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

Программный комплекс CSP VPN Gate. Версия 3.11

Руководство администратора

Протоколирование событий

РЛКЕ.00005-02 90 03

17.12.2013

Содержание

Протоколирование событий

Настройка Syslog-клиента

В Продукте протоколирование событий происходит только по протоколу Syslog и получатель лога может быть только один, в отличие от Cisco.

Cisco-like конфигурация

В интерфейсе командной строки для настройки Syslog-клиента и отправки сообщений о протоколируемых событиях используются команды:

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

logging facility – задание источника сообщений

logging trap – задание текущего уровня важности для всех событий. При отсутствии этой команды уровень лога равен `INFO`.

Все эти настройки записываются в файл ***syslog.ini***.

Если эти команды отсутствуют, то действуют настройки по умолчанию, записанные в файле ***syslog.ini***, а именно:

```
Severity = INFO
Facility = log_local7
IP-addr = 127.0.0.1
```

LSP (native) конфигурация

Для настройки Syslog-клиента в текстовом файле конфигурации используются:

структура SyslogSettings – задание IP-адреса хоста, на который будут направляться сообщения, и задание источника сообщений. В этой же структуре можно отключить использование протокола Syslog. Если эта структура отсутствует, то действуют настройки, задаваемые в файле syslog.ini.

структура GlobalParameters – задание уровня лога для разных событий:

- атрибут ***SystemLogMessageLevel*** – задает уровень лога для системных событий
- атрибут ***PolicyLogMessageLevel*** – задает уровень лога для событий, связанных с применением политики безопасности
- атрибут ***CertificatesLogMessageLevel*** – задает уровень лога для событий, связанных с сертификатами
- атрибут ***LDAPLogMessageLevel*** – задает уровень лога для событий, связанных с доступом к LDAP серверу.

Если эти атрибуты не заданы или LSP конфигурация не загружена, то действует уровень лога, установленный по умолчанию, который задается при помощи утилиты ***log_mgr set***. Если это значение не менялось, то оно равно ***Debug***.

Если заданы уровни протоколирования для разных событий и задан уровень протоколирования по умолчанию, то действуют уровни протоколирования, заданные для разных событий.

Файл syslog.ini

При создании конфигурации в интерфейсе командной строки (консоли) все настройки syslog будут записываться в файл ***syslog.ini***, поэтому этот файл вручную не редактируется.

При создании политики в виде конфигурационного файла (LSP) и отсутствии в нем структуры SyslogSettings будут действовать настройки из файла ***syslog.ini***. В этом случае этот файл можно отредактировать вручную.

Файл ***syslog.ini*** расположен в каталоге ***/opt/VPNagent/bin***. 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: log_kern, log_user, log_mail, log_daemon, log_auth, log_syslog, log_lpr, log_news, log_uucp, log_cron, log_authpriv, log_ftp, log_ntp, log_audit, log_alert, log_cron2, log_local0, log_local1, ..., log_local7.

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

Значение Facility в файле syslog.ini	Числовой код протокола Syslog[2]	define из стандартного файла syslog.h	Значение Facility в LSP	Значение в Cisco-like команде logging facility
log_kern	0 << 3	LOG_KERN	LOG_KERN	kern
log_user	1 << 3	LOG_USER	LOG_USER	user
log_mail	2 << 3	LOG_MAIL	LOG_MAIL	mail
log_daemon	3 << 3	LOG_DAEMON	LOG_DAEMON	daemon
log_auth	4 << 3	LOG_AUTH	LOG_AUTH	auth
log_syslog	5 << 3	LOG_SYSLOG	LOG_SYSLOG	syslog
log_lpr	6 << 3	LOG_LPR	LOG_LPR	lpr
log_news	7 << 3	LOG_NEWS	LOG_NEWS	news
log_uucp	8 << 3	LOG_UUCP	LOG_UUCP	uucp
log_cron	9 << 3	LOG_CRON	LOG_CRON	sys9

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

[2] << – обозначение операции битового сдвига влево

log_authpriv	10 << 3	LOG_AUTHPRIV	LOG_AUTHPRIV	sys10
log_ftp	11 << 3	LOG_FTP	LOG_FTP	sys11
log_ntp	12 << 3		LOG_NTP	sys12
log_audit	13 << 3		LOG_AUDIT	sys13
log_alert	14 << 3		LOG_ALERT	sys14
log_cron2	15 << 3		LOG_CRON2	cron
log_local0	16 << 3	LOG_LOCAL0	LOG_LOCAL0	local0
log_local1	17 << 3	LOG_LOCAL1	LOG_LOCAL1	local1
log_local2	18 << 3	LOG_LOCAL2	LOG_LOCAL2	local2
log_local3	19 << 3	LOG_LOCAL3	LOG_LOCAL3	local3
log_local4	20 << 3	LOG_LOCAL4	LOG_LOCAL4	local4
log_local5	21 << 3	LOG_LOCAL5	LOG_LOCAL5	local5
log_local6	22 << 3	LOG_LOCAL6	LOG_LOCAL6	local6
log_local7	23 << 3	LOG_LOCAL7	LOG_LOCAL7	local7

Если в файле ***syslog.ini*** были установлены значения, отличные от начальных, то после запуска консоли они изменятся на начальные значения.

При изменении файла настройки вступят в действие только после рестарта демона.

Настройки из файла ***syslog.ini*** используются в двух случаях:

- когда в LSP отсутствует структура ***SyslogSettings*** (только для LSP, написанной вручную в виде конфигурационного файла)
- когда политика безопасности не загружена или политика безопасности отгружена командой ***lsp_mgr unload***.

Следует учитывать возможные побочные эффекты сохранения получателя лога в файл `syslog.ini`:

- файл `syslog.ini` может меняться при старте консоли (даже если не была введена ни одна команда). Это произойдет, если файл перед стартом консоли менялся вручную. В этом случае его содержимое будет заменено на то, что прописано в Cisco-like конфигурации

- конфигурирование в `cs_console` может повлиять на получателя лога в том случае, если после этого будет загружена LSP, в которой не указана структура `SyslogSettings` (это означает, что лог идет получателю, указанному в `syslog.ini`). Примечание: такая LSP может быть только написана вручную, и не может быть получена с помощью `cs_converter`

- конфигурирование в `cs_console` также может повлиять на получателя лога в случаях, когда не загружена LSP (при старте сервиса или при отгрузке LSP).

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*** для аппаратных платформ с жестким диском
  - в файл ***/tmp/cspvpngate.log*** для аппаратных платформ с флеш-диском
- лог уровня важности ***err и выше*** дополнительно направляется в консоль
- Syslog-сервер запускается автоматически при каждом старте ОС с включенной возможностью приёма сообщений по UDP порту 514
- 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 производится 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***.

Для изменения установленных настроек Syslog-сервера произведите настройки лога в стандартном файле ***/etc/syslog.conf***:

- например, для сохранения информации в файл `/var/adm/message`, пришедшей от источника `facility local0` и имеющей все уровни важности, добавьте строку (поля разделяются символами табуляции):

```
local0.debug            /var/adm/message
```

- например, для сохранения информации в файл `/var/adm/message`, пришедшей от источника `facility local2` и имеющей уровень важности NOTICE и выше, добавьте строку (поля разделяются символами табуляции):

```
local2.notice           /var/adm/message
```

В ОС Red Hat Enterprise Linux 5 (CentOS 5) после изменения конфигурационного файла выполните перезапуск syslog:

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


Для изменения максимального размера файла лога, количества файлов лога и периода проверки размера файла отредактируйте в файле ***/etc/logwatch.conf*** следующие параметры:

```
LOGSIZE=1024
LOGNUM=2
LOGDELAY=10
```

где

1024 кбайт	максимальный размер файла ***/var/log/cspvpngate.log (/tmp/cspvpngate.log)*** с протоколируемыми событиями
2	количество файлов архива
10 секунд	период времени, через который проводится проверка размера файла лога.

После изменения файла перезапустить программу ***logwatch*** с помощью команд:

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

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

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

Каждому протоколируемому событию присваивается фиксированный идентификатор (***MSG ID***) и соответствующий ему уровень важности (***Severity***) для протокола Syslog: EMERG, ALERT, CRIT, ERR, WARNING, NOTICE, INFO, DEBUG.

Строки протоколируемых событий формируются посредством шаблонов, задаваемых во внешнем текстовом файле ***s_res.ini*** .

Все протоколируемые события для `cs_console` относятся к разделу SYSTEM. Чтобы отличать эти события, в таблицах сообщения представлены под разделами CONSOLE – для cs_console и CONVERTER – для cs_converter. Выдаваемые сообщения и описание событий по этим сообщениям представлены в Таблицах 1-5.

Ведется также протоколирование ошибок криптографической подсистемы (драйвера `cryptopm`, `cp_plg1` и др.). Эти ошибки доводятся до сведения пользователя также через Syslog, используя источник сообщений (Facility) `kern`. Перечень важнейших ошибок приведен в Таблица 8.

Сообщения уровня ERROR

Таблица 1

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Локальный сертификат непригоден	ERR	CERT	Searching local certificate failed. Reason: %s[3]. Subject: %s Issuer: %s SN: %s
2	Локальный сертификат не найден	ERR	CERT	Searching local certificate failed. Reason: not found. Search template: %s
3	Секретный ключ локального сертификата недоступен	ERR	CERT	Local certificate '%{1}s' is invalid: private key %{2}s%{3}s'%{4}s' is inaccessible где: %{1}s – значение поля Subject локального сертификата %{2}s – «», если ключ был задан явно, иначе «at container» %{3}s – «», если ключ был задан явно, иначе « » %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера
4	Контейнер ключа локального сертификата недоступен	ERR	CERT	Local certificate '%{1}s' is invalid: container '%{4}s' is inaccessible где: %{1}s – значение поля Subject локального сертификата %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера
5	Секретный ключ не соответствует локальному сертификату. Это возможно только после установки OCI	ERR	CERT	Local certificate '%{1}s' is invalid: private key %{2}s%{3}s'%{4}s' is inconsistent with the certificate где: %{1}s – значение поля Subject локального сертификата %{2}s – «», если ключ был задан явно, иначе «at container» %{3}s – «», если ключ был задан явно, иначе « » %{4}s – путь к ключу, если он был задан явно, иначе имя контейнера
6	cs_console: Команда {1} введена не полностью	ERR	CONSOLE	Uncomplete command: "%{1}s"

[3] revoked | expired | not verified

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
7	cs_console: Ошибка в процессе выполнения команды	ERR	CONSOLE	Command “{1}”, processed with status FAIL
8	cs_console: Ошибка разбора сертификата для ca {1}	ERR	CONSOLE	Certificate for ca “%{1}s”, parse error
9	cs_console: Ошибка при чтении файла cs_cons_reg.ini.	ERR	CONSOLE	Could not read ini file {1}
10	cs_console: В команде {1} ошибка в позиции {2}	ERR	CONSOLE	Error in command: “%{1}s”, pos: %{2}d
11	cs_config: CA сертификат {1} уже присутствует в trustpoint {2}. Добавление сертификата проигнорировано.	ERR	CONSOLE	CA certificate “%{1}s” is already exist in the trustpoint “%{2}”. Certificate addition ignored.
12	cs_config: Данная запись в пуле пересекается с другими	ERR	CONSOLE	Current pool entry has intersection with others, no entry will be added
13	cs_config: Не удалось сохранить предыдущую пользовательскую LSP в файл “{1}”	ERR	CONSOLE	Could not save previous user-defined LSP in file “{1}”
14	cs_config: Не удалось сохранить внутренние настройки в файл “{1}”	ERR	CONSOLE	Could not save internal settings in file “{1}”
15	cs_config: LSP конвертор отработал с ошибками	ERR	CONSOLE	LSP converter finished with errors
16	cs_config: Неверный тип сертификата для ca {1}	ERR	CONSOLE	Wrong certificate type for ca “%{1}s”, must be CA certificate
17	Невозможно прочитать настройки из INI-файла.	ERR	CONVERTER	Cannot read settings form INI file. Conversion failed.
18	Не заданы интерфейсы в INI-файле при выключенном Host-режиме. Необходимо сконфигурировать интерфейсы или включить Host-режим.	ERR	CONVERTER	No interfaces were found in the INI file. Configure interfaces or set host mode to proceed.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
19	В импортируемой конфигурации не заданы интерфейсы. Конвертирование не имеет смысла.	ERR	CONVERTER	No interfaces were found in the configuration.
20	Интерфейс {1} не задан в INI-файле. Конвертирование остановлено.	ERR	CONVERTER	Interface “%{1}s” not found in the INI file. Conversion aborted.
21	Не удалось разобрать введенный сертификат.	ERR	CONVERTER	Certificate parse failed
22	Невозможно сконвертировать crypto map “{1}”. Причина: <Причина>, где <Причина> одна из: Отсутствует isakmp policy Отсутствует CA или подходящий Preshared Key, либо isakmp policy неправильного типа (rsa-sig или pre-share) Отсутствует peer Отсутствуют transform sets Crypto map неполная (не хватает crypto map ACL, transform set или peer) Неизвестная причина	ERR	CONVERTER	Could not convert crypto map “{1}”. Reason: <Reason> где <Reason>: There is no isakmp policy There is no CA or appropriate preshared key. Also isakmp policy - can have wrong type (rsa-sig or pre-share) There is no peer There are no transform sets Crypto map is incomplete Unknown
23	Не удалось загрузить сформированную LSP. Ошибочная LSP сохранена в файле “{1}”	ERR	CONVERTER	LSP load failed. Erroneous LSP saved in file “%{1}s”.
24	Не удалось загрузить сформированную LSP	ERR	CONVERTER	LSP load failed
25	Не поддерживается данный формат маски подсети	ERR	CONVERTER	Unsupported network wildcard “%{1}s”
26	Произошла некоторая невыясненная ошибка	ERR	CONVERTER	LSP conversion failed
27	Не найден пул адресов “{1}”. Конвертирование прервано	ERR	CONVERTER	Address pool “{1}” not found. Conversion aborted

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
28	Неуспешная попытка установить соединение в качестве инициатора	ERR	POLICY	Connection request FAILED, Reason: %s[4], ip: %s, protocol: %s[5], IKERule: “%s”, IPsecAction: “%s”, FilteringRule: “%s”[6], Stopped at: %s[7]
29	Ошибка при добавлении IP-адреса {1} в ARP-таблицу	ERR	POLICY	Failed to add IP-address %{1}s to the ARP table
30	Обнаружены некорректные данные в базе данных, связанные с LSP	ERR	POLICY	There is a bad lsp object in product db: ‘%{1}s’, %{1}s – имя некорректного файла описания объекта в базе данных
31	Обнаружена более чем одна активная LSP в базе данных	ERR	POLICY	There are at least two active configurations in product db: ‘%{1}s’ and ‘%{2}s’ где: %{1}s – имя первого файла описания объекта в базе данных с активной LSP %{2}s – имя второго файла описания объекта в базе данных с активной LSP

[4] Session timeout | Invalid packet | No proposal chosen | Invalid ID | Authentication failed | Process blocked by Local Policy (попытка установить соединение блокируется из-за перезагрузки LSP) | Internal error

[5] ISAKMP либо IPSec

[6] Если на момент вывода сообщения сведения о правилах ISAKMP, IPSec либо о фильтре отсутствуют, то соответствующие сведения не выводятся

[7] Дополнительные сведения об операции, на которой прервался процесс установления соединения

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
32	Невозможно загрузить политику безопасности	ERR	SYSTEM	Cannot load security policy: “%s” Где %s может принимать значения: Failed to retrieve LSP from product db Internal error Failed to recover from previous error. Last successfully loaded LSP will be reloaded, all connections will be closed Failed to delete %{1}s trap receiver with community “%{2}s” %{3}s %{4}s , где : {%1} – ip адрес {%2} – snmp community (произвольная строка) {%3} – может быть “-“, в этом случае {%4} – no such entry Или {%3} = “”, в этом случае {%4} = “” “%{1}s” has invalid DN(GN) format, где {%1}- имя из структуры сертификата, которое может быть X509_SUBJECT, X509_ALT_SUBJECT, X509_ISSUER, X509_ALT_ISSUER Unable to map local identity to certificate description(s) in authentication method “%{1}s”, line %{2}d, где {%1} – название метода аутентификации {%2} – номер строки в LSP Algorithm “{%1}” not supported.
33	Ошибка в записи маршрутизации	ERR	SYSTEM	Invalid route to %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s где: %{1}s%{2}d – destination в виде одиночного IP или подсети %{3}s – gw или interface %{4}s – адрес gateway или имя интерфейса %{5}s – “, metric”, если указана метрика в LSP %{6}s – значение метрики %{7}s – описание ошибки: inconsistency, invalid gateway (matches local address)

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
34	Ошибка при добавлении записи в таблицу маршрутизации	ERR, WARNING	SYSTEM	Failed to add route to %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s где: %{1}s%{2}d – destination в виде одиночного IP или подсети %{3}s – gw или interface %{4}s – адрес gateway или имя интерфейса %{5}s – “, metric”, если указана метрика в LSP %{6}s – значение метрики %{7}s – описание ошибки: inconsistency, invalid gateway (matches local address) На уровне ERROR параметр %{7}s может принимать следующие значения: system error, unknown network interface, internal error. На уровне WARNING параметр %{7}s может принимать следующие значения: already exists.
35	Ошибка при удалении записи из таблицы маршрутизации	ERR, WARNING	SYSTEM	Failed to delete route to %{1}s%{2}d through %{3}s %{4}s%{5}s%{6}s - %{7}s где: %{1}s%{2}d – destination в виде одиночного IP или подсети %{3}s – gw или interface %{4}s – адрес gateway или имя интерфейса %{5}s – “, metric”, если указана метрика в LSP %{6}s – значение метрики %{7}s – описание ошибки: inconsistency, invalid gateway (matches local address) На уровне ERROR параметр %{7}s может принимать следующие значения: system error, internal error. На уровне WARNING параметр %{7}s может принимать следующие значения: not found.

Сообщения уровня WARNING

Таблица 2

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	При старте cs_console из конфигурации автоматически был удален сертификат, отсутствующий в базе локальных настроек. Образовался пустой trustpoint, который также был автоматически удален.	WARNING	CERT	Removing CA Trustpoint “{1}”, no certificate found
2	При старте cs_console из конфигурации автоматически был удален preshared key, отсутствующий в базе локальных настроек	WARNING	CERT	Removing KEY “{1}”, no key found in agent
3	В файле x509conv.ini указана неподдерживаемая кодировка	WARNING	CERT	Unsupported encoding “%{1}s” has been specified in x509conv.ini, “%{2}s” will be used где: %{1}s – неподдерживаемая кодировка %{2}s – кодировка, которая будет использована для соответствующего ASN.1-типа
4	В файле x509conv.ini указан неизвестный параметр	WARNING	CERT	Unexpected parameter “%{1}s” has been specified in x509conv.ini, ignored где: %{1}s – имя неизвестного параметра
5	Ошибка при перекодировке полей Issuer или Subject сертификата в UTF-8	WARNING	CERT	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. где: %{1}s – строковое представление поля Subject сертификата.
6	Возникает при старте, если в конфигурации присутствует некорректная команда	WARNING	CONSOLE	Command “{1}” removed from configuration automatically
7	cs_config: Обнаружена некорректная политика. Конвертирование политики не делается.	WARNING	CONSOLE	Incorrect config detected. Policy conversion ignored

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
8	Введенный LDAP url {1} проигнорирован, поскольку допускаются только IP-адрес и порт.	WARNING	CONVERTER	LDAP url “%{1}s” ignored. IP address and port allowed only.
9	Проигнорирован access-group out в интерфейсе {1}, поскольку допускается только access-group in.	WARNING	CONVERTER	OUT access group in the interface “%{1}s” ignored. Only IN access group is used.
10	При включенном Host-режиме допускается только один интерфейс. Остальные интерфейсы игнорируются.	WARNING	CONVERTER	Only one interface is used while host mode is on. Other interfaces ignored.
11	Импортирован только первый по списку CA-сертификат. End-User сертификаты и оставшиеся CA-сертификаты проигнорированы.	WARNING	CONVERTER	Only one CA certificate imported. Other certs ignored.
12	В crypto map-е {1} прописаны несколько peer-ов. Peer(s) {2} проигнорированы из-за того, что для них не совпадает аутентификационная информация	WARNING	CONVERTER	Crypto map “{1}” contains several peers. Peer(s) “{2}” ignored due to authentication information mismatch
13	Crypto maps {1} содержат transform sets, в которых заданы разные encapsulation режимы. Используется туннельный режим.	WARNING	CONVERTER	Crypto map(s) “{1}” contain transform sets with different encapsulation modes. Tunnel mode is used.
14	Crypto maps {1} содержат transform sets, в которых заданы разные encapsulation режимы. Используется транспортный режим.	WARNING	CONVERTER	Crypto map(s) “{1}” contain transform sets with different encapsulation modes. Transport mode is used.
15	Crypto map set(s) “{1}” содержат статические crypto map(s) с приоритетом ниже, чем у динамических	WARNING	CONVERTER	Crypto map set(s) “{1}” contain static crypto map(s) with priorities lower than dynamic.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
16	Crypto map “{1}” содержит несколько peers с разными preshared keys. Это не рекомендуемая ситуация.	WARNING	CONVERTER	Crypto map “{1}” contains several peers with different preshared keys. This is not recommended.
17	LDAP запрос {1} закончился неудачей. Причина: {2}	WARNING	LDAP	LDAP request failed. Reason: %{2}s[8]. Query[9]: “%{1}s”.
18	Неуспешная попытка установить соединение в качестве ответчика	WARNING	POLICY	Incoming connection request FAILED, Reason: %s[10], ip: %s, protocol: %s[11], IKERule: “%s”, IPsecAction: “%s”[12], FilteringRule: “%s”[13], Stopped at: %s[14]
19	При конфигурировании текущего партнера {4}:{5} в пуле обнаружен IKE-CFG адрес {1}, который закреплен за другим партнером {2}:{3} с той же самой identity	WARNING	POLICY	IKE-CFG IP-address %{1}s already bound with the partner %{2}s:%{3}d with the same identity as partner %{4}s:%{5}d has. Initiating DPD to resolve IKE-CFG IP-address conflict где: %{1}s – IKE-CFG IP-адрес %{2}s:%{3}d – IP-адрес и порт «старого» партнера %{4}s:%{5}d – IP-адрес и порт «нового» партнера

[8] Create request failed – Не удалось сформировать корректный запрос

Failed to parse message – Ошибка разбора сообщения LDAP

Timeout

LDAP server is not responding – LDAP сервер недоступен

Request canceled – Запрос прерван (например при выгрузке конфигурации)

Unknown – Причина неизвестна

[9] Здесь и далее Query показывается в виде URL. По возможности пишется адрес LDAP-сервера (как правило во всех случаях, кроме “LDAP request ignored…”). Данный Query может отличаться от URL, указанного в сообщении о формировании LDAP-запроса (случай “CRL by URL”), если исходный URL не содержал адреса LDAP-сервера.

[10] Session timeout | Limit of %u responded sessions achieved | Invalid packet | No proposal chosen | No rule chosen | Invalid ID | Authentication failed | Internal error

[11] ISAKMP либо IPSec

[12] Если на момент вывода сообщения правило ISAKMP, либо IPSec не выбрано, то сведения о нём не выводятся

[13] Если на момент вывода сообщения сведения о правилах ISAKMP, IPSec либо о фильтре отсутствуют, то соответствующие сведения не выводятся

[14] Дополнительные сведения об операции, на которой прервался процесс установления соединения

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
20	DPD показал, что предыдущий партнер {2}:{3} жив. Соединение с новым партнером {4}:{5} будет прервано.	WARNING	POLICY	Partner %{2}s:%{3}d is alive, connection with partner %{4}s:%{5}d going to be broken где: %{2}s:%{3}d – IP-адрес и порт «старого» партнера %{4}s:%{5}d – IP-адрес и порт «нового» партнера
21	Невозможно выдать IKE-CFG адрес в ответ на запрос со стороны клиента, так как пул адресов закончился.	WARNING	POLICY	Unable to respond to IKE-CFG request: address pool is over. Partner: %{4}s:%{5}d где: %{4}s:%{5}d – IP-адрес и порт «нового» партнера
22	Невозможно инициировать выдачу IKE-CFG адреса партнеру, так как пул адресов закончился.	WARNING	POLICY	Unable to initiate IKE-CFG session: address pool is over. Partner: %{4}s:%{5}d где: %{4}s:%{5}d – IP-адрес и порт «нового» партнера
23	Значение параметра DefaultCryptoContextsPerIPSecSA задано неверно	WARNING	POLICY	DefaultCryptoContextsPerIPSecSA in “agent.ini” is not valid (must be from 1 to 128), %{1}d will be used instead. где: %{1}d – значение, которое будет использовано для параметра DefaultCryptoContextsPerIPSecSA
24	В правиле IKERule задано несколько трансформов с различными группами. Если в качестве инициатора Агент будет использовать Aggressive Mode, то в этом случае будут высылаться только трансформы с такой же группой как у первого трансформа в правиле.	WARNING	POLICY	WARNING: IKERule ‘%{2}s’, line %{3}d: in Aggressive Mode initiator will use %{1}s only. где: %{1}s – название выбранной группы, по которой будет работать Агент в качестве инициатора в Aggressive Mode. %{2}s – имя IKERule, для которого выведена эта диагностика %{3}d – строка, на которой располагается IKERule.
25	Удаление локального сертификата, либо Сертифицирующего Центра из базы данных	WARNING	SYSTEM	Certificate disabled, Subject: “%s”, Issuer: “%s”, Serial number=%s

Сообщения уровня NOTICE

Таблица 3

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	cs_console: Старт консоли	NOTICE	CONSOLE	Cisco-like console has started by user “%{1}s”
2	cs_console: Завершение работы консоли, в том числе и ошибочное	NOTICE	CONSOLE	Cisco-like console has exited (user “%{1}s”)
3	cs_console: Пользователь успешно создан. Может выдаваться как при ручном вводе команды, так и при старте cs_console (в случае, если в конфигурации присутствует пользователь, отсутствующий в системе).	NOTICE	CONSOLE	User “%{1}s” has created
4	cs_console: Пользователь успешно удален. Может выдаваться при ручном вводе команды no username …	NOTICE	CONSOLE	User “%{1}s” has removed
5	Пароль пользователя 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). Одна команда username… может порождать сразу два сообщения: о смене пароля и о смене привилегии.	NOTICE	CONSOLE	User “%{1}s” password has changed

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
6	Привилегия пользователя изменена на новое значение (указано какое). 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.	NOTICE	CONSOLE	User “%{1}s” privilege has changed to %{2}d
7	Пользователь вошел в привилегированный режим (по команде enable). Выдается только при ручном вводе команды enable.	NOTICE	CONSOLE	User “%{1}s” has entered into the privileged EXEC mode
8	cs_console: Начата загрузка начальной конфигурации	NOTICE	CONSOLE	Start loading initial configuration
9	cs_console: Начальная конфигурация загружена успешно	NOTICE	CONSOLE	Initial configuration loaded
10	cs_config: Старт интерпретатора команд	NOTICE	CONSOLE	Command interpreter started
11	cs_config: Предыдущая пользовательская LSP сохранена в файле “{1}”	NOTICE	CONSOLE	Previous user-defined LSP saved in file “{1}”
12	cs_config: Обнаружена несинхронизированная политика. Тип политики: <type>, где <type> один из: DDP Drop All User-defined (Source: <source>), где <source> – Agent или Command-line utility.	NOTICE	CONSOLE	Non-synchronized policy detected. Policy type: <type>

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
13	cs_config: Обнаружена несинхронизированная политика. Изменились сертификаты, preshared ключи или интерфейсы.	NOTICE	CONSOLE	Non-synchronized policy detected. Certificates, preshared keys or interfaces were changed
14	cs_config: Инкрементальная политика отключена из-за настройки policy_sync (файл cs_conv.ini)	NOTICE	CONSOLE	Incremental policy loading disabled by policy_sync setting (file cs_conv.ini)
15	cs_config: Инкрементальная политика отключена из-за того, что не удалось провести синхронизацию политик	NOTICE	CONSOLE	Incremental policy loading disabled due to policy synchronization fail
16	Начат процесс конвертирования	NOTICE	CONVERTER	LSP conversion started
17	Процесс конвертирования завершен успешно. Предупреждения не выдавались.	NOTICE	CONVERTER	LSP conversion complete
18	Процесс конвертирования завершен успешно. Выдано {1} предупреждений.	NOTICE	CONVERTER	LSP conversion complete. Warnings: %{1}u
19	Включен Host-режим	NOTICE	CONVERTER	Host mode is enabled.
20	Результат LDAP запроса {1} – объекты не найдены	NOTICE	LDAP	LDAP request result: NOT FOUND. Query: “%{1}s”.
21	Результат LDAP запроса {1} – найдено {2} объектов	NOTICE	LDAP	LDAP request result: %{2}s object(s) found. Query: “%{1}s”.
22	Присвоен IP-адрес из удалённого IKE-CFG пула	NOTICE	POLICY	VPN ip-address %s obtained, Partner: %s:%d[15]
23	Партнёру присвоен IP-адрес из IKE-CFG пула	NOTICE	POLICY	VPN ip-address %s assigned to external host Partner: %s:%d[16]

[15] ip:port

[16] ip:port

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
24	Превышено ограничение на количество инициированных IKE-сессий. Инициированная сессия отложена до завершения любой активной инициированной IKE-сессии.	NOTICE	POLICY	[ISAKMP]: Exchange pended. Limit of %u initiated sessions achieved. Partner: %s:%d[17]
25	Превышено ограничение на количество IKE-сессий, инициированных партнерами. Запрос от партнера игнорируется, новая сессия не создается.	NOTICE	POLICY	[ISAKMP]: Exchange cancelled. Limit of %u responded sessions achieved. Partner: %s:%d[18]
26	Невозможно использование DPD для разрешения ситуации, описанной в п. 21 таблицы сообщений уровня WARNING	NOTICE	POLICY	Unable to resolve IKE-CFG IP-address conflict - DPD is disabled. Connection with partner %{4}s:%{5}d going to be broken где: %{4}s:%{5}d - IP-адрес и порт «нового» партнера
27	DPD показал, что предыдущий партнер {2}:{3} не отвечает. IKE-CFG адрес {1} закрепляется за новым партнером {4}:{5}	NOTICE	POLICY	Partner %{2}s:%{3}d is not responding, IKE-CFG IP-address %{1}s become bound with the partner %{4}s:%{5}d где: %{1}s – IKE-CFG IP-адрес %{2}s:%{3}d – IP-адрес и порт «старого» партнера %{4}s:%{5}d – IP-адрес и порт «нового» партнера
28	Старт сервиса	NOTICE	SYSTEM	Service started, version %s
29	Остановка сервиса	NOTICE	SYSTEM	Service stopped
30	Загружена политика безопасности	NOTICE	SYSTEM	Security policy loaded, Name: “%s”
31	Восстановлена политика безопасности	NOTICE	SYSTEM	Previous security policy has been restored, Name: “%s”

[17] ip:port. Порт партёра может указываться нулевым в случаях, когда он ещё не определен. Это возможно, поскольку ISAKMP обмен на момент вывода сообщения ещё не начат, а другие источники фактической информации о партнёре могут быть недоступны. Порт партнера в таких случаях определяется после возобновления ISAKMP обмена.

[18] ip:port

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
32	Добавление локального сертификата в базу данных	NOTICE	SYSTEM	New local certificate added, Subject: “%s”, Issuer: “%s”, Serial number=%s
33	Добавление Сертифицирующего Центра в базу данных	NOTICE	SYSTEM	New certificate authority added, Subject: “%s”, Issuer: “%s”, Serial number=%s
34	Доступ Пользователя к Агенту	NOTICE	SYSTEM	User logged in
35	Отключение доступа Пользователя к Агенту	NOTICE	SYSTEM	User logged out

Сообщения уровня INFO

Таблица 4

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	cs_console: Команда {1} успешно обработана консолью	INFO	CONSOLE	Command processed successfully: “%{1}s”
2	cs_config: Запуск LSP конвертора для конвертации политики в LSP. В конверторе после него идет сообщение: “LSP conversion started” с уровнем NOTICE	INFO	CONSOLE	Starting LSP converter
3	cs_config: LSP конвертор отработал без ошибок. В конверторе перед ним выдается сообщение: “LSP conversion complete” с уровнем NOTICE	INFO	CONSOLE	LSP converter finished successfully
4	Установлено соединение	INFO	POLICY	Connection established, %u.%u.%u.%u[-%u.%u.%u.%u][:%u]<->%u.%u.%u.%u[-%u.%u.%u.%u][:%u][, proto %u], FilteringRule: “%s”, IPsecAction: “%s” где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” – IP-адрес или диапазон IP-адресов и порт, которые

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
				защищаются Агентом второй аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” –IP-адрес или диапазон IP-адресов и порт, которые защищаются партнером [, proto %u] – защищаемый протокол FilteringRule: “%s” – фильтр, на который загружена созданная цепочка IPSec SA-ев IPsecAction: “%s” – правило IPsecAction по которому создалось соединение
5	Получен ISAKMP-пакет от партнера, с которым запрещен IKE-трафик[19]	INFO	POLICY	Inbound IKE packet dropped, Reason: Access denied, Partner: %s:%d[20]
6	Закрытие соединения	INFO	POLICY	Connection closed, %u.%u.%u.%u[-%u.%u.%u.%u][:%u]<->%u.%u.%u.%u[-%u.%u.%u.%u][:%u][, proto %u], bytes sent/received: %d / %d, Reason: %s где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” – IP-адрес или диапазон IP-адресов и порт, которые защищаются Агентом второй аргумент вида “%u.%u.%u.%u[-%u.%u.%u.%u][:%u]” –IP-адрес или диапазон IP-адресов и порт, которые защищаются партнером [, proto %u] – защищаемый протокол-bytes sent/received: %d / %d – количество байт, который были отосланы и приняты под защитой этого соединения Reason: %s – причина удаления соединения, возможны следующие варианты: Loading new configuration – соединение уничтожено по причине загрузки новой конфигурации

[19] Партнер (идентифицируется по паре ip:port) может быть помещен в «черный список», если с ним нет ни одного ISAKMP соединения, и за определенный промежуток времени он неуспешно пытался установить ISAKMP соединение достаточно большое количество раз. При получении нового IKE-пакета от такого партнера любая обработка IKE-пакетов игнорируется, поэтому невозможно определить намерение партнера: это может быть новая попытка установления ISAKMP соединения, продолжение старых попыток, информационное сообщение, либо просто пакет неправильного формата. Обмен с таким партнером разрешается спустя установленный промежуток времени, либо при инициировании соединения со стороны локального устройства.

[20] ip:port

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
				Delete payload received – от партнера пришел запрос на удаление этого соединения Time expired – истек лимит действия соединения по времени Traffic expired – истек лимит действия соединения по трафику Dead peer detected – партнер признан «мертвым» Initial contact – соединение удалено при получении нотификации INITIAL-CONTACT Cannot start DPD (no ISAKMP SA) – нет возможности инициировать DPD, партнер признается «мертвым» и соединение с ним удаляется Replaced with new one – соединение удаляется в связи с тем, что построено новое SA bundle destroyed – возникает в случае использования вложенного IPSec, когда удаляется одна из цепочек IPSec SAs, что приводит к уничтожению всей связки цепочек.
7	IPSec-соединение не установилось из-за превышения количества, разрешенного лицензией	INFO	POLICY	Unable to establish connection: resources exceeded
8	Информация о лицензии Продукта	INFO	SYSTEM	Product licence: product code: %s, customer code: %s, license number: %n, license code: %s

Сообщения уровня DEBUG

Таблица 5

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	cs_console: Начало обработки команды {1} интерпретатором	DEBUG	CONSOLE	Start interpreting command: “%{1}s”
2	cs_console: Обработка команды завершена успешно	DEBUG	CONSOLE	Command processed with status OK
3	Выбран локальный сертификат	DEBUG	CERT	Using local certificate: Subject: %s Issuer: %s SN:%s

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
4	Не найден сертификат партнёра	DEBUG	CERT	Searching peer certificate failed. Reason: not found. Search template: %s
5	Найден непригодный сертификат партнёра	DEBUG	CERT	Searching peer certificate failed. Reason: %s[21]. Subject: %s Issuer: %s SN: %s
6	Выбран сертификат партнёра	DEBUG	CERT	Use peer certificate: Subject: %s Issuer: %s SN: %s
7	Сформирован LDAP запрос {1}	DEBUG	LDAP	LDAP request: "%{1}s[22]". Где %{1}s – 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).
8	LDAP запрос {1} проигнорирован: не задан LDAP сервер	DEBUG	LDAP	LDAP request ignored: there is no LDAP server available. Query: "%{1}s".
9	Запрос на создание соединения	DEBUG	POLICY	Connection request, packet: %u.%u.%u.%u[:%u]-> %u.%u.%u.%u[:%u][, proto %u], FilteringRule: "%s" где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида "%u.%u.%u.%u[:%u]" – IP-адрес источника и порт, если он указан в пакете второй аргумент вида "%u.%u.%u.%u[:%u]" - IP-адрес приемника и порт, если он указан в пакете [,proto %u] – номер протокола, если указан в пакете, иначе не пишется FilteringRule "%s" – название фильтра, под который попал пакет

[21] revoked | expired | not verified

[22] Во всех сообщениях LDAP запрос описывается в виде URL. В настоящее время если используются IP-адрес и порт, заданные в LSP, они в URL не указываются.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
10	Ошибка инициирования создания соединения	DEBUG	POLICY	Failed to initiate connection request processing, packet: %u.%u.%u.%u[:%u]->%u.%u.%u.%u[:%u][, proto %u] где: квадратные скобки обозначают, что данная часть сообщения может отсутствовать первый аргумент вида “%u.%u.%u.%u[:%u]” – IP-адрес источника и порт, если он указан в пакете второй аргумент вида “%u.%u.%u.%u[:%u]” - IP-адрес приемника и порт, если он указан в пакете [,proto %u] – номер протокола, если указан в пакете, иначе не пишется
11	Создание ISAKMP SA	DEBUG	POLICY	ISAKMP connection [%u] established, Partner: %s:%d[23], Identity: %s, IKERule: “%s”
12	Удаление ISAKMP SA	DEBUG	POLICY	ISAKMP connection [%u] closed, Partner: %s:%d[24], Identity: %s, bytes sent/received: %d / %d, Exchanges passed: %d
13	Обнаружение устройства NAT	DEBUG	POLICY	NAT detected on ...[25] side, Partner: %s:%d[26]
14	Proposals высланы партнёру	DEBUG	POLICY	(Phase I): [27] Sending IKE proposals. Rule “%s”: Auth: %s Transform #1: Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: % Transform #2: ..

[23] ip:port

[24] ip:port

[25] Local | remote

[26] ip:port

[27] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
				(Phase II):[28] Sending IPSec proposals. Rule “%s”: Encapsulation mode: %s, Group: %s Proposal #1: Protocol AH: Transform #1: Integrity: %s, Life Time: %s, Life Traffic: %s Transform #2: Protocol ESP: Transform #1: Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s Transform #2: Proposal #2:
15	Партнёр прислал набор proposals	DEBUG	POLICY	(Phase I): [29] IKE proposals received. Transform #1: Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: % Transform #2:
				(Phase II):[30] IPSec proposals received. Encapsulation mode: %s, Group: %s Proposal #1: Protocol AH: Transform #1: Integrity: %s, Life Time: %s, Life Traffic: %s Transform #2 Protocol ESP: Transform #1: Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s Transform #2: Proposal #2
16	Проверка proposal для правила	DEBUG	POLICY	Check proposal #%u, Protocol %s[31], Transform #%u for Rule “%s”. Result: %s[32], attribute: %s[33]

[28] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[29] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[30] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[31] ISAKMP | AH | ESP

[32] Not matched | OK

[33] Authentication method | Hash | Cipher | Oakley group | Integrity | mode – только для не совпавших proposals

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
17	Выбран proposal	DEBUG	POLICY	(Phase I): [34] ISAKMP proposal selected. Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: %s
				(Phase II):[35] IPSec proposal selected. Mode: %s[36], Group: %s, AH Integrity: %s, ESP Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s
18	Выбран Preshared ключ	DEBUG	POLICY	Using preshared key “%{1}s” for partner %{2}s:%{3}d, где: %{1}s – Идентификатор выбранного ключа, указанный в LSP %{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену
19	Недоступен выбранный Preshared ключ	DEBUG	POLICY	Preshared key “%{1}s” not found, где: %{1}s – Идентификатор выбранного ключа, указанный в LSP
20	Присланный идентификатор партнера по IKE-обмену не подошел ни под одно правило ISAKMP. Предпринимается попытка идентифицировать партнера по его IP-адресу.	DEBUG	POLICY	WARNING: Unable to proceed IKE remote ID for partner %{2}s:%{3}d. Using ip-address from IKE packet instead, где: %{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену
21	Не удалось подобрать правило аутентификации для данного партнера по IKE-обмену	DEBUG	POLICY	Unable to choose authentication rule for partner %{2}s:%{3}d, где: %{2}s:%{3}d - IP-адрес и порт партнера по IKE-обмену
22	Информация об используемом локальном IKE-Identity	DEBUG	POLICY	[ISAKMP]: Sending identity “%s” to partner <ip:port>
23	Информация об IKE-Identity, присланном партнером	DEBUG	POLICY	[ISAKMP]: Identity “%s” is received from partner <ip:port>

[34] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[35] Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

[36] Transport | Tunnel

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
24	Информация о сообщении (IKE-Notification), присланном партнером	DEBUG	POLICY	[ISAKMP]: Notification [%s[37]] has been received for Exchange <%u[38]>: %s[39]
25	Инициированный IKE-обмен завершился с ошибкой	DEBUG	POLICY	[ISAKMP]: Connection request FAILED. %s где: %s – дополнительная доступная информация о несостоявшемся обмене: причина аварийного завершения [40] (см. Таблица 6) стек выполняемых операций (см. Таблица 7) сведения о партнере: <ip:port>, IKE-Identity [41]
26	IKE-обмен, инициированный партнером, завершился с ошибкой	DEBUG	POLICY	[ISAKMP]: Incoming connection FAILED. %s где: %s – дополнительная доступная информация о несостоявшемся обмене: причина аварийного завершения [42] (см. Таблица 6) стек выполняемых операций (см. Таблица 7) сведения о партнере: <ip:port>, IKE-Identity[43]

[37] Согласно списку п. 3.14.1 в RFC 2408 и п. 4.6.3 в RFC 2407.

[38] Номер-идентификатор IKE-обмена.

[39] Реакция Агента на присланное сообщение: Ignore | Ignore unprotected Notification | Cancel target connection | Correct TTL for target connection | Start IPsec traffic | Target connection is already disabled | Peer is alive | Wrong sequence: Ignore | Peer is interested in my liveness: send acknowledgement | Clear all old connections

[40] Если к моменту завершения партнерам удалось договориться о применении метода аутентификации на Preshared-ключах, и в списке операций присутствует «*Unable to decode packet*», то, наряду с ошибкой собственно расшифрования, либо IKE-пакета, неправильно сформированного партнером, причиной отказа в соединении может быть применение неправильного ключа.

[41] *IKE Identity* указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.

[42] Если к моменту завершения партнерам удалось договориться о применении метода аутентификации на Preshared-ключах, и в списке операций присутствует «Unable to decode packet», то, наряду с ошибкой собственно расшифрования, либо IKE-пакета, неправильно сформированного партнером, причиной отказа в соединении может быть применение неправильного ключа.

[43] *IKE Identity* указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
27	Пересечение соединений по адресам от разных партнеров на одном фильтре	DEBUG	POLICY	Connection to %{1}s:%{2}d conflicts with connection to %{3}s:%{4}d, conflicting address range: %{5}s %{1}s:%{2}d – IP-адрес и порт партнера, который блокирует соединение к партнеру %{3}s:%{4}d в адресном пространстве %{5}s

Список ошибок протокола ISAKMP

(см.пункты 25,26 уровня DEBUG)

Таблица 6

	Описание ошибки	Запись об ошибке в строке сообщения
1	Не удалось сформировать подпись	Unable to Form Signature
2	От партнера пришло сообщение неверного типа вместо ожидаемого сообщения CONNECTED (свидетельствующего о готовности IPSec-соединения на стороне партнера)	Unexpected Notification type: need CONNECTED
3	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)
4	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
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

	Описание ошибки	Запись об ошибке в строке сообщения
9	Не обнаружен локальный сертификат	Local Certificate is not present
10	Не обнаружен сертификат партнера	Remote Certificate is not present
11	Не найден сертификат	Certificate not found
12	Нет доступа к публичному ключу сертификата	Cert Public Key is inaccessible
13	Не найден один из необходимых компонентов пакета	Can’t find proposal
14	Потеряны данные с ключевой информацией	Encryption container missed
15	Партнер вернул неправильную идентификационную информацию ответчика IKE-обмена при создании IPSec-соединения	Bad IDcr returned
16	Потеряны данные входящего пакета	IN packet missed
17	Партнер вернул неправильную идентификационную информацию инициатора IKE-обмена при создании IPSec-соединения	Bad IDci returned
18	Партнер прислал IKE-пакет с неправильной структурой, либо пакет не удалось правильно расшифровать.	Invalid packet (invalid structure).

Список выполняемых действий по протоколу ISAKMP

(см.пункты 25,26 уровня DEBUG)

Таблица 7

	Описание дествия	Информация в строке сообщения
1	Шифрование сформированного IKE-пакета перед отправкой партнеру	Coding packet
2	Расшифрование IKE-пакета, присланного партнером	Decoding packet

	Описание дествия	Информация в строке сообщения
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
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	Формирование подписи	Encrypt 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

	Описание дествия	Информация в строке сообщения
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	Проверка локального сертификата для метода аутентификации с использованием сертификатов	Authentification uses Certificates: Check for Local Certificates
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

	Описание дествия	Информация в строке сообщения
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
38	Распознавание команды дополнительного конфигурирования ISAKMP-соединения (XAuth, IKE-CFG, и т.п.)	Determine ike-cfg 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[44]
42	Проверка структуры компонента IKE-пакета	Analyse payload structure %s[45]
43	Формирование компонента IKE-пакета	Form payload %s[46]
44	Заполнение блока данных указанного компонента IKE-пакета	Fill payload %s[47]

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

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

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

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

	Описание дествия	Информация в строке сообщения
45	Проверка содержимого компонента IKE-пакета	Check %s[48]
46	Вычисление хэша – содержимого указанного компонента	Calculate %s[49]
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]
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]

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

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

	Описание дествия	Информация в строке сообщения
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]
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]

	Описание дествия	Информация в строке сообщения
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]
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]

	Описание дествия	Информация в строке сообщения
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	Выбор ISAKMP либо IPSec правила	[Choose Rule]
85	Проверка присланного атрибута – компонента пакета IKE	[Check Attr]
86	Проверка присланного сертификата – компонента пакета IKE	[Check Cert]
87	Проверка присланного хэша – компонента пакета IKE	[Check HASH]
88	Проверка присланного идентификатора – компонента пакета IKE	[Check ID]
89	Проверка присланного ключа – компонента пакета IKE	[Check KE]
90	Проверка присланного NAT-детектора – компонента пакета IKE	[Check NAT-D]
91	Проверка присланного NAT Original Address – компонента пакета IKE	[Check NAT-OA]
92	Проверка присланного Nonce – компонента пакета IKE	[Check Nonce]
93	Проверка присланного сообщения – компонента пакета IKE	[Check Notif]

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

Ошибки криптографической подсистемы

Список сообщений об ошибках криптографической подсистемы, работающей в ядре ОС, при которых пользователю рекомендуется выполнить какие-либо действия, приведены в Таблица 8. При всех остальных сообщениях – обращайтесь в службу поддержки - support@s-terra.com.

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, обратиться в службу поддержки.
2	CP_ReOpen: bad check handle	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратиться в службу поддержки.
3	CP_Transform: bad handle 0x%x	Если есть проблемы с прохождением трафика, переустановить IPsec соединение, обратиться в службу поддержки.
4	CPCCreateProvider failed with return code 0x%.8X!	Удалить файл лицензии крипто-провайдера и ввести ее заново. В случае повторения ошибки - обратиться в службу поддержки.
5	%s: Can't get function addresses from CSP	Удалить файл лицензии крипто-провайдера и ввести ее заново. В случае повторения ошибки - обратиться в службу поддержки.
6	CP_Open: can't find alg %s	Удалить файл лицензии крипто-провайдера и ввести ее заново. В случае повторения ошибки - обратиться в службу поддержки.
7	Skipping unused algorithm [%s]	Не ошибка, можно игнорировать.
8	forced close: %u contexts	Не ошибка, можно игнорировать.
9	drvcsp:_info()=OK	Не ошибка, можно игнорировать.
10	drvcsp: loglevel=0x1, logformat=0x39	Не ошибка, можно игнорировать.
11	drvcsp: serial= <...>	Не ошибка, можно игнорировать.

Ошибки подсистемы RRI

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

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[50]. 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.

[50] 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.

Использование logrotate для ротации логов

Утилита ***logrotate*** позволяет автоматически отслеживать размер файлов логов, создавать, сжимать и удалять файлы логов. Каждый файл логов может обрабатываться ежедневно, еженедельно, ежемесячно, либо по достижении заданного размера.

Конфигурация ***logrotate*** настраивается в файле ***/etc/logrotate.conf***.

Рассмотрим некоторые параметры, которые можно использовать в конфигурации ***logrotate***:

- `rotate <количество сдвигов>` – файлы логов будут сдвинуты заданное количество раз; после n-ого сдвига файл будет удален; если задан 0 – старые логи будут удаляться;
- `compress` – старые версии файлов логов будут сжаты (по умолчанию gzip);
- `nocompress` – не сжимать сдвинутые файлы логов;
- `delaycompress` – отложить сжатие предыдущего файла журнала до следующего циклического сдвига;
- `create <права доступа> <владелец> <группа>` – непосредственно после обращения создать файл логов, где
  - `<права доступа>` – прописываются как для команды chmod, например 0644 будет означать, что все пользователи имеют право чтения, владелец может редактировать;
  - `<владелец>` – определяет имя пользователя, владеющего файлом;
  - `<группа>` – определяет группу, к которой будет принадлежать файл журнала;
- `olddir <папка>` – переместить сдвинутые логи в заданную папку;
- `size <размер>` – файлы логов будут сдвинуты, когда станут больше указанного размера в байтах; для интерпретации размера в мегабайтах используется M, для килобайтов – k;
- `minsize <размер>` – файлы логов будут сдвинуты, когда станут больше указанного размера, но не раньше указанного срока (день, неделя, месяц). Если указанный срок прошел, и при обращении файл логов меньше заданного размера `minsize` – логи сдвинуты не будут;
- `daily` – сдвиг логов происходит раз в день;
- `weekly` – сдвиг логов происходит раз в неделю, обычно в воскресенье;
- `monthly` – сдвиг логов происходит раз в месяц, обычно первого числа;
- `ifempty` – сдвигать файл журнала, даже если он пустой (по умолчанию применяется `ifempty`);
- `notifempty` – не сдвигать лог если он пустой.

Программа ***logrotate*** может использоваться для ротации любых файлов логов.

Для примера зададим правила для файлов ***/var/log/wtmp*** и ***/var/log/btmp***. Отсутствие контроля за данными файлами может привести к быстрому исчерпанию дискового пространства на шлюзе.

Файл ***/var/log/wtmp*** хранит информацию об успешных входах пользователей в систему и выходах из нее (применение утилиты login). Формат файла – двоичный. Для чтения файла используется команда `last`.

Файл ***/var/log/btmp*** хранит информацию о неудачных попытках входа пользователей в систему. Формат файла – двоичный. Для чтения файла используется команда `lastb`.

Отредактируем файл ***/etc/logrotate.conf***, чтобы получилась следующая конфигурация:

```
# see "man logrotate" for details
# rotate log files weekly
weekly

# keep 4 weeks worth of backlogs
rotate 4

# create new (empty) log files after rotating old ones
create

# uncomment this if you want your log files compressed
#compress

# RPM packages drop log rotation information into this directory
include /etc/logrotate.d

# no packages own wtmp -- we'll rotate them here
/var/log/wtmp {
    daily
    minsize 1M
    compress
    delaycompress
    create 0664 root utmp
    rotate 5
}

# system-specific logs may be also be configured here.

# btmp
/var/log/btmp {
    daily
    minsize 1M
    compress
    delaycompress
    create 0664 root utmp
    rotate 5
}
```

В результате каждый день (параметр `daily`) размер файла логов ***/var/log/wtmp*** и ***/var/log/btmp*** будет проверяться и если размер превысит 1 мегабайт (параметр `minsize`) – произойдет сдвиг, файл изменит свое название на ***/var/log/wtmp*** и ***/var/log/btmp.1*** соответственно. При этом создадутся новые файлы ***/var/log/wtmp*** и ***/var/log/btmp*** с правами 0644, владельцем root и группой utmp. Каждый раз, когда файлы ***/var/log/wtmp*** и ***/var/log/btmp***

при обращении будут больше 1 мегабайта, будет происходить сдвиг. Файлы после 1 сдвига будут сжиматься (параметр `delaycompress`). То есть файл ***wtmp.1/btmp.1*** сдвинется и сожмется в файл ***wtmp.2.gz/btmp.2.gz***. Файлы после ***wtmp.5.gz/btmp.5.gz*** (параметр `rotate 5`) будут удаляться.

Запуск logrotate

Cron – демон-планировщик задач, использующийся для периодического выполнения заданий в определенное время. Через ***cron*** можно изменить частоту проверки логов при помощи ***logrotate***.

По умолчанию скрипт, запускающий ***logrotate***, находится в daily-папке ***/etc/cron.daily/logrotate***:

```
#!/bin/sh


/usr/sbin/logrotate /etc/logrotate.conf
EXITVALUE=$?
if [ $EXITVALUE != 0 ]; then
    /usr/bin/logger -t logrotate "ALERT exited abnormally with
[$EXITVALUE]"
fi
exit 0
```

Время запуска скриптов задается в файле ***/etc/crontab***:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=""
HOME=/


# run-parts
01 * * * * root run-parts /etc/cron.hourly
02 4 * * * root run-parts /etc/cron.daily
22 4 * * 0 root run-parts /etc/cron.weekly
42 4 1 * * root run-parts /etc/cron.monthly
```

Первая цифра – минута часа для запуска (0-59).

Вторая цифра – час дня запуска (0-23).

Третья цифра – день месяца (1-31).

Четвертая цифра – месяц года (1-12).

Пятая цифра – день недели (0-6, Воскресенье=0).

Из этого файла видно, что daily скрипт выполняется в 4:02 каждого дня. То есть по умолчанию ***logrotate*** будет запускаться каждый день в 4:02.

Если по каким-то причинам необходимо изменить это время, то после внесения изменений в ***/etc/crontab***, перезапустите демон ***crond***:

```
/etc/init.d/crond restart
Stopping crond: [  OK  ]
Starting crond: [  OK  ]
```