN. "CRL by URL: <url>" – запрос CRL по URL (берется из CDP). {32} - идентификатор сессии IKE обмена
00327002	MSG_ID_LDAP_REQ_IGNORED	LDAP	DEBUG	%[%{32}s %]LDAP request ignored: there is no LDAP server available.	LDAP запрос "{1}" проигнорирован: не задан LDAP сервер {32} - идентификатор сессии IKE обмена
00723001	MSG_ID_CSCONF_CONV_END_FAIL	Cisco-like console & converter	ERR	LSP converter finished with errors	LSP конвертор завершил работу с ошибками
00723003	MSG_ID_CSCONF_PARSE_CERT	Cisco-like console & converter	ERR	Certificate for CA "%{1}s", parse error	Ошибка разбора сертификата для CA {1}
00723004	MSG_ID_CSCONF_NOCA_CERT	Cisco-like console & converter	ERR	Wrong certificate type for CA "%{1}s", must be CA certificate	Неверный тип сертификата для CA {1}
00723005	MSG_ID_CSCONF_CERT_EXIST	Cisco-like console & converter	ERR	CA certificate "%{1}s" already exists in the trustpoint "%{2}s". Certificate addition ignored.	CA сертификат {1} уже присутствует в trustpoint {2}. Добавление сертификата проигнорировано

00723006	MSG_ID_CSCONF_POOL_INTERSECT	Cisco-like console & converter	ERR	Current pool entry has intersection with others, no entry will be added	Текущий пул адресов имеют пересечения с другими пулами. Запись не будет добавлена.
00723007	MSG_ID_CSCONF_NON_CSCONS_SAVE_FAIL	Cisco-like console & converter	ERR	Could not save previous user-defined LSP in file "%{1}s"	Не удалось сохранить предыдущую пользовательскую LSP в файл "{1}"
00724001	MSG_ID_CSCONF_CMD_REMOVED_AUTO	Cisco-like console & converter	WARNING	Command "%{1}s" removed from configuration automatically	Команда "{1}" автоматически удалена из конфигурации.
00724002	MSG_ID_CSCONF_REMOVE_CERT	Cisco-like console & converter	WARNING	Removing CA Trustpoint "%{1}s", no certificate found	При старте cs_console из конфигурации автоматически был удален сертификат, отсутствующий в базе локальных настроек. Образовался пустой trustpoint, который также был автоматически удален.
00724003	MSG_ID_CSCONF_REMOVE_KEY	Cisco-like console & converter	WARNING	Removing KEY "%{1}s", no key found in agent	При старте cs_console из конфигурации автоматически был удален preshared key, отсутствующий в базе локальных настроек.
00724004	MSG_ID_CSCONF_USER_AUTOMATICALLY_REUSED	Cisco-like console & converter	WARNING	User(s) %{1}s were automatically added to configuration. Zero privilege level was assigned to them.	При старте cs_console обнаружены пользователи системы, отсутствующие в конфигурации, но для которых в качестве shell выставлена cs_console. Данные пользователи автоматически добавлены в конфигурацию с нулевым уровнем привилегий.
00725001	MSG_ID_CSCONS_START	Cisco-like console & converter	NOTICE	Cisco-like console started by user "%{1}s"	cs_console запущена пользователем "{1}".
00725002	MSG_ID_CSCONS_EXIT	Cisco-like console & converter	NOTICE	Cisco-like console exited (user "%{1}s")	Пользователь "{1}" вышел из cs_console.

00725003	MSG_ID_CSCONF_USER_CREATED	Cisco-like console & converter	NOTICE	User "%{1}s" created	Успешно создан пользователь операционной системы "{1}". Может выдаваться как при ручном вводе команды, так и при старте cs_console (в случае, если в конфигурации присутствует пользователь, отсутствующий в системе).
00725004	MSG_ID_CSCONF_USER_REMOVED	Cisco-like console & converter	NOTICE	User "%{1}s" removed	Пользователь операционной системы "{1}" успешно удален. Может выдаваться при ручном вводе команды no username ...
00725005	MSG_ID_CSCONF_USER_PWD_CHANGED	Cisco-like console & converter	NOTICE	User "%{1}s" password changed	Пароль пользователя операционной системы {1} успешно сменен. Может выдаваться как при ручном вводе команды (только для уже существующего пользователя), так и при старте cs_console (в случае, если пароль пользователя в конфигурации не совпадает с паролем пользователя в системе).
00725006	MSG_ID_CSCONF_USER_PRIVL_CHANGED	Cisco-like console & converter	NOTICE	User "%{1}s" privilege changed to %{2}d	Привилегия пользователя операционной системы {1} изменена на новое значение {2}. Может выдаваться при ручном вводе команды username ... (только для уже существующего пользователя). Одна команда username... может порождать сразу два сообщения: о смене пароля и о смене привилегии.
00725007	MSG_ID_CSCONF_USER_EXEC_ENTERED	Cisco-like console & converter	NOTICE	User "%{1}s" has entered into the privileged EXEC mode	Пользователь вошел в привилегированный режим (по команде enable). Выдается только при ручном вводе команды enable.

00725008	MSG_ID_CSCONF_NON_CSCONS_LSP	Cisco-like console & converter	NOTICE	Previous user-defined LSP saved in file "%{1}s"	Предыдущая пользовательская LSP сохранена в файле "{1}"
00725009	MSG_ID_CSCONF_POLICY_NON_SYNC	Cisco-like console & converter	INFO	Non-synchronized policy detected. Policy type: %{1}s	Обнаружена несинхронизированная политика. Тип политики: <type> где <type> один из: DDP DHCP Only User-defined (Source: Command-line utility)
0072500A	MSG_ID_CSCONF_PRESHARED_KEYS_OR_CERTS_CHANGED	Cisco-like console & converter	INFO	Certificates or preshared keys were changed. Conversion required	Сертификаты или preshared keys изменились. Требуется конвертирование
0072500B	MSG_ID_CSCONF_START	Cisco-like console & converter	NOTICE	Command interpreter started	Старт интерпретатора команд
0072500C	MSG_ID_CSCONF_USER_SHELL_CHANGED	Cisco-like console & converter	NOTICE	User "%{1}s" shell changed to /opt/VPNagent/bin/cs_console	Shell пользователя операционной системы {1} успешно сменен. Может выдаваться при старте cs_console (в случае, если пользователь присутствует в конфигурации и в системе, но в системе в качестве shell прописано другое приложение).
00726001	MSG_ID_CSCONF_CONV_BEGIN	Cisco-like console & converter	INFO	Starting LSP converter	Запуск LSP конвертора
00726002	MSG_ID_CSCONF_CONV_END_OK	Cisco-like console & converter	INFO	LSP converter finished successfully	LSP конвертор отработал без ошибок
00727001	MSG_ID_CSCONF_CMD_START	Cisco-like console & converter	DEBUG	Start interpreting command: "%{1}s"	Начало обработки команды {1} интерпретатором

00727002	MSG_ID_CSCONF_CMD_END_OK	Cisco-like console & converter	DEBUG	Command "%{1}s" processed with status OK	Обработка команды "{1}" завершена успешно
00727003	MSG_ID_CSCONF_CMD_END_FAIL	Cisco-like console & converter	DEBUG	Command "%{1}s" processed with status FAIL	Команда "{1}" обработана с ошибкой
00733001	MSG_ID_CSCONV_INTERFACE_EMPTY_ACL	Cisco-like console & converter	ERR	Interface "%{1}s" references to the empty access list "%{2}s".	Интерфейс "{1}" ссылается на пустой ACL "{2}"
00733002	MSG_ID_CSCONV_NO_ACTIVE_POOL	Cisco-like console & converter	ERR	Address pool "%{1}s" not found.	Не найден пул адресов "{1}".
00733003	MSG_ID_CSCONV_CLASS_MAP_EMPTY_ACL	Cisco-like console & converter	ERR	Class map "%{1}s" (from policy map "%{2}s") references to the empty or absent access list "%{3}s".	Class map "{1}" (из policy map "{2}") ссылается на пустой или отсутствующий ACL "{3}"
00733101	MSG_ID_CSCONV_NO_ISAKMP_POLICY	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: There is no isakmp policy.	Невозможно сконвертировать crypto map "{1}". Причина: Отсутствует isakmp policy.
00733102	MSG_ID_CSCONV_WRONG_AUTH	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: There is no CA or appropriate preshared key. Also isakmp policy can have wrong type (rsa-sig or pre-share).	Невозможно сконвертировать crypto map "{1}". Причина: Отсутствует CA или подходящий Preshared Key, либо isakmp policy неправильного типа (rsa-sig или pre-share).
00733103	MSG_ID_CSCONV_NO_PEER	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: There is no peer.	Невозможно сконвертировать crypto map "{1}". Причина: Отсутствует peer.

00733104	MSG_ID_CSCONV_NO_TRANSFORM_SET	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: There are no transform sets.	Невозможно сконвертировать crypto map "{1}". Причина: Отсутствуют transform sets.
00733105	MSG_ID_CSCONV_INCOMPLETE_CRYPTO_MAP	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: It is incomplete.	Невозможно сконвертировать crypto map или dynamic crypto map template: Причина: Crypto map неполная (в случае crypto map: не хватает crypto ACL или peer; в случае crypto map или dynamic crypto map template: ссылка на пустой crypto ACL). %{1}s - один из двух вариантов: crypto map "<name> <seq-num>" или dynamic crypto map template "<name> <seq-num>"
00733106	MSG_ID_CSCONV_CRYPTO_MAP_EMPTY_ACL	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: Reference to the empty access list "%{2}s" for a clear-text packets filtration.	Невозможно сконвертировать crypto map "{1}". Причина: Ссылка на пустой ACL "{2}" для Clear-Text фильтрации (внутри защищенного туннеля).
00733107	MSG_ID_CSCONV_CRYPTO_MAP_IKECFG_MISMATCH	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: %{2}s references to the same pool ("%{3}s") but the additional parameters to send to client are different.	Невозможно сконвертировать crypto map "{1}". Причина: crypto map (или dynamic crypto map template) "{2}" ссылается на тот же самый пул ("{3}"), но дополнительные параметры, отсылаемые клиенту, различаются.
00733108	MSG_ID_CSCONV_CRYPTO_MAP_PH1_MODE_MISMATCH	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: conflicting Phase 1 modes (main and aggressive) for different peers. Check the "crypto isakmp peer" commands.	Невозможно сконвертировать crypto map "{1}". Причина: конфликтующие режимы первой фазы (main mode и aggressive mode) для разных peer-ов. Проверьте команды "crypto isakmp peer".

00733109	MSG_ID_CSCONV_CRYPTO_MAP_ACL_WITH_TIME_RANGE	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: access list "%{2}s" references time range.	Невозможно сконвертировать crypto map "{1}". Причина: ACL "{2}" ссылается на time range.
0073310A	MSG_ID_CSCONV_CRYPTO_MAP_NO_CLIENT_USERNAME	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: AAA client authentication list has been referenced without username source ("set client username...").	Невозможно сконвертировать crypto map "{1}". Причина: Пристуствует ссылка на список AAA аутентификации, но отсутствует источник имени пользователя ("set client username...").
0073310B	MSG_ID_CSCONV_CRYPTO_MAP_NO_AUTH_LIST_REF	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: AAA client authentication username source has been set without authentication list reference ("set client authentication list...").	Невозможно сконвертировать crypto map "{1}". Причина: задан источник имени пользователя, но отсутствует список AAA аутентификации ("set client authentication list...")
0073310C	MSG_ID_CSCONV_CRYPTO_MAP_UNKNOWN_AUTH_LIST	Cisco-like console & converter	ERR	Could not convert %{1}s. Reason: Reference to unknown AAA client authentication list.	Невозможно сконвертировать crypto map "{1}". Причина: Ссылка на неизвестный список AAA аутентификации.
007331FF	MSG_ID_CSCONV_CRYPTO_MAP_NOT_CONVERTED	Cisco-like console & converter	ERR	Could not convert crypto map "%{1}s". Reason: Unknown	Невозможно сконвертировать crypto map "{1}" по неизвестной причине.
00733A01	MSG_ID_CSCONV_LSP_LOAD_FAILED	Cisco-like console & converter	ERR	LSP load failed%[: %{1}s%].%[Erroneous LSP saved in file "%{2}s".%]	Не удалось прогрузить сформированную LSP. Расшифровка ошибки: {1} Ошибочная LSP сохранена в файле "{2}".
00733A02	MSG_ID_CSCONV_LSP_LOAD_FAILED_VPNSVC_NOT_RUNNING	Cisco-like console & converter	ERR	LSP load failed: vpnsvc daemon is not running.	Не удалось прогрузить сформированную LSP. Невозможно установить связь с сервисом vpnsvc.

00733A03	MSG_ID_CSCONV_NO_TIME_RANGE	Cisco-like console & converter	ERR	Access list "%{1}s" references absent time range "%{2}s".	ACL "{1}" ссылается на отсутствующий time range "{2}"
00733A04	MSG_ID_CSCONV_AUTH_LIST_RADIUS_WITHOUT_SERVER	Cisco-like console & converter	ERR	AAA authentication list has been set without RADIUS server.	Задан список AAA аутентификации, но не задан адрес RADIUS сервера
00733A05	MSG_ID_CSCONV_RADIUS_SERVER_WITHOUT_KEY	Cisco-like console & converter	ERR	RADIUS server has been set without shared secret.	Задан RADIUS сервер, но не задан пароль доступа к нему
00733FFF	MSG_ID_CSCONV_FAILED	Cisco-like console & converter	ERR	LSP conversion failed	Неизвестная ошибка конвертирования LSP.
00734001	MSG_ID_CSCONV_LDAP_IGNORED	Cisco-like console & converter	WARNING	LDAP url "%{1}s" ignored. IP address and port allowed only.	Введенный LDAP url {1} проигнорирован, поскольку допускаются только IP-адрес и порт.
00734002	MSG_ID_CSCONV_SOME_PEERS_IGNORED	Cisco-like console & converter	WARNING	Crypto map "%{1}s" contains several peers. Peer(s) "%{2}s" ignored due to authentication information mismatch.	В crypto map-е {1} прописаны несколько peer-ов. Peer(s) {2} проигнорированы из-за того, что для них не совпадает аутентификационная информация.
00734003	MSG_ID_CSCONV_SEVERAL_IPSEC_ACTIONS	Cisco-like console & converter	WARNING	Crypto map "%{1}s" contains several peers with different preshared keys. This is not recommended.	Crypto map "{1}" содержит несколько peers с разными preshared keys. Это нерекомендуемая ситуация.
00734004	MSG_ID_CSCONV_MIXED_MODE_TUNNEL	Cisco-like console & converter	WARNING	Crypto map(s) "%{1}s" contain transform sets with different encapsulation modes. Tunnel mode is used.	Crypto map(-ы) {1} содержат transform set-ы, в которых заданы разные encapsulation режимы. Используется туннельный режим.

00734005	MSG_ID_CSCONV_MIXED_MODE_TRANSPORT	Cisco-like console & converter	WARNING	Crypto map(s) "%{1}s" contain transform sets with different encapsulation modes. Transport mode is used.	Crypto map(-ы) {1} содержат transform set-ы, в которых заданы разные encapsulation режимы. Используется транспортный режим.
00734006	MSG_ID_CSCONV_STATIC_AFTER_DYNAMIC	Cisco-like console & converter	WARNING	Crypto map set(s) "%{1}s" contain static crypto map(s) with priorities lower than dynamic.	Crypto map set(s) "{1}" содержат статические crypto map(s) с приоритетом ниже, чем у динамических.
00734101	MSG_ID_CSCONV_LSP_LOAD_WITH_ONE_WARNING	Cisco-like console & converter	WARNING	LSP successfully loaded with warning: %{1}s.	Сформированная LSP загружена с одним предупреждением. {1} - текст предупреждения
00734102	MSG_ID_CSCONV_LSP_LOAD_WITH_WARNINGS	Cisco-like console & converter	WARNING	LSP successfully loaded, %{1}u potential problems were reported to syslog.	Сформированная LSP загружена с двумя и более предупреждениями. {1} - количество выданных предупреждений (если было выдано два и больше)
00735001	MSG_ID_CSCONV_START	Cisco-like console & converter	NOTICE	LSP conversion started	Начат процесс конвертирования
00735002	MSG_ID_CSCONV_STOP	Cisco-like console & converter	NOTICE	LSP conversion complete%[. Warnings: %{1}u%]	Процесс конвертирования завершен успешно. Опционально: выдано {1} предупреждений.
00793001	MSG_ID_INCORRECT_CPU USAGE	Statistics & SNMP	WARNING	SNMP polling of CPU usage is unavailable. SNMP variables cpmCPUTotal* will be invalid.	Невозможно получать информацию о загрузке CPU для SNMP. Переменные SNMP cpmCPUTotal* будут иметь неверное значение.
00793002	MSG_ID_USE_INTERCALARY_INSTANEOUS_CPUUSAGE	Statistics & SNMP	INFO	The system clock changed. SNMP cpmCPUTotal* statistics may be incorrect for a while.	Время на часах OS изменено. Статистика о загрузке CPU для SNMP может быть некорректна какое-то время.

00200001	MSG_ID_LOCAL_CERTIFICATE_ADDED	Certificates	NOTICE	New local certificate added%[Subject="%{1}s"%]%[Issuer="%{2}s"%]%[SN="%{3}s"%]	Добавление локального сертификата в базу данных
00200002	MSG_ID_CA_CERTIFICATE_ADDED	Certificates	NOTICE	New certificate authority added%[Subject="%{1}s"%]%[Issuer="%{2}s"%]%[SN="%{3}s"%]	Добавление Сертифицирующего Центра в базу данных
00200003	MSG_ID_CERTIFICATE_DISABLED	Certificates	WARNING	Certificate disabled%[Subject="%{1}s"%]%[Issuer="%{2}s"%]%[SN="%{3}s"%]	Удаление локального сертификата, либо Сертифицирующего Центра из базы данных
00200004	MSG_ID_LOG_PRIV_KEY_INACCESSIBLE	Certificates	CRIT	Local certificate '%{1}s' is invalid: private key %[at container%{3}s %]'%{4}s' is inaccessible	Приватный ключ локального сертификата недоступен Где: %{1}s – значение поля Subject локального сертификата «at container» – если ключ не был задан явно %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера
00200005	MSG_ID_LOG_PRIV_CONT_INACCESSIBLE	Certificates	CRIT	Local certificate '%{1}s' is invalid: container '%{4}s' is inaccessible	Контейнер ключа локального сертификата недоступен Где: %{1}s – значение поля Subject локального сертификата %{4}s – имя контейнера
00200006	MSG_ID_LOG_PRIV_KEY_INCONSISTENCY	Certificates	CRIT	Local certificate '%{1}s' is invalid: private key %[at container%{3}s %]'%{4}s' is inconsistent with the certificate	Приватный ключ не соответствует локальному сертификату. Это возможно только после установки OCI Где параметры - см.описание MSG_ID_LOG_PRIV_KEY_INACCESSIBLE

006F0001	MSG_ID_LOG_X509_CONV_UNSUP_ENCODING	Certificates	CRIT	Unsupported "%{1}s" iconv encoding	В файле x509conv.ini указана неподдерживаемая кодировка
006F0002	MSG_ID_LOG_X509_CONV_UNSUP_ENCODING_USE_DEFAULT	Certificates	WARNING	Unsupported encoding "%{1}s" has been specified in x509conv.ini, "%{2}s" will be used	В файле x509conv.ini указана неподдерживаемая кодировка %{1}, будет использоваться умолчательная %{2}
006F0003	MSG_ID_LOG_X509_CONV_UNEXP_INI_FIELD	Certificates	WARNING	Unexpected parameter "%{1}s" has been specified in x509conv.ini, ignored	В файле x509conv.ini указан неизвестный параметр
006F0004	MSG_ID_LOG_X509_CONV_INCOMP_ENCODING_ATTR	Certificates	WARNING	Certificate with subject "%{1}s" has incompatible attribute value encoding. Probably, the connection won't be established. Please, configure x509conv.ini according to actual attribute encoding.	Ошибка при перекодировке полей Issuer или Subject сертификата в UTF-8
00650001	MSG_ID_USER_LOGIN	<MAIN_APPLICATION>	NOTICE	User logged in	Доступ Пользователя к Агенту
00650002	MSG_ID_USER_LOGOUT	<MAIN_APPLICATION>	NOTICE	User logged out	Отключение доступа Пользователя к Агенту
00290001	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_STATS_TRAIL	Firewall	INFO	Session closed: initiator %{8}s%[:%{9}u%] sent %{3}U bytes -- responder(%{18}s%[:%{19}u%]) sent -> %{13}U bytes	Сообщение инициируется когда закрывается соединение. Сообщает, сколько байт было послано и принято. Где %{8} – ip адрес источника %{3} – кол-во байт посланных инициатором %{18} – ip адрес принимающей стороны %{13} – кол-во байт посланных принимающей стороной

00290002	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT	Firewall	WARNING	getting aggresive, count(%{1}u/%{2}u), current 1-minute rate: %{3}u	Появление такого сообщения в логе может свидетельствовать о начале DOS атаки. где, %{1} – кол-во полуоткрытых соединений %{2} – кол-во новых соединений %{3} – кол-во новых соединений за минуту
00290003	MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT_OFF	Firewall	WARNING	calming down, count (%{1}u/%{2}u), 1-minute rate %{3}u	Появление такого сообщения может свидетельствовать об окончании DOS атаки где параметры - см.описание MSG_ID_ON_IPSM_LOG_MID_FW_TCP_HCONN_ALERT
00290004	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_PRIV_PORT	Firewall	WARNING	Privileged port %{9}u, used in PORT command -- FTP client %{8}s FTP server %{18}s	FTP клиент пытается выполнить команду PORT на привилегированном порту (<1024) где, %{9} – номер порта %{8} – ip FTP клиента %{18} – ip FTP сервера
00290005	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PASV_PRIV_PORT	Firewall	WARNING	Privileged port %{9}u, used in PASV response command -- FTP client %{8}s FTP server %{18}s	FTP сервер пытается выполнить ответ на PASV команду на привилегированном порту. где параметры - см.описание MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_PRIV_PORT
00290006	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PORT_NOTAUTH	Firewall	WARNING	Command issued before the session is authenticated -- FTP client %{8}s (client side)	Попытка выполнить FTP команду до окончании аутентификации со стороны FTP клиента где %{8} – ip FTP клиента
00290007	MSG_ID_ON_IPSM_LOG_MID_FW_FTP_PASV_NOTAUTH	Firewall	WARNING	Command issued before the session is authenticated -- FTP client %{8}s (server side)	Попытка выполнить FTP команду до окончании аутентификации со стороны FTP сервера где %{8} – ip FTP клиента

00290008	MSG_ID_ON_IPSM_LOG_OTHERS	Firewall	DEBUG	no format string: message id %{1}u	Нет формата строки: сообщение номер…
00290009	MSG_ID_KLOGLIB_INIT_NO_MEMORY	Firewall	DEBUG	Can't create statistic states(no memory)	Недостаточно памяти для создания объектов статистики
0029000A	MSG_ID_KLOGLIB_INIT_CANT_ATTACH	Firewall	DEBUG	unable to attach as listener	Невозможно присоединится к драйверу “klogview” в режиме слушателя
0029000B	MSG_ID_KLOGLIB_INIT_CANT_SET_FILTER	Firewall	DEBUG	unable to set event filter	Невозможно установить фильтр сообщений из ядра
0029000C	MSG_ID_KLOGLIB_INIT_MISSED_ALERT_PACKETS	Firewall	WARNING	access-list logging missed %{1}u alert packets	Оповещение о количестве пропущенных тревожных сообщений, превысивших допустимую частоту их обновления
0029000D	MSG_ID_KLOGLIB_INIT_MISSED_PACKETS	Firewall	WARNING	access-list logging rate-limited or missed %{1}u packets	Оповещение о количестве пропущенных сообщений из IPSEC драйвера, превысивших допустимую частоту их обновления.
0029000E	MSG_ID_KLOGLIB_INIT_PRINT_SUMMARY	Firewall	INFO	list %{1}s %{2}s %[%{3}s %]%[%{13}u %]%{8}s(%{4}u) -> %{18}s(%{14}u), %{5}U packet(s)	Статистика по соединению за интервал времени где: %{1} – название access list, если задано в LSP %{2} - статус, %{3}/%(13} - выдается или имя протокола или его номер %{8} - ip адрес источника, %{18} – ip адрес приемника, %{5} - количество пакетов
08530001	MSG_ID_WATCHDOG_VPNSVC_CRASHED	Installer for Unix	WARNING	IPsec daemon (vpnsvc) crashed (see /tmp/vpnsvc/error.log for details)	Оповещение watchdog: IPsec демон (vpnsvc) аварийно завершился

08530002	MSG_ID_WATCHDOG_VPNSVC_RUNNING_AGAIN	Installer for Unix	NOTICE	IPsec daemon (vpnsvc) is running	Оповещение watchdog: IPsec демон (vpnsvc) запущен
08530003	MSG_ID_WATCHDOG_VPNSVC_RUN_ERROR	Installer for Unix	ERR	Error restarting IPsec daemon (vpnsvc)	Оповещение watchdog: перезапуск IPsec демона (vpnsvc) не удался
08530004	MSG_ID_WATCHDOG_VPNSVCLOG_CRASHED	Installer for Unix	WARNING	VPN log daemon (vpnlogsvc) crashed (see /tmp/vpnlogsvc/error.log for details)	Оповещение watchdog: демон логирования (vpnlogsvc) аварийно завершился
08530005	MSG_ID_WATCHDOG_VPNSVCLOG_RUNNING_AGAIN	Installer for Unix	NOTICE	VPN log daemon (vpnlogsvc) is running	Оповещение watchdog: демон логирования (vpnlogsvc) запущен
08530006	MSG_ID_WATCHDOG_VPNSVCLOG_RUN_ERROR	Installer for Unix	ERR	Error restarting VPN log daemon (vpnlogsvc)	Оповещение watchdog: перезапуск демона логирования (vpnlogsvc) не удался
08530007	MSG_ID_VPNSVC_RUN_ERROR	Installer for Unix	ERR	Starting IPsec daemon failed. See /tmp/vpnsvc/error.log for details.	Оповещение скрипта запуска: запуск IPsec демона (vpnsvc) не удался
08530008	MSG_ID_VPNSVCLOG_RUN_ERROR	Installer for Unix	ERR	Starting VPN log daemon failed. See /tmp/vpnlogsvc/error.log for details.	Оповещение скрипта запуска: запуск демона логирования (vpnlogsvc) не удался
08530009	MSG_ID_WATCHDOG_VPNSVC_STOPPED	Installer for Unix	NOTICE	IPsec daemon (vpnsvc) stopped	Оповещение watchdog: IPsec демон (vpnsvc) остановлен
0853000A	MSG_ID_WATCHDOG_VPNSVCLOG_STOPPED	Installer for Unix	NOTICE	VPN log daemon (vpnlogsvc) stopped	Оповещение watchdog: демон логирования (vpnlogsvc) остановлен

00020001	MSG_ID_LOG_SET_DEFAULT_LOGLEVEL	Log	INFO	Default log level is %{1}s	Нефильтруемое сообщение об установке умолчательного уровня логирования сообщений. Выдается при каждом его изменении и в начале сессии VPN Сервиса. Где: %{1} – значение установленного log level - {emerg | alert | crit | err | warning | notice | info | debug}
00020002	MSG_ID_LOG_SET_SYSLOG_SETTINGS	Log	INFO	Syslog settings are: %{1}s, %{2}s, %{3}s	Нефильтруемое сообщение об установках syslog. Выдается при каждом их изменении и в начале сессии VPN Сервиса. Где: %{1} – разрешение отсылки сообщений - {enable | disable}; %{2} – IP адрес syslog сервера %{3} – параметр facility, указываемый при передаче сообщений syslog серверу
00020003	MSG_ID_LOG_SET_PARTICULAR_LOGLEVELS	Log	INFO	Some particular log levels are set	Нефильтруемое сообщение об установке частных уровней логирования некоторым сообщениям. Выдается при каждом их изменениях и в начале сессии VPN Сервиса.
00020004	MSG_ID_LOG_SAVE_PARTICULAR_LOGLEVELS	Log	INFO	Current particular log levels are permanently saved	Нефильтруемое сообщение о сохранении всех текущих частных уровней логирования сообщений для использования в следующих сессиях VPN Сервиса. Выдается при каждом таком сохранении.
00020005	MSG_ID_LOG_RESET_PARTICULAR_LOGLEVELS	Log	INFO	All particular log levels are reset	Нефильтруемое сообщение о сбросе частных уровней логирования всем сообщениям. Выдается при каждом таком сбросе.

Список ошибок протокола ISAKMP

(указываются в поле «Reason:» %{20}s шаблона сообщений для описанных событий в Таблица 4)

Таблица 5

	Описание ошибки	Запись об ошибке в строке сообщения
1	От партнера пришло сообщение неверного типа вместо ожидаемого сообщения CONNECTED (свидетельствующего о готовности IPSec-соединения на стороне партнера)	Unexpected Notification type: need CONNECTED
2	Получен компонент IKE-пакета типа 130, соответствующий компоненту для обнаружения устройства NAT, что не соответствует протоколу обмена для данного этапа	Unexpected payload found (payload type - 130, possibly NAT Discovery)
3	От партнера пришла команда дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.), не соответствующая протоколу обмена для данного этапа	Unexpected configuration message type
4	От партнера пришли параметры дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.), не соответствующие текущей политике безопасности	Bad Config proposal
5	Потеряны внутренние данные от предыдущего пакета	Previous packet missed
6	Потеряны данные формируемого пакета	OUT packet missed
7	Потерян SA-компонент предыдущего пакета	Missing SA payload
8	Невозможно выбрать сценарий IKE-обмена для выбранного типа аутентификации	Unknown IKE-scenario for chosen Authentification method
9	Не найден один из необходимых компонентов пакета	Can’t find proposal
10	Партнер вернул неправильную идентификационную информацию ответчика IKE-обмена при создании IPSec-соединения	Bad IDcr returned
11	Потеряны данные входящего пакета	IN packet missed
12	Партнер вернул неправильную идентификационную информацию инициатора IKE-обмена при создании IPSec-соединения	Bad IDci returned

	Описание ошибки	Запись об ошибке в строке сообщения
13	Сессия дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.) была прервана встречным запросом – другой сессией дополнительного конфигурирования XAuth	Replaced with new XAuth request
14	Сессия Quick Mode остановлена для перезапуска с новыми параметрами запроса после дополнительного конфигурирования защищающего ISAKMP-соединения.	Restart session
15	Невозможность продолжить IKE-обмен после выполнения асинхронного запроса. (Возможно, за время выполнения запроса произошло событие, вызвавшее прекращение обмена)	Can't Complete Async Task
16	Невозможно создать информационный IKE-обмен	Can't create new Informational Exchange
17	Невозможно создать IKE-обмен 2-й фазы	Can't create new Phase-II
18	Невозможно создать IKE-обмен 1-й фазы	Can't create new Exchange
19	Невозможно создать IKE-обмен 2-й фазы из-за незавершенности обмена 1-й фазы	Request to create Phase-II without completed Phase-I
20	IKE-обмен не начат по причине чрезмерной активности недоверяемого партнёра	Access denied
21	Фактический размер IKE-пакета не соответствует указанному в его заголовке	Invalid packet (size mismatch)
22	Партнер прислал IKE-пакет с неправильной структурой, либо пакет не удалось правильно расшифровать	Invalid packet (invalid structure)
23	Некорректный компонент IKE-пакета	Invalid packet (invalid payload)
24	Зашифрованность (либо незашифрованность) присланного пакета не соответствует IKE-сценарию, либо ошибка в процессе дешифрования IKE-пакета	Unable to decode packet
25	Внутренняя (системная) ошибка	Internal error
26	Переполнение памяти	Out of memory
27	IKE-пакет распознан как перепосылка для ранее созданного IKE-обмена	Retransmission detected
28	Присланный IKE-пакет не распознан, либо не актуален для существующего обмена	Wrong IKE packet received

	Описание ошибки	Запись об ошибке в строке сообщения
29	Присланный IKE-пакет не актуален для существующего обмена	IKE packet dropped
30	Присланный IKE-пакет является перепосылкой для только что созданного IKE-обмена	Repeat for the first packet in exch
31	Для присланного IKE-пакета сценарий не поддерживается	Unable to determine IKE scenario
32	Запрет на создание нового IKE-обмена в процессе смены политики безопасности	Process blocked by Local Policy
33	Незавершённый асинхронный запрос	Asynchronous request was started...
34	Ошибка при шифровании IKE-пакета	CP coding error
35	Ошибка установки таймера для сервиса перепосылок IKE-пакетов	Unable to set Timer

Список выполняемых действий по протоколу ISAKMP

(указываются в поле «Stopped at: %{1}s» шаблона сообщений для описанных событий в Таблица 4)

Таблица 6

	Описание действия	Информация в строке сообщения
1	Шифрование сформированного IKE-пакета перед отправкой партнеру	[Coding packet]
2	Расшифрование IKE-пакета, присланного партнером	[Decoding packet]
3	Проверка предложений, на которые согласился партнер	[Check replied SA]
4	Проверка сертификата, присланного партнером	[Check for Remote Certificate]
5	Запрос локального сертификата	[Check for Local Certificate]
6	Проверка идентификационной информации, присланной партнером	[Check incom IDs]

	Описание действия	Информация в строке сообщения
7	Использование в качестве идентификационной информации партнера его IP-адреса	[Check IDs as IP-addresses]
8	Проверка используемого алгоритма хэширования	[Check for Hash method]
9	Синтаксический разбор пакета, присланного партнером на отдельные компоненты (payloads)	[Make payload set for received packet]
10	Проверка всех компонентов присланного пакета	[Check received payloads]
11	Проверка формируемого пакета на наличие компонентов перед отправкой партнеру. Используется только при создании пакетов Informational обменов чтобы удостовериться, что информация не была отправлена с другим пакетом.	[Check for added payloads]
12	Вычисление подписи	[Calculate Signature]
13	Выбор правила IKE согласно текущей конфигурации по идентификационной информации партнера	[Choose Rule for Partner’s identity]
14	Создание ключевых пар текущей IKE-сессии	[Generate Keys]
15	Формирование ключевого материала	[Generate SKEYIDs]
16	Выбор политики безопасности согласно текущей конфигурации на основании предложений от партнера	[Compare policy]
17	Формирование SPI	[Set SPI]
18	Проверка и принятие параметров устанавливаемого соединения, на которые согласился партнер	[Accept Transform]
19	Вычисление хэша для обнаружения устройства NAT	[Calculate NAT Discovery payload]
20	Вычисление общего ключа	[Calculate Shared Key]
21	Вычисление инициализационного вектора	[Calculate InitVector]
22	Определение метода аутентификации	[Detect Authentification Method]
23	Запрос локального сертификата для метода аутентификации с использованием сертификатов	[Get Local Certificates]

	Описание действия	Информация в строке сообщения
24	Проверка метода аутентификации, предложенного партнером, на соответствие текущей политике безопасности	[Check Authentification Method]
25	Выбор метода аутентификации	[Choose Authentification Method]
26	Проверка выбранной комбинации параметров устанавливаемого соединения	[Get Proposal]
27	Задание выбранного алгоритма шифрации для устанавливаемого соединения	[Get Algorithm]
28	Запрос возможных параметров устанавливаемого соединения согласно текущей конфигурации для их согласования с партнером	[Get Local Policy]
29	Проверка на наличие в предложении партнера параметра, устанавливающего MODP-группу	[Get DH group for QM]
30	Выбор используемой идентификационной информации для отправки партнеру	[Get ID from Local Policy]
31	Выбор используемой идентификационной информации для отправки партнеру при создании ISAKMP-соединения в качестве инициатора	[Get IDii from Local Policy
32	Выбор используемой идентификационной информации для отправки партнеру при создании ISAKMP-соединения в качестве ответчика	[Get IDir from Local Policy]
33	Выбор используемой идентификационной информации для отправки партнеру при создании IPSec-соединения в качестве инициатора IKE-обмена	[Get IDci from Local Policy]
34	Выбор используемой идентификационной информации для отправки партнеру при создании IPSec-соединения в качестве ответчика IKE-обмена	[Get IDcr from Local Policy]
35	Инициализация ключевой информации для формирования IPSec-соединения	[Initialize Encryption Container for QM
36	Формирование готового IPSec-соединения	[Create contexts
37	Распознавание метода дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.)	[Determine IKE configuration method]

	Описание действия	Информация в строке сообщения
38	Распознавание команды дополнительного конфигурирования ISAKMP-соединения (XAuth, IKECFG, и т.п.)	[Determine Config message type]
39	Распаковка параметров присланного запроса на дополнительную аутентификацию (XAuth) и формирование соответствующего графического пользовательского диалога	[Analyse attributes and fill user dialog fields]
40	Запуск графического пользовательского диалога дополнительной аутентификации (XAuth).	[Start dialog for user extended authentication]
41	Проверка наличия компонента IKE-пакета	[Check payload %s[3]]
42	Проверка структуры компонента IKE-пакета	[Analyse payload structure %s[4]]
43	Формирование компонента IKE-пакета	[Form payload %s[5]]
44	Заполнение блока данных указанного компонента IKE-пакета	[Fill payload %s[6]]
45	Проверка содержимого компонента IKE-пакета	[Check %s[7]]
46	Вычисление хэша – содержимого указанного компонента	[Calculate %s[8]]
47	Выполнение сценария инициации информационного обмена IKE согласно RFC 2409	[Informational Exchange, Initiator, Packet 1]
48	Выполнение сценария обработки пакета информационного обмена IKE согласно RFC 2409	[Informational Exchange, Responder, Packet 1]
49	Выполнение шага сценария формирования 1-го пакета IKE Main Mode согласно RFC 2409	[Main Mode, Initiator, Packet 1]
50	Выполнение шага сценария обработки 1-го пакета IKE Main Mode согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 1,2]
51	Выполнение шага сценария начала обработки 2-го пакета IKE Main Mode согласно RFC 2409	[Main Mode, Initiator, Packets 2,3]

[3] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[4] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[5] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[6] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[7] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

[8] Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

	Описание действия	Информация в строке сообщения
52	Выполнение шага сценария продолжения обработки 2-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 2,3, Pre-Shared Key]
53	Выполнение шага сценария продолжения обработки 2-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 2,3, Signature]
54	Выполнение шага сценария обработки 3-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 3,4, Pre-Shared Key]
55	Выполнение шага сценария обработки 3-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 3,4, Signature]
56	Выполнение шага сценария обработки 4-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 4,5, Pre-Shared Key]
57	Выполнение шага сценария обработки 4-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Initiator, Packets 4,5, Signature]
58	Выполнение шага сценария обработки 5-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 5,6, Pre-Shared Key]
59	Выполнение шага сценария обработки 5-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Main Mode, Responder, Packets 5,6, Signature]
60	Выполнение шага сценария обработки 6-го пакета IKE Main Mode для аутентификации на общих ключах согласно RFC 2409	[Main Mode, Initiator, Packet 6, Pre-Shared Key]
61	Выполнение шага сценария обработки 6-го пакета IKE Main Mode для аутентификации на сертификатах согласно RFC 2409	[Main Mode, Initiator, Packet 6, Signature]
62	Выполнение шага сценария начала формирования 1-го пакета IKE Aggressive Mode Mode согласно RFC 2409	[Aggressive Mode, Initiator, Packet 1]
63	Выполнение шага сценария продолжения формирования 1-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409	[Aggressive Mode, Initiator, Packet 1, Pre-Shared Key]

	Описание действия	Информация в строке сообщения
64	Выполнение шага сценария продолжения формирования 1-го пакета IKE Aggressive Mode для аутентиф икации на сертификатах согласно RFC 2409	[Aggressive Mode, Initiator, Packet 1, Signature]
65	Выполнение шага сценария начала обработки 2-го пакета IKE Aggressive Mode согласно RFC 2409	[Aggressive Mode, Responder, Packets 1,2]
66	Выполнение шага сценария продолжения обработки 1-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Responder, Packets 1,2, Pre-Shared Key]
67	Выполнение шага сценария продолжения обработки 1-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Responder, Packets 1,2, Signature]
68	Выполнение шага сценария обработки 2-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Initiator, Packets 2,3, Pre-Shared Key]
69	Выполнение шага сценария обработки 2-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409 и формирование ответного пакета	[Aggressive Mode, Initiator, Packets 2,3, Signature]
70	Выполнение шага сценария обработки 3-го пакета IKE Aggressive Mode для аутентификации на общих ключах согласно RFC 2409	[Aggressive Mode, Responder, Packet 3, Pre-Shared Key]
71	Выполнение шага сценария обработки 3-го пакета IKE Aggressive Mode для аутентификации на сертификатах согласно RFC 2409	[Aggressive Mode, Responder, Packet 3, Signature]
72	Выполнение шага сценария формирования 1-го пакета IKE New Group Mode согласно RFC 2409	[New Group Mode, Initiator, Packet 1]
73	Выполнение шага сценария обработки 1-го пакета IKE New Group Mode согласно RFC 2409 и формирование ответного пакета	[New Group Mode, Responder, Packets 1,2]
74	Выполнение шага сценария обработки 2-го пакета IKE New Group Mode согласно RFC 2409	[New Group Mode, Initiator, Packet 2]
75	Выполнение шага сценария формирования 1-го пакета служебного обмена IKE	[Transaction Exchange, Initiator, Packet 1]
76	Выполнение шага сценария обработки 1-го пакета служебного обмена IKE и формирование ответного пакета	[Transaction Exchange, Responder, Packets 1,2]

	Описание действия	Информация в строке сообщения
77	Выполнение шага сценария обработки 2-го пакета служебного обмена IKE	[Transaction Exchange, Initiator, Packet 2]
78	Выполнение шага сценария формирования 1-го пакета IKE Quick Mode согласно RFC 2409	[Quick Mode, Initiator, Packet 1]
79	Выполнение шага сценария обработки 1-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета	[Quick Mode, Responder, Packets 1,2]
80	Выполнение шага сценария обработки 2-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета	[Quick Mode, Initiator, Packets 2,3]
81	Выполнение шага сценария обработки 3-го пакета IKE Quick Mode согласно RFC 2409 и формирование ответного пакета (при поддержке партнером Commit Bit)	[Quick Mode, Responder, Packet 3,(4)]
82	Выполнение шага сценария обработки 4-го пакета IKE Quick Mode (при поддержке партнером Commit Bit)	[Quick Mode, Initiator, Packet 4]
83	Вычисление ключевого материала	[Make SKEYID]
84	Проведение PFS - создание отдельной ключевой пары для IPSec соединения	[Make PFS]
85	Выбор ISAKMP либо IPSec правила	[Choose Rule]
86	Проверка присланного атрибута – компонента пакета IKE	[Check Attr]
87	Проверка присланного сертификата – компонента пакета IKE	[Check Cert]
88	Проверка присланного хэша – компонента пакета IKE	[Check HASH]
89	Проверка присланного идентификатора – компонента пакета IKE	[Check ID]
90	Проверка присланного ключа – компонента пакета IKE	[Check KE]
91	Проверка присланного NAT-детектора – компонента пакета IKE	[Check NAT-D]
92	Проверка присланного NAT Original Address – компонента пакета IKE	[Check NAT-OA]
93	Проверка присланного Nonce – компонента пакета IKE	[Check Nonce]

	Описание действия	Информация в строке сообщения
94	Проверка присланного сообщения – компонента пакета IKE	[Check Notif]
95	Проверка присланного запроса на сертификат – компонента пакета IKE	[Check REQ]
96	Проверка присланных предложений на создание соединения – компонента пакета IKE	[Check SA]
97	Проверка присланной подписи – компонента пакета IKE	[Check SIG]
98	Проверка вендор-идентификатора – компонента пакета IKE	[Check VID]
99	Формирование атрибута – компонента пакета IKE	[Form Attr]
100	Формирование сертификата – компонента пакета IKE	[Form Cert]
101	Формирование хэша – компонента пакета IKE	[Form HASH]
102	Формирование идентификатора – компонента пакета IKE	[Form ID]
103	Формирование ключа – компонента пакета IKE	[Form KE]
104	Формирование NAT-детектора – компонента пакета IKE	[Form NAT-D]
105	Формирование NAT Original Address – компонента пакета IKE	[Form NAT-OA]
106	Формирование Nonce – компонента пакета IKE	[Form Nonce]
107	Формирование запроса на сертификат – компонента пакета IKE	[Form CertReq]
108	Формирование подписи – компонента пакета IKE	[Form SIG]
109	Формирование вендор-идентификатора – компонента пакета IKE	[Form VendorID]
110	Проверка на наличие устройства NAT	[NAT existence check]

Список причин инициации IKE сессии

(указываются в сообщениях IKE в поле «Request: %{1}s» в Таблица 4)

Таблица 7

	Причина инициации	Шаблон, используемый в сообщениях	Параметр
1	IKE-обмен в роли респондера	Inbound ISAKMP packet	
2	Запрос на создание IPsec соединения	Create IPSec #%{1}u	%{1}u – номер инициации IPSec-соединения
3	Пересоздание устаревшего IPsec соединения	IPSec %{1}u re-establishing	%{1}u – номер пересоздаваемого IPsec соединения
4	Удаление IPsec соединения	IPSec %{1}u deletion	%{1}u – номер удаляемого IPsec соединения
5	Пересоздание устаревшего ISAKMP соединения	ISAKMP %{1}s re-establishing	%{1}s – идентификатор пересоздаваемого ISAKMP соединения
6	Конфигурирование ISAKMP соединения (проведение IKECFG, XAuth)	ISAKMP %{1}s configure	%{1}s – идентификатор конфигурируемого ISAKMP соединения
7	Информирование партнёра по IKE-обмену (коррекция ISAKMP соединения, прекращение IKE-обмена)	ISAKMP notification	
8	Удаление ISAKMP соединения	ISAKMP %{1}s deletion	%{1}s – идентификатор удаляемого ISAKMP соединения
9	Удаление соединения по запросу пользователя[9]	User request	

[9] Посредством использования команды sa_mgr clear <…>

Ошибки криптографической подсистемы

Список сообщений об ошибках криптографической подсистемы, работающей в ядре ОС, приведен в таблице ниже.

Таблица 8

	Текст шаблона сообщения	Рекомендуемые пользователю действия, краткое описание
1	CP_Conf_K2U_PushPluginConf: Plugin is not properly loaded	Если есть проблемы с загрузкой LSP или прохождением трафика, обратитесь в службу поддержки.
2	CP_ReOpen: bad check handle	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратитесь в службу поддержки.
3	CP_Transform: bad handle 0x%x	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратитесь в службу поддержки.
4	Skipping unused algorithm [%s]	Не ошибка, можно игнорировать.
5	forced close: 0x%x,0x%x	В результате падения приложения были автоматически уничтожены созданные им криптоконтексты. Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратитесь в службу поддержки.
6	drvcsp!info: 243, error=1(OK	Не ошибка, можно игнорировать.
7	drvcsp!_init9	Не ошибка, можно игнорировать.

Ошибки подсистемы RRI

Список сообщений об ошибках подсистемы Reverse Route Injection приведен в таблице ниже.

Таблица 9

	Текст сообщения	Описание события
1	[RRI] SA conflicts with the route created for different SA, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255	Для двух SA с разными селекторами требуются конфликтующие маршруты. Правило маршрутизации создается только для первого из конфликтующих SA
2	[RRI] SA selector shouldn't have protocols, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255 proto 6 [RRI] destination part of SA selector shouldn't have ports, route not created: destination 10.0.16.96, SA selector 10.0.16.61:32798->192.168.1.6:23 proto 6 [RRI] destination part of SA selector shouldn't have arbitrary IP range, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.1..192.168.1.255	ID второй фазы IKE не является подсетью (содержит диапазон IP-адресов, порты и/или протоколы). Правило маршрутизации не добавляется.
3	[RRI] no route to destination, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255	Отсутствие маршрута до туннельного адреса[10]. Маршрут не добавляется.
4	[RRI] can't read system routing table, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255	Системная или внутренняя ошибка – не удалось получить таблицу маршрутизации.
5	[RRI] can't add route 10.0.0.0/8 via 192.168.1.4: <rtctl err> Возможные варианты <rtctl err>: out of memory syscall error route not found route already exists gateway unreachable	Системная или внутренняя ошибка – не удалось добавить маршрут в системную таблицу.

[10] Ситуация экзотическая – маршрут нужен для построения SA. Ошибка возможна если маршрут удалится в процессе создания SA или из-за ошибки чтения/разбора таблицы маршрутизации.

	Текст сообщения	Описание события
6	[RRI] can't delete route 10.0.0.0/8 via 192.168.1.4: <rtctl err> Возможные варианты <rtctl err>: out of memory syscall error route not found route already exists gateway unreachable	Ошибка удаления правила из системной таблицы маршрутизации. Ошибки такого типа не приводят к каким-либо дополнительным действиям кроме выдачи данного сообщения.
7	[RRI] route already exists, route not created: destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255	В системной таблице уже есть маршрут, соответствующий SA, но подсистема RRI его не создавала.
8	[RRI] created route 192.168.1.0/24 via 10.0.135.1 for destination 10.0.16.96, SA selector 10.0.16.61->192.168.1.0..192.168.1.255	Добавление нового RR.
9	[RRI] updated route to 192.168.1.0/24: new gw 10.0.16.96, old gw 10.0.135.1	Обновление RR. Сообщение выдается, если при создание нового SA обнаружено, что изменилась таблица маршрутизации и надо обновить ранее созданный RR.
10	[RRI] removed route 192.168.1.0/24 via 10.0.135.1 for destination 10.0.16.96	Удаление RR. Сообщение выводится при удалении записи из системной таблицы. То есть когда удалены все SA, использующие данный маршрут.

