

04.02.2010

**Программное средство
“Сервер безопасности
CSP VPN Server. Версия 3.0”**

**Руководство
администратора**

Содержание

1. Комплект поставки	12
2. Назначение и функции Продукта	13
3. Требования на базовые платформы и совместимость	14
4. Три режима управления сервером	15
5. Процесс подготовки инсталляционного пакета для конечного устройства	16
6. Подготовка рабочего места администратора безопасности	17
7. Атрибуты аутентификации	21
8. Подготовка инсталляционного пакета с предустановленными ключами (Preshared Keys) с помощью утилиты make_inst	22
9. Два сценария подготовки инсталляционного пакета с открытыми ключами (сертификатами) с помощью утилиты make_inst	23
9.1. Первый сценарий	24
9.2. Второй сценарий	26
10. Создание нескольких инсталляционных пакетов одновременно	27
11. Подготовка инсталляционного пакета с помощью графического интерфейса	30
11.1. Первый сценарий подготовки инсталляционного пакета с аутентификацией сторон на сертификатах	31
11.2. Второй сценарий подготовки инсталляционного пакета с аутентификацией сторон на сертификатах	32
11.3. Графический интерфейс	33
11.3.1. Формат заполняемых полей	34
11.4. Вкладка Authentication	35
11.4.1. Аутентификация при помощи сертификатов	35
11.4.2. Аутентификация при помощи Preshared Key	38
11.5. Вкладка Rules	40
11.5.1. Создание и редактирование правила	41
11.6. Вкладка IKE	46
11.7. Вкладка IPsec	48
11.8. Локальная политика безопасности	50
11.8.1. Режим автоматического формирования LSP	50
11.8.2. Режим ручного задания LSP	67
11.9. Settings	68
11.10. License	70
11.11. RNG container	71

11.12. Создание инсталляционного файла	73
11.13. Сохранение данных проекта	74
11.14. Формат задания имен алгоритмов в файле admintool.ini	75
12. Инсталляция CSP VPN Server	76
12.1. Режим basic	77
12.2. Режим normal	81
12.3. Режим silent	86
12.4. Копирование контейнера при инсталляции	88
12.5. Сообщения об ошибках	89
13. Деинсталляция CSP VPN Server	91
14. Восстановление CSP VPN Server	92
15. Создание локальной политики безопасности. Конфигурационный файл	93
15.1. Описание грамматики LSP	94
15.2. Структура конфигурации	100
15.3. Заголовок конфигурации	105
15.4. Структура LDAPSettings	110
15.5. Структура IKEParameters	114
15.5.1. Обработка пакетов – ретрансмиссии	118
15.6. Структура SNMPPollSettings	119
15.7. Структура SNMPTrapSettings	121
15.8. Структура TrapReceiver	122
15.9. Структура SyslogSettings	124
15.10. Структура RoutingTable	126
15.11. Структура Route	127
15.12. Правила пакетной фильтрации. Структура FilteringRule	129
15.13. Структура FilterEntry	132
15.14. Структура IPsecAction	133
15.15. Структура TunnelEntry	137
15.16. Структуры AHProposal и ESPProposal	139
15.17. Структура AHTransform	140
15.18. Структура ESPTTransform	142
15.19. Структура IKERule	145
15.20. Структура IKETTransform	151
15.21. Структуры для аутентификации	155
15.22. Структуры AuthMethodDSSSign, AuthMethodRSASign, AuthMethodGOSTSign	156

15.23. Структура AuthMethodPreshared	160
15.24. Структура IdentityEntry	161
15.25. Структура CertDescription	164
15.26. Формат задания DistinguishedName (GeneralNames) в LSP	167
15.27. Работа с сертификатами в LSP	169
15.28. Пример локальной политики безопасности	171
16. Специализированные команды	173
16.1. cert_mgr show	174
16.2. cert_mgr import	175
16.3. cert_mgr create	177
16.4. cert_mgr remove	178
16.5. cert_mgr check	179
16.6. key_mgr show	180
16.7. key_mgr import	181
16.8. key_mgr remove	182
16.9. lsp_mgr show	183
16.10. lsp_mgr load	184
16.11. lsp_mgr unload	185
16.12. lsp_mgr reload	186
16.13. if_mgr show	187
16.14. if_mgr add	188
16.15. if_mgr remove	189
16.16. dp_mgr show	190
16.17. dp_mgr set	191
16.18. log_mgr set	192
16.19. log_mgr show	193
16.20. sa_show	194
16.21. klogview	196
16.21.1.События группы pass и drop	198
16.21.2.События группы filt_trace	201
16.21.3.События группы sa_minor, sa_major	201
16.21.4.События группы sa_trace	203
16.21.5.События группы sa_error	203
16.22. Сообщения об ошибках	204
17. Протоколирование событий	208
17.1. Текущие настройки	208
17.2. Общие настройки	208

17.3. Действие текущих и общих настроек	208
17.4. Получение лога в Windows	209
17.5. Настройки Syslog сервера для получения лога в Solaris	209
17.6. Список протоколируемых событий	209
17.6.1.Список ошибок протокола ISAKMP	222
17.6.2.Список выполняемых действий по протоколу ISAKMP	224
18. Мониторинг	231
18.1. Выдача статистики	231
18.2. Трап-сообщения	242
19. Приложение	245
19.1. Утилита make_inst.exe	246
19.2. Сообщения об ошибках утилиты make_inst.exe	253
19.3. Создание сертификата конечного устройства с использованием "Signal-COM CSP"	256
19.3.1.Установка "Signal-COM CSP"	256
19.3.2.Установка и настройка Удостоверяющего Центра. Создание CA сертификата	260
19.3.3.Установка "Admin-PKI"	272
19.3.4.Создание ключевой пары и запроса на сертификат конечного устройства	275
19.3.5.Создание сертификата конечного устройства	279



Лицензионное Соглашение

о праве пользования Продуктом CSP VPN ServerB производства ЗАО "С-Терра СиЭсПи"

© 2003 - 2009 ЗАО "С-Терра СиЭсПи". Все права защищены.

Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного Продукта CSP VPN ServerB (далее - Изделия) Конечным Пользователем (физическим или юридическим лицом, указанным в Лицензии на использование Продукта, являющейся неотъемлемой частью настоящего Лицензионного Соглашения). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных непередаваемых прав пользования Изделием.

Под Изделием понимается комплекс материальных объектов (программных средств, носителей информации, кода программных Продуктов, документации в печатной и электронной формах), состав которых определяется артикулом из прайс-листа ЗАО «С-Терра СиЭсПи».

Изделие может использоваться только в качестве Агента защиты специализированных устройств в составе платежных систем: банкоматов, расчетных терминалов, кассовых аппаратов (POS-терминалов) и датчиков автоматизированных систем управления технологическими процессами и не предназначено для использования в других целях. Использование Изделия в прочих системах и/или в иных целях является нарушением настоящего Лицензионного Соглашения.

Изделие может включать компоненты (программные средства, информационные носители и прочее) от третьих поставщиков. Конечный Пользователь получает права на использование этих компонент на основе Лицензий и Лицензионных Соглашений этих поставщиков, которые являются в совокупности неотъемлемой частью настоящего Лицензионного Соглашения.

Изделие в полном комплекте передается Конечному Пользователю на условиях настоящего Лицензионного Соглашения.

Изделие и его компоненты являются интеллектуальной собственностью Производителя и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Российской Федерации об авторском и имущественном праве на объекты интеллектуальной собственности.

Установка Изделия после предъявления Конечному Пользователю текста Лицензионного Соглашения рассматривается как согласие Конечного Пользователя с условиями Лицензионного Соглашения и вступление его в законную силу, после чего настоящее Лицензионное Соглашение в соответствии со ст. 433 ГК РФ имеет силу договора между Конечным Пользователем и Производителем Изделия (ЗАО «С-Терра СиЭсПи»).

При наличии компонент третьих поставщиков Производитель является законным и полномочным представителем третьих поставщиков, если обратное не оговорено в Лицензионных Соглашениях третьих поставщиков или в других документах, регламентирующих отношения между Конечным Пользователем и третьими поставщиками.

Все компоненты третьих поставщиков объединяются в программный Продукт (комплекс) в процессе установки Изделия. Конечный Пользователь имеет право на копирование, установку и эксплуатацию всех компонент третьих поставщиков, поставленных в составе Изделия только в составе работ, связанных с эксплуатацией Изделия. Копирование, распространение, установка и эксплуатация отдельных компонент являются нарушением настоящего Лицензионного Соглашения и авторских прав как Производителя, так и третьих поставщиков (если обратное не оговорено в Лицензиях и Лицензионных Соглашениях третьих поставщиков).

Конечный Пользователь может устанавливать и использовать в рамках настоящего Лицензионного Соглашения только один экземпляр Изделия и не имеет права устанавливать и использовать большее количество экземпляров Изделия.

Конечный Пользователь не имеет права распространять Изделие в формах предоставления доступа третьим лицам к воспроизведению или к воспроизведенным в любой форме компонентам Изделия путем продажи, проката, сдачи внаем, предоставления займа или иными другими способами отчуждения.

Конечный Пользователь не имеет права дисассемблировать, декомпилировать (преобразовывать бинарный код в исходный текст) программы и другие компоненты Изделия, вносить какие-либо изменения в бинарный код программ и совершать относительно Изделия другие действия, нарушающие Российские и международные нормы по авторскому праву и использованию программных средств.

Настоящее Лицензионное Соглашение вступает в силу с момента установки Изделия и действует на протяжении всего срока использования Изделия.

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" и преследуется по закону.

Настоящее Лицензионное Соглашение предоставляет Конечному Пользователю Ограниченные гарантии, состоящие в том, что

1. В случае, если в ходе эксплуатации Изделия Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Изделия (ЗАО «С-Терра СиЭсПи») обеспечивает:

а) информирование доступными способами Конечного Пользователя о существовании Критичной Проблемы и о способах ее устранения

б) бесплатное предоставление обновлений программного обеспечения Производителя Изделия, в которых устранены Критичные Проблемы.

Примечание 1. Гарантийное обязательство 1 базируется на следующем определении: Критичная Проблема заключается в том, что Изделие, вследствие ошибки в программном обеспечении, не выполняет основные функции безопасности, а именно шифрование трафика и контроль доступа, что приводит к нарушению безопасности сети Конечного Пользователя.

Примечание 2. Обновления программного обеспечения в соответствии с гарантийным обязательством п.1б предоставляются по запросу Конечного Пользователя и по мере разработки обновлений.

2. Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки Изделия дефекты в составе информационных носителей или некомплектность Изделия, то информационные носители будут заменены, а комплектность Изделия восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности изделия и/или дефектам носителей информации рассматриваться не будут.

Настоящее Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию Изделия любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Изделия и его компонент в установленном порядке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

Настоящее Лицензионное Соглашение (в рамках законодательства Российской Федерации и если противное не оговорено в виде отдельного дополнительного соглашения с Конечным Пользователем) не регламентирует вопросы технических, организационных и прочих возможных проблем, связанных с эксплуатацией Изделия и возможных материальных, финансовых и прочих потерь Конечного Пользователя в результате эксплуатации Изделия.

Срок действия настоящего Лицензионного Соглашения распространяется на весь период эксплуатации Изделия Конечным Пользователем. Действие настоящего Лицензионного Соглашения может быть прекращено по решению Конечного Пользователя. В этом случае Конечный Пользователь должен уничтожить все информационные носители, содержащие код и прочие информационные компоненты Изделия, включая информацию на внутренних носителях Изделия. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

Программный Продукт Системная Библиотека GNU libc является свободно распространяемым Продуктом и используется в составе Изделия без каких либо модификаций в соответствии с лицензией "The GNU General Public License" (<http://www.gnu.org/licenses/licenses.html>).

MS-DOS, Windows, Windows 98/NT/2000/XP/Vista являются торговыми марками компании Microsoft Corporation в США и в других странах.

Sun Solaris и Java являются торговыми марками компании Sun Microsystems, Inc в США и в других странах.

Cisco, Cisco PIX Firewall, Cisco IOS Router, CiscoWorks, CiscoWorks VPN/Security Management Solution, CiscoWorks Management Center for VPN Routers, CiscoWorks Management Center for PIX Firewall являются торговыми марками компании Cisco Systems в США и в других странах.

Изделие включает в себя программное обеспечение, написанное Эриком Янгом (Eric Young, eay@cryptsoft.com)

Другие названия компаний и Продуктов, упомянутые в настоящем Лицензионном Соглашении и в составе информационных источников Изделия могут являться зарегистрированными торговыми марками соответствующих им компаний. Упоминание наименований, Продуктов, торговых марок третьих организаций исключительно неформально и не является ни поддержкой, рекомендацией либо рекламой. ЗАО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.

Напечатано в Российской Федерации

Закрытое Акционерное Общество «С-Терра СиЭсПи»

124498, г. Москва, Зеленоград, проезд 4806, д.5, стр.20

Телефон: +7 (499) 720-6928

Факс: +7 (499) 720-6928

Эл.почта: information@s-terra.com

<http://www.s-terra.com>



Лицензионное Соглашение

о праве пользования Продуктом

CSP VPN Server

производства ЗАО "С-Терра СиЭсПи"

© 2003 - 2009 ЗАО "С-Терра СиЭсПи". Все права защищены.

Настоящее Лицензионное Соглашение определяет условия использования законно приобретенного Продукта CSP VPN Server (далее - Изделия) Конечным Пользователем (физическим или юридическим лицом, указанным в Лицензии на использование Продукта, являющейся неотъемлемой частью настоящего Лицензионного Соглашения). Предметом настоящего Лицензионного Соглашения является возмездная передача Конечному Пользователю неисключительных непередаваемых прав пользования Изделием.

Под Изделием понимается комплекс материальных объектов (программных средств, носителей информации, кода программных Продуктов, документации в печатной и электронной формах), состав которых определяется артикулом из прайс-листа ЗАО «С-Терра СиЭсПи».

Изделие может использоваться только в качестве Агента защиты автономного сервера и не предназначено для использования в других целях. Использование Изделия в прочих системах и/или в иных целях является нарушением настоящего Лицензионного Соглашения.

Изделие может включать компоненты (программные средства, информационные носители и прочее) от третьих поставщиков. Конечный Пользователь получает права на использование этих компонент на основе Лицензий и Лицензионных Соглашений этих поставщиков, которые являются в совокупности неотъемлемой частью настоящего Лицензионного Соглашения.

Изделие в полном комплекте передается Конечному Пользователю на условиях настоящего Лицензионного Соглашения.

Изделие и его компоненты являются интеллектуальной собственностью Производителя и, при наличии третьих поставщиков, интеллектуальной собственностью третьих поставщиков и защищаются законодательством Российской Федерации об авторском и имущественном праве на объекты интеллектуальной собственности.

Установка Изделия после предъявления Конечному Пользователю текста Лицензионного Соглашения рассматривается как согласие Конечного Пользователя с условиями Лицензионного Соглашения и вступление его в законную силу, после чего настоящее Лицензионное Соглашение в соответствии со ст. 433 ГК РФ имеет силу договора между Конечным Пользователем и Производителем Изделия (ЗАО «С-Терра СиЭсПи»).

При наличии компонент третьих поставщиков Производитель является законным и полномочным представителем третьих поставщиков, если обратное не оговорено в Лицензионных Соглашениях третьих поставщиков или в других документах, регламентирующих отношения между Конечным Пользователем и третьими поставщиками.

Все компоненты третьих поставщиков объединяются в программный Продукт (комплекс) в процессе установки Изделия. Конечный Пользователь имеет право на копирование, установку и эксплуатацию всех компонент третьих поставщиков, поставленных в составе Изделия только в составе работ, связанных с эксплуатацией Изделия. Копирование, распространение, установка и эксплуатация отдельных компонент являются нарушением настоящего Лицензионного Соглашения и авторских прав как Производителя, так и третьих поставщиков (если обратное не оговорено в Лицензиях и Лицензионных Соглашениях третьих поставщиков).

Конечный Пользователь может устанавливать и использовать в рамках настоящего Лицензионного Соглашения только один экземпляр Изделия и не имеет права устанавливать и использовать большее количество экземпляров Изделия.

Конечный Пользователь не имеет права распространять Изделие в формах предоставления доступа третьим лицам к воспроизведению или к воспроизведенным в любой форме компонентам Изделия путем продажи, проката, сдачи внаем, предоставления взаймы или иными другими способами отчуждения.

Конечный Пользователь не имеет права дисасемблировать, декомпилировать (преобразовывать бинарный код в исходный текст) программы и другие компоненты Изделия, вносить какие-либо изменения в бинарный код программ и совершать относительно Изделия другие действия, нарушающие Российские и международные нормы по авторскому праву и использованию программных средств.

Настоящее Лицензионное Соглашение вступает в силу с момента установки Изделия и действует на протяжении всего срока использования Изделия.

Неисполнение требований настоящего Лицензионного Соглашения является нарушением Закона Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" и преследуется по закону.

Настоящее Лицензионное Соглашение предоставляет Конечному Пользователю Ограниченные гарантии, состоящие в том, что

1. В случае, если в ходе эксплуатации Изделия Конечным Пользователем или любым третьим лицом будет обнаружена Критичная Проблема, Производитель Изделия (ЗАО «С-Терра СиЭсПи») обеспечивает:

- а) информирование доступными способами Конечного Пользователя о существовании Критичной Проблемы и о способах ее устранения
- б) бесплатное предоставление обновлений программного обеспечения Производителя Изделия, в которых устранены Критичные Проблемы.

Примечание 1. Гарантийное обязательство 1 базируется на следующем определении: Критичная Проблема заключается в том, что Изделие, вследствие ошибки в программном обеспечении, не выполняет основные функции безопасности, а именно шифрование трафика и контроль доступа, что приводит к нарушению безопасности сети Конечного Пользователя.

Примечание 2. Обновления программного обеспечения в соответствии с гарантийным обязательством п.1б предоставляются по запросу Конечного Пользователя и по мере разработки обновлений.

3. Если Конечный Пользователь обнаружит в течение 90 (девяноста) дней со дня поставки Изделия дефекты в составе информационных носителей или некомплектность Изделия, то информационные носители будут заменены, а комплектность Изделия восстановлена. По истечении 90 дней претензии Конечного Пользователя по некомплектности изделия и/или дефектам носителей информации рассматриваться не будут.

Настоящее Лицензионное Соглашение не содержит никаких гарантий по поставке, функциональности и соответствию Изделия любым техническим требованиям, стандартам и условиям. Эти вопросы относятся к области лицензирования деятельности поставщика, сертификации Изделия и его компонент в установленном порядке, договоров о поставке, техническом сопровождении и технической поддержке и регламентируются в рамках отдельных документов.

Настоящее Лицензионное Соглашение (в рамках законодательства Российской Федерации и если противное не оговорено в виде отдельного дополнительного соглашения с Конечным Пользователем) не регламентирует вопросы технических, организационных и прочих возможных проблем, связанных с эксплуатацией Изделия и возможных материальных, финансовых и прочих потерь Конечного Пользователя в результате эксплуатации Изделия.

Срок действия настоящего Лицензионного Соглашения распространяется на весь период эксплуатации Изделия Конечным Пользователем. Действие настоящего Лицензионного Соглашения может быть прекращено по решению Конечного Пользователя. В этом случае Конечный Пользователь должен уничтожить все информационные носители, содержащие код и прочие информационные компоненты Изделия, включая информацию на внутренних носителях Изделия. Прекращение действия Лицензионного Соглашения по инициативе Конечного Пользователя является односторонней добровольной акцией Конечного Пользователя и не является предметом для взаиморасчетов и других хозяйственных операций.

Программный Продукт Системная Библиотека GNU libc является свободно распространяемым Продуктом и используется в составе Изделия без каких либо модификаций в соответствии с лицензией "The GNU General Public License" (<http://www.gnu.org/licenses/licenses.html>).

MS-DOS, Windows, Windows 98/NT/2000/XP/Vista являются торговыми марками компании Microsoft Corporation в США и в других странах.

Sun Solaris и Java являются торговыми марками компании Sun Microsystems, Inc в США и в других странах.

Cisco, Cisco PIX Firewall, Cisco IOS Router, CiscoWorks, CiscoWorks VPN/Security Management Solution, CiscoWorks Management Center for VPN Routers, CiscoWorks Management Center for PIX Firewall являются торговыми марками компании Cisco Systems в США и в других странах.

Изделие включает в себя программное обеспечение, написанное Эриком Янгом (Eric Young, eay@cryptsoft.com)

Другие названия компаний и Продуктов, упомянутые в настоящем Лицензионном Соглашении и в составе информационных источников Изделия могут являться зарегистрированными торговыми марками соответствующих им компаний. Упоминание наименований, Продуктов, торговых марок третьих организаций исключительно неформально и не является ни поддержкой, рекомендацией либо рекламой. ЗАО «С-Терра СиЭсПи» не несет какой-либо ответственности в отношении работоспособности и использования этих Продуктов.

Напечатано в Российской Федерации

Закрытое Акционерное Общество «С-Терра СиЭсПи»

124498, г. Москва, Зеленоград, проезд 4806, д.5, стр.20

Телефон: +7 (499) 720-6928

Факс: +7 (499) 720-6928

Эл.почта: information@s-terra.com

<http://www.s-terra.com>

1. Комплект поставки

В комплект поставки CSP VPN Server входят:

- компакт-диск, на котором записаны:
 - дистрибутив CSP VPN Server 3.0 – каталог Server_SC
 - документация – каталог PDF:
 - Руководство администратора – CSP_VPN_Server_Admin_Guide_sc.pdf
- Лицензия на использование программного продукта CSP VPN Server версии 3.0
- Лицензия на использование программного продукта криптоплагин версии 2.1.0.2 (на основе СКЗИ «Крипто-Ком 3.2») компании «Сигнал-КОМ».

2. Назначение и функции Продукта

Продукт CSP VPN Server предназначен для защиты и фильтрации трафика протоколов семейства TCP/IP.

Защита трафика осуществляется в рамках международных стандартов IKE/IPSec:

- Security Architecture for the Internet Protocol – RFC2401
- IP Authentication Header (AH) – RFC2402
- IP Encapsulating Security Payload (ESP) – RFC2406
- Internet Security Association and Key Management Protocol (ISAKMP) – RFC2408
- The Internet Key Exchange (IKE) – RFC2409
- The Internet IP Security Domain of Interpretation for ISAKMP (DOI) – RFC2407.

Программный Продукт CSP VPN Server обеспечивает:

- защиту трафика на уровне аутентификации/шифрования сетевых пакетов по протоколам IPSec AH и/или IPSec ESP
- аутентификацию конечного устройства и аутентификацию узла сети
- пакетную фильтрацию трафика с использованием информации в полях заголовков сетевого и транспортного уровней
- событийное протоколирование и сбор статистики
- реализацию заданной дисциплины взаимодействия (аутентификацию и/или защиту трафика) для каждого защищенного соединения, доступ в заданном защищенном режиме только для зарегистрированных, в том числе и для мобильных партнеров по взаимодействию
- регулируемую стойкость защиты трафика.

Все эти функции описываются в файле локальной политики безопасности (LSP- Local Security Policy). Локальная политика безопасности определяет какие из сетевых соединений следует защищать, а какие следует использовать открытыми, какие режимы и алгоритмы защиты использовать для каждого из соединений.

Продукт CSP VPN Server использует в качестве внешней криптографической библиотеки средство криптографической защиты информации (СКЗИ) "Крипто-КОМ 3.2", разработанное компанией "Сигнал-КОМ".

СКЗИ "Крипто-КОМ 3.2" реализует российские криптографические алгоритмы:

- **ГОСТ 28147-89** – шифрование/расшифрование данных
- **ГОСТ Р 34.11-94 НМАС** – целостность данных
- **ГОСТ Р 34.11-94** – алгоритм хеширования
- **ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001** – формирование и проверку электронно-цифровой подписи (ЭЦП)
- генерацию случайных чисел.

CSP VPN Server является Продуктом для корпоративного использования в том смысле, что политику и настройки режимов этого Продукта осуществляет системный администратор или администратор безопасности предприятия.

3. Требования на базовые платформы и совместимость

Продукт CSP VPN Server выпущен для следующих базовых платформ:

- MS Windows Vista (32-bit) Business SP1 Russian Edition
- MS Windows XP Professional SP2 Russian Edition.

Продукт совместим с криптографическими плагинами "Крипто-КОМ 3.2", разработанными компанией "Сигнал-КОМ".

Продукт работает корректно на компьютерах с сетевыми адаптерами, которые поддерживают "task offloading".

В части реализации протоколов IPsec/IKE и их расширений Продукт совместим с Cisco IOS v.12.4.

В части удаленного мониторинга и сбора статистики управления Продукт совместим с CiscoWorks Monitoring Center for Performance 2.0.2, входящим в состав CiscoWorks VMS 2.3.

Продукт совместим с токенами eToken PRO 32k, eToken PRO 64k производства компании Aladdin.

4. Три режима управления сервером

Для управления локальной политикой безопасности и настройками CSP VPN Server администратору предоставляется три режима:

- создание политики безопасности и настроек с помощью графического интерфейса `pkg_maker.exe`. Результатом является инсталляционный пакет
- формирование политики безопасности в виде текстового конфигурационного файла, и создание инсталляционного пакета с помощью утилиты командной строки `make_inst.exe`.
- создание политики безопасности в виде текстового конфигурационного файла, загрузка его и задание настроек с помощью Специализированных команд.

Создание инсталляционного пакета с помощью утилиты командной строки `make_inst.exe` и графического интерфейса описано в главах 5-10.

Создание политики безопасности в виде текстового конфигурационного файла описано в главе ["Создание локальной политики безопасности. Конфигурационный файл"](#).

Для третьего режима загрузка конфигурационного файла на хост, регистрация сертификатов и предустановленных ключей, задание настроек осуществляется с помощью [Специализированных команд](#).

Продукт CSP VPN Server позволяет создавать для разных интерфейсов разные правила (фильтрации, шифрования) – в этом заключается его отличие от продукта CSP VPN Client, который задает одни и те же правила для всех интерфейсов.

5. Процесс подготовки инсталляционного пакета для конечного устройства

Продукт CSP VPN Server предназначен для виртуальных корпоративных сетей.

CSP VPN Server разработан таким образом, что администратор безопасности корпоративной сети формирует инсталляционный пакет для конечного устройства (компьютер, на котором будет установлен CSP VPN Server).

Процесс подготовки инсталляционного пакета производится следующим образом.

- Администратор безопасности получает административный пакет в виде отдельного Продукта, размещенного в каталоге Server_SC поставляемого диска. Администратор устанавливает на своем компьютере административный пакет, с помощью которого и создает инсталляционный пакет для конечного устройства.

Используя предустановленные ключи либо сертификаты открытых ключей, корневой сертификат Удостоверяющего Центра и локальную политику безопасности, предписанную для конечного устройства, администратор готовит инсталляционный пакет.

Создание инсталляционного пакета осуществляется одним из двух способов:

- использование графического интерфейса
- использование утилиты командной строки `make_inst.exe`.

Использование графического интерфейса для определения локальной политики безопасности, локальных настроек и создания инсталляционного пакета с использованием сертификатов открытых ключей либо предустановленных (разделяемых) ключей (Preshared Keys) описано в главе ["Подготовка инсталляционного пакета с помощью графического интерфейса"](#).

Для создания инсталляционного пакета используется технология One Click Installation, которая реализуется с помощью утилиты командной строки `make_inst.exe`. Эта утилита описана в Приложении ["Утилита make_inst.exe"](#).

Технологические процессы формирования инсталляционного пакета с использованием сертификатов открытых ключей или предустановленных (разделяемых) ключей (Preshared Keys) и утилиты `make_inst.exe` описаны в главах ["Подготовка инсталляционного пакета с предустановленными ключами \(Preshared Keys\)"](#) и ["Два сценария подготовки инсталляционного пакета с открытыми ключами \(сертификатами\)"](#), соответственно.

Перед использованием утилиты `make_inst.exe` должна быть создана и записана в файл в текстовом формате локальная политика безопасности. Создание конфигурационного файла описано в главе ["Создание локальной политики безопасности. Конфигурационный файл"](#).

Администратор, используя подготовленный инсталляционный пакет, производит установку Продукта CSP VPN Server на конечное устройство.

6. Подготовка рабочего места администратора безопасности

Администратор безопасности на своем компьютере устанавливает с диска с дистрибутивом административный пакет CSP VPN Server AdminTool (sc), размещенный в каталоге Server_sc. В состав дистрибутива этого пакета входит:

- `setup.exe` – утилита запуска Windows Installer
- `setup.ini` – настроечный файл, необходимый для `setup.exe`
- `sysdlls.cab` – хранилище системных DLL
- `version.txt` – текстовый файл, содержащий версию Продукта
- `VPN_SERVER_ADMIN.msi` – MSI-база инсталлятора (MSI – MicroSoft Installer)
- `VPN_SERVER_ADMIN.cab` – хранилище файлов

Инсталляция административного пакета запускается командой `setup.exe` с дистрибутива.

При запуске инсталляции административного пакета появляется окно визарда с приглашением к инсталляции:

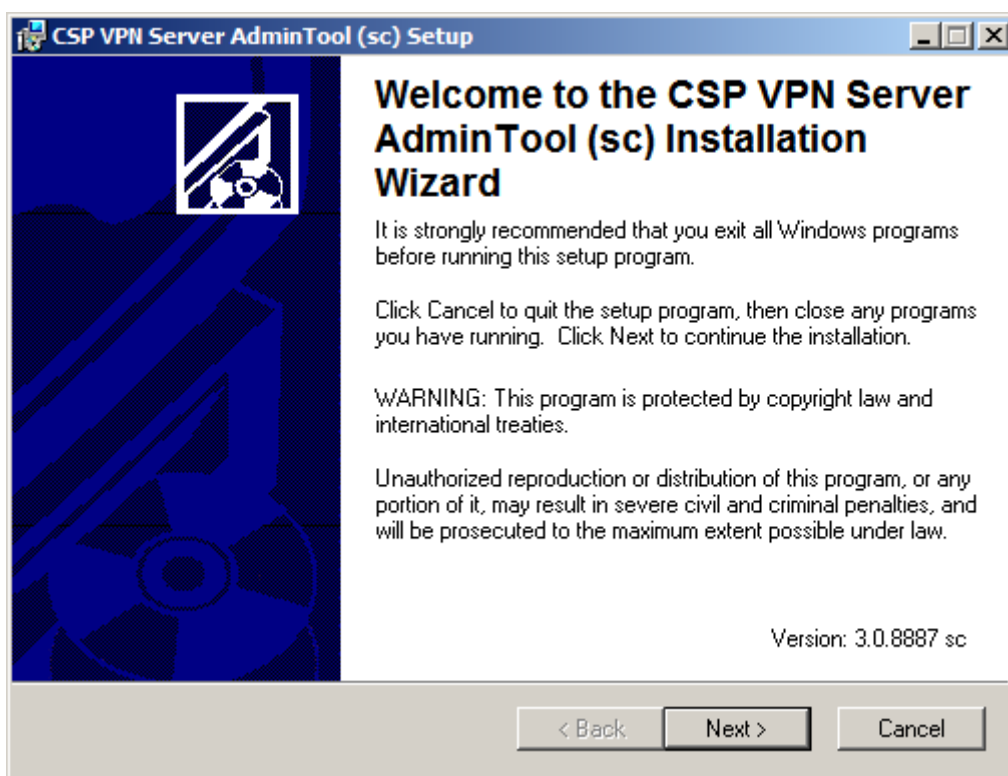


Рисунок 1

В окне с текстом Лицензионных Соглашений на CSP VPN ServerB и CSP VPN Server после установки переключателя в положение "I accept the license agreement" кнопка `Next` становится доступной:

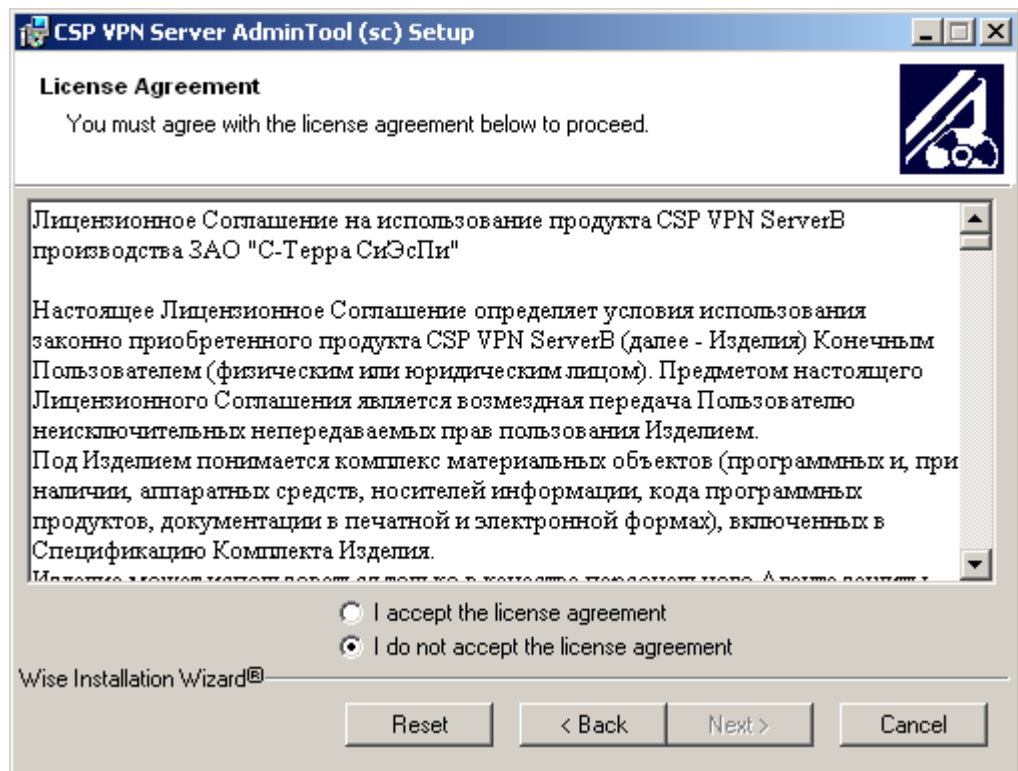


Рисунок 2

Выбрать папку, в которую будет установлен административный пакет, нажав на кнопку Browse:

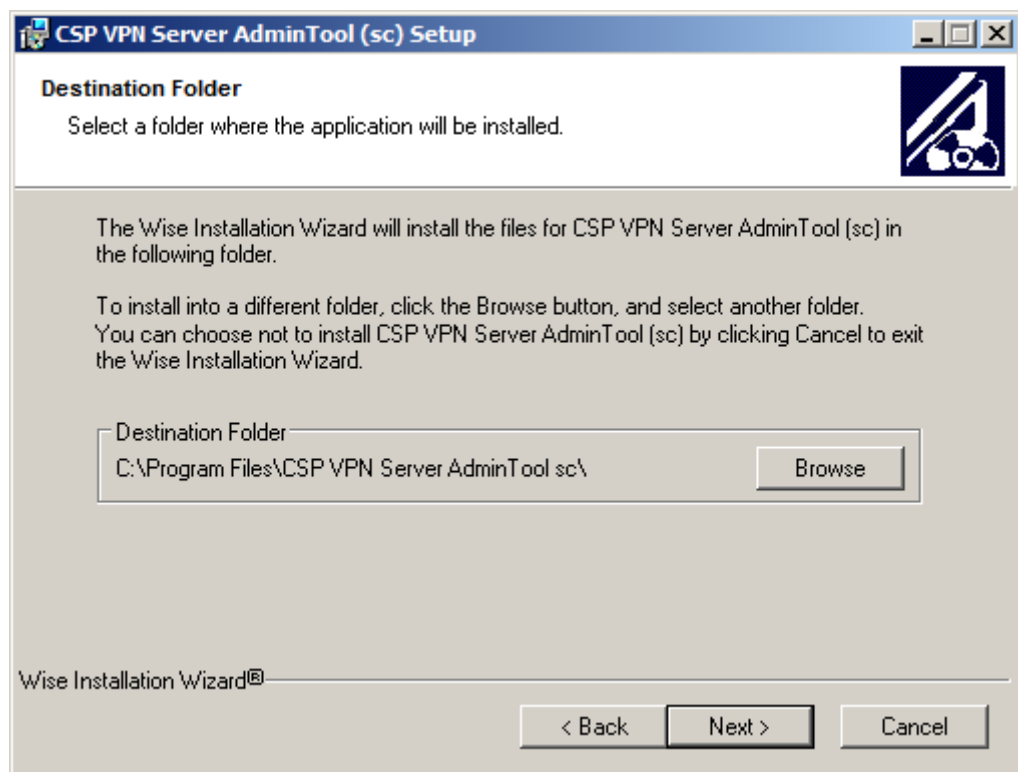


Рисунок 3

Для начала процесса инсталляции нажать кнопку Next:

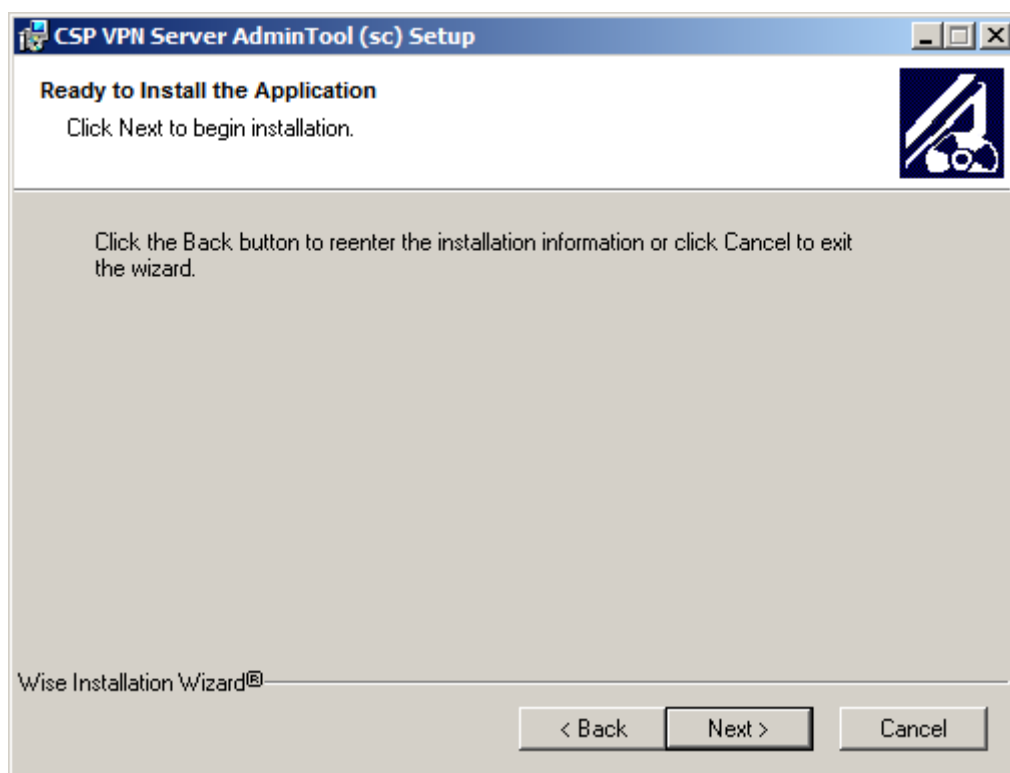


Рисунок 4

Индикатор процесса инсталляции:

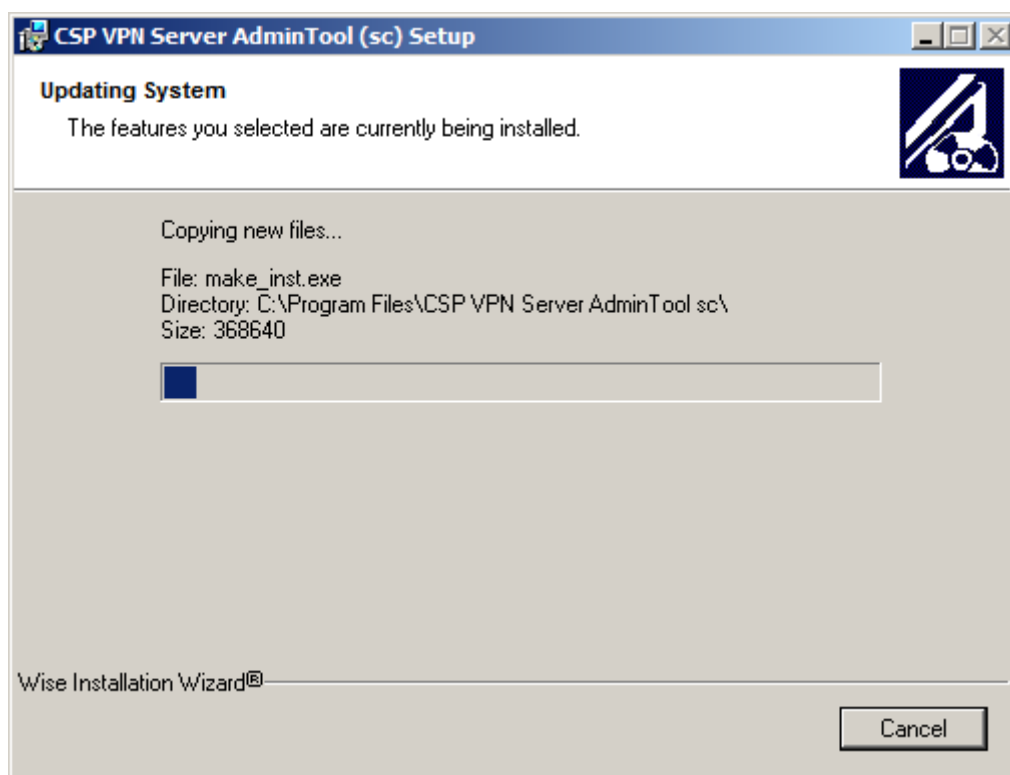


Рисунок 5

Инсталляция завершена, нажать кнопку **Finish**:

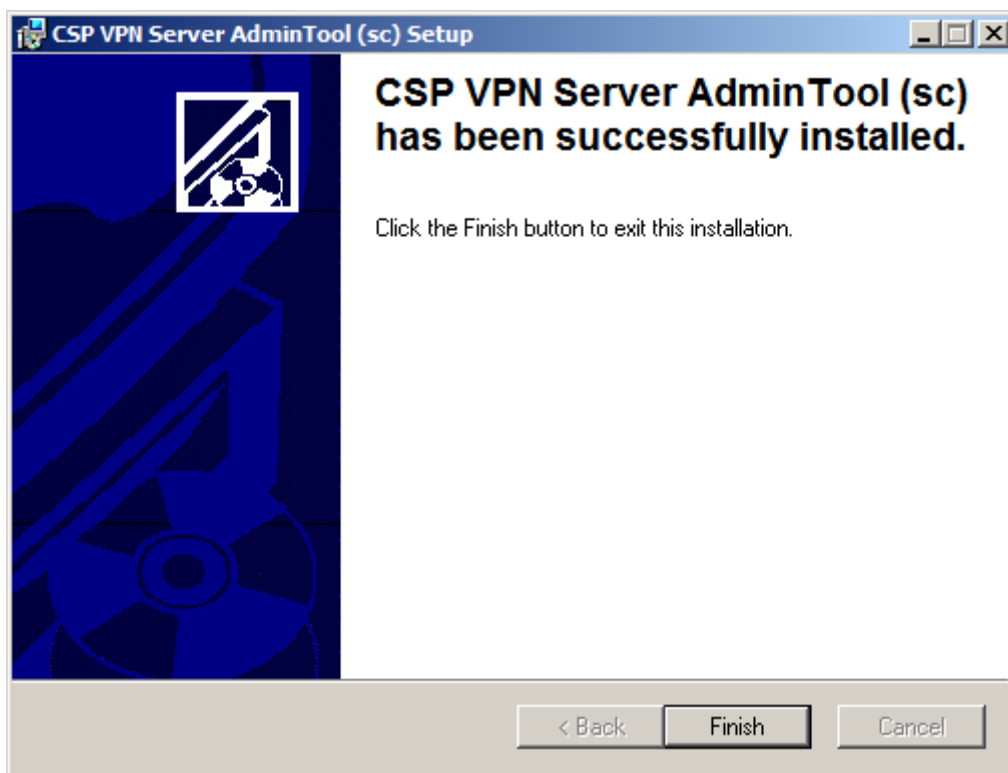


Рисунок 6

Установленный административный пакет состоит из следующих папок и файлов:

Корневая папка:

- `make_inst.exe` – утилита командной строки для создания инсталляционного файла и локальных настроек
- `pkg_maker.exe` – утилита графического интерфейса для создания локальной политики, локальных настроек и инсталляционного файла, которая вызывает утилиту `make_inst.exe`
- `version.txt` – текстовый файл, содержащий версию Продукта
- вспомогательные файлы (`dll`, `ini`) для обеспечения работы утилит.

Папка `Agent` содержит основные файлы инсталлятора:

- `VPN_SERVER_WIN2K.msi` – MSI-база инсталлятора (MSI – MicroSoft Installer)
- `VPN_SERVER_WIN2K.cab` – хранилище файлов сервера
- `sysdlls.cab` – хранилище системных DLL.

Папка `SFX` содержит:

- служебные файлы, необходимые для сборки SFX-архива (execution stub и прототипы comment, задающие параметры для распаковки SFX-архива)

Системная папка `system32` содержит файлы криптографической библиотеки "Крипто-КОМ 3.2":

- `sc_gost.dll`
- `sccrypto.dll`
- `etsdk.dll` и др.

7. Атрибуты аутентификации

Технология IPSec обеспечивает аутентификацию, шифрование и целостность данных на уровне передаваемых IP пакетов.

Для реализации этих функций технологии IPSec необходима дополнительная информация, которая поставляется протоколом IKE: ключевой материал и согласованная политика защиты.

Для аутентификации взаимодействующих сторон протоколу IKE необходима некоторая аутентификационная информация.

Такой аутентификационной информацией может быть:

- предустановленный (разделяемый) ключ (Preshared Key)
- сертификат стандарта X.509.

Имеются некоторые ограничения при работе с расширениями сертификата (Extensions), которые помечены как критичные. В таблице приведен список расширений сертификата, которые будут распознаваться и обрабатываться Продуктом, если у них установлен признак критичности TRUE. Если в сертификате будут присутствовать другие расширения, не указанные в таблице и заданные как критичные, то такой сертификат не может быть использован. Если же расширение отсутствует в таблице, но является некритичным, то оно игнорируется, и сертификат используется.

Name	OID value
Subject Key Identifier	2.5.29.14
Key Usage	2.5.29.15
Subject Alternative Name	2.5.29.17
Issuer Alternative Name	2.5.29.18
Basic Constraints	2.5.29.19
Name Constraints	2.5.29.30
CRL Distribution Points	2.5.29.31
Authority Key Identifier	2.5.29.35

Описания значений и полный список Certificate Extensions можно посмотреть в документе RFC 5280 (<http://tools.ietf.org/html/rfc5280#section-4.2>).

8. Подготовка инсталляционного пакета с предустановленными ключами (Preshared Keys) с помощью утилиты `make_inst`

Ключ – произвольная последовательность байтов. Ключ может быть записан в файл.

Создать предустановленный (разделяемый) ключ (Preshared Key) можно разными способами. Самый простой – записать в файл любую произвольную последовательность символов.

Имя ключа – идентификатор, состоящий из латинских букв, цифр, символов `"_"` и `"-"`, и должен начинаться с латинской буквы или символа `"_"`. Например, `key1`.

Примечание: Если предустановленный ключ задан несколькими строками, то каждый перенос в теле ключа будет представлен двумя символами `0x0D 0x0A` (символ возврата и перевода каретки) и тогда при подготовке предустановленного ключа для партнера должны быть использованы эти символы.

Имя предустановленного ключа используется:

- при подготовке инсталляционного пакета для конечного устройства
- при создании локальной политики безопасности (LSP) – в структуре `AuthMethodPreshared` в атрибуте `SharedIKESecret`.

Создание инсталляционного пакета для конечного устройства осуществляется в несколько этапов:

- администратор безопасности создает предустановленный ключ
- администратор задает локальную политику безопасности для конечного устройства и записывает ее в файл (см. главу ["Создание локальной политики безопасности. Конфигурационный файл"](#) или ["Подготовка инсталляционного пакета с помощью графического интерфейса"](#))
- администратор на своем рабочем месте запускает команду `make_inst.exe` из каталога административного пакета. В противном случае будет выдано сообщение об ошибке. В опциях этой команды обязательно указывается имя инсталляционного файла, имя файла с LSP, имя предустановленного ключа, ключ или файл, в котором он размещен. Команда `make_inst.exe` в этом случае имеет следующие опции (подробно описана в Приложении ["Утилита `make\_inst.exe`"](#)):

```
make_inst.exe -o SFX_file_path -l LSP_file_path  
-kn <Preshared_key_name> {-kv <Preshared_key_val> |  
-kvf <file_path_Preshared_key_val>}
```

- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Server, локальные настройки, локальную политику безопасности. В данном случае подготовленный инсталляционный пакет состоит из одного инсталляционного файла.

9. Два сценария подготовки инсталляционного пакета с открытыми ключами (сертификатами) с помощью утилиты `make_inst`

Опишем два сценария подготовки инсталляционного пакета для конечного устройства с аутентификацией сторон на открытых ключах (сертификатах).

Секретный ключ, соответствующий открытому ключу сертификата конечного устройства, находится либо в контейнере, либо в файле. Контейнер имеет сложную структуру, в котором содержится служебная информация и какая-то ключевая информация, необходимая для обеспечения защиты и целостности ключа. Этот контейнер является каталогом файловой системы. Секретный ключ может быть расположен либо в контейнере, либо в файле, которые размещаются на жестком диске или внешнем ключевом носителе, например дискете, электронном ключе e-Token и др.

Сценарии отличаются тем, кто создает ключевую пару для локального сертификата и на каком ключевом носителе размещен контейнер и файл с секретным ключом, возможна или нет проверка соответствия сертификата и секретного ключа, копируется или нет контейнер с секретным ключом во время инсталляции на конечное устройство.

9.1. Первый сценарий

Все действия по созданию ключевой пары, формированию запроса и созданию сертификата конечного устройства производятся администратором СА. При этом контейнер и файл с секретным ключом размещаются на внешнем ключевом носителе, например дискете. В этом сценарии возможно включить контейнер и секретный ключ в инсталляционный файл, при этом будет проведена проверка соответствия сертификата конечного устройства и секретного ключа при создании инсталляционного файла. А при установке CSP VPN Server на конечное устройство можно скопировать контейнер и файл с секретным ключом с дискеты на другой ключевой носитель.

Опишем действия администратора безопасности по этому сценарию:

- администратор безопасности получает от администратора СА сертификат конечного устройства и корневой сертификат Удостоверяющего Центра (Trusted CA Certificate), экспортированные в файлы. Ему передается либо контейнер с секретным ключом либо контейнер и файл с секретным ключом на внешнем носителе
- администратор безопасности определяет для конечного устройства локальную политику безопасности (LSP) и записывает ее в файл (см. главу ["Создание локальной политики безопасности. Конфигурационный файл"](#))
- администратор безопасности на своем рабочем месте из командной строки запускает команду `make_inst.exe`. В опциях этой команды указывается имя инсталляционного файла, путь к локальному сертификату и СА сертификату, путь к файлу с LSP, имя контейнера и файла с секретным ключом на конечном устройстве, локальные настройки и др. В имени контейнера и файла с секретным ключом указывается полный путь к ним на конечном устройстве (в данном сценарии – дискета `a:\`):
- если при подготовке инсталляционного файла контейнер и файл с секретным ключом не включать в инсталляционный файл и не выполнять проверку соответствия сертификата конечного устройства и секретного ключа, но задать копирование контейнера и файла с секретным ключом при инсталляции CSP VPN Server, то в команде `make_inst.exe` указываются опции (подробно утилита описана в Приложении ["Утилита make_inst.exe"](#)):

```
make_inst.exe -o SFX_file_path -l LSP_file_path
-c CA_file_path
-u USER_cert_file_path
-uc USER_cert_container_name
-kf Secret_Key_Path
{[-skp Secret_Key_Password] |
[-skpf file_path_Secret_Key_Password]}
{[-up USER_cert_container_password] |
[-ufp file_path_USER_cert_container_password]}
-cs Source_USER_cert_container_name
-kfs Source_Secret_Key_Path
```

- если при подготовке инсталляционного файла будет производиться копирование контейнера и секретного ключа в инсталляционный файл, а также проверка соответствия сертификата и секретного ключа конечного устройства, то в команде `make_inst.exe` указываются опции:

```
-ucpkgcopy on
-chksecret on
-uac USER_cert_container_name_ADMIN
{[-uap USER_cert_container_password_ADMIN] |
[-uafp file_path_USER_cert_container_password_ADMIN]}
-kaf Secret_Key_Path_ADMIN
```


- существуют другие дополнительные опции, например, для протоколирования сообщений при инсталляции CSP VPN Server в файл C:\inst_client_log.txt указывается опция:

```
-a /l* C:\inst_client_log.txt /i
```

- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Server, локальные настройки, локальную политику безопасности, CA сертификат и сертификат конечного устройства со ссылкой местоположения контейнера и файла с секретным ключом на конечном устройстве либо контейнер и секретный ключ включены в инсталляционный файл. В результате инсталляционный пакет состоит либо из инсталляционного файла, контейнера и файла с секретным ключом конечного устройства на внешнем ключевом носителе, например, дискете либо из одного инсталляционного файла.

Все сообщения, выдаваемые программной утилитой `make_inst` в процессе ее работы, выводятся в файл `make_inst_log.txt` (при каждом создании инсталляционного файла `make_inst_log.txt` переписывается).

9.2. Второй сценарий

Создание ключевой пары и формирование запроса на локальный сертификат конечного устройства производятся администратором безопасности на конечном устройстве. При этом контейнер и файл с секретным ключом размещаются на жестком диске конечного устройства. В этом сценарии невозможна проверка соответствия сертификата конечного устройства и секретного ключа при создании инсталляционного файла, копирование контейнера и файла с секретным ключом с жесткого диска в этом случае не производится.

Действия администратора безопасности по этому сценарию следующие:

- администратор безопасности на конечном устройстве создает ключевую пару и формирует запрос на локальный сертификат конечного устройства. Созданный запрос посылается на сервер Удостоверяющего Центра сертификатов. При этом контейнер и файл с секретным ключом конечного устройства размещаются на жестком диске
- администратор СА на сервере удостоверяющего центра по полученному запросу создает локальный сертификат конечного устройства и экспортирует его в файл. Корневой сертификат Удостоверяющего Центра (Trusted CA Certificate) также экспортируется в файл. Администратор безопасности получает оба эти сертификата от администратора СА
- администратор безопасности определяет для конечного устройства локальную политику безопасности и записывает ее в файл (см. главу ["Создание локальной политики безопасности. Конфигурационный файл"](#))
- администратор безопасности на своем рабочем месте запускает команду `make_inst.exe`. В опциях этой команды указывается имя инсталляционного файла, путь к сертификату конечного устройства и СА сертификату, путь к файлу с LSP, имя контейнера и файла с секретным ключом на конечном устройстве, локальные настройки и др. В имени контейнера и файла с секретным ключом указывается полный путь к ним на конечном устройстве. В команде `make_inst.exe` указываются опции (подробно утилита описана в Приложении ["Утилита make_inst.exe"](#)):

```
make_inst.exe -o SFX_file_path -l LSP_file_path
-c CA_file_path
-u USER_cert_file_path
-uc USER_cert_container_name
-kf Secret_Key_Path
{[-skp Secret_Key_Password]}
[-skpf file_path_Secret_Key_Password]}
{[-up USER_cert_container_password] |
[-ufp file_path_USER_cert_container_password]}
```

существуют другие дополнительные опции, например, для протоколирования событий в файл `C:\inst_client_log.txt` при инсталляции CSP VPN Server указывается опция:

```
-a /l* C:\inst_client_log.txt /i
```

- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Server, локальные настройки, локальную политику безопасности, СА сертификат и сертификат конечного устройства со ссылкой местоположения контейнера и файла с секретным ключом конечного устройства. В результате инсталляционный пакет состоит из одного инсталляционного файла.

Все сообщения, выдаваемые программной утилитой `make_inst` в процессе ее работы, выводятся в файл `make_inst_log.txt` (при каждом создании инсталляционного файла `make_inst_log.txt` переписывается).

10. Создание нескольких инсталляционных пакетов одновременно

Для создания инсталляционных пакетов для большого числа конечных устройств одновременно предлагается использовать BAT-файлы, вызывающие в цикле утилиту `make_inst.exe`. Далее описаны несколько BAT-файлов типичных сценариев. На компьютере администратора должна быть создана специальная папка для файлов конечных устройств. В этой папке создаются подпапки, которые называются по имени конечных устройств. Например, папка `c:\vpn_Server`, в ней подпапки `c:\vpn_Server\alice` и `c:\vpn_Server\bob` (важно, чтобы не было посторонних подпапок). В этих подпапках лежит файл `localcert.crt`, а также для некоторых сценариев могут лежать файлы `ca.crt`, `lsp.txt` и `pwd.txt` (пароль на контейнер).

Сценарий 1. В этом сценарии контейнеры с секретными ключами конечных устройств имеют пустой пароль. Получаемые SFX-файлы кладутся в папки конечных устройств под именем `vpnclient.exe`. В папках конечных устройств лежат локальные сертификаты. Используется один CA сертификат и одна LSP для всех конечных устройств:

```
@echo off

SET TEMPLATE_DIR=c:\vpn_Server
SET MAKE_INST_PATH=D:\CSP VPN Server\make_inst.exe
SET CONTAINER_NAME=c:\container
SET LSP_PATH=c:\vpn_Server\lsp.txt
SET CA_PATH=c:\vpn_Server\ca.crt

for /r %TEMPLATE_DIR% /d %%i in (*) do (%MAKE_INST_PATH% -o
%%i\vpnServer.exe -c %CA_PATH% -u %%i\localcert.crt -uc
%CONTAINER_NAME% -l %LSP_PATH%) & (if errorlevel 1 goto err)

goto :end

:err

echo An error occurred
exit

:end

echo Make installations complete
```

Используются следующие настройки:

`TEMPLATE_DIR` – папка, в которой лежат подпапки конечных устройств. Путь должен быть без пробелов.

MAKE_INST_PATH – путь к утилите make_inst.exe.

CONTAINER_NAME – имя контейнера.

LSP_PATH – путь к общей LSP.

CA_PATH – путь к общему CA сертификату.

Здесь и далее фраза в конце "Make installations complete" обозначает успешное завершение, а "An error occurred" – что произошла ошибка.

Сценарий 2. Используется общий пароль для всех контейнеров с секретными ключами всех конечных устройств. Получаемые SFX-файлы кладутся в папки конечных устройств под именем vpnServer.exe. Каждое конечное устройство имеет свой CA сертификат и свою LSP:

```
@echo off

SET TEMPLATE_DIR=c:\vpn_Server
SET MAKE_INST_PATH=D:\CSP VPN Server\make_inst.exe
SET CONTAINER_NAME=c:\container
SET CONTAINER_PASSWORD=somepwd

for /r %TEMPLATE_DIR% /d %%i in (*) do (%MAKE_INST_PATH% -o
%%i\vpnServer.exe -c %%i\ca.crt -u %%i\localcert.crt -uc
%CONTAINER_NAME% -up %CONTAINER_PASSWORD% -l %%i\lsp.txt) & (if
errorlevel 1 goto err)

goto :end

:err

echo An error occurred
exit

:end

echo Make installations complete
```

Новые настройки:

CONTAINER_PASSWORD – общий пароль.

Сценарий 3. Все условия аналогичны сценарию 2, но получаемые файлы кладутся в одну папку с именами username.exe (где username совпадает с именем подпапки конечного устройства, например alice.exe или bob.exe):

```
@echo off

SET TEMPLATE_DIR=c:\vpn_Server
SET MAKE_INST_PATH=D:\CSP VPN Server\make_inst.exe
SET CONTAINER_NAME=c:\container
SET CONTAINER_PASSWORD=somepwd
SET SFX_DIR=c:\sfx
```

```
cd %TEMPLATE_DIR%

for /d %%i in (*) do (%MAKE_INST_PATH% -o %SFX_DIR%\%%i.exe -c
%%~fi\ca.crt -u %%~fi\localcert.crt -uc %CONTAINER_NAME% -up
%CONTAINER_PASSWORD% -l %%~fi\lsp.txt) & (if errorlevel 1 goto
err)

goto :end

:err

echo An error occurred
exit

:end

echo Make installations complete
```

Здесь SFX_DIR – папка, в которую кладутся получаемые файлы.

Сценарий 4. Выполняется при тех же условиях, что и в сценарии 2, но в каждой папке конечного устройства дополнительно лежит файл pwd.txt, содержащий пароль контейнера для конечного устройства. Кроме того, когда администратор будет устанавливать Продукт CSP VPN Server из подготовленного инсталляционного файла, то он будет ставиться не в папку по умолчанию, а в папку c:\my vpn (с пробелом):

```
@echo off

SET TEMPLATE_DIR=c:\vpn_Server
SET MAKE_INST_PATH=D:\CSP VPN Server\make_inst.exe
SET CONTAINER_NAME=c:\container
SET SFX_DIR=c:\sfx

cd %TEMPLATE_DIR%

for /d %%i in (*) do (%MAKE_INST_PATH% -o %SFX_DIR%\%%i.exe -c
%%~fi\ca.crt -u %%~fi\localcert.crt -uc %CONTAINER_NAME% -ufp
%%~fi\pwd.txt -l %%~fi\lsp.txt -a "INSTALLDIR=\"c:\my vpn\"" &
(if errorlevel 1 goto err)

goto :end

:err

echo An error occurred
exit

:end

echo Make installations complete
```

11. Подготовка инсталляционного пакета с помощью графического интерфейса

Утилита `pkg_maker.exe` предоставляет администратору безопасности удобный графический интерфейс для создания локальной политики безопасности, задания настроек Продукта CSP VPN Server и создания инсталляционного пакета.

При подготовке инсталляционного пакета с аутентификацией сторон на Preshared Keys графический интерфейс предоставляет возможность считать созданный ключ из файла либо ввести его с клавиатуры.

Секретный ключ, соответствующий открытому ключу сертификата конечного устройства, может находиться в контейнере (стандартный способ) либо в отдельном файле. Контейнер содержит служебную и ключевую информацию, и является каталогом файловой системы. Контейнер и файл с секретным ключом могут быть размещены на жестком диске либо на внешнем ключевом носителе - дискете, электронном ключе eToken и др.

Сценарии создания инсталляционного пакета отличаются тем, кто создает ключевую пару для сертификата конечного устройства и на каком ключевом носителе размещен контейнер и файл с секретным ключом, возможна или нет проверка соответствия локального сертификата и секретного ключа при создании инсталляционного файла, копируется или нет контейнер и файл с секретным ключом во время инсталляции CSP VPN Server на конечное устройство.

11.1. Первый сценарий подготовки инсталляционного пакета с аутентификацией сторон на сертификатах

Все действия по созданию ключевой пары, формированию запроса и созданию сертификата конечного устройства производятся администратором СА. При этом контейнер и файл с секретным ключом размещаются на внешнем ключевом носителе, например дискете. Администратор безопасности получает от администратора СА контейнер и файл с секретным ключом на внешнем носителе, поэтому в данном сценарии возможно включить контейнер и файл с секретным ключом в инсталляционный файл и провести проверку соответствия сертификата и секретного ключа на компьютере администратора, а также скопировать контейнер и файл секретным ключом с одного носителя на другой во время инсталляции.

Опишем действия администратора безопасности по этому сценарию:

- администратор безопасности получает от администратора СА локальный сертификат конечного устройства и корневой сертификат Удостоверяющего Центра (Trusted CA Certificate), экспортированные в файлы. Ему передается контейнер и файл с секретным ключом на внешнем носителе
- администратор безопасности запускает утилиту графического интерфейса: `Пуск – Все программы – CSP VPN Server AdminTool sc –Package Maker`
- с помощью графического интерфейса администратор безопасности определяет для конечного устройства локальную политику безопасности, указывает имя инсталляционного файла, путь к локальному и СА сертификату, локальные настройки и др. Определяет включать или не включать контейнер и файл с секретным ключом в инсталляционный файл, проводить или нет проверку, копировать ли контейнер и файл с секретным ключом при инсталляции CSP VPN Server. Заполнив все вкладки графического интерфейса, администратор создает инсталляционный файл. Работа с графическим интерфейсом описана в разделе ["Графический интерфейс"](#)
- созданный инсталляционный файл содержит исполняемый код Продукта CSP VPN Server, локальную политику безопасности, локальный сертификат конечного устройства и СА сертификат, персональные настройки. В результате инсталляционный пакет состоит либо из инсталляционного файла, контейнера и файла с секретным ключом на внешнем ключевом носителе, либо из одного инсталляционного файла (контейнер и секретный ключ включены в инсталляционный файл).

11.2. Второй сценарий подготовки инсталляционного пакета с аутентификацией сторон на сертификатах

Создание ключевой пары и формирование запроса на локальный сертификат конечного устройства производятся администратором безопасности на конечном устройстве. При этом контейнер и файл с секретным ключом размещаются на жестком диске на конечном устройстве. В этом сценарии невозможна проверка соответствия сертификата и секретного ключа на компьютере администратора, и копирование контейнера с жесткого диска на другой ключевой носитель не производится.

Действия администратора безопасности по этому сценарию:

- администратор безопасности на конечном устройстве создает ключевую пару и формирует запрос на создание локального сертификата конечного устройства. Созданный запрос посылается на сервер Удостоверяющего Центра сертификатов. При этом контейнер и файл с секретным ключом размещаются на жестком диске на конечном устройстве
- администратор СА на сервере Удостоверяющего Центра по полученному запросу создает локальный сертификат и экспортирует его в файл. Корневой сертификат Удостоверяющего Центра (Trusted CA Certificate) также экспортируется в файл. Администратор безопасности получает оба эти сертификата от администратора СА
- администратор безопасности на своем компьютере запускает утилиту графического интерфейса:
Пуск – Все программы – CSP VPN Server AdminTool sc –Package Maker
- с помощью графического интерфейса администратор безопасности определяет для конечного устройства локальную политику безопасности, указывает имя инсталляционного файла, путь к локальному и СА сертификату, имя контейнера и файла с секретным ключом на конечном устройстве, локальные настройки и др. Заполнив все вкладки графического интерфейса, администратор создает инсталляционный файл. Работа с графическим интерфейсом описана в разделе ["Графический интерфейс"](#)
- подготовленный инсталляционный файл содержит исполняемый код Продукта CSP VPN Server, локальную политику безопасности, локальный сертификат конечного устройства и СА сертификат, локальные настройки. В результате инсталляционный пакет состоит из одного инсталляционного файла.

11.3. Графический интерфейс

При запуске утилиты `pkg_maker.exe` (Пуск – Все программы – CSP VPN Server AdminTool sc – Package Maker) открывается окно главной формы.

Главная форма представляет собой диалоговое окно со вкладками, в котором можно создавать LSP, делать локальные настройки и создавать инсталляционный файл.

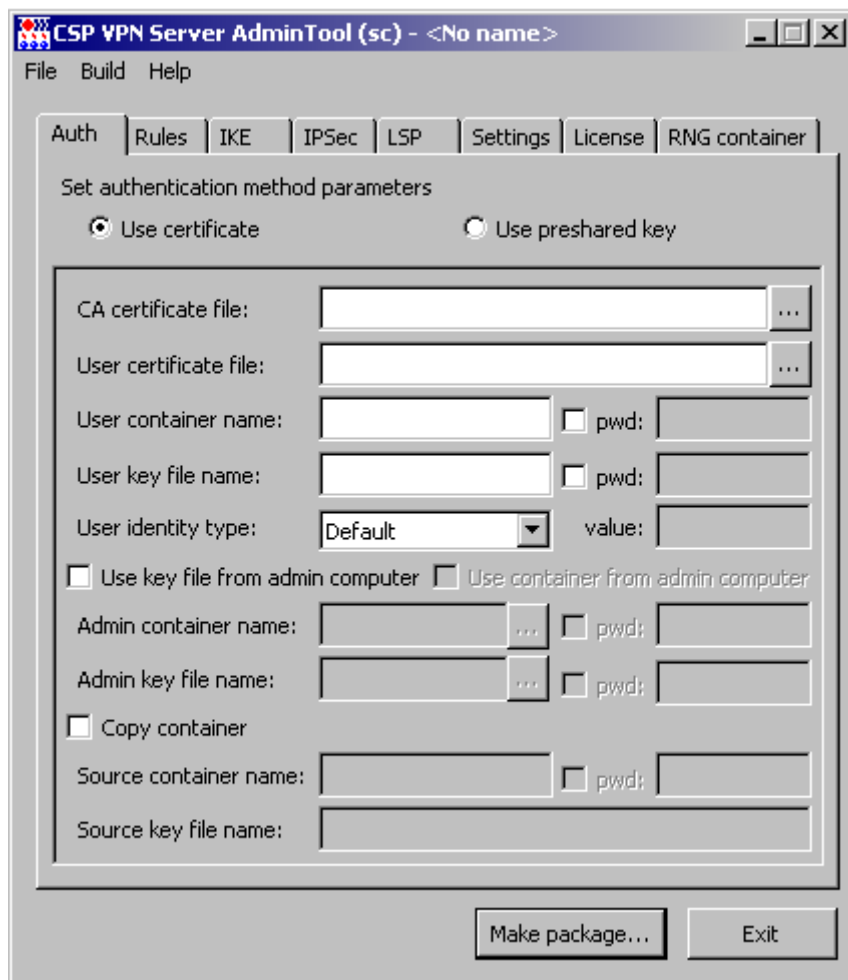


Рисунок 7

Кроме того, главная форма содержит Меню и две функциональные кнопки.

Вкладки главной формы предназначены:

- Auth – для задания способа аутентификации сторон
- Rules – для задания правил сетевой обработки трафика
- IKE – задание параметров IKE соединений
- IPSec – задание параметров IPSec соединений
- LSP – просмотр и редактирование локальной политики безопасности
- Settings – задание параметров протоколирования событий и LSP по умолчанию
- License – задание параметров Лицензии
- RNG container – задание криптографического RNG контейнера.

Меню содержит три раздела:

- Раздел File имеет следующие предложения:
 - New Project – открывает новый проект. Проект – это файл в текстовом формате с расширением dsc, в котором будет записана LSP с установленными параметрами во вкладках и локальными настройками.
 - Open Project... – открывает существующий проект
 - Save Project – сохраняет текущее состояние проекта в открытый файл
 - Save Project As... – сохраняет текущее состояние проекта в указанный файл.
 - Exit – выход из GUI.
- Раздел Build имеет одно предложение:
 - Make package... – создает инсталляционный файл Продукта CSP VPN Server (аналогично кнопке "Make package...").
- Раздел Help имеет три предложения:
 - Contents – вызывает окно Help-системы с активной вкладкой Contents
 - Index – вызывает окно Help-системы с активной вкладкой Index
 - About... – открывает окно, содержащее название Продукта, версию, номер сборки, копирайт и логотип компании.

Функциональные кнопки:

- Make package – кнопка создания инсталляционного файла для конечного устройства
- Exit- выход из GUI.

11.3.1. Формат заполняемых полей

Все поля графического интерфейса, в которые вводится имя папки и файла, могут содержать парные кавычки, пробелы в начале и в конце строки. Все эти символы игнорируются.

Для всех других полей любой введенный символ является значимым.

11.4. Вкладка Authentication

Вкладка Auth предназначена для выбора метода аутентификации и ввода идентификационных данных конечного устройства. Поддерживаются два метода аутентификации – при помощи GOST сертификата стандарта X.509 или предустановленного (разделяемого) ключа (Preshared Key).

11.4.1. Аутентификация при помощи сертификатов

При аутентификации сторон при помощи сертификатов открытых ключей поставить переключатель в положение Use certificate:

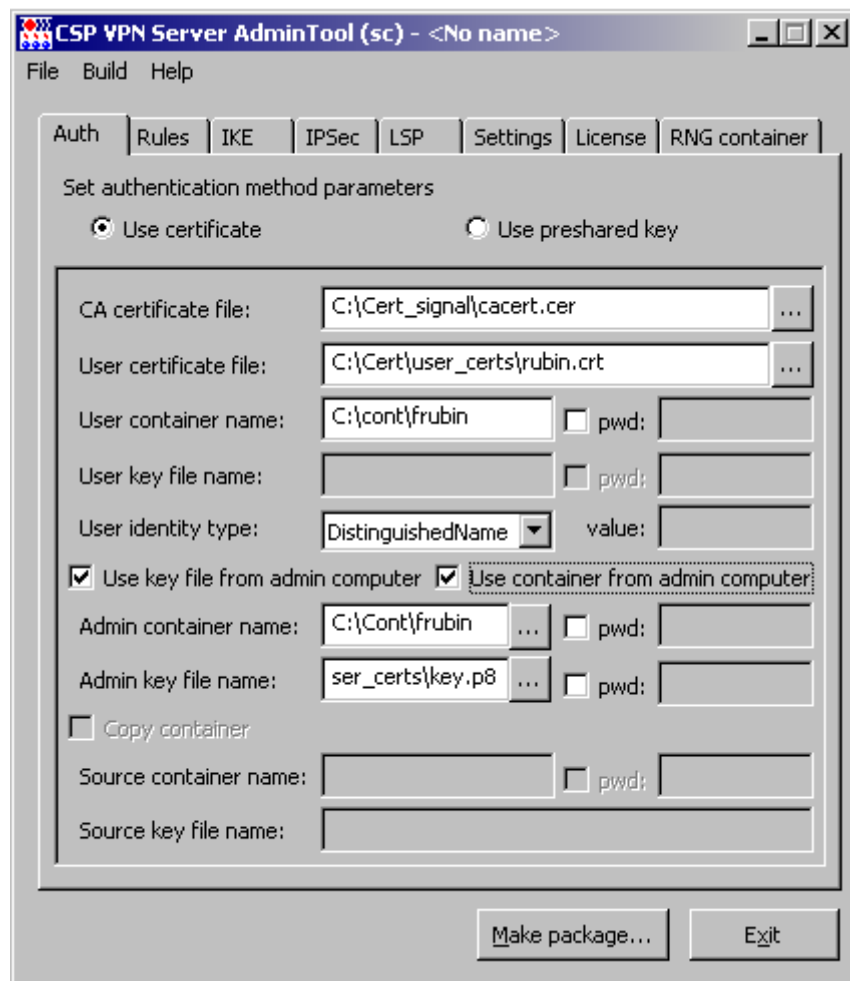


Рисунок 8

При этом становятся доступными для заполнения следующие поля:

- **CA certificate file** – поле для ввода имени файла с корневым сертификатом Удостоверяющего Центра (Trusted CA Certificate), размещенного на компьютере администратора. Имя файла включает в себя и полный путь к этому файлу. Обязательный параметр. При нажатии кнопки [...] открывается окно, в котором можно выбрать файл с сертификатом. Смотрите формат таких полей в разделе ["Формат заполняемых полей"](#).
- **User certificate file** – имя файла с локальным GOST сертификатом конечного устройства, размещенного на компьютере администратора. Обязательный параметр.

- **User container name** – имя контейнера, содержащего файлы ключевой и служебной информации, может содержать и секретный ключ сертификата конечного устройства (стандартное размещение). Имя контейнера должно включать и путь к нему на конечном устройстве. Обязательный параметр, если используется сертификат.
- **User container pwd** – пароль к контейнеру
- **User key file name** – имя файла с секретным ключом, размещенного на конечном устройстве. Если это поле не заполнено, то ключ будет считываться из контейнера. Обязательный параметр, если секретный ключ размещен в файле. Если файл с секретным ключом будет браться с компьютера администратора, то это поле блокируется.
- **User key file pwd** – пароль к файлу с секретным ключом
- **User identity type** – тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Обязательный параметр. Поле содержит выпадающий список со следующими значениями:
 - Default – в качестве идентификатора партнеру будет высылаться действительный IP-адрес конечного устройства, на котором будет установлен CSP VPN Server
 - Distinguished Name – в качестве идентификатора партнеру будет высылаться значение Subject из сертификата конечного устройства, показываемое в поле User identity value, если оно там задано.
 - Email – в качестве идентификатора партнеру будет высылаться значение поля E-mail расширения сертификата конечного устройства, показываемое в поле User identity value, если оно там задано.
 - FQDN – в качестве идентификатора партнеру будет высылаться значение доменного имени конечного устройства, считываемое из поля DNS расширения сертификата и показываемое в поле User identity value, если оно там задано.
 - IPV4Addr – в качестве идентификатора партнеру будет высылаться первый IP-адрес, указанный в расширении сертификата, и показываемый в поле User identity value, если он там задан.
- **User identity value** – идентификационная информация, пересылаемая партнеру. Поле доступно только для чтения и заполняется автоматически соответствующим типу идентификатора значением, считываемым из сертификата конечного устройства. Заполнение происходит в момент выбора типа идентификатора или изменения имени файла с сертификатом конечного устройства. Параметр обязательный.
- **Use key file from admin computer** – установка этого флажка означает, что файл с секретным ключом с компьютера администратора будет размещен в инсталляционный файл. При этом на компьютере администратора будет проведена проверка соответствия сертификата конечного устройства и секретного ключа. Размещение файла и контейнера задается полями .Admin container name, Admin key file name, Admin key file pwd. При инсталляции CSP VPN Server файл с секретным ключом будет размещен в базе данных Продукта.
- **Use container from admin computer** – установка этого флажка означает, что контейнер с именем, указанным в поле Admin container name, с компьютера администратора будет размещен в инсталляционный файл. При инсталляции CSP VPN Server контейнер будет скопирован в контейнер с именем User container name. Рекомендуется не устанавливать этот флажок, если канал доставки инсталляционного файла не защищен.
- **Admin container name** – имя контейнера на компьютере администратора для проведения проверки и размещения в инсталляционный файл.

- **Admin key file name** – имя файла с секретным ключом на компьютере администратора для проведения проверки и размещения в инсталляционный файл, если секретный ключ находится в файле.
- **Admin container pwd** – пароль к контейнеру с секретным ключом
- **Admin key file pwd** – пароль к файлу с секретным ключом
- **Copy container** – установка этого флажка означает, что во время инсталляции CSP VPN Server на конечное устройство будет проведено копирование контейнера с именем, указанным в поле Source container name, в контейнер с именем, указанным в поле User container name. Копирование файла с секретным ключом будет проведено из файла с именем, указанным в поле Source key file name в файл с именем, указанным в поле User key file name, если секретный ключ размещен в файле.
- **Source container name** - имя контейнера на конечном устройстве, который будет копироваться во время инсталляции.
- **Source key file name** – имя файла с секретным ключом на конечном устройстве, который будет копироваться во время инсталляции.

11.4.2. Аутентификация при помощи Preshared Key

При аутентификации сторон при помощи предустановленного ключа поставить переключатель в положение Use preshared key:

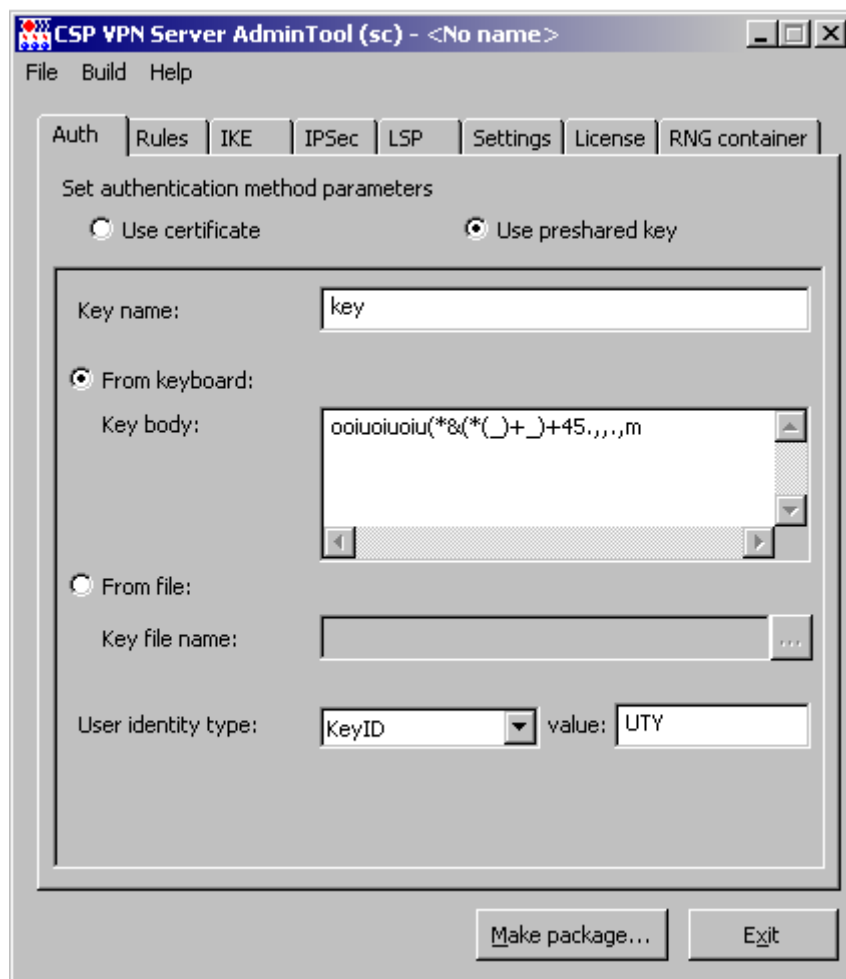


Рисунок 9

Следующие поля становятся доступными для заполнения:

- **Key name** – имя предустановленного ключа. Обязательный параметр.

Для ввода предустановленного ключа имеется переключатель с двумя положениями:

- **From keyboard** – предустановленный ключ нужно ввести с клавиатуры.
Примечание: Если предустановленный ключ задан несколькими строками, то каждый перенос в теле ключа будет представлен двумя символами 0x0D 0x0A (символ возврата и перевода каретки) и тогда при подготовке предустановленного ключа для партнера должны быть использованы эти символы.
- **From file** – предустановленный ключ считывается из файла с именем, указанным в поле **Key file name**
- **User identity type** – тип идентификационной информации, пересылаемой партнеру при создании защищенного соединения. Обязательный параметр. Поле содержит выпадающий список со следующими значениями:
 - **Default** – в качестве идентификатора партнеру будет высылаться действительный IP-адрес конечного устройства, на котором будет установлен CSP VPN Server

- **IPV4Addr** – в качестве идентификатора партнеру будет высылаться IP-адрес конечного устройства, который нужно задать в поле "User identity value"
- **KeyID** – в поле "User identity value" нужно ввести любую последовательность символов, которая может включать в себя пробелы и русские буквы. Во вкладке LSP атрибуту KeyID будет присвоено шестнадцатеричное представление заданной последовательности символов, которое и будет высылаться партнеру в качестве идентификатора.
- **User identity value** – значение идентификатора, вводимого вручную. Параметр обязательный.

11.5. Вкладка Rules

Во вкладке Rules можно создавать, редактировать, удалять правила фильтрации и защиты трафика.

Правила нужно располагать в списке в порядке убывания приоритета. В списке должно находиться хотя бы одно правило.

При получении TCP/IP пакета правила будут просматриваться в порядке убывания приоритета и сравниваться параметры заголовка пакета, относящиеся к IP-адресам, с этими же параметрами в правиле до нахождения первого подходящего правила. Если правило не найдено – пакет уничтожается.

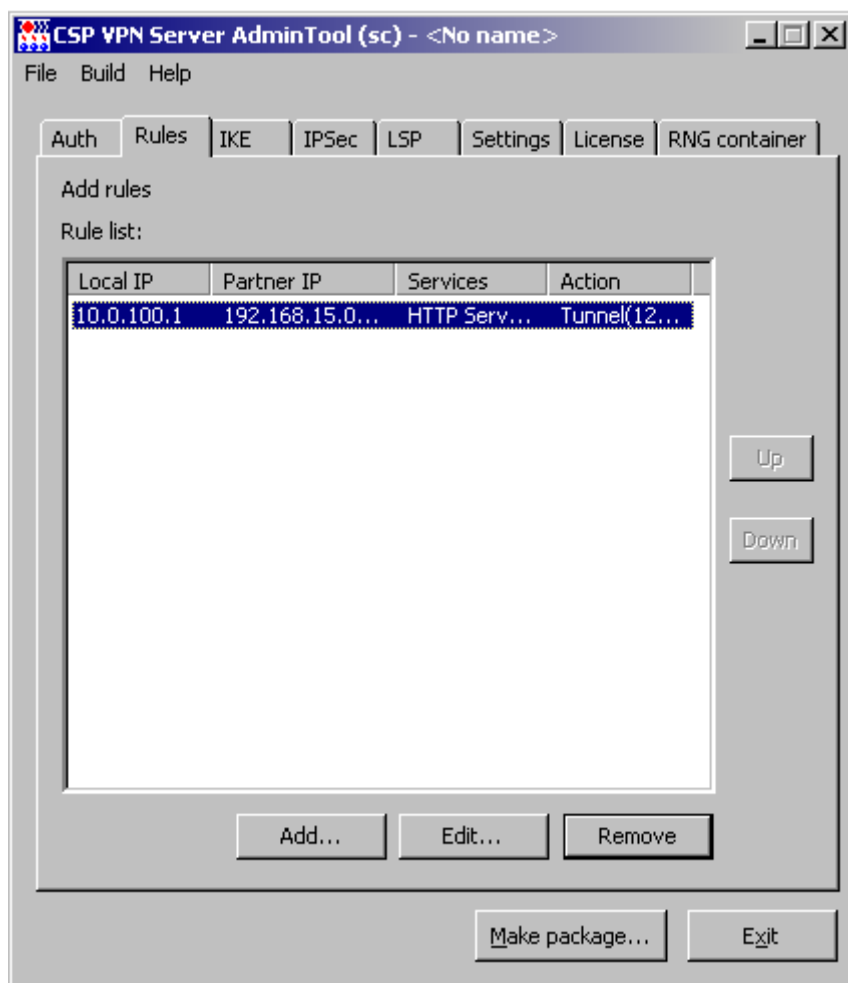


Рисунок 10

Кнопки управления:

- Add – вызывает окно, в котором производится создание нового правила
- Edit – вызывает окно для редактирования выделенного правила
- Remove - удаление выделенного правила с требованием подтверждения операции удаления. Если в списке содержится только одно правило, то при попытке удалить его будет выдано сообщение о невозможности такого удаления (правило не удаляется)
- Up – при нажатии этой кнопки выделенное правило в списке перемещается на одну строчку вверх, увеличивая свой приоритет
- Down – при нажатии этой кнопки выделенное правило в списке перемещается на одну строчку вниз, уменьшая свой приоритет.

11.5.1. Создание и редактирование правила

Создание и редактирование правила производится в окне Add/Edit Rule, которое вызывается кнопкой Add или Edit во вкладке Rules:

Add Rule

Set rule parameters

Local IP Addresses

☐ Any

☒ Custom

IP Address	Subnet Mask
10.0.100.1	255.255.255.255

Add... Edit... Remove

Partner IP Addresses

☐ Any

☒ Custom

IP Address	Subnet Mask
192.168.15.0	255.255.255.0

Add... Edit... Remove

Services and Protocols

☐ Any

☒ Custom

Name	Ports
HTTP Server	-
Protocol TCP	(0..65535)-(0.....

Add... Edit... Remove

Action

☐ Pass

☐ Drop

☒ Protect using IPSec

Tunnel IP Addresses of IPSec partner:

☐ Use random IP Address order

12.12.12.1 Up Down

Add... Edit... Remove

OK Cancel

Рисунок 11

Диалоговое окно Rule имеет 4 области для задания правила:

- **Local IP Addresses** – в этой области задаются IP-адреса локального VPN устройства (конечного устройства) или подсети, на которые будет распространяться правило. Область имеет переключатель с двумя положениями:
 - Any – используется любой IP-адрес
 - Custom – становится доступным окно для ввода IP-адреса и маски подсети
- **Partner IP Addresses** – в этой области задаются IP-адреса или подсети партнеров, на которые распространяется правило
- **Services and Protocols** – область для задания сетевых сервисов и протоколов, на которые распространяется правило
- **Action** – в этой области задаются действия, применяемые к сетевому трафику этого правила.

Кнопки управления:

- Add – вызывает окно для ввода новой записи
- Edit – вызывает окно для редактирования выделенной записи
- Remove - удаление выделенной записи с требованием подтверждения операции удаления
- Up, Down – кнопки для изменения приоритета выделенного туннельного адреса партнера.

Задание IP-адреса и маски подсети в правиле

Для создания/редактирования IP-адреса хоста (подсети) и маски подсети в правиле в областях Local IP Addresses и Partner IP Addresses установить переключатель в положение Custom и кнопкой Add или Edit вызвать окно Add/Edit IP Address (Рисунок 12). Если сетевая маска равна 255.255.255.255, то задается IP-адрес хоста. Адрес не может быть нулевым.

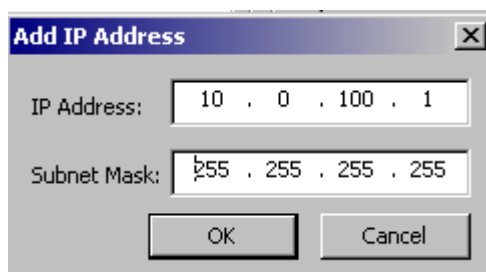


Рисунок 12

Задание сетевого сервиса или протокола в правиле

В области Services and Protocols установить переключатель в положение Custom и кнопкой Add вызвать окно Add Service (Рисунок 13):

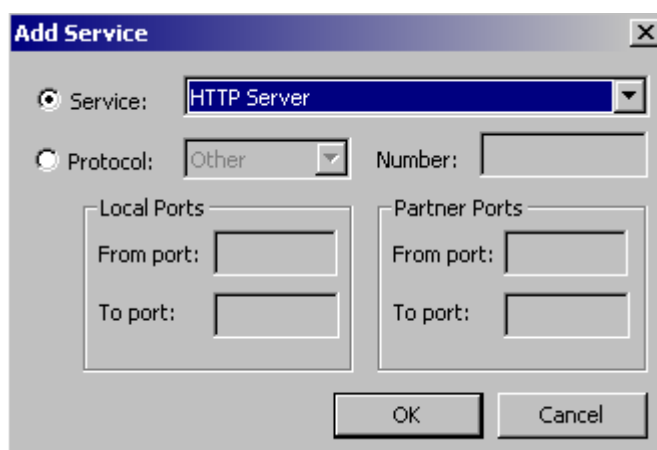


Рисунок 13

В окне Add Service имеется переключатель с двумя положениями:

- **Service** – при установке переключателя в это положение доступным становится только поле Service, которое содержит выпадающий предопределенный не редактируемый список сервисов. Из этого списка нужно выбрать значение и нажать кнопку ОК
- **Protocol** – при установке переключателя в это положение доступными становятся все поля, кроме поля Service (Рисунок 14). Сетевой протокол выбирается из выпадающего списка, а в поле Number будет автоматически выводиться номер выбранного протокола. Задать протокол можно и по номеру из зарезервированного пространства (0-255). При указании протокола так же возможно указание диапазона портов (в тех протоколах, в которых это возможно). Область Local Ports предназначена для задания портов на локальном компьютере, а область Partner Ports - для задания портов на компьютере партнера. В полях From port и To port задается порт или диапазон портов из зарезервированного пространства (0-65535). Значение в поле From port должно быть меньше или равно значению в поле To port.

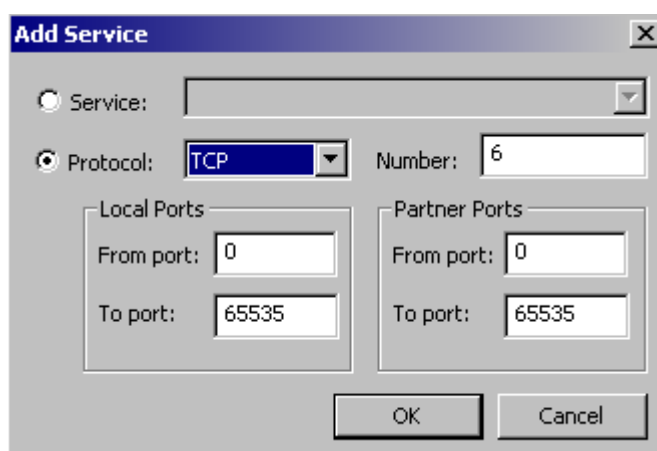


Рисунок 14

Список предлагаемых сетевых сервисов:

- HTTP Client – все пакеты протокола TCP идущие на(с) порт(порта) 80 компьютера партнера
- HTTP Server – все пакеты протокола TCP идущие на(с) порт(порта) 80 локального компьютера
- LDAP Client – все пакеты протокола TCP идущие на(с) порт(порта) 389 компьютера партнера
- LDAP Server – все пакеты протокола TCP идущие на(с) порт(порта) 389 локального компьютера
- LDAPS Client – все пакеты протокола TCP идущие на(с) порт(порта) 636 компьютера партнера
- LDAPS Server – все пакеты протокола TCP идущие на(с) порт(порта) 636 локального компьютера
- RTELNET Client – все пакеты протокола TCP идущие на(с) порт(порта) 107 компьютера партнера
- RTELNET Server – все пакеты протокола TCP идущие на(с) порт(порта) 107 локального компьютера
- SMTP Client – все пакеты протокола TCP идущие на(с) порт(порта) 25 компьютера партнера

- SMTP Server – все пакеты протокола TCP идущие на(с) порт(порта) 25 локального компьютера
- SNMP – все пакеты протокола UDP идущие на(с) порт(порта) 161 локального компьютера
- SNMP Trap – все пакеты протокола UDP идущие на(с) порт(порта) 162 компьютера партнера
- TELNET Client – все пакеты протокола TCP идущие на(с) порт(порта) 23 компьютера партнера
- TELNET Server – все пакеты протокола TCP идущие на(с) порт(порта) 23 локального компьютера
- DHCP Client - все пакеты протокола UDP, идущие на порт 67 компьютера партнера и все пакеты протокола UDP, идущие на порт 68 локального компьютера
- DHCP Server - все пакеты протокола UDP, идущие на порт 68 компьютера партнера и все пакеты протокола UDP, идущие на порт 67 локального компьютера
- SSH Client - все пакеты протоколов TCP и UDP, идущие на(с) порт(порта) 22 компьютера партнера
- SSH Server - все пакеты протоколов TCP и UDP, идущие на(с) порт(порта) 22 локального компьютера.

Список предлагаемых сетевых протоколов:

EGP, GGP, HMP, ICMP, PUP, RDP, RVD, TCP, UDP, XNS-IDP.

Редактирование выделенного сервиса или протокола производится в окне Edit Service, совпадающем с окном Add Service.

Задание действия в правиле

Задание действия в правиле, распространяющегося на пакет, в области Action (Рисунок 11) производится при помощи переключателя с тремя положениями:

- **Pass** – пропускать сетевой трафик без шифрования
- **Drop** – не пропускать сетевой трафик
- **Protect using IPsec** – защищать сетевой трафик (шифровать). Сетевой трафик защищается между платформой, на которой установлен Продукт, и указанным туннельным адресом партнера (это может быть адрес интерфейса шлюза безопасности, защищающего подсеть, в которой находится партнер либо адрес интерфейса партнера). В результате этого строится туннель. При установке переключателя в это положение нажмите кнопку Add и в открывшемся окне Add IP Address (Рисунок 15) укажите IP-адрес интерфейса, до которого будет построен туннель с партнером. Адрес не может быть нулевым.

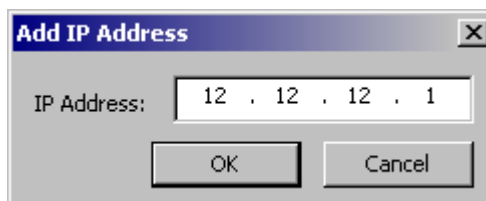


Рисунок 15

Можно указать список IP-адресов, до которых возможно построить туннель. Адреса в списке можно расположить в порядке убывания приоритета – первый в списке имеет самый высокий приоритет. Если не удалось построить туннель до интерфейса с первым указанным адресом в списке, то производится попытка построить туннель со вторым туннельным адресом и т.д. Кнопки Up и Down предназначены для изменения приоритета адресов в списке.

Используя кнопки Add, Edit и Remove, адреса в список можно добавлять, редактировать и удалять из списка.

Use random IP Address order – при установке этого флажка туннельный адрес партнера будет выбираться из списка случайным образом. При неудачной попытке построить туннель с этим адресом, следующий туннельный адрес будет выбираться также случайным образом.

11.6. Вкладка IKE

В этой вкладке определены наборы политик IKE, которые предлагаются партнеру для согласования при создании ISAKMP SA.

IKE-пакеты отсылаются с выставленным значением поля Type of Service (ToS) =0x4 (максимальная надежность доставки). Это значение записывается в реестре при инсталляции Продукта.

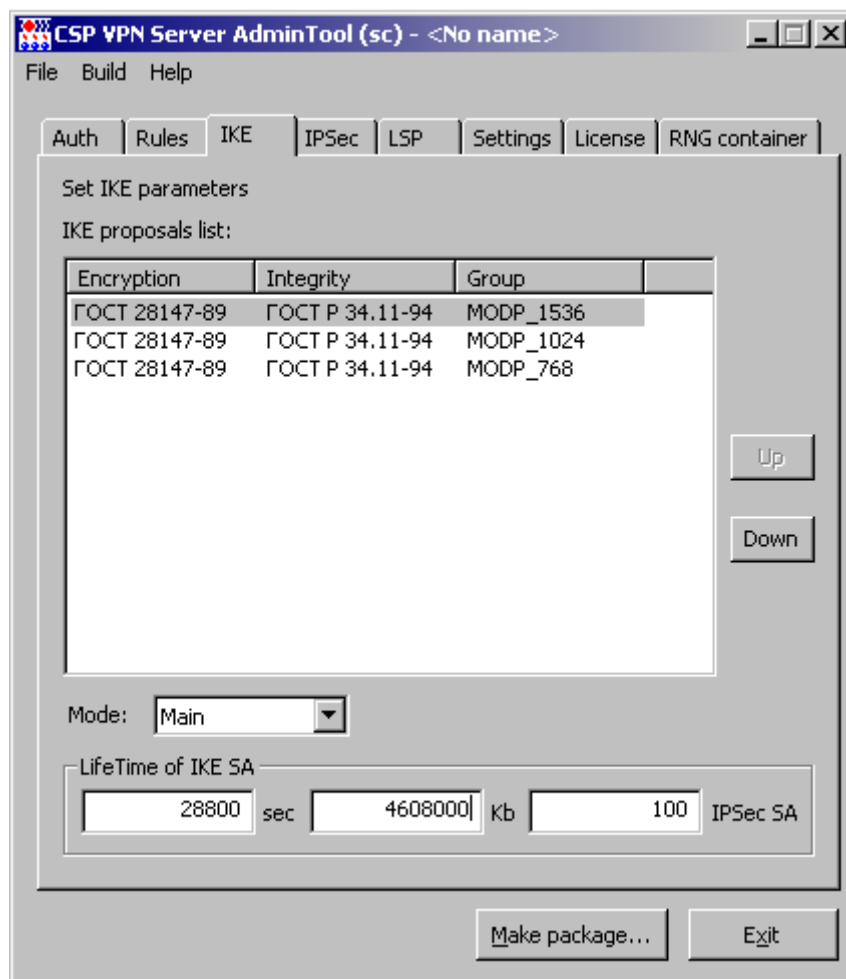


Рисунок 16

IKE proposals list – упорядоченный список IKE предложений по приоритету. В верхней строчке находится предложение с наивысшим приоритетом.

Encryption – предлагаемые алгоритмы шифрования пакетов: Предлагается только один российский криптографический алгоритм:

- ГОСТ 28147-89 - российский криптографический алгоритм, представленный в конфигурации (вкладке LSP) как G2814789CPRO1-K256-CBC-65534

Integrity – предлагаемые алгоритмы проверки целостности. Предлагается только один российский криптографический алгоритм:

- ГОСТ Р 34.11-94 - российский криптографический алгоритм, представленный в конфигурации (вкладке LSP) как GR341194CPRO1-65534.

Имена алгоритмов шифрования пакетов и проверки целостности данных считываются из файла `admintool.ini`, размещенного в папке Продукта CSP VPN Server AdminTool sc. Для изменения имен алгоритмов необходимо отредактировать этот файл, описанный в разделе ["Формат задания имен алгоритмов в файле admintool.ini"](#), и перезапустить графический интерфейс.

Group – параметры обмена сеансовыми ключами:

- MODP_768 - группа 1 (768-битовый вариант алгоритма Диффи-Хеллмана)
- MODP_1024 - группа 2 (1024-битовый вариант алгоритма Диффи-Хеллмана)
- MODP_1536 - группа 5 (1536-битовый вариант алгоритма Диффи-Хеллмана).

Mode - режим обмена информацией о параметрах защиты и установления IKE SA. Имеет два значения:

- Main - в этом режиме партнеру высылаются все IKE политики для выбора и согласования.
- Aggressive - в этом режиме партнеру высылается только первая IKE политика из списка, имеющая самый высокий приоритет. При выборе этого режима выдается об этом предупреждение. Если для аутентификации используется предустановленный ключ и выбран тип идентификатора KeyID, то должен использоваться только режим Aggressive.

LifeTime of IKE SA (sec) – время в секундах, в течение которого ISAKMP SA будет существовать. Возможное значение – целое число из диапазона 0 .. 4 294 967 295. Рекомендуемое значение – 28800, которое выставлено при открытии нового проекта. Значение 0 означает, что время действия SA не ограничено. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

LifeTime of IKE SA (Kb) – указывает объем данных в килобайтах, который могут передать стороны во всех IPsec SA, созданных в рамках одного ISAKMP SA. Возможное значение – целое число из диапазона 0 .. 4 294 967 295. Рекомендуемое значение – 0, которое выставлено при открытии нового проекта. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

IPsec SA - количество IPsec SA, созданных в рамках одного ISAKMP SA. Значение 0 означает, что количество IPsec SA не ограничено.

Кнопки Up и Down предназначены для упорядочивания списка предложений по приоритету.

11.7. Вкладка IPsec

В данной вкладке задаются политики IPsec для защиты трафика в виде набора преобразований, каждый из которых есть комбинация AH преобразования и ESP преобразования. Партнеру направляется список наборов преобразований и по протоколу IKE происходит согласование и выбор конкретного набора преобразований, который будет использоваться для защиты трафика для одной SA.

При обработке пакетов IPsec происходит копирование значения флага Type of Service (ToS) из внутреннего заголовка во внешний заголовок пакета.

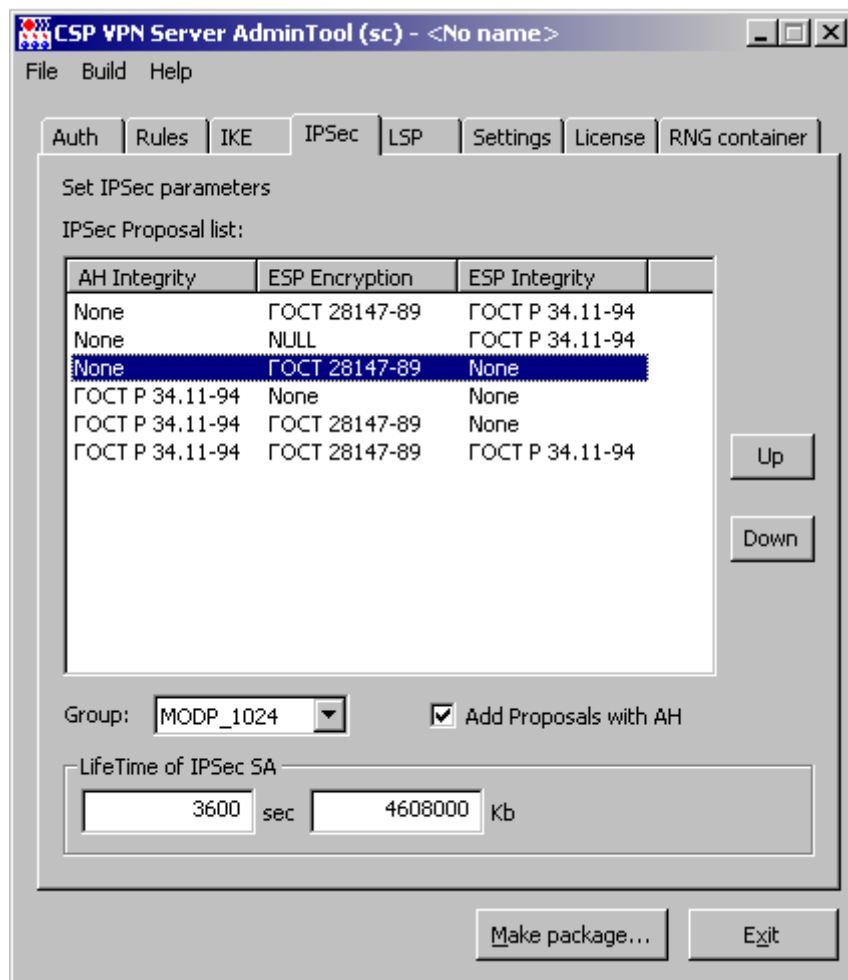


Рисунок 17

IPsec Proposal list – упорядоченный список наборов преобразований, высылаемых партнеру для согласования. При помощи кнопок Up и Down выполняется упорядочивание списка по приоритету.

AH Integrity – предлагаемые алгоритмы проверки целостности по протоколу AH. Имеется два значения:

- None – алгоритм проверки целостности не применяется
- ГОСТ P 34.11-94 - российский криптографический алгоритм, представленный в конфигурации (вкладке LSP) как GR341194CPRO1-H96-HMAC-254.

ESP Integrity – предлагаемые алгоритмы проверки целостности по протоколу ESP. Имеется два значения:

- None – алгоритм проверки целостности не применяется
- ГОСТ P 34.11-94 - российский криптографический алгоритм, представленный в конфигурации (вкладке LSP) как GR341194CPRO1-H96-HMAC-65534.

ESP Encryption – предлагаемые алгоритмы шифрования пакетов по протоколу ESP: Предлагается только один российский криптографический алгоритм:

- None – алгоритм шифрования ESP не применяется
- Null – алгоритм применять, но не шифровать
- ГОСТ 28147-89 - российский криптографический алгоритм, представленный в конфигурации (вкладке LSP) как G2814789CPRO1-K256-CBC-254.

Имена алгоритмов шифрования пакетов и проверки целостности данных считываются из файла `admintool.ini`, размещенного в папке Продукта CSP VPN Server AdminTool sc. Для изменения имен алгоритмов необходимо отредактировать этот файл, описанный в разделе ["Формат задания имен алгоритмов в файле admintool.ini"](#), и перезапустить графический интерфейс.

Add Proposals with AH – при установке этого флажка выводится сообщение:

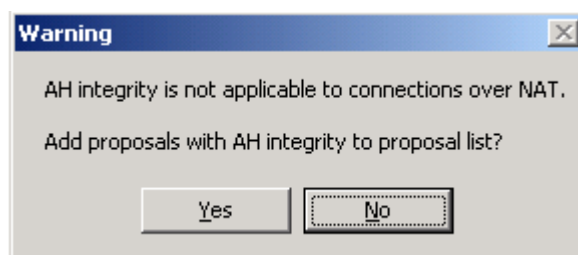


Рисунок 18

Оно означает, что протокол AH несовместим со средствами NAT, так как NAT изменяют IP-адрес в заголовке TCP/IP пакета. Протокол AH обеспечивает проверку аутентичности и целостности пакетов, а NAT нарушает данные аутентификации. После нажатия кнопки Yes добавляется российский криптографический алгоритм ГОСТ Р 34.11-94.

Group – параметры обмена сеансовыми ключами, высылаемые партнеру для согласования:

- No PFS – опция PFS не включена и при согласовании новой SA новый обмен Диффи-Хеллмана не выполняется. Ключевой материал заимствуется из первой фазы IKE.
- Выбранные группы означают, что при согласовании новой SA выполняется новый обмен Диффи-Хеллмана в рамках IPsec и может использоваться одна из групп:
 - MODP_768 - . группа 1 (768-битовый вариант алгоритма Диффи-Хеллмана)
 - MODP_1024 - группа 2 (1024-битовый вариант алгоритма Диффи-Хеллмана)
 - MODP_1536 - группа 5 (1536-битовый вариант алгоритма Диффи-Хеллмана).

LifeTime (sec) – время в секундах, в течение которого IPsec SA будет существовать. Возможное значение – целое число из диапазона 1.. 4 294 967 295. Рекомендуемое значение – 3600, которое выставлено при открытии нового проекта. Пустая строка и значение 0, которое означает неограниченное время жизни IPsec SA, – недопустимы, при создании инсталляционного файла будет выдано сообщение об ошибке.

LifeTime (Kb) – указывает объем данных в килобайтах, который могут передать стороны в рамках одной IPsec SA. Возможное значение – целое число из диапазона 0.. 4 294 967 295. Рекомендуемое значение – 4608000, которое выставлено при открытии нового проекта. Значение 0 означает, что объем данных в килобайтах не ограничен. Пустая строка – недопустима, при создании инсталляционного файла будет выдано сообщение об ошибке.

Кнопки Up и Down предназначены для упорядочивания списка предложений по приоритету.

11.8. Локальная политика безопасности

Во вкладке LSP просматривается и редактируется локальная политика безопасности для конечного устройства, определенная в предыдущих вкладках.

Существует два режима работы с LSP:

- режим автоматического формирования LSP
- режим ручного задания LSP.

11.8.1. Режим автоматического формирования LSP

В режиме автоматического формирования (флажок "Use custom LSP" не установлен) локальная политика безопасности формируется на основе данных вкладок Auth, Rules, IKE, IPSec и расширенных параметров, задаваемых в диалоговом окне, вызываемом кнопкой Advanced.

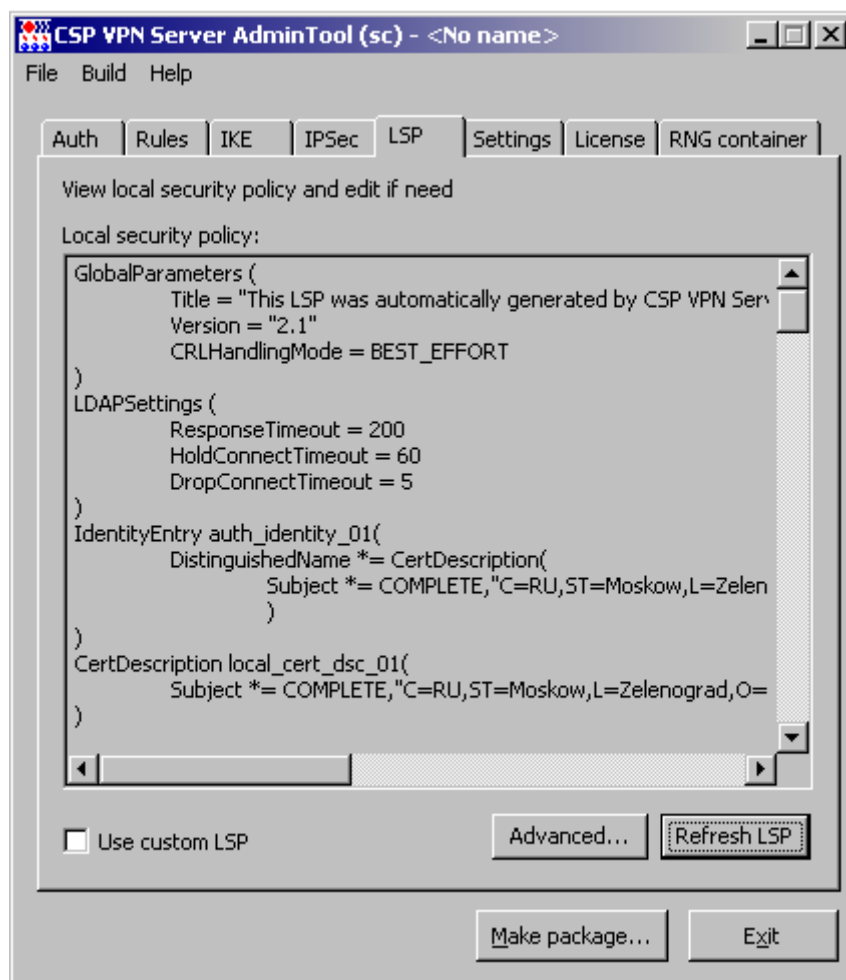


Рисунок 19

Local security policy – поле с LSP в текстовом формате

Use custom LSP – установка этого флажка переключает в режим ручного формирования LSP

Refresh LSP – кнопка для обновления LSP в окне Local security policy для отображения текущей конфигурации с изменениями.

Advanced - кнопка вызова окна [Advanced LSP Settings](#) для настройки расширенного списка параметров LSP.

Advanced LSP Settings

Это окно отображает расширенный список переменных LSP и их текущие значения, которые можно отредактировать и установить значения по умолчанию. Переменные объединены в пять групп.

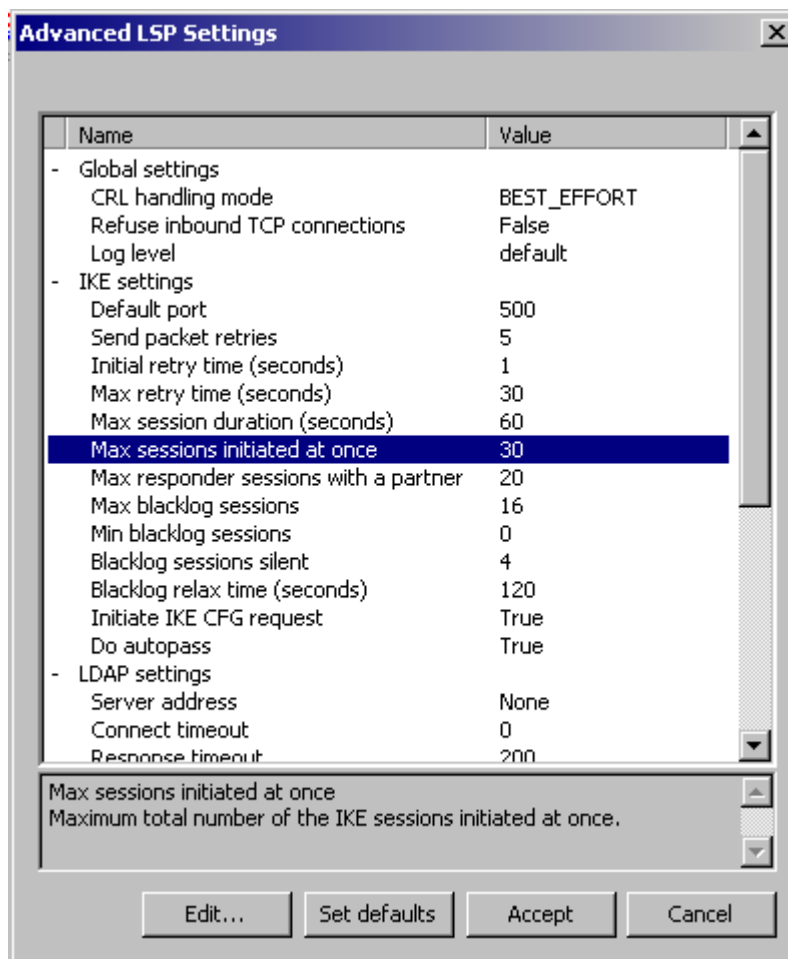


Рисунок 20

Окно содержит 4 функциональные кнопки:

- Edit - кнопка вызова окна для редактирования выделенной переменной. Окно редактирования открывается также при двойном клике левой кнопки "мыши" на выделенной строке.
- Set defaults - кнопка для установки значений по умолчанию для всех переменных.
- Accept - кнопка для закрытия окна с сохранением отредактированных значений переменных.
- Cancel - кнопка для закрытия окна без сохранения изменений.

Global settings

CRL handling mode

Переменная задает режим использования списков отозванных сертификатов (CRL). При нажатии кнопки Edit появляется окно для выбора значений из выпадающего списка:

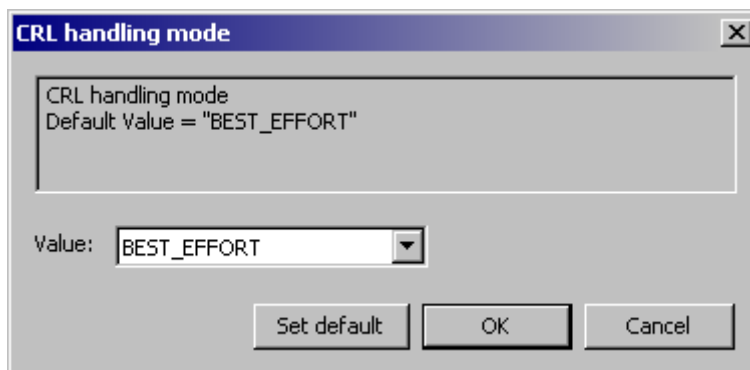


Рисунок 21

Возможные значения:

- **DISABLE** - при проверке сертификата список отозванных сертификатов не обрабатывается
- **OPTIONAL** - список отозванных сертификатов используется только в случае, если он был предустановлен или получен (и обработан) в процессе IKE обмена и является действующим
- **BEST_EFFORT** – список отозванных сертификатов используется при проверке сертификата только в том случае, если он является действующим. Этот режим отличается от режима **OPTIONAL** тем, что CRL может быть получен посредством протокола LDAP (если он настроен). Это значение используется по умолчанию.
- **ENABLE** – для успешной проверки сертификата обрабатывается список отозванных сертификатов.

Значение по умолчанию - **BEST_EFFORT**.

Все окна для редактирования переменных имеют три функциональные кнопки:

- **Set default** – кнопка для установления значения по умолчанию данной переменной
- **OK** – кнопка для закрытия окна с сохранением выбранного значения переменной.
- **Cancel** – кнопка для закрытия окна без сохранения выбранного значения переменной.

Refuse inbound TCP connections

Задаёт блокировку входящих TCP-соединений. Используется как дополнительное ограничение к действию. При редактировании появляется окно:

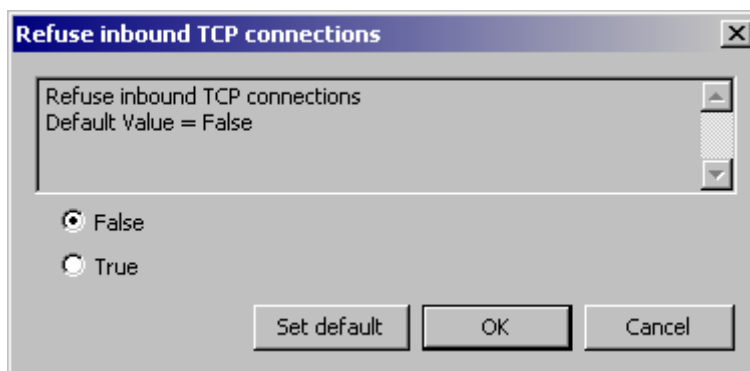


Рисунок 22

Переключатель имеет два положения:

- TRUE - уничтожается первый входящий TCP-пакет соединения, если он входящий. В результате отвергаются все TCP-соединения, инициированные извне.
- FALSE - не производится никаких дополнительных действий. Значение по умолчанию.

Значение по умолчанию -FALSE.

Log level

Задаёт уровень важности протоколируемых событий, связанных с разными событиями - системными, с доступом к LDAP серверу, связанных с применением LSP и получением, обработкой сертификатов и их сохранением в базе данных Продукта. При редактировании появляется окно:

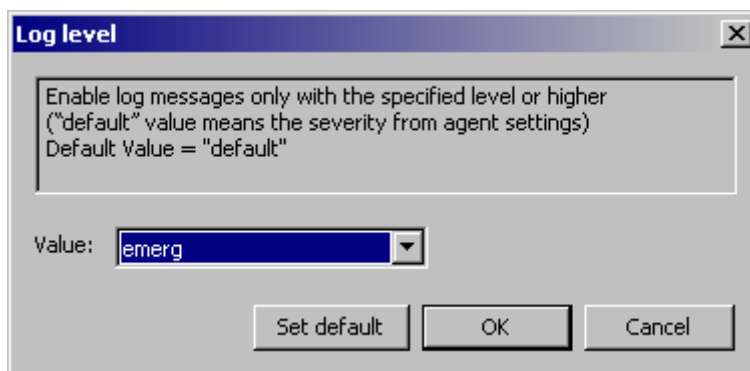


Рисунок 23

Значение по умолчанию – default, которое берется из глобального уровня протоколируемых событий, выставляемого во вкладке Settings [в none Severity](#).

IKE settings

Default port

Порт для протокола IKE, который будет использован по умолчанию. Возможное значение - целое число из диапазона 1..65535. Значение по умолчанию - 500.

Окно для выбора значения порта:

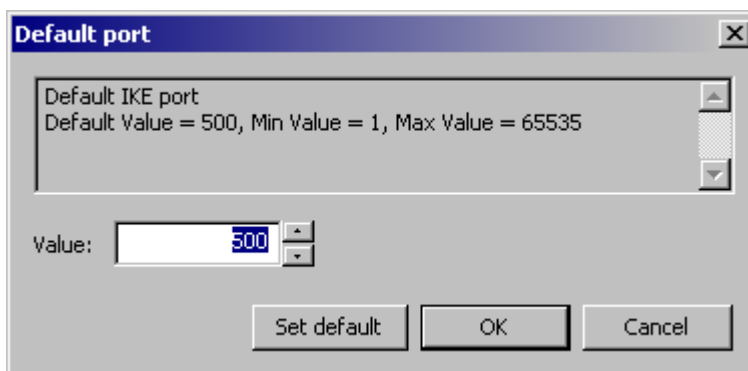


Рисунок 24

Send packet retries

Количество попыток отправки IKE-пакетов партнеру. Возможное значение - целое число из диапазона 1..30. Значение по умолчанию - 5.

Окно для установки значения:

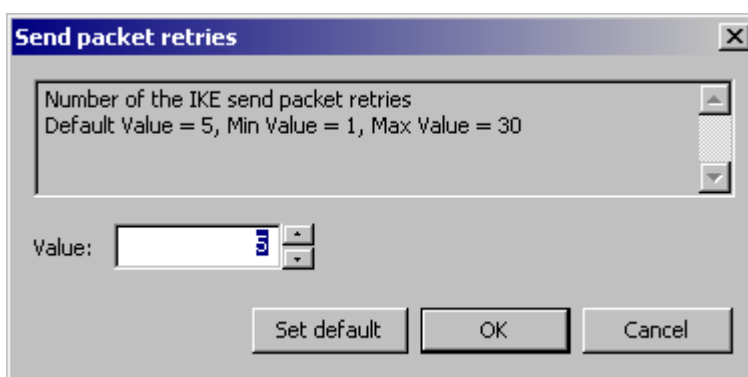


Рисунок 25

Initial retry time (seconds)

Начальный интервал времени между повторными попытками отправки IKE-пакетов партнеру (в секундах). Если ответ не получен в течение начального интервала, то запрос посылается повторно и интервал между повторными попытками увеличивается в два раза. Этот интервал увеличивается в два раза до тех пор, пока:

- не будет получен ответ или
- значение интервала Initial retry time не достигнет значения Max retry time, (повторные попытки будут продолжаться с интервалом Max retry time) и количество попыток не достигнет значения Send packet retries.

Возможное значение - целое число из диапазона 1..5. Значение по умолчанию - 1.

Окно для установки начального интервала времени:

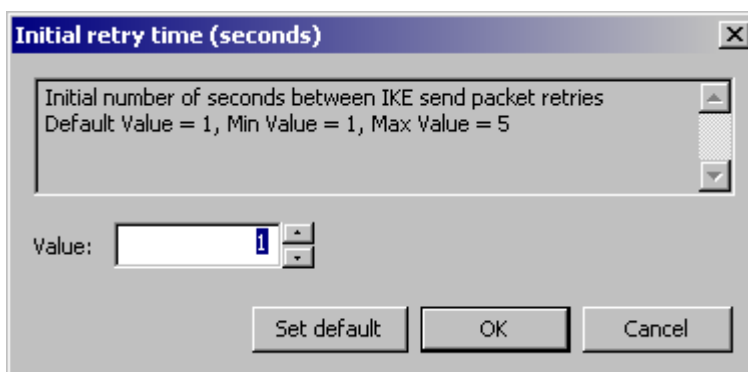


Рисунок 26

Max retry time (seconds)

Максимальный интервал времени между повторными попытками послылки IKE-пакетов партнеру (в секундах). Если выставленное значение Max retry time меньше, чем значение Initial retry time, то при загрузке конфигурации Max retry time присваивается значение Initial retry time. Возможное значение - целое число из диапазона 1..60. Значение по умолчанию - 30.

Окно для установки максимального интервала времени:

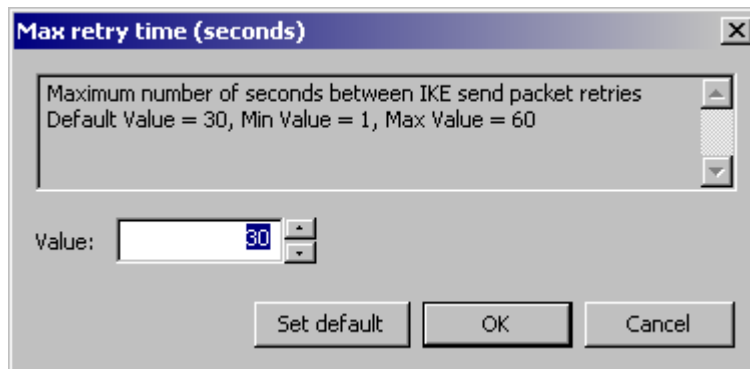


Рисунок 27

Max session duration (seconds)

Максимальный интервал времени на каждую сессию IKE (в секундах). Возможное значение - целое число из диапазона 10..300. Значение по умолчанию - 60. Окно для выбора значения:

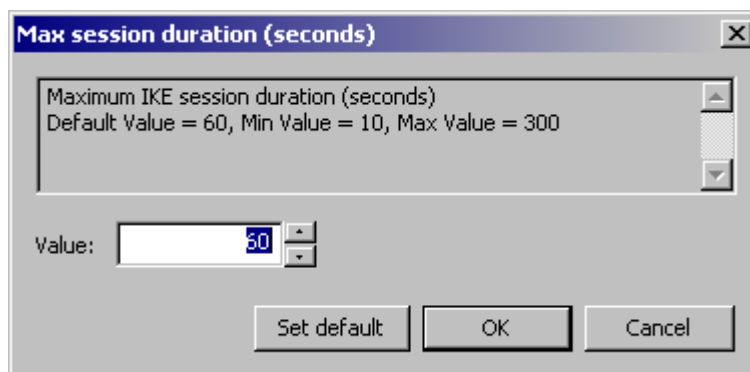


Рисунок 28

Max sessions initiated at once

Максимальное количество одновременно иницируемых IKE-сессий для всех партнёров. Возможное значение - целое число из диапазона 1..10000. Значение по умолчанию - 30. Окно для выбора значения:

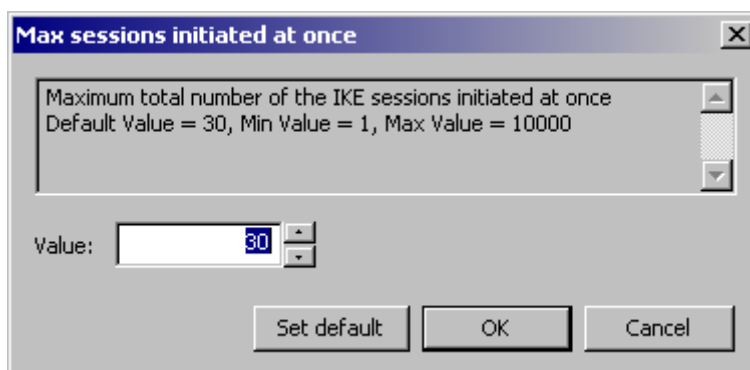


Рисунок 29

Max responder sessions with a partner

Максимально допустимое количество одновременных обменов, проводимых VPN-устройством с одним неаутентифицированным партнером, в качестве ответчика. С таким партнером нет ни одного ISAKMP SA. Как только создается хотя бы один ISAKMP SA, данный атрибут перестает действовать.

Возможное значение - целое число из диапазона 1..20. Значение по умолчанию - 20.

Окно для установки значения:

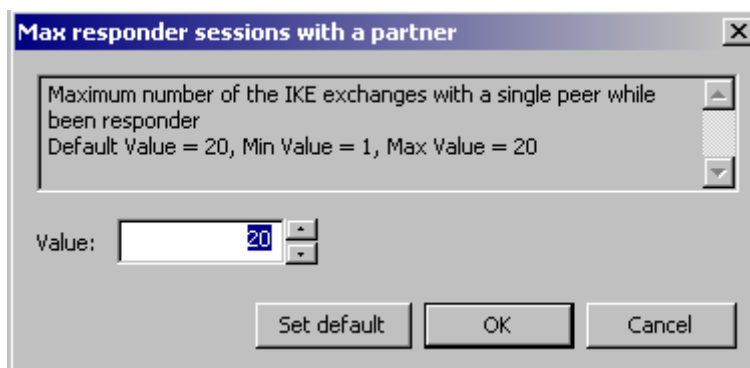


Рисунок 30

Max backlog sessions

"Черный список" предназначен для защиты от DoS-атак (Denial of Service –отказ от обслуживания). "Черный список" минимизирует обработку IKE-пакетов от партнеров, находящихся в "черном списке". В случае первой неуспешной IKE-сессии, инициированной со стороны партнера, партнер сразу же заносится в "черный список". Max backlog sessions устанавливает число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером, только что попавшим в "черный список". При каждом следующем неудачном завершении IKE обмена число разрешенных одновременных IKE обменов для данного партнера снижается вдвое с округлением в меньшую сторону, вплоть до полного запрещения IKE трафика с данным партнером.

Примечание: как только партнер заносится в "черный список", для него текущее значение разрешенных одновременно проводимых IKE обменов не только начинает уменьшаться в два раза после каждого неуспешного завершения обмена, но и увеличиваться на единицу по истечении каждого интервала времени Blacklog relax time (описанного далее).

Возможное значение - целое число из диапазона - 0..4294967295.

Если значение равно 0, то "черный список" не используется.¹

Если значение Max backlog sessions больше или равно значению Max responder sessions with a partner, то Max backlog sessions присваивается значение Max responder sessions with a partner -1.

Значение по умолчанию - 16.

¹ При загрузке конфигурации с *отключенным* "черным списком" вся статистическая информация о "плохих" партнерах сбрасывается. Если же "черный список" *включен*, то к уже имеющейся накопленной статистике применяются новые параметры настроек "черного списка".

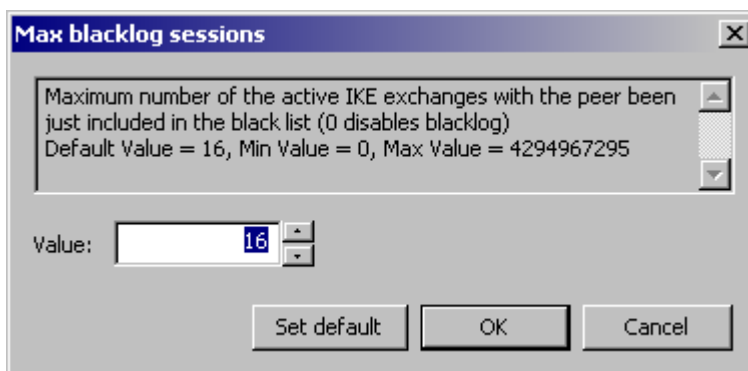


Рисунок 31

Min blacklog sessions

Минимальное число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером, находящимся в "черном списке".

Возможное значение - целое число из диапазона - 0..4294967295.

Если значение Min blacklog sessions больше, чем Max blacklog sessions, то Min blacklog sessions присваивается значение Max blacklog sessions.

Значение по умолчанию - 0 означает, что нет ограничения снизу на активные обмены с партнером, находящимся в "черном списке".

Окно для выбора минимального количества обменов с партнером из "черного списка":

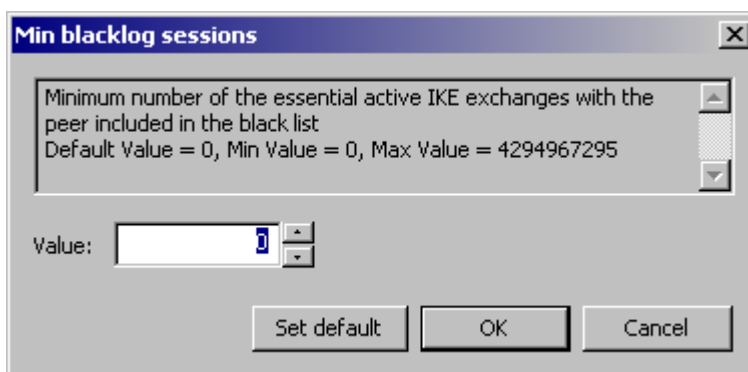


Рисунок 32

Blacklog sessions silent

Число активных обменов, инициированных партнером, находящимся в "черном списке", по достижении которого VPN-устройство перестает информировать партнера о причине отказа в создании IKE-контекста (ISAKMP SA).

Возможное значение - целое число из диапазона - 0.. 4294967295.

Если значение Blacklog sessions silent больше, чем Max blacklog sessions, то Blacklog sessions silent присваивается значение Max blacklog sessions.

Значение по умолчанию - 4.

Окно для выбора количества обменов:

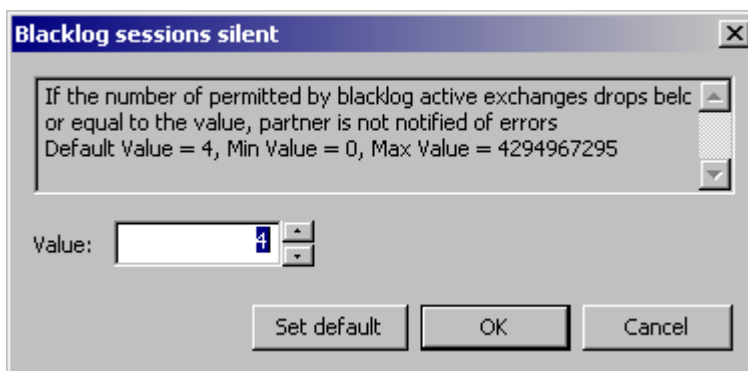


Рисунок 33

Blacklog relax time (seconds)

Устанавливает интервал времени (в секундах) релаксации "черного списка".

За указанный период времени число разрешенных одновременных IKE обменов для каждого партнера, находящегося в "черном списке", увеличивается на единицу. По истечении следующего такого же интервала времени, текущие значения разрешенных одновременно проводимых IKE обменов для каждого партнера опять увеличивается на единицу и т.д. Этот интервал времени отсчитывается с момента последней загрузки конфигурации.

Как только текущее значение разрешенных одновременно проводимых партнером IKE обменов начинает превышать значение Max blacklog sessions, такой партнер исключается из "черного списка".

Возможное значение - целое число из диапазона 0..4294967295. Значение 0 означает бесконечное время релаксации "черного списка" (партнер попадает в "черный список" навсегда).

Значение по умолчанию – 120 секунд.

Примечание: помимо механизма релаксации, партнер также может быть исключен из "черного списка" в следующих случаях:

- при перезапуске сервиса
- при загрузке конфигурации с отключенным "черным списком" (Max blacklog sessions = 0)
- при инициации IKE обмена со стороны локального VPN устройства с целью установления ISAKMP (IPSec) соединения²
- если партнеру удалось установить ISAKMP (IPSec) соединение с локальным VPN устройством, и тем самым партнер был успешно аутентифицирован.

Окно для выбора интервала времени:

² В данном случае считается, что локальное VPN устройство потенциально доверяет партнеру, с которым оно хочет установить соединение, и информация, накопленная в "черном списке", для такого партнера сбрасывается.

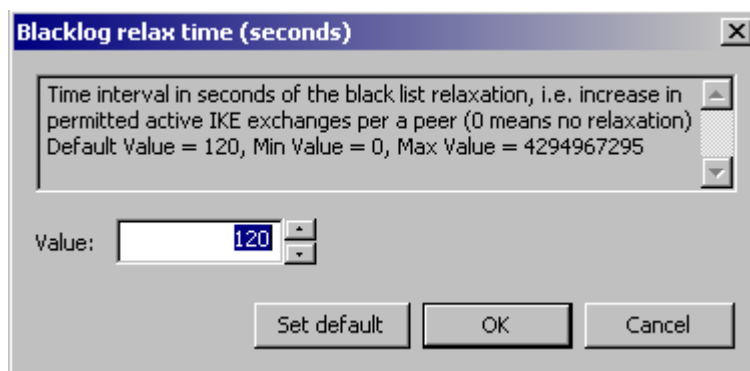


Рисунок 34

Initiate IKE CFG request

Задает режим работы IKECFG клиента. Возможные значения:

- TRUE - агент является активным IKECFG клиентом, т.е. агент инициирует посылку запроса на получение адреса у партнера сразу после создания IKE SA (если партнер не является IKECFG-сервером – строительство SA продолжается как с обычным партнером)
- FALSE - не производится никаких действий.

Значение по умолчанию - TRUE.

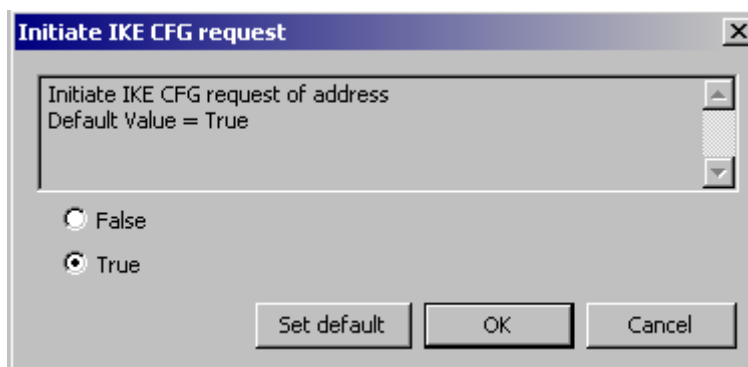


Рисунок 35

Do autopass

Задает режим автоматического пропуска ISAKMP-трафика. Возможные значения:

- TRUE - автоматически пропускать ISAKMP-пакеты по всем фильтрам, по которым защищается трафик.
- FALSE - не пропускать автоматически ISAKMP-пакеты. Правило фильтрации для пропуска ISAKMP-трафика должно быть задано явно (вручную) с действием PASS.

Значение по умолчанию - TRUE.

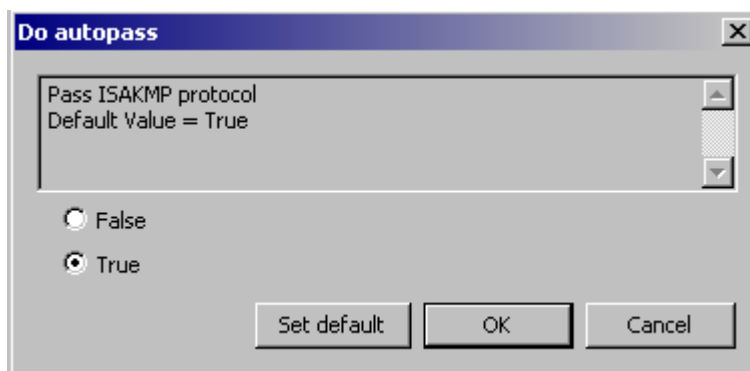


Рисунок 36

LDAP settings

Server address

Задаваемые здесь параметры LDAP-сервера используются тогда, когда сертификат, для которого производится проверка подписи, не содержит расширение CDP (CRL Distribution Point) с адресом LDAP-сервера либо в этом поле прописанный путь к LDAP-серверу является неполным и тогда добавляются данные из этой структуры.

В окне Server address задаются параметры LDAP-сервера. Возможные значения:

- LDAP-сервер не используется, когда флажок Use default LDAP Server не установлен
- LDAP-сервер используется, когда флажок Use default LDAP Server установлен. При необходимости будет производиться поиск сертификатов и CRL на заданном LDAP-сервере. При этом нужно заполнить поля:
 - IP Address – сетевой адрес LDAP-сервера.
 - Port – сетевой порт LDAP-сервера, на который будут посылаться LDAP запросы. Значение по умолчанию – 389.
 - Searchbase - имя (Distinguished Name, DN) корневого X.500-объекта, в поддереве которого производится поиск сертификатов и CRL на LDAP-сервере. Если DN сертификата и DN X.500-объекта не совпадают, и если DN сертификата является частью имени DN X.500-объекта, то заполняется поле Searchbase, чтобы дополнить запрос, созданный на основе имени из сертификата или CRL, для нахождения соответствующего X.500-объекта. Для запроса на основе URL данное имя не используется. См. Пример в структуре LDAPSettings.
- Pass LDAP protocol with the LDAP Server – при установке этого флажка производится автоматическая генерация сетевого фильтра для пропускания пакетов между агентом и LDAP-сервером.

Значение по умолчанию – LDAP-сервер не используется.

Сначала делается попытка установить соединение по LDAP версии 2. Если эта попытка завершается с ошибкой LDAP_PROTOCOL_ERROR (наиболее вероятная причина - не поддерживается версия 2), то повторяется попытка установить соединение по LDAP версии 3.

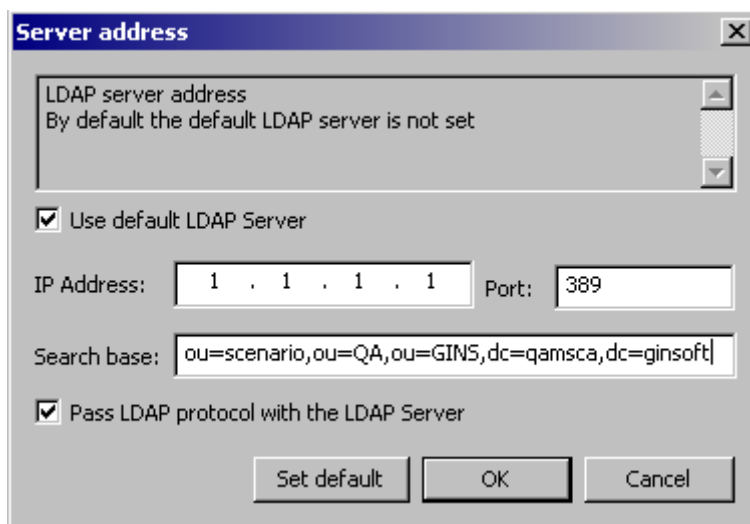


Рисунок 37

ConnectTimeout

ConnectTimeout позволяет ограничить время (в секундах) создания TCP-соединения с LDAP-сервером. Возможное значение - целое число из диапазона 1..6000. Значение по умолчанию – 0, которое означает, что время создания TCP-соединения с LDAP-сервером ограничивается установленным для ОС временем создания TCP-соединения.

Примечание: Если в момент обращения к LDAP-серверу устройство, на котором он установлен, недоступно, то процесс создания TCP-соединения может занимать продолжительное время (до 3 минут, зависит от ОС). По этой причине могут наблюдаться внешние признаки зависания агента, и это может служить причиной неудачной попытки создания соединения.

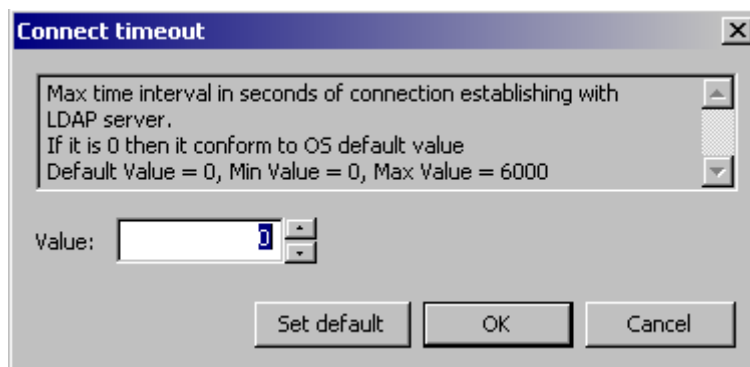


Рисунок 38

ResponseTimeout

Поиск посредством протокола LDAP может занимать достаточно продолжительное время, оно зависит от многих факторов, в том числе от масштаба запроса и характеристик канала передачи данных. ResponseTimeout позволяет ограничить время (в секундах), в течение которого ожидается ответ от LDAP-сервера на единственный запрос. Возможное значение - целое число из диапазона 2..6000. Значение по умолчанию – 200.

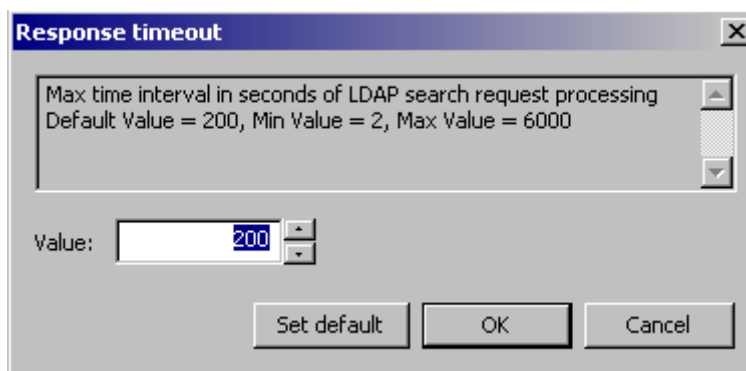


Рисунок 39

HoldConnectTimeout

HoldConnectTimeout устанавливает период времени, в течение которого держится установленное соединение к серверу на случай, если придет к нему повторный запрос. Возможное значение - целое число из диапазона 0..6000.

При значении 0 после обмена с LDAP-сервером соединение с ним сразу закрывается.

Не рекомендуется выставлять значение в 1 секунду в виду наличия погрешности в 1 секунду, поскольку это может привести в некоторых случаях к немедленному закрытию соединения и к избыточному открытию нового соединения.

Значение по умолчанию – 60.

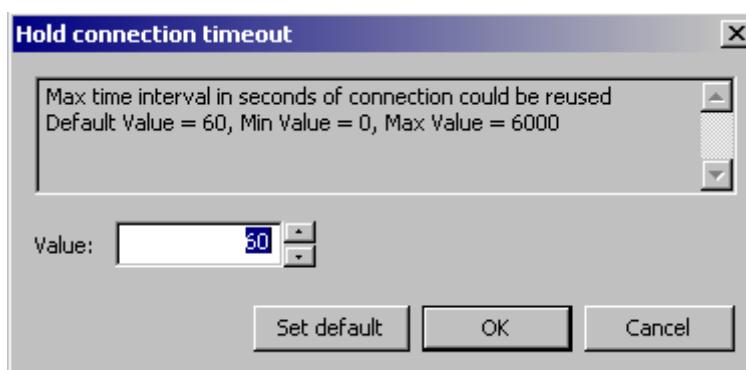


Рисунок 40

DropConnectTimeout

Атрибут DropConnectTimeout устанавливает период времени, начиная с первой неудачной попытки создания соединения с LDAP-сервером, в течение которого новые попытки создания соединения с ним игнорируются. Возможное значение - целое число из диапазона 0..6000.

При значении 0 в случае неудачной попытки установления соединения с LDAP-сервером новые попытки не игнорируются.

Не рекомендуется выставлять значение в 1 секунду в виду наличия погрешности в одну секунду, поскольку это может привести в некоторых случаях к избыточным попыткам создания соединения.

Значение по умолчанию – 5.

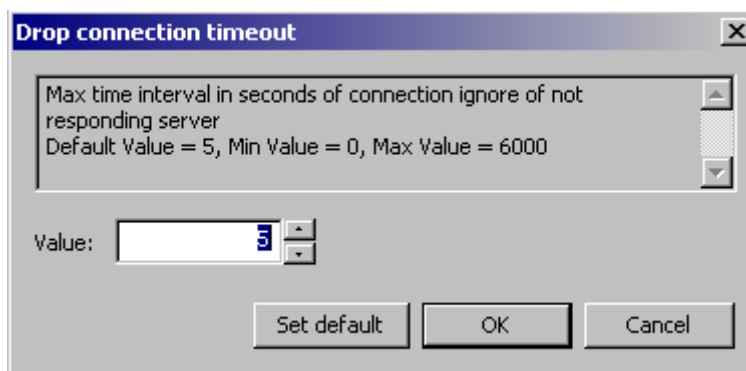


Рисунок 41

SNMP settings

SNMP polling

Задаёт настройки по выдаче информации по запросу SNMP-менеджера. Возможные значения:

- не принимаются и не обрабатываются запросы на выдачу SNMP статистики
- принимаются и обрабатываются запросы на выдачу SNMP статистики.

Значение по умолчанию - SNMP статистика не выдается.

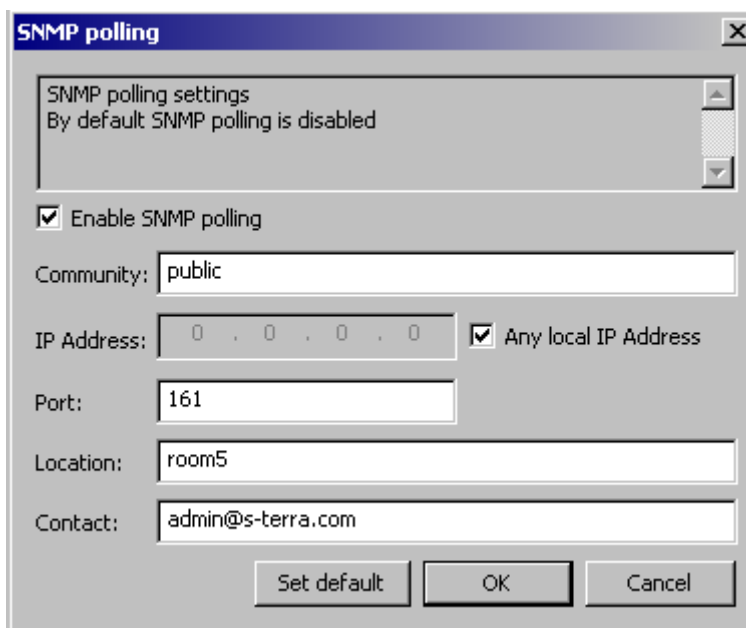


Рисунок 42

Enable SNMP polling - при установке этого флажка задаются настройки для принятия запроса и выдачи статистики.

Community - эта строка действует подобно паролю и разрешает доступ к чтению статистики SNMP-менеджеру.

IP Address - локальный IPv4-адрес, на который можно получать запросы от SNMP-менеджера.

Any local IP Address - установка этого флажка разрешает получение запроса от SNMP-менеджера на любой локальный IP-адрес.

Port - задаёт порт, на который можно получать SNMP-запросы.

Location - информация о физическом расположении SNMP-агента.

Contact - информация о контактном лице, ответственном за работу SNMP-агента.

Trap receiver

Задаёт настройки получателя SNMP-трапов и дополнительные настройки для трапов, отсылаемых на него. Возможные значения:

- получатель SNMP-трапов не задан
- получатель SNMP-трапов задан.

Значение по умолчанию - получатель SNMP-трапов не задан.

Можно задать до трех получателей SNMP-трапов.

Enable the trap receiver - при установке этого флажка задаются настройки получателя SNMP-трапов.

Community - текстовая строка, играющая роль идентификатора отправителя трап-сообщения.

Receiver's IP Address - IP-адрес получателя SNMP-трапов.

Receiver's Port - UDP-порт, на который менеджеру будут высылаться трап-сообщения.

SNMP Version - версия SNMP, в которой формируются трап-сообщения.

Agent's IP Address - IP-адрес отправителя трап-сообщения. Этот атрибут указывается только для Version = V1.

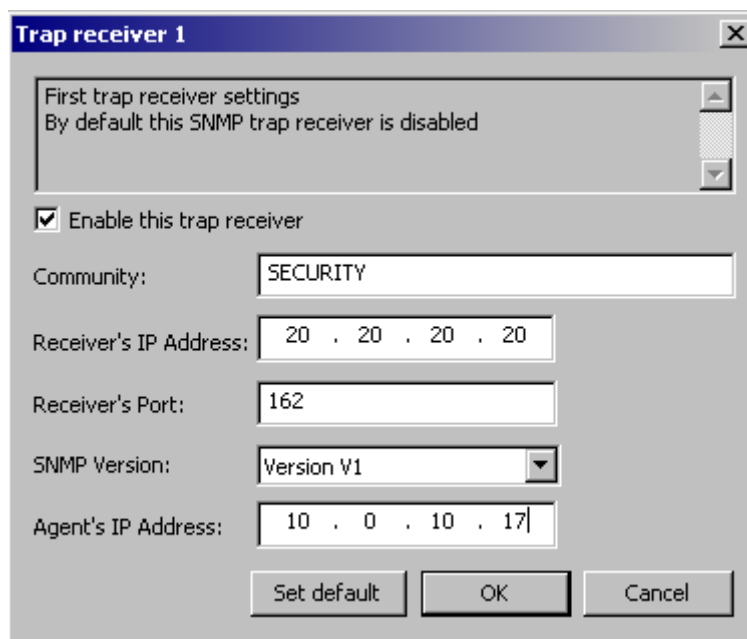


Рисунок 43

DPD settings

Use DPD

Задаёт режим использования протокола DPD (Dead-Peer-Detection). Возможные значения:

- TRUE - использовать протокол DPD.
- FALSE – не использовать протокол DPD. В этом случае другие переменные этого раздела не появляются.

Значение по умолчанию - TRUE.

Окно для установки переключателя:

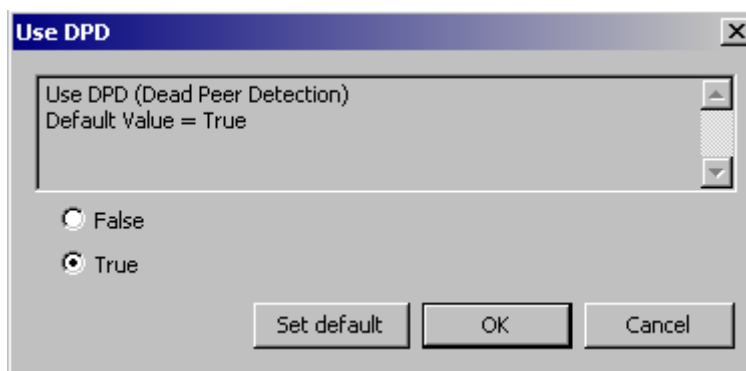


Рисунок 44

Idle duration (seconds)

Интервал времени отсутствия входящего трафика от партнера, по истечению которого, при наличии исходящего трафика, активируется DPD-сессия. Возможные значения - целое число из диапазона 1..32762. Значение по умолчанию - 60. Окно для установки значения:

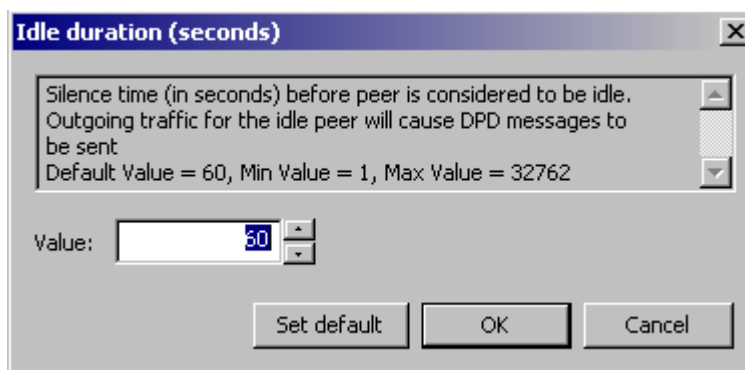


Рисунок 45

Response duration

Время ожидания ответа от партнера на DPD-запрос в секундах. Возможные значения - целое число из диапазона 1..300. Значение по умолчанию - 5. Окно для выбора значения:

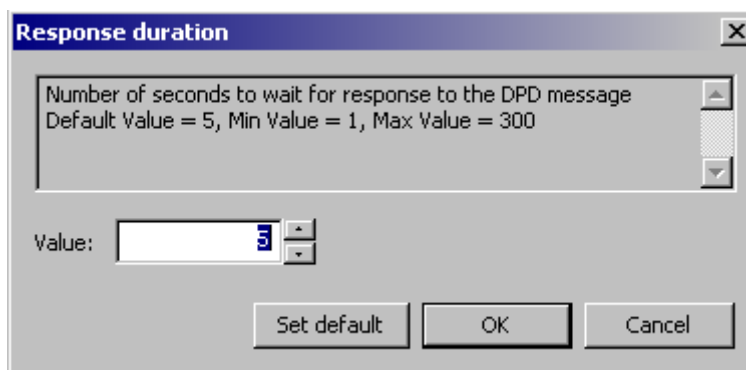


Рисунок 46

Retries

Количество попыток провести DPD-обмен. Если все попытки закончились неудачей, защищенное соединение (IKE-контекст) считается "мертвым", и производится

попытка создать его заново. Возможные значения - целое число из диапазона 1..10. Значение по умолчанию - 3. Окно для выбора значения:

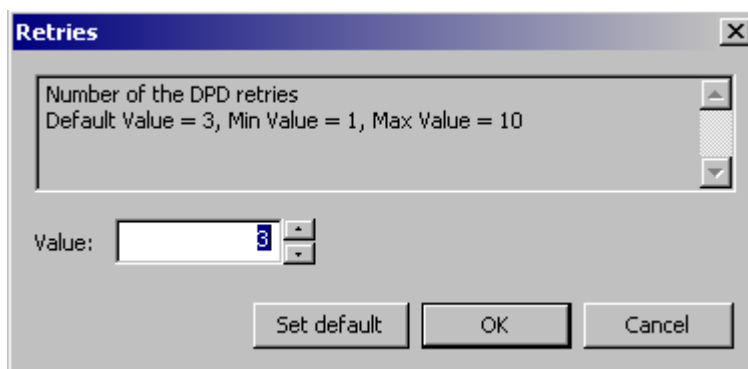


Рисунок 47

11.8.2. Режим ручного задания LSP

В режиме ручного задания локальная политика безопасности задается администратором (вкладки Rules, IKE и IPSec становятся невидимыми)

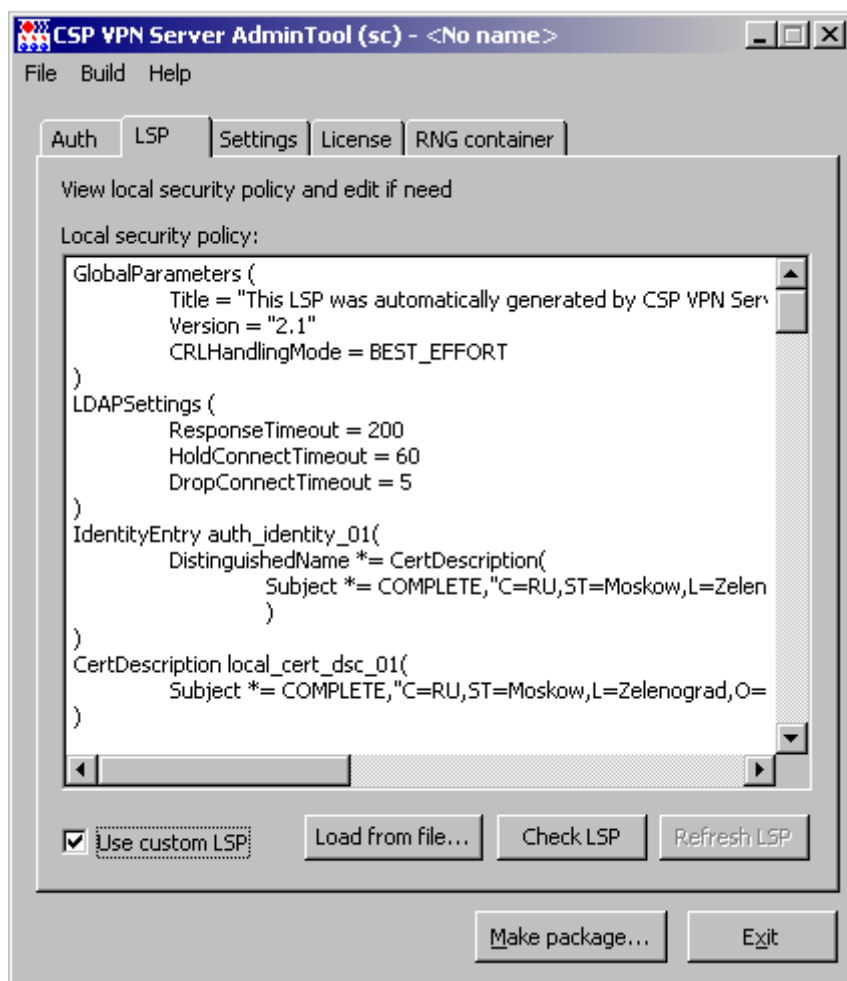


Рисунок 48

Local security policy – поле с текстовым представлением локальной политики безопасности. В этом поле можно создавать и редактировать LSP.

User custom LSP – снятие этого флажка переводит в режим автоматического формирования LSP

Load from file – при нажатии этой кнопки происходит загрузка LSP из файла в поле Local security policy.

Check LSP – при нажатии этой кнопки происходит проверка заданной LSP по выявлению синтаксических ошибок. При обнаружении ошибки выдается сообщение с описанием ошибки (если строка с ошибочными символами определена, то она выделяется и на эту строку автоматически переводится фокус). Если данная LSP не содержит синтаксических ошибок, то выдается сообщение, что синтаксических ошибок не найдено.

11.9. Settings

Во вкладке Settings задаются настройки протоколирования событий, политика по умолчанию и дополнительные параметры инсталляции Продукта CSP VPN Server.

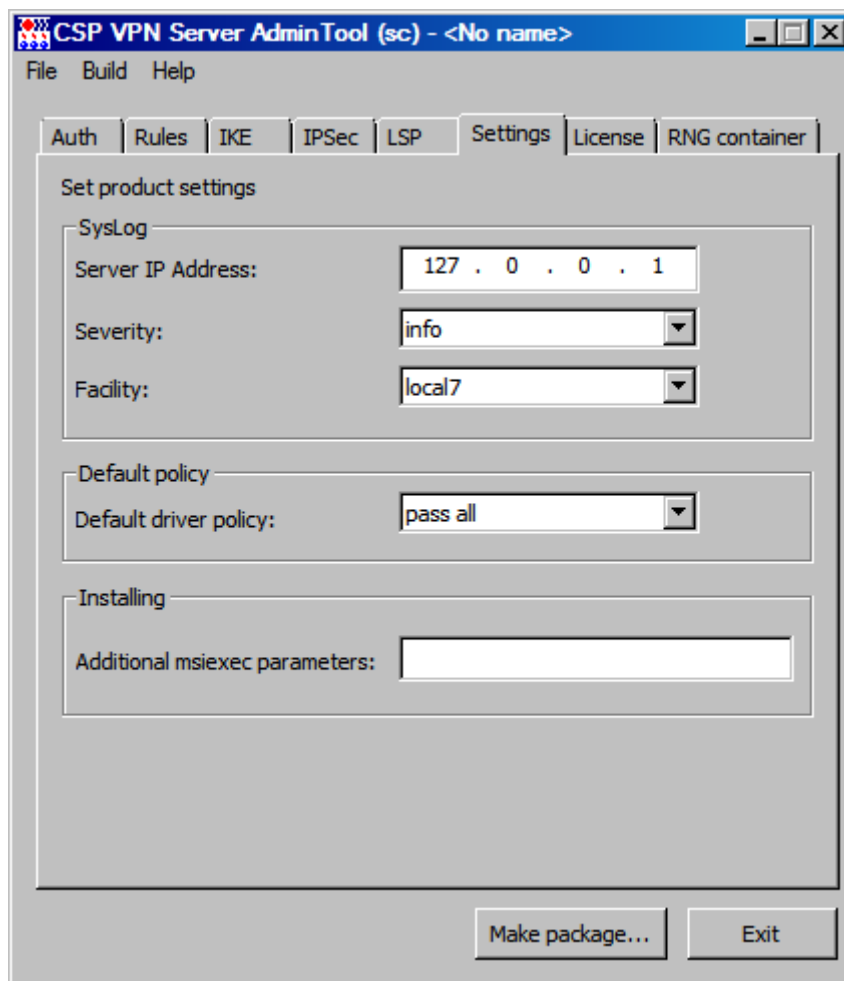


Рисунок 49

Для задания настроек Syslog-клиента заполняются следующие поля:

- **Server IP-Address** – IP-адрес компьютера, на который будут посылаться сообщения о протоколируемых событиях. Значение по умолчанию – 127.0.0.1, которое означает, что сообщения посылаются на локальный хост.
- **Severity** – задание глобального уровня протоколирования событий. Содержит выпадающий список значений - emerg, alert, crit, err, warning, notice, info, debug. Значение по умолчанию – notice. Заданный глобальный уровень протоколирования используется тогда, когда не задан уровень протоколирования для разных событий во вкладке LSP в окне Advanced LSP Settings переменной [Log level](#). Уровни в выпадающем списке указаны в порядке убывания серьезности сообщений. Если выбран уровень *info*, то будут переданы сообщения и о более важных событиях.
- **Facility** – задание источника, который будет выдавать сообщения об ошибках. Содержит выпадающий список значений -local0, local1, local2, local3, local4, local5, local6, local7. Значение по умолчанию -local7.
- **Default Driver Policy (DDP)** – политика драйвера по умолчанию. Выпадающий список содержит два значения:
 - правило Passall – пропускать все пакеты. Значение по умолчанию

- правило PassDHCP – пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для настройки TCP/IP стека по протоколу DHCP.

Политика DDP, которая определяется администратором, загружается в следующих случаях:

- при ошибочной загрузке конфигурации – до старта VPN Service
- при остановке VPN Service.

Additional msixec parameters - дополнительные параметры запуска WinInstaller, которые можно установить. Например, альтернативная инсталляционная директория, настройки лога Windows Installer и т.п. Эти параметры можно посмотреть по ссылке http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp

Например, для протоколирования событий при инсталляции CSP VPN Server в файл C:\Server\install_log_file.txt нужно выставить опцию

```
/l* C:\Server\install_log_file.txt.
```

Эту опцию рекомендуется указать, если планируется выбрать режим инсталляции silent.

Можно задать максимальное время (в секундах), которое необходимо для инициализации VPN-сервиса (vpnsvc). В поле дополнительных параметров запуска указывается параметр MAX_SERVICE_START_TIMEOUT и его значение, например,

MAX_SERVICE_START_TIMEOUT=45. Значение по умолчанию - 30 секунд. Максимальное значение – 600 секунд.

11.10. License

Во вкладке License задаются регистрационные данные Лицензии на Продукт CSP VPN Server:

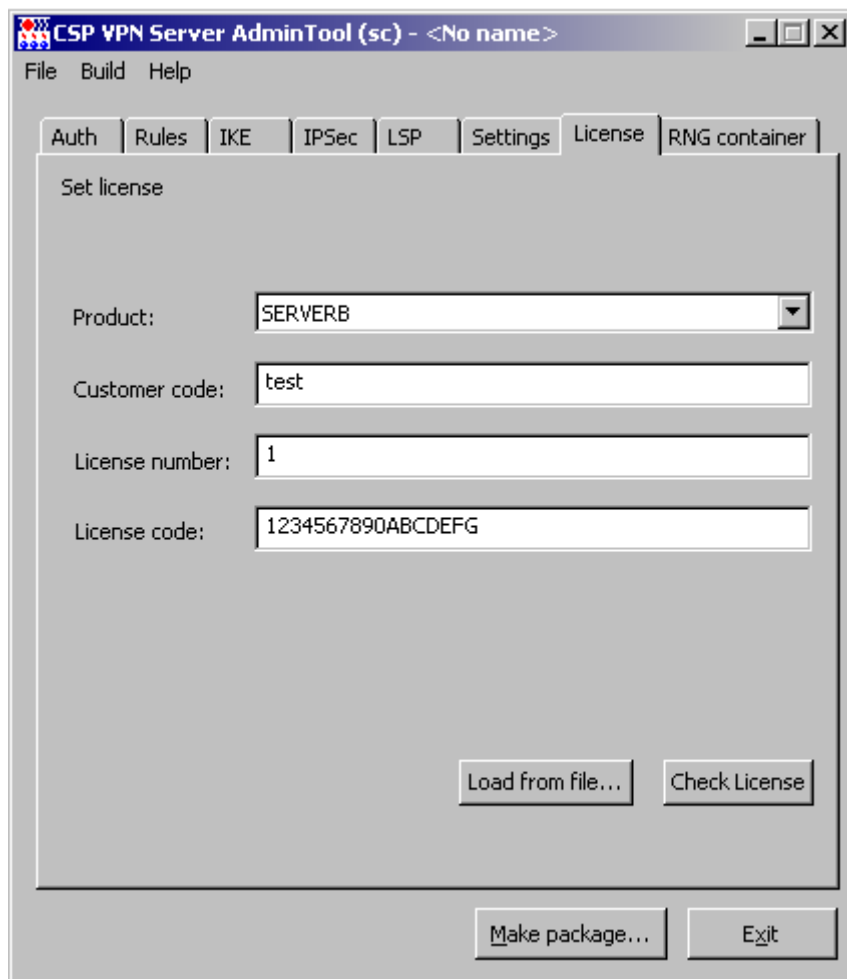


Рисунок 50

Данные Лицензии:

- **Product** – выпадающий список для задания типа Продукта - SERVERB/SERVER
- **Customer code** – код конечного пользователя
- **License number** – номер лицензии
- **License code** – код лицензии.

Кнопки управления:

- **Load from file** – при нажатии этой кнопки происходит загрузка данных Лицензии из указанного текстового файла. В файле данные Лицензии должны быть записаны в виде:

```
[license]
CustomerCode=NNNN
ProductCode=SERVERB/SERVER
LicenseNumber=NNNN
LicenseCode=NNNNNNN
```

- **Check License** – проверка правильности введенных данных Лицензии.

11.11. RNG container

Во вкладке RNG container задается информация о местонахождении криптографического (RNG) контейнера, который содержит инициализационные данные для датчика случайных чисел (ДСЧ). RNG контейнер представляет собой каталог, поэтому имя контейнера – имя каталога.

Примечание: RNG контейнер должен храниться на носителе, доступ к которому осуществляется без каких-либо паролей под пользователем System. Например, нельзя задавать контейнер на токене или сетевом диске.

Для задания размещения контейнера переключатель ставится в одно из четырех положений:

- При выборе **Create new RNG container** новый RNG контейнер будет создан на этапе инсталляции Продукта CSP VPN Server. В поле `RNG container` нужно указать полный путь к новому создаваемому контейнеру, если указанного каталога не существует, то он будет создан на конечном устройстве. Во время инсталляции CSP VPN Server появится окно, в котором нужно будет ввести начальную информацию для RNG контейнера с клавиатуры, например: "Step= 1/16 Press k [6b]: " (введите символ "к" и нажмите Enter) и т.д. Таким образом, формируется уникальное число для датчика случайных чисел, которое практически невозможно подобрать.
- При выборе **Use existing container** будет использоваться существующий RNG контейнер при инсталляции. Нужно указать полный путь к существующему RNG контейнеру на конечном устройстве в поле `RNG container`. Датчик случайных чисел, при каждом использовании этого контейнера, будет зачитывать из него информацию и модифицировать его.
- При выборе **Copy RNG container** во время инсталляции CSP VPN Server будет копироваться содержимое одного контейнера в другой. В поле `Source RNG container` нужно указать полный путь к существующему контейнеру и контейнеру, в который он будет скопирован в поле `RNG container`. Если каталога для нового контейнера не существует, то он будет создан. ДСЧ будет использовать информацию, которая была записана в контейнере.
- При выборе **Copy RNG container from admin computer** контейнер RNG будет перемещен с компьютера администратора в инсталляционный файл, а во время инсталляции CSP VPN Server будет скопирован на конечное устройство. В поле `Source RNG container` нужно указать полный путь к существующему RNG контейнеру на компьютере администратора, а в поле `RNG container` - полный путь к контейнеру на конечном устройстве. Если каталога для нового контейнера не существует, то он будет создан.

Source RNG container - поле, в которое вводится полный путь и имя RNG контейнера для копирования.

RNG container - поле, в которое вводится полный путь и имя RNG контейнера для создания нового контейнера и использования существующего. В этом поле может использоваться подстановка `%INSTALLDIR%`, которая означает каталог, в который будет установлен Продукт (по умолчанию – CSP VPN Server).

Use certificate container as RNG container – флажок, установка которого означает, что в качестве RNG контейнера будет использоваться контейнер с сертификатом конечного устройства. При этом контейнер с сертификатом конечного устройства не должен иметь пароль. Этот элемент доступен только при аутентификации на сертификатах. При выставлении в активное состояние этого элемента все другие элементы вкладки становятся неактивными.

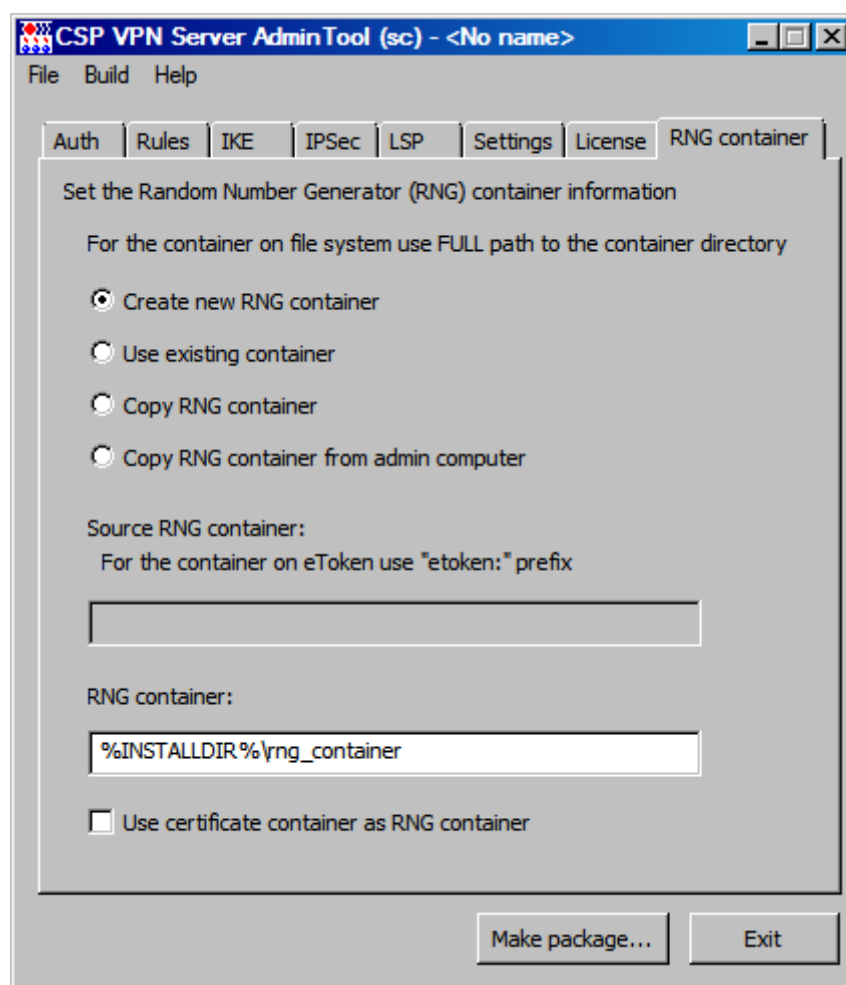


Рисунок 51

11.12. Создание инсталляционного файла

Создание инсталляционного файла происходит при нажатии кнопки **Make package** в главной форме. При этом происходит проверка корректности введенных данных и при обнаружении ошибки выводится сообщение о возможных причинах, и переключение на вкладку с некорректными данными. Если ошибки не обнаружено, то появляется окно **Package parameters**:

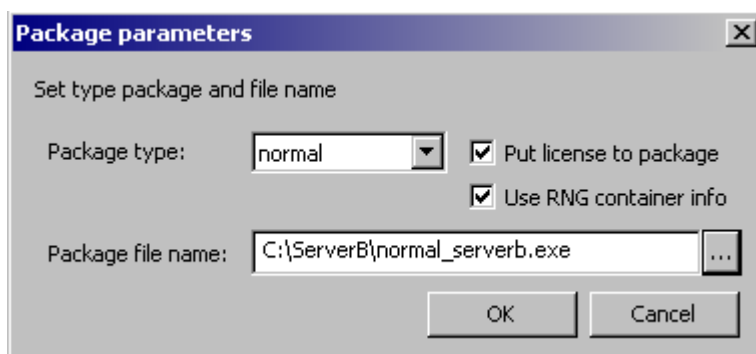


Рисунок 52

В этом окне необходимо задать:

- **Package type** – поле для выбора режима инсталляции. Возможные значения:
 - `basic` – неинтерактивная установка с запросом на инсталляцию. Вариант по умолчанию
 - `normal` – интерактивная установка (в диалоговом режиме) с демонстрацией Лицензионного Соглашения и другими окнами
 - `silent` – неинтерактивная установка без запросов. Стартует сразу после запуска EXE-файла без дополнительных запросов.
- **Package file name** – поле для ввода имени инсталляционного файла на компьютере администратора
- **Put license to package** – при установке этого флажка введенные данные Лицензии будут включены в инсталляционный файл. При этом вкладка `License` должна содержать корректные данные Лицензии.
- **Use RNG container info** – при установке этого флажка введенная информация об RNG контейнере будет включена в инсталляционный файл.

При нажатии кнопки **OK** вызывается утилита `make_inst.exe` с соответствующими опциями, которая и создает инсталляционный файл. На время работы утилиты появляется окно с просьбой подождать:

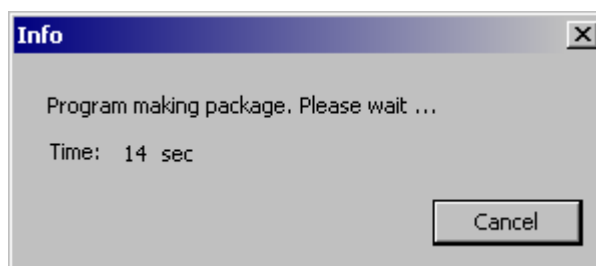


Рисунок 53

В случае выявления ошибки выдается сообщение о коде ошибки.

При нажатии на кнопку Cancel работа утилиты make_inst.exe прерывается (инсталляционный файл не создается). В случае успешного завершения работы утилиты выдается сообщение о создании инсталляционного файла:

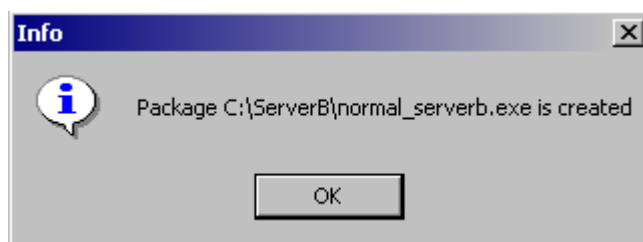


Рисунок 54

Все сообщения, выдаваемые программной утилитой make_inst в процессе ее работы, выводятся в файл make_inst_log.txt (при каждом создании инсталляционного файла make_inst_log.txt переписывается).

11.13. Сохранение данных проекта

В процессе сохранения проекта – Save Project as (Save Project)- сохраняются данные тех вкладок, которые на данный момент являются активными. Данные вкладок, которые являются невидимыми, не сохраняются. Исключение составляет ситуация: при переключении на ручное задание LSP (вкладка LSP, выставление флажка "Use custom LSP") данные вкладок Rules, IKE и IPSec сохраняются в проекте, не смотря на то, что после переключения эти вкладки являются неактивными и не показываются администратору. При повторном открытии сохраненного проекта, при переходе к режиму автоматического формирования LSP (снятие флажка "Use custom LSP"), все введенные ранее администратором данные во вкладках Rules, IKE и IPSec будут доступны для дальнейшего редактирования. Данная особенность реализована для облегчения редактирования LSP при ее автоматическом формировании.

11.14. Формат задания имен алгоритмов в файле admintool.ini

Имена алгоритмов, используемые во вкладках IKE, IPSec и LSP, задаются в файле admintool.ini в секции [algorithm_names]:

```
[algorithm_names]
ike-hash=GR341194CPR01-65534
ike-cipher=G2814789CPR01-K256-CBC-65534
ah-integrity=GR341194CPR01-H96-HMAC-254
esp-integrity=GR341194CPR01-H96-HMAC-65534
esp-cipher=G2814789CPR01-K256-CBC-254
```

Для большей наглядности разрешается назначать алгоритмам пользовательские псевдонимы (в этом случае во вкладках IKE и IPSec будут отображаться не реальные имена, а назначенные псевдонимы). Для задания псевдонима необходимо дополнить строку имени алгоритма именем псевдонима, заключенного в круглые скобки:

```
[algorithm_names]
ike-hash=GR341194CPR01-65534
ike-cipher=G2814789CPR01-K256-CBC-65534 (ГОСТ 28147-89)
ah-integrity=GR341194CPR01-H96-HMAC-254 (ГОСТ Р 34.11-94)
esp-integrity=GR341194CPR01-H96-HMAC-65534 (ГОСТ Р 34.11-94)
esp-cipher=G2814789CPR01-K256-CBC-254 (ГОСТ 28147-89)
```

12. Установка CSP VPN Server

Продукт CSP VPN Server работает под управлением операционных систем:

- MS Windows Vista (32-bit) Business SP1 Russian Edition
- MS Windows XP Professional SP2 Russian Edition.

Установка программного Продукта CSP VPN Server на конечное устройство осуществляется администратором запуском инсталляционного файла, который он подготовил.

Инсталляция должна производиться пользователем, имеющим права администратора.

Инсталляция CSP VPN Server происходит в одном из 3 режимов, который был выбран администратором при подготовке инсталляционного файла:

- режим `basic` – основной режим, неинтерактивная установка с запросом на инсталляцию, вариант по умолчанию
- режим `normal` – интерактивная установка
- режим `silent` – неинтерактивная установка без запросов.

Все протоколируемые события при инсталляции CSP VPN Server будут записываться в файл, если администратор задал его при создании инсталляционного файла для конечного устройства.

При возникновении ошибок во время инсталляции или работы Продукта устраните их и попытайтесь повторно провести инсталляцию Продукта. При появлении сбоев во время работы Продукта перезагрузите компьютер, но если перезагрузка не устраняет проблему – обратитесь в службу поддержки по адресу <mailto:support@s-terra.com>.

При инсталляции CSP VPN Server происходит отключение стандартного сервиса, связанного с IPsec и IKE и перевод его в состояние Manual. В Windows XP – это Служба IPSEC, внутреннее название которой PolicyAgent. В Windows Vista – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности» (внутреннее название – IKEEXT).

В Windows Vista производится настройка штатного FireWall сервиса (Брандмауэр Windows). При установке CSP VPN Server в Windows FireWall добавляется новое правило:

- правило для входящих подключений
- имя – CSP VPN Service – UDP allowed (predefined)
- правило включено
- действие – разрешить подключение
- протокол – UDP (все порты)
- программа – полный путь к установленному файлу `vpnsvc.exe`
- службы – применять только к службам
- профили – все профили
- остальные параметры – по умолчанию.

Эти настройки можно посмотреть следующим образом: Панель управления – Администрирование – Брандмауэр Windows в режиме повышенной безопасности – Правила для входящих подключений.

12.1. Режим basic

В ОС **Windows Vista** при установке CSP VPN Server выдается окно (Рисунок 55). Необходимо разрешить запуск инсталлятора – выберите предложение **Разрешить**.

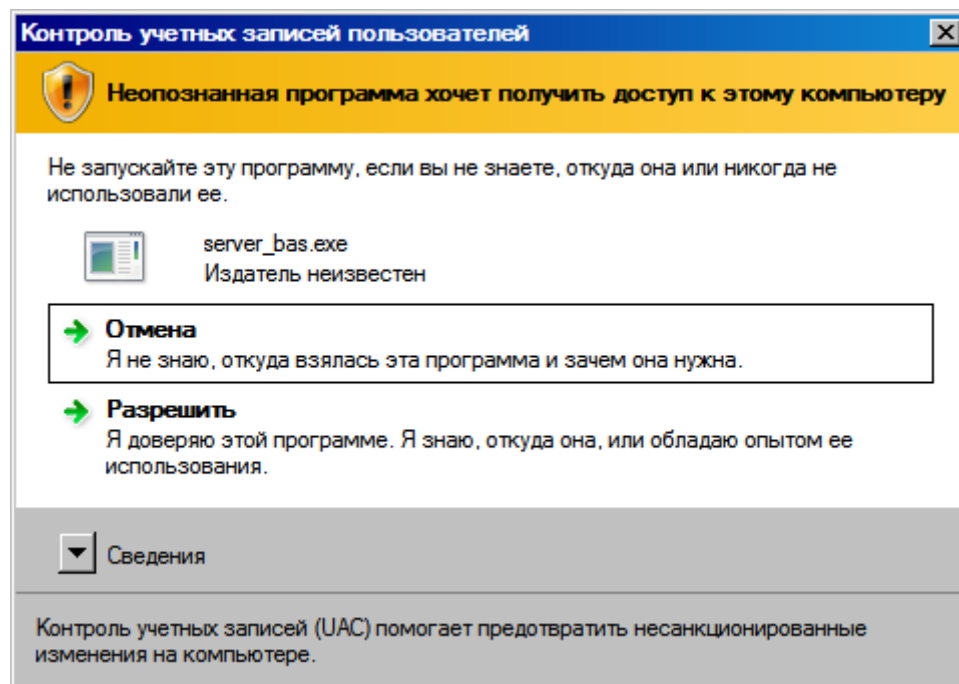


Рисунок 55

Затем выдается запрос на инсталляцию CSP VPN Server (в ОС Windows XP это окно появляется первым):

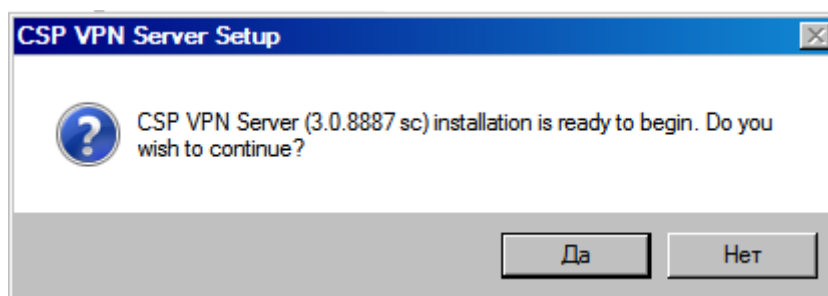


Рисунок 56

После нажатия кнопки **Да** происходит установка Продукта:



Рисунок 57

И появляется окно с индикатором процесса инсталляции:

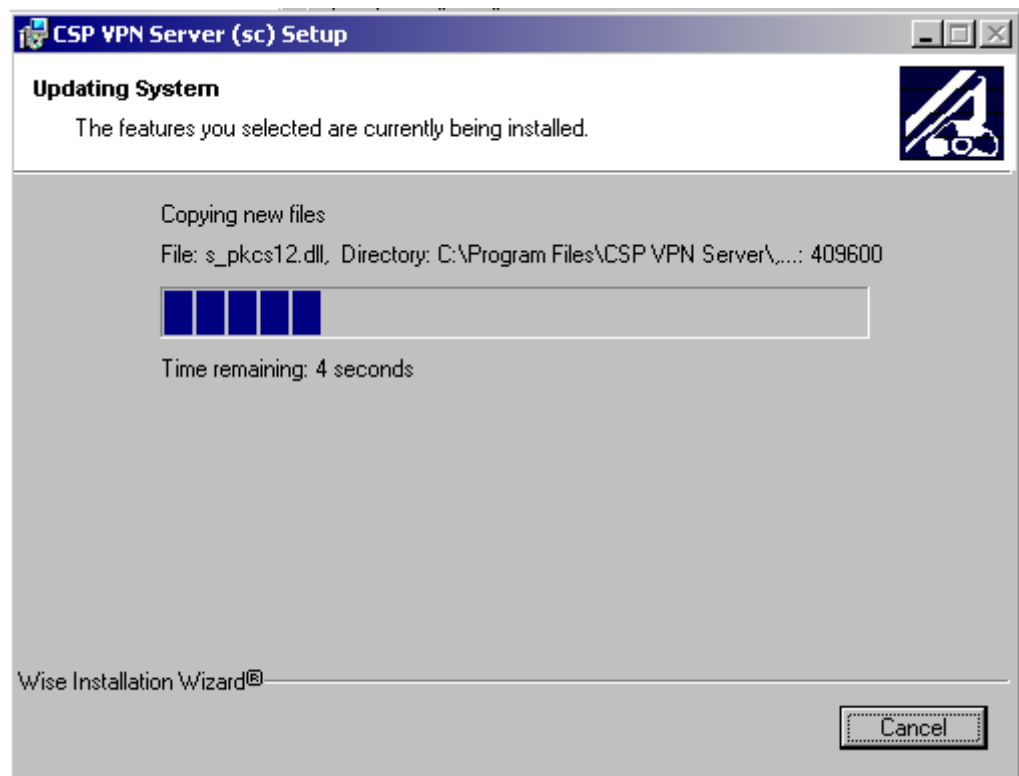


Рисунок 58

Если в процессе инсталляции происходит создание RNG контейнера, то появится окно, в котором просят ввести какую-то начальную информацию для датчика случайных чисел (ввести символы, которые выводятся на экран, и нажать Enter):

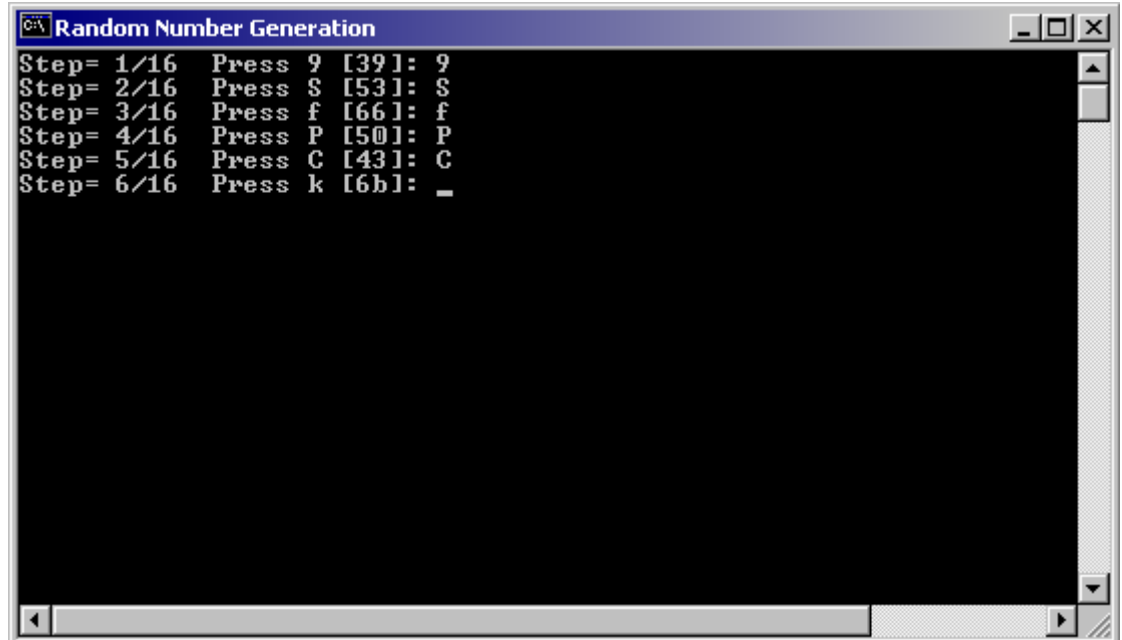


Рисунок 59

Если используется существующий RNG контейнер или происходит его копирование, то окно Random Number Generation не появляется.

Если создается новый RNG контейнер или происходит его копирование, а перед инсталляцией уже существует контейнер с указанным именем, то он будет замещен новым контейнером (без дополнительных запросов).

При инсталляции в ОС Windows Vista появляется окно (Рисунок 60) с запросом на установку драйверов. Выберите предложение – Все равно установить этот драйвер.

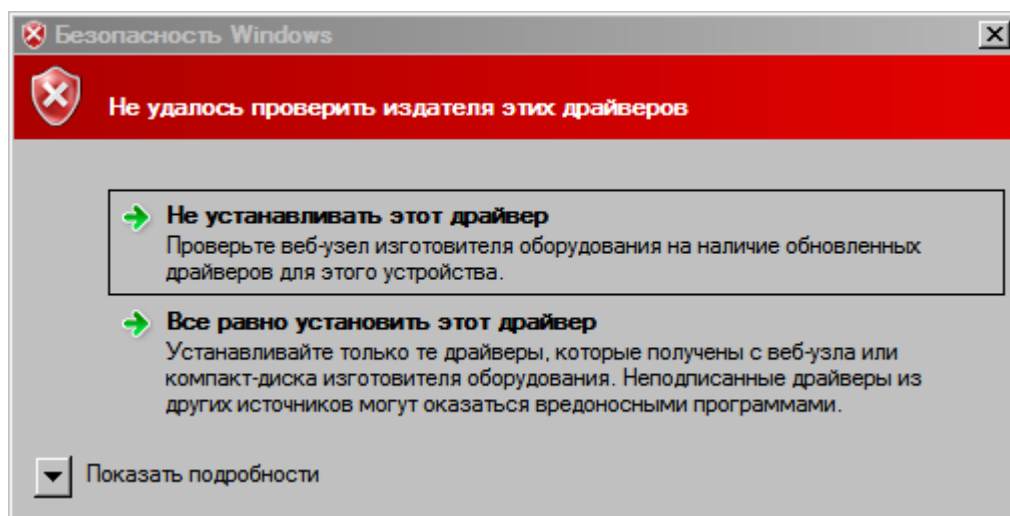


Рисунок 60

При инсталляции в ОС Windows XP, если реакция системы Windows на установку неподписанных драйверов установлена в положение Предупреждать (Пуск – Настройка – Панель управления – Система – Свойства системы – Оборудование – Подписывание драйверов – Предупреждать), возможно появление окна (Рисунок 61) для подтверждения установки на интерфейс VPN Filter. Таких окон может появиться несколько. Для продолжения процесса инсталляции нажмите кнопку Все равно продолжить в каждом из этих окон:



Рисунок 61

Для отключения возможности появления такого окна, установите реакцию системы Windows на установку неподписанных драйверов в положение Пропускать (Пуск – Настройка – Панель управления – Система – Свойства системы – Оборудование – Подписывание драйверов – Пропускать).

После инсталляции CSP VPN Server появляется окно с предупреждением о необходимости перезагрузки системы:

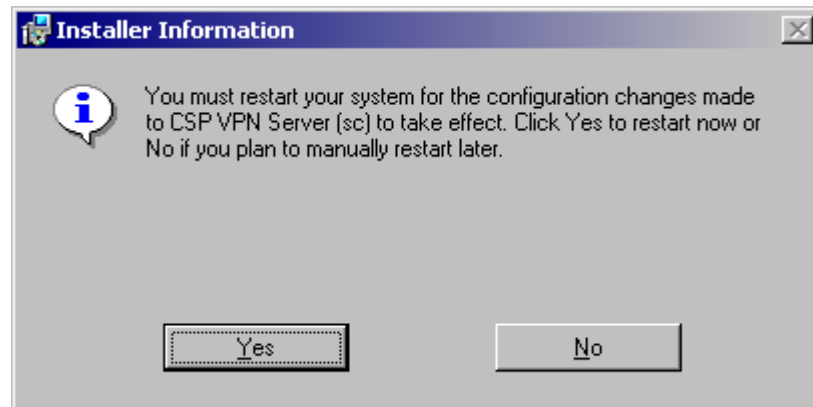


Рисунок 62

12.2. Режим normal

Этот режим является диалоговым режимом.

В ОС **Windows Vista** при установке CSP VPN Client выдается окно (Рисунок 55). Необходимо разрешить запуск инсталлятора – выберите предложение **Разрешить**.

Открывается стартовое окно с приглашением к инсталляции:



Рисунок 63

После нажатия кнопки **Next** будет открыто окно с текстом Лицензионного Соглашения. Установка переключателя в положение "I accept the license agreement" делает кнопку **Next** доступной:

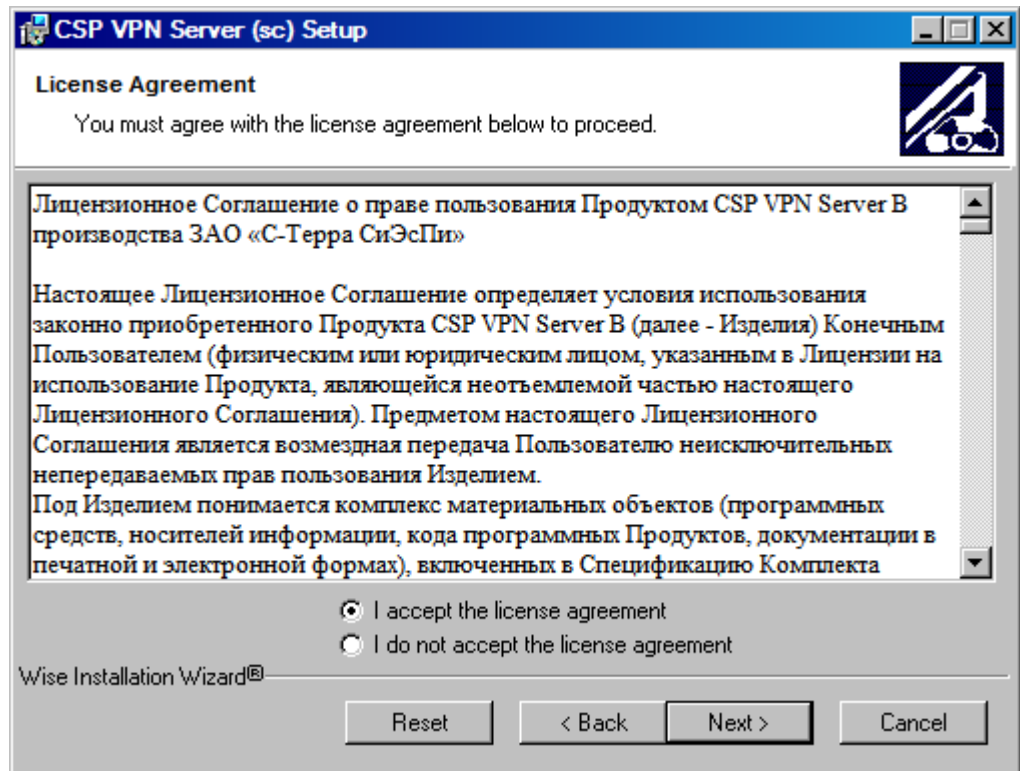


Рисунок 64

Для указания папки, в которую будет установлен Продукт, нажать кнопку **Browse** и сделать выбор:

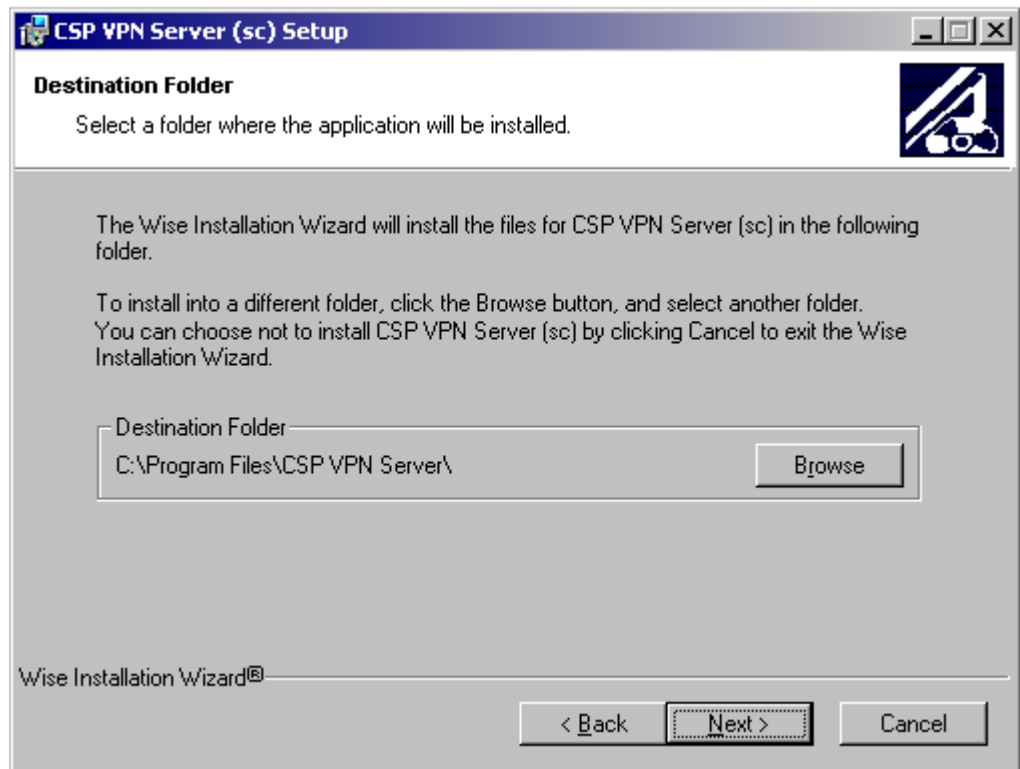


Рисунок 65

Если при создании инсталляционного файла настройки RNG контейнера не были включены в инсталляционный файл, то появится окно ввода информации о размещении RNG контейнера, который содержит инициализационные данные для датчика случайных чисел (Рисунок 66).

Для задания размещения RNG контейнера нужно установить переключатель в одно из трех положений:

- **Create new RNG container** – будет создан новый RNG контейнер на этапе инсталляции Продукта CSP VPN Server. В поле **RNG container** нужно указать полный путь к новому создаваемому контейнеру, если указанного каталога не существует, то он будет создан.
- **Use existing container** – будет использоваться существующий RNG контейнер. Нужно указать полный путь к существующему RNG контейнеру в поле **RNG container**. Датчик случайных чисел, при каждом использовании этого контейнера, будет зачитывать из него информацию и модифицировать его.
- **Copy RNG container** – во время инсталляции CSP VPN Server будет копироваться содержимое одного контейнера в другой. В поле **Source RNG container** нужно указать полный путь к существующему RNG контейнеру и контейнеру, в который он будет скопирован в поле **RNG container**. Если каталога для нового контейнера не существует, то он будет создан. ДСЧ будет использовать информацию, которая была записана в контейнере.

Если создается новый RNG контейнер или происходит его копирование, а перед инсталляцией уже существует контейнер с указанным именем, то он будет замещен новым контейнером (без дополнительных запросов).

В поле **RNG container** может использоваться подстановка **%INSTALLDIR%**, которая означает каталог, в который будет установлен Продукт (по умолчанию – CSP VPN Server), например, **%INSTALLDIR%\rng_cont**.

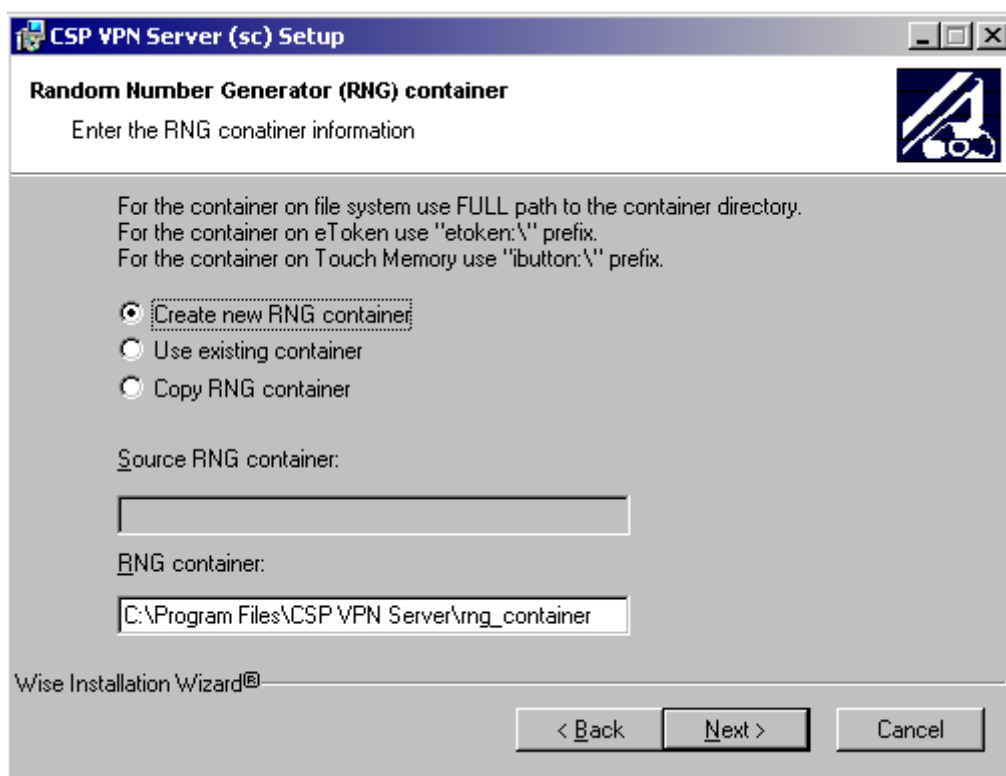


Рисунок 66

Если при создании инсталляционного файла регистрационные данные Лицензии на Продукт CSP VPN Server не были включены в инсталляционный файл, то появится окно для ввода данных Лицензии на Продукт:

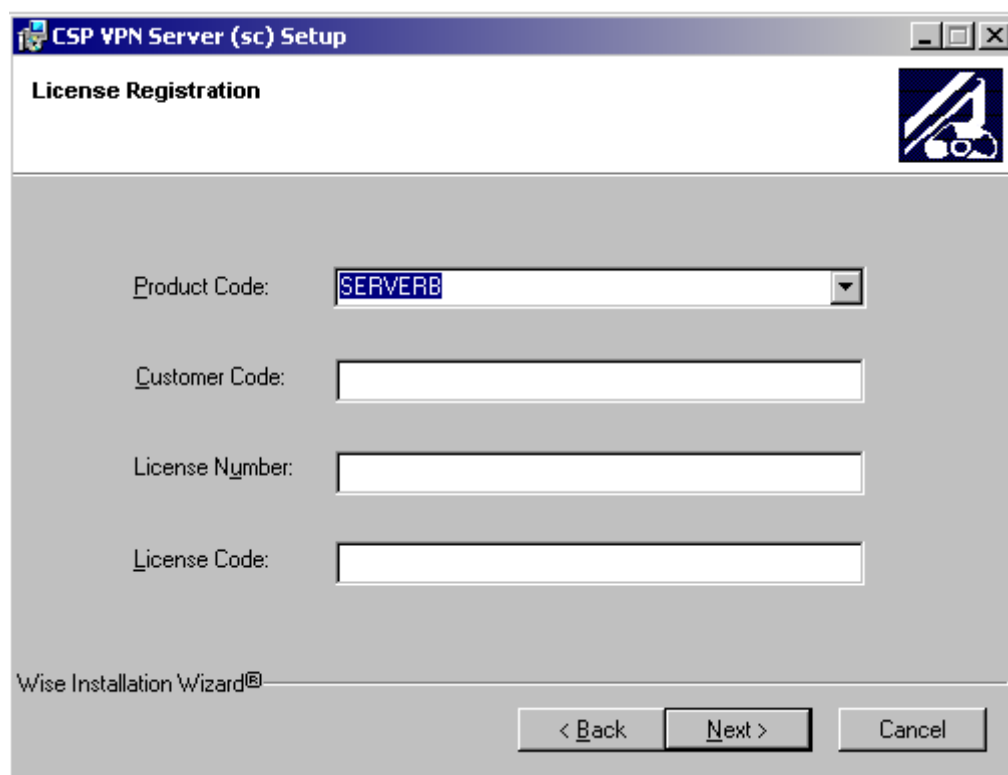


Рисунок 67

Стандартное окно сообщает о готовности к инсталляции. Для начала инсталляции нажать Next:

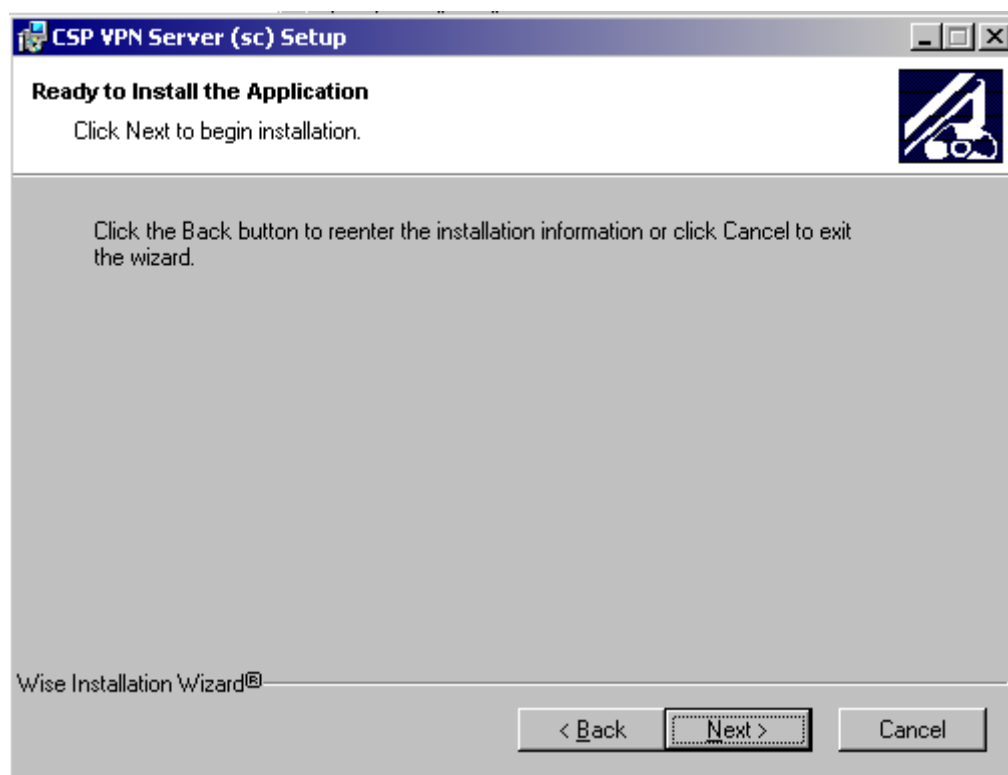


Рисунок 68

Далее появляется окно с индикатором процесса инсталляции:

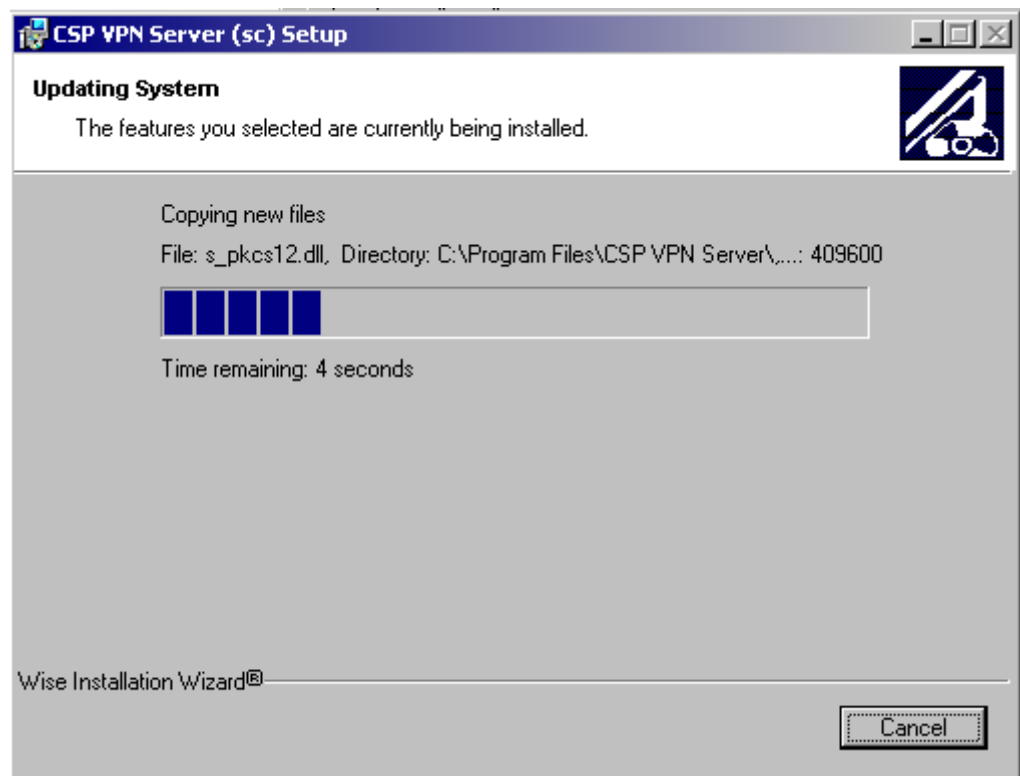


Рисунок 69

Если происходит создание RNG контейнера, то в следующем окне просят ввести какую-то начальную информацию для датчика случайных чисел (ввести символы, которые выводятся на экран, и нажать **Enter**). Таким образом, формируется уникальное число для датчика случайных чисел, которое практически невозможно подобрать:

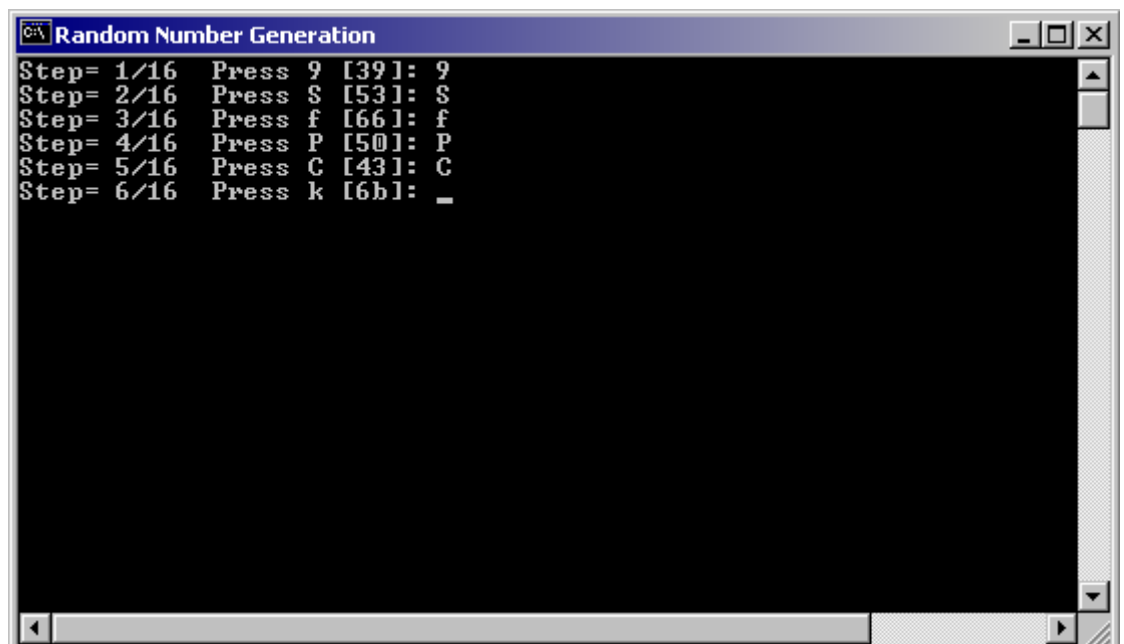


Рисунок 70

Если используется существующий RNG контейнер или происходит его копирование, то окно Random Number Generation не появляется.

Дальнейшее поведение инсталлятора зависит от ОС и установленной администратором опции Подписывание драйверов, описанной в разделе ["Режим basic"](#).

После завершения процедуры инсталляции нажать **Finish**:



Рисунок 71

После инсталляции CSP VPN Server появляется окно с предупреждением о необходимости перезагрузки системы (Рисунок 62).

12.3. Режим silent

В ОС **Windows Vista** при установке CSP VPN Server выдается окно (Рисунок 55). Необходимо разрешить запуск инсталлятора – выберите предложение **Разрешить**.

В режиме **silent** происходит установка CSP VPN Server без запросов, но могут появляться либо системные диалоговые окна, либо некоторые интерактивные компоненты, относящиеся к криптоподсистеме.



Рисунок 72

Если происходит создание RNG контейнера, то в следующем окне просят ввести какую-то начальную информацию для датчика случайных чисел (ввести символы, которые выводятся на экран, и нажать **Enter**):

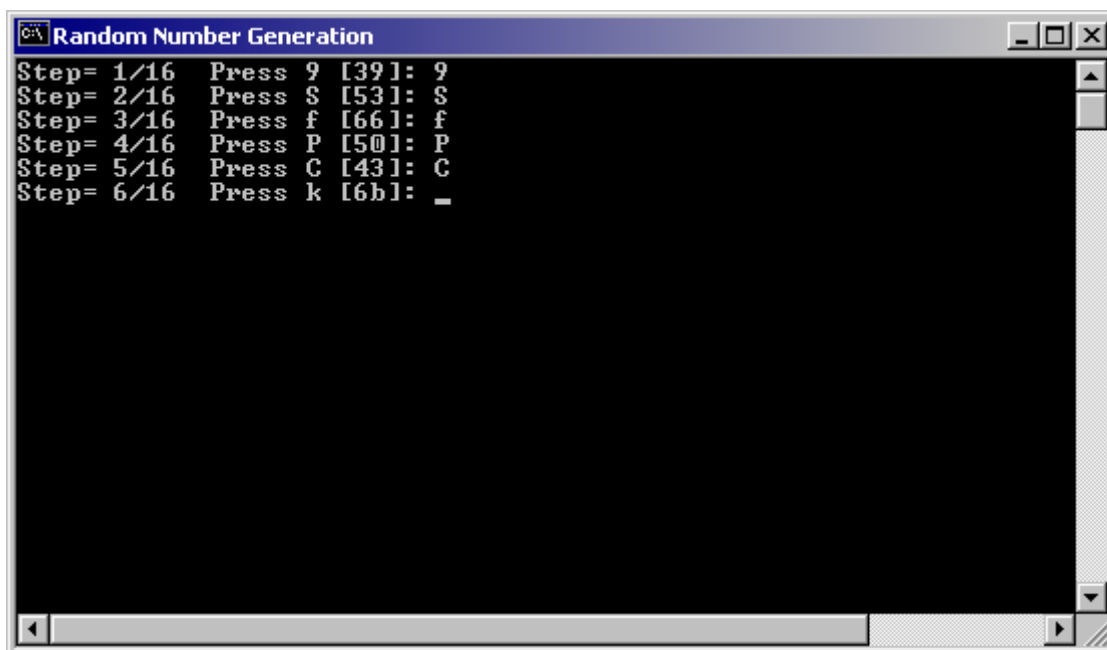


Рисунок 73

Если используется существующий RNG контейнер или происходит его копирование, то окно Random Number Generation не появляется.

При инсталляции в ОС **Windows Vista** появится окно (Рисунок 60) с запросом на установку драйверов. Выберите предложение – Все равно установить этот драйвер.

Если инсталляция происходит в ОС **Windows XP** и реакция системы Windows на установку неподписанных драйверов поставлена в положение Предупреждать (Пуск – Настройка – Панель управления – Система – Свойства системы – Оборудование – Подписывание драйверов – Предупреждать), то возможно появление сообщения (Рисунок 61). для подтверждения установки на интерфейс VPN Filter. Для продолжения процесса инсталляции нажмите кнопку Все равно продолжить на каждом из этих сообщений.

По окончании установки CSP VPN Server происходит перезагрузка операционной системы без предупреждений.

Примечание: если при инсталляции будет обнаружена база локальных настроек, оставшаяся от предыдущей установки продукта, то по умолчанию, выбирается вариант сохранения найденной базы. В некоторых ситуациях это может привести к неработоспособности или некорректной работе продукта.

В случае возникновения ошибок и прерывания инсталляции никакие сообщения на экран не выводятся. Эти сообщения можно посмотреть программой ОС Windows «Просмотр событий» или, если при подготовке инсталляционного пакета Администратором была указана опция протоколирования событий при инсталляции в файл, то сообщения можно посмотреть в заданном файле.

12.4. Копирование контейнера при инсталляции

Если при подготовке инсталляционного файла с использованием сертификатов была указана опция `-cs` (в случае создания инсталляционного пакета при помощи утилиты `make_inst.exe`) или задано копирование контейнера с сертификатом (инсталляционный пакет создавался при помощи графического интерфейса), то при инсталляции CSP VPN Server будет происходить копирование контейнера с секретным ключом.

Если на момент инсталляции не существовало контейнера с тем же именем, в который происходит копирование, и копирование контейнера прошло без ошибок, то никаких дополнительных сообщений и запросов администратору не выдается.

В случае если контейнер, в который происходит копирование уже существует, то выдается окно следующего вида:

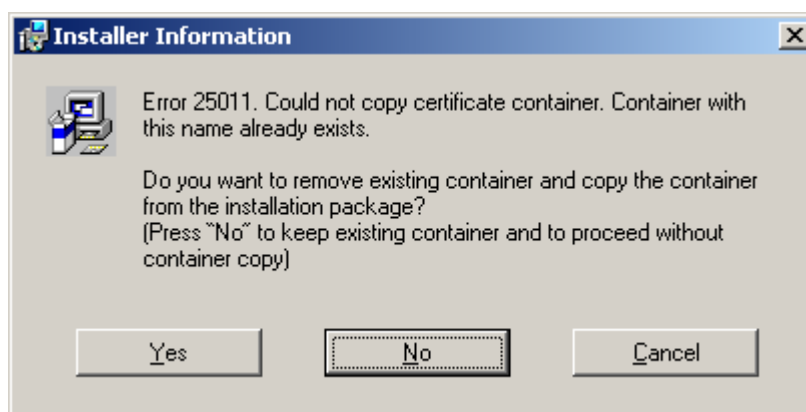


Рисунок 74

Если нажать "Yes", то существующий контейнер будет удален и процедура копирования будет продолжена.

Если нажать "No", существующий контейнер останется, а процедура копирования будет отменена.

Если нажать "Cancel", то инсталляция CSP VPN Server будет прервана.

Если происходит копирование в файловую систему, то недостающие папки пути к создаваемому контейнеру (опция `-uc`) при копировании будут созданы (если есть такая возможность).

Если секретный ключ расположен внутри контейнера (по стандартному пути), то он будет скопирован без дополнительных усилий.

Если заданы опции `-kfs` и `-kf`, то происходит копирование секретного ключа из файла, заданного в опции `-kfs`, в файл, заданный в опции `-kf`. Недостающие папки пути к создаваемому файлу (опция `-kf`) при копировании будут созданы (если есть такая возможность). Происходит простое копирование файла, поэтому эти опции нельзя использовать для копирования секретного ключа, расположенного на токене.

Примечание: если инсталляции происходит в режиме `silent`, и на компьютере пользователя уже существует контейнер с указанным именем, в который происходит копирование, то инсталляция прерывается без выдачи на экран каких-либо запросов пользователю.

12.5. Сообщения об ошибках

Ниже приведены тексты сообщений об ошибках, которые могут возникать при установке CSP VPN Server.

Таблица 1

	Текст сообщения	Примечание
25001	License check failed.	Неправильная лицензия
25006	RNG initialization failed. {Reason: <reason>}. Installation aborted. RNG container path: <path> где <reason> может быть одним из следующих (здесь и далее для других сообщений, связанных с контейнерами для СигналКОМ): Bad path syntax (use only FULL pathname). Wrong path (possibly wrong drive letter is used). Possibly token error or bad path syntax. <Win_err_message> – системное сообщение об ошибке, например "Access is denied", "The system cannot find the drive specified", "The media is write protected", "There is not enough space on the disk" и т.п. System error: <win_err_code> – числовой код системной ошибки, для которой не удалось подобрать словесного описания. В отдельных случаях Reason может отсутствовать.	Не удалось создать RNG контейнер. {Причина: <reason>} Установка прервана. Путь к RNG контейнеру: <path> Перевод основных <reason>: Неправильный синтаксис пути к контейнеру (можно использовать только ПОЛНЫЙ путь). Неправильный путь (вероятно использовано ошибочное имя диска). Вероятно ошибка токена или неправильный путь к контейнеру.
25007	Existing RNG initial value not found or invalid. {Reason: <reason>}. Installation aborted. RNG container path: <path> где <path> – путь к RNG-контейнеру.	Не найден корректный RNG контейнер. Установка прервана. Путь к RNG контейнеру: <path>
25008	Copy RNG container failed. {Reason: <reason>}. Installation aborted. Source RNG container path: <src>. Destination RNG container path: <dst>.	Не удалось скопировать RNG контейнер. {Причина: <reason>} Установка прервана. Путь к исходному RNG контейнеру: <src>. Путь к новому RNG контейнеру: <dst>.
25009	Copy certificate container failed. {Reason: <reason>}. Installation aborted. Source container path: <src>. Destination container path: <dst>.	Не удалось скопировать сертификатный контейнер. {Причина: <reason>} Установка прервана. Путь к исходному контейнеру: <src>. Путь к новому контейнеру: <dst>.

	Текст сообщения	Примечание
25010	Copy secret key file failed. Installation aborted.	Не удалось скопировать файл секретного ключа.
25011	Could not copy certificate container. Container with this name already exists. Do you want to remove existing container and copy the container from the installation package? (Press "No" to keep existing container and to proceed without container copy)	Нельзя скопировать сертификатный контейнер, поскольку контейнер с таким именем уже есть. Хотите ли вы удалить существующий контейнер и скопировать контейнер из инсталляционного пакета? (Нажмите "No" для того, чтобы сохранить существующий контейнер и продолжить без копирования)
25017	Product "<Product_name version>" was detected. You should uninstall it first before the installation.	Был обнаружен продукт "<Product_name version>". Вам необходимо сначала деинсталлировать его.
	You must have Administrator privileges	Вам необходимы администраторские привилегии
	This product needs Windows 2000 or higher	Для продукта необходима Windows 2000 или выше
25019	The "<dll_path>" was wrongly marked as the previous GINA DLL. The system GINA DLL will be used instead.	[Windows XP] Файл <dll_path> был ошибочно помечен, как предыдущая GINA DLL. Будет использована системная GINA DLL.
25020	The previous GINA DLL "<dll_path>" was not found. The system GINA DLL will be used instead.	[Windows XP] Предыдущая GINA DLL <dll_path> не найдена. Будет использована системная GINA DLL.
25021	Driver "<driver_name>" installation failed. Product installation aborted.	Не удалось установить драйвер <driver_name>. Инсталляция продукта прервана.
25022	Product "<Product_name version>" was advertised. You should uninstall it first before the installation.	Для продукта <Product_name version> была выполнена операция объявления пользователям (advertisement). Вы должны деинсталлировать его до инсталляции.
25024	Network interface configuration failed.	Ошибка при настройке сетевого интерфейса.
25025	Windows Firewall setup failed.	[Windows Vista] Не удалось настроить Windows Firewall.
25026	You must have Administrator privileges.	Вам необходимы администраторские привилегии.
25027	Invalid RNG initialization method.	Неправильно задан тип инициализации ДСЧ (параметр RNG_CONTAINER_CHOICE).

13. Деинсталляция CSP VPN Server

Деинсталляция CSP VPN Server производится стандартными средствами операционной системы – вызовом модуля Add/Remove Programs и выбором из списка строки CSP VPN Server.

При деинсталляции CSP VPN Server происходит включение стандартного сервиса, связанного с IPsec и IKE. В Windows XP – это Служба IPSEC, в Windows Vista – это Служба «Модули ключей IPsec для обмена ключами в Интернете и протокола IP с проверкой подлинности».

В Windows Vista при деинсталляции CSP VPN Server выдается окно (Рисунок 75). Необходимо разрешить запуск деинсталлятора.

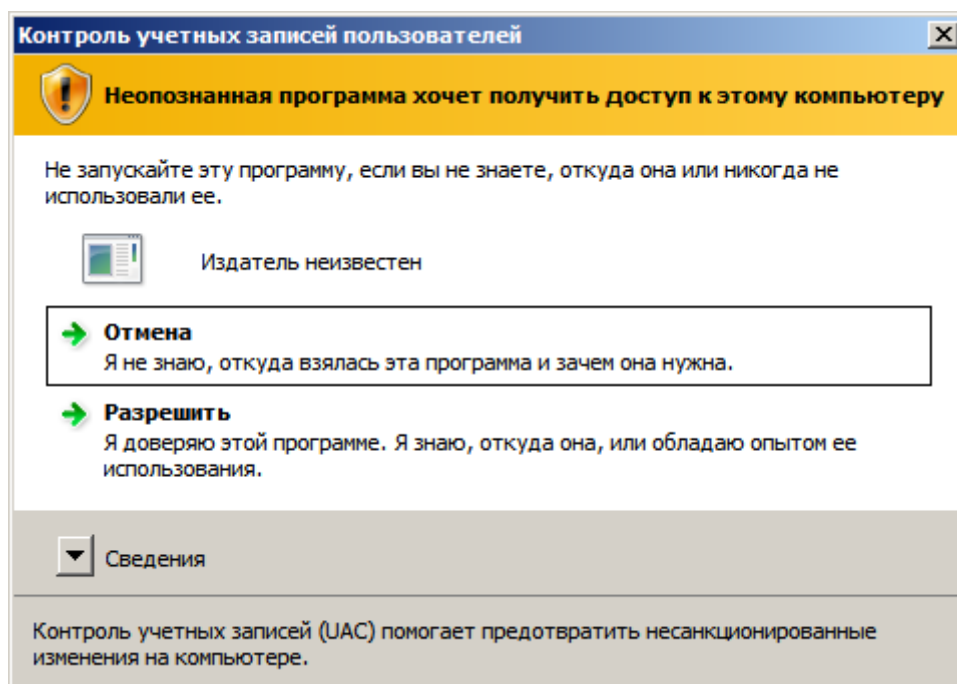


Рисунок 75

14. Восстановление CSP VPN Server

Во внештатных ситуациях – сбой в работе продукта, зависание продукта и др. перезагрузите LSP конфигурацию командой `lsp_reload` (если это возможно) или перезапустите компьютер. Если функции продукта не восстановились, то переустановите CSP VPN Server.

15. Создание локальной политики безопасности. Конфигурационный файл

Под политикой безопасности понимается совокупность правил, по которым обрабатываются пакеты входящего и исходящего трафика. Пакеты могут проходить как пакетную фильтрацию, так и обработку с использованием криптографических алгоритмов – построение защищенных (VPN) туннелей между партнерами.

Создание локальной политики безопасности (LSP – Local Security Policy) CSP VPN Server осуществляется путем написания конфигурационного файла в текстовом формате для VPN устройства (конечного устройства).

15.1. Описание грамматики LSP

Синтаксические диаграммы верхнего уровня языка описания конфигурации

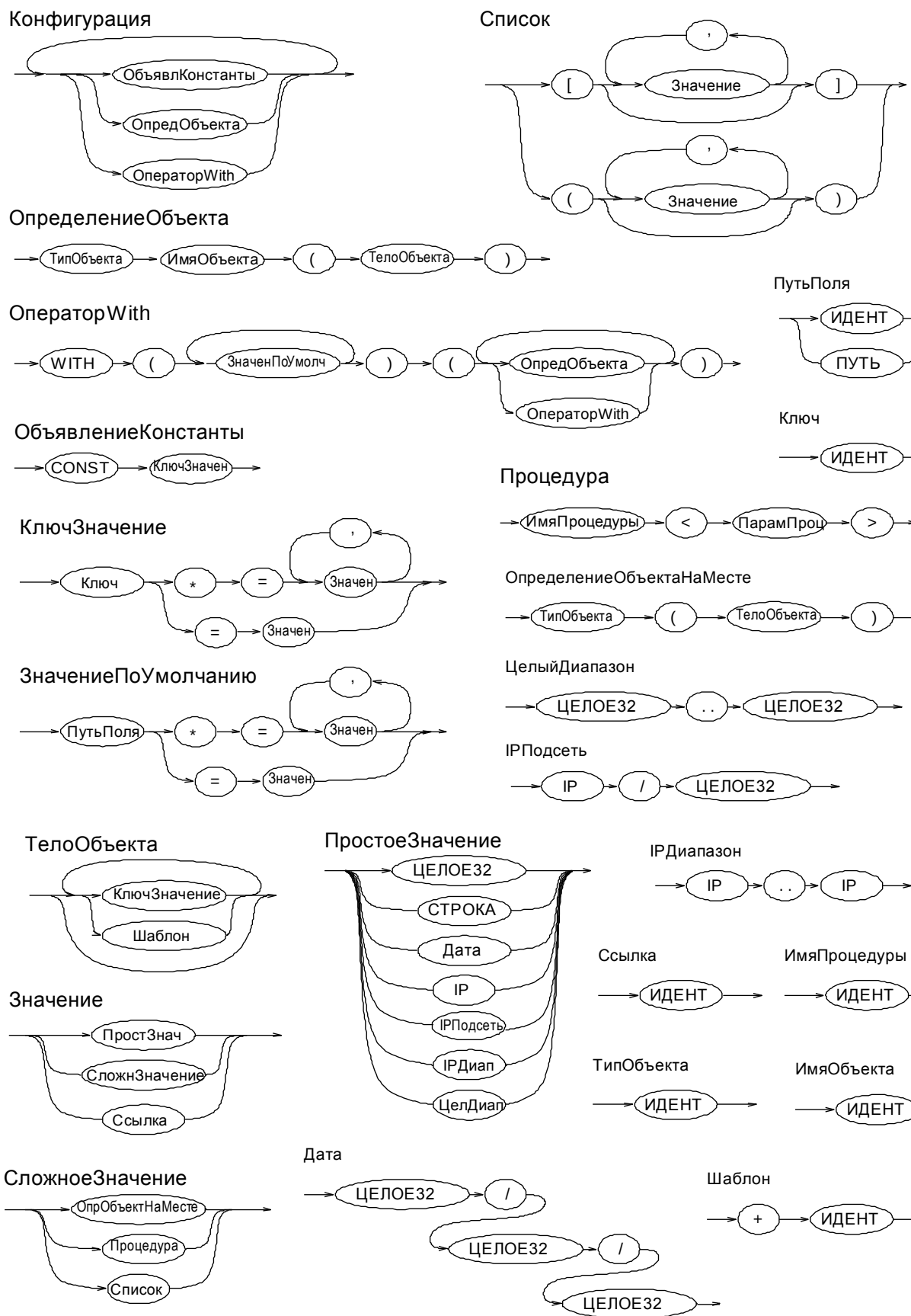


Рисунок 76

Описание LSP представляет собой последовательное описание структур данных, определяемых типом, именем, списком параметров (полей) и их значений. Синтаксис языка определяет формат описания структур данных, базовые типы значений полей структур. Синтаксические конструкции позволяют описывать иерархические структуры данных, число уровней которых не ограничено.

Терминальные символы

Терминальный символ **идент** обозначает идентификатор. Идентификатор состоит из латинских букв, цифр, символов '_' и '-'. Он должен начинаться с латинской буквы или символа '_'. Запрещено использование идентификаторов, совпадающих с ключевыми словами `with` и `const`. Внутри имен подстановок оператора `with` могут быть использованы символы '.'.

Примеры идентификаторов:

```
Moscow-16
_WWW_
IKECFGRequestAddress
IKERule
LOCAL_IP_ADDRESSES
```

Терминальный символ **СТРОКА** служит для обозначения строки, состоящей из любых символов, заключенных в двойные кавычки (".."). Если внутри строки необходим символ двойной кавычки, то его следует дополнить слева символом '\'. Для использования символа '\' (back-slash) в строке, его нужно ставить два раза подряд ('\\' – двойной back-slash). Допустимо указывать и один back-slash, т.к. при перекодировании восстанавливается двойной back-slash.

Примеры задания значений типа СТРОКА:

```
Title = "Moon Gate LSP"
IntegrityAlg = "MD5-H96-KPDK"
X509SubjectDN *= "C=RU,O=OrgName,OU=qa0,CN=snickers0"
```

Терминальный символ **ЦЕЛОЕ32** представляет 32-битное целое число без знака. Число может быть записано в десятичной или шестнадцатеричной системе счисления. Во втором случае оно должно начинаться цифрой и заканчиваться буквой 'h' или 'H'. В шестнадцатеричном и десятичном представлении запись числа не может быть длиннее 10 символов, включая букву 'h'.

Примеры задания числовых значений параметров:

```
RetryTimeBase = 4
BlacklogSessionsMax = 16
LifetimeKilobytes = 0abcdh
```

Терминальный символ **IP** обозначает сетевой адрес четвертой версии IP-протокола. IP-адрес состоит из четырех чисел, разделенных точками, где каждое из чисел принадлежит диапазону от 0 до 255.

Примеры IP-адресов:

```
PeerIPAddress = 192.168.2.1
```

Значения типа ДАТА

Тип **дата** представляется тремя целыми числами без знака, разделенными символом '/' – число/месяц/год.

Пример даты:

```
StartOfValidity = 24/03/ 2004  
EndOfValidity = 3/6/2004
```

Ключевые слова

Ключевые слова **with**, **const** используются при создании специальных конструкций.

На диаграмме (Рисунок 76) эти ключевые слова написаны прописными (большими) буквами. В конфигурационном файле ключевые слова должны быть написаны строчными буквами.

Комментарии

Комментарии могут размещаться в любом месте текста между другими терминалами и являются разделителями, эквивалентными символу пробела. Вложения комментариев одного типа не допускаются. Поддерживаются следующие два вида комментариев:

Блочный. Начинается с символов "**"**" и заканчивается символами "**"**" или начинается символом "**{**" и заканчивается символом "**}**".

Строковый. Начинается с символа "**#**", заканчивается символом перевода каретки **<LF>**.

Примеры комментариев:

```
20..30 # Диапазон чисел 20-30  
Action *= (tunnel_ipsec_des_md5_action) (* будет описан ниже *)
```

Разделители

В качестве разделителей в LSP-языке могут быть использованы следующие символы: пробел, табуляция, **<LF>** и **<CR>**. Переходом на новую строку считается символ **<LF>**.

Разделители необходимы только для отделения терминалов **идент**, **целое32**, **ip**, ключевых слов **const**, **with** друг от друга.

Диапазоны значений

```
ProtocolID *= 20..30  
IKECFGPool *= 192.168.13.17..192.168.13.127
```

Списки значений

При указании списка значений для какого-либо параметра перед знаком '=' должен стоять символ '*'. Если параметр может иметь список значений, но необходимо указать только одно, то символ '*' можно опустить.

```
GroupID *= MPDP_768, MODP_1024
```

Вложенные списки

Для описания вложенных **списков** могут использоваться круглые или квадратные скобки.

```
ContainedProposals *= (ipsec_ah_md5, ipsec_esp_des3),  
                      (ipsec_ah_md5, ipsec_esp_idea)
```


Ссылки на структуры

```
LocalCredential *= cert1
```

Определение вложенных структур

```
Transform *= IKETransform(  
  CipherAlg *= "DES-CBC"  
  HashAlg *= "MD5"  
  GroupID *= MODP_768  
  LifetimeSeconds = 86400  
  LifetimeKilobytes = 4608000  
  LifetimeDerivedKeys = 100000  
)
```

Объявление структуры верхнего уровня

```
FilteringRule Client_Gate(  
  LocalIPFilter* = FilterEntry( IPAddress *= 250.192.32.5 )  
  PeerIPFilter* = FilterEntry( IPAddress *= 10.10.12.4 )  
  Action* = ( Client_Gate )  
)
```

Специальные конструкции

Для упрощения описания повторяющихся параметров предусмотрена возможность использования именованных констант, значений по умолчанию и шаблонов.

В отличие от других конструкций языка, которые подвергаются семантическому анализу, константы и шаблоны полностью обрабатываются на этапе синтаксического разбора.

Описание каждой **константы** начинается с ключевого слова `const`, за которым следует имя константы и ее значение (или список значений). Значением константы может являться любая конструкция, которая может быть значением поля структуры. Использование константы заключается в подстановке ее имени вместо значения поля структуры.

Пример:

```
const A = FilterEntry(  
  IPAddress *= 10.10.12.5  
  ProtocolID = 6  
  Port =80  
)  
  
FilteringRule Filter_1 (  
  PeerIPFilter* = A  
  Action* = ( PASS)  
)
```

Шаблон (template) является константой, единственное значение которой является структурой того типа, к которой этот шаблон будет применен. Для использования шаблона, внутри описания структуры необходимо написать символ '+' и имя константы за ним. Подстановка шаблона заключается в копировании всех полей из структуры, которая является значением константы, в структуру, в которую шаблон подставляется.

Не допускается задавать одни и те же поля и в шаблоне и структуре, в которую он подставляется.

Пример описания:

```
const Transform_DES_MD5 = IKETransform(  
    CipherAlg *= "DES-CBC"  
    HashAlg *= "MD5"  
    GroupID *= MODP_768  
  
)  
  
Transform *= IKETransform(  
    + Transform_DES_MD5  
    LifetimeSeconds = 86400  
    LifetimeKilobytes = 4608000  
  
)
```

Эквивалентное описание:

```
Transform *= IKETransform(  
    CipherAlg *= "DES-CBC"  
    HashAlg *= "MD5"  
    GroupID *= MODP_768  
    LifetimeSeconds = 86400  
    LifetimeKilobytes = 4608000  
  
)
```

Конструкция WITH используется для задания значений по умолчанию для полей структур, которые описываются внутри конструкции. После ключевого слова 'with' указываются пути к полям и значения по-умолчанию для них. Путь к полю структуры может быть записан двумя способами:

- первый вариант - это просто имя поля. В этом случае в каждую структуру, которая описана внутри with, будет добавлено указанное поле, если в структуре такого поля нет.
- во втором варианте путь записывается в форме тип_верх_ур.имя_поля1.имя_поля2имя_поляМ. В этом случае имя_поляМ с указанным значением будет добавлено только для структур, которые указаны в качестве значения соответствующего поля структуры уровнем выше. Тип структуры, содержащей имя_поля1 должен быть тип_верх_ур. Значения добавляются только в те структуры, которые определены непосредственно внутри других, а не в виде ссылки.

Значения добавляются только в том случае, если в структуре явно не указано других значений для поля.

Пример:

```
(* Указание значения по умолчанию, используя полное имя поля  
(путь).*)  
  
with (  
    (* Значение по умолчанию для FilteringRule.LocalIPFilter *)  
    FilteringRule.LocalIPFilter = FilterEntry(IPAddress =  
        10.0.16.84)  
) (  
  
    FilteringRule f0 (  
        PeerIPFilter = FilterEntry(IPAddress= 192.168.12.11)  
        Action = (DROP))  
  
    FilteringRule f1 (  
        PeerIPFilter = FilterEntry(IPAddress= 192.168.19.22)
```

```
    Action = (PASS)
  )
)

(* Та же конфигурация, сокращённая форма - задано значение по
умолчанию для всех структур верхнего уровня, независимо от
типа.*)

with (
  LocalIPFilter = FilterEntry(IPAddress = 10.0.16.84)
) (

  FilteringRule f0 (
    PeerIPFilter = FilterEntry(IPAddress= 192.168.12.11)
    Action = (DROP)
  )

  FilteringRule f1 (
    PeerIPFilter = FilterEntry(IPAddress= 192.168.19.22)
    Action = (PASS)
  )
)

(* Результирующая конфигурация.*)

FilteringRule f0 (
  PeerIPFilter = FilterEntry(IPAddress= 192.168.12.11)
  LocalIPFilter = FilterEntry(IPAddress = 10.0.16.84)
  Action = (DROP)
)

FilteringRule f1 (
  PeerIPFilter = FilterEntry(IPAddress= 192.168.19.22)
  LocalIPFilter = FilterEntry(IPAddress = 10.0.16.84)
  Action = (PASS)
)
```

15.2. Структура конфигурации

Структуру конфигурации можно разделить на три логические части:

- Заголовок (GlobalParameters)
- Глобальные параметры протокола IKE (IKEParameters)
- Правила фильтрации (FilteringRules)

Структура конфигурации предполагает наличие только одного заголовка (GlobalParameters), одной структуры глобальных параметров протокола IKE (IKEParameters) и неограниченное количество правил фильтрации (FilteringRule).

Диаграмма структуры конфигурации и взаимосвязь между ее элементами

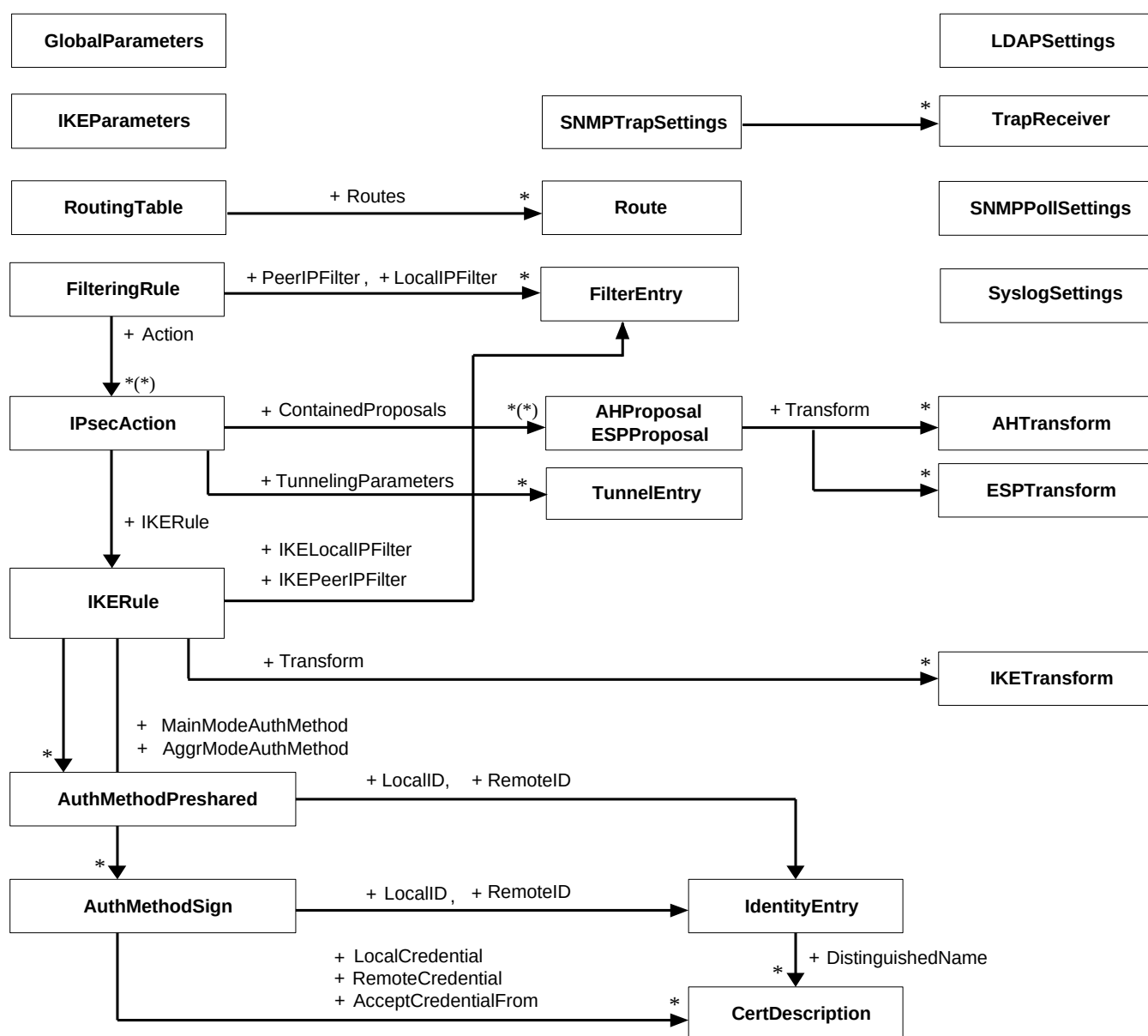


Рисунок 77

Пояснения к диаграмме:

- в прямоугольниках указаны имена структур данных, составляющих локальную политику безопасности
- стрелка обозначает отношение использования между структурами данных
- рядом со стрелкой указан атрибут структуры, который ссылается на используемую структуру
- '*' рядом со стрелкой обозначает, что атрибут содержит список используемых структур
- '*(*)' обозначает, что атрибут содержит список списков используемых структур.

Таблица 2

Структура конфигурации в табличном виде		
<u>GlobalParameters</u>		<u>LDAPSettings</u>
Title Version Type Serial StartOfValidity EndOfValidity CRLHandlingMode LDAPLogMessageLevel SystemLogMessageLevel PolicyLogMessageLevel CertificatesLogMessageLevel		Server Port SearchBase ConnectTimeout ResponseTimeout HoldConnectTimeout DropConnectTimeout
<u>IKEParameters</u>		<u>SyslogSettings</u>
SendRetries RetryTimeBase RetryTimeMax SACreationTimeMax InitiatorSessionsMax ResponderSessionsMax BlacklogSessionsMax BlacklogSessionsMin BlacklogSilentSessions BlacklogRelaxTime		Server Facility
<u>SNMPPollSettings</u>	<u>SNMPTrapSettings</u>	<u>TrapReceiver</u>
LocalIPAddress Port ReadCommunity SysLocation SysContact	Receivers	IPAddress Port Community Version SNMPv1AgentAddress
<u>RoutingTable</u>		
Routes _____	Route Destination Gateway NetworkInterface Metric	
<u>FilteringRule</u>		
PeerIPFilter _____ * LocalIPFilter _____ * NetworkInterfaces RefuseTCPPeerInit Action _____ * (*)		<u>FilterEntry</u> <u>FilterEntry</u> IPAddress ProtocolID Port
<u>IPsecAction</u> _____		

Структура конфигурации в табличном виде

IPsecAction TunnelingParameters _____ GroupID _____ ShuffleTunnelEntries _____ ContainedProposals _____ * (*) NoSmoothRekeying _____ IKERule _____ 	
--	--

В таблице жирным шрифтом выделены имена структур, а курсивом – обязательные атрибуты.

Название структуры в таблице также является ссылкой на описание этой структуры и ее атрибутов.

Знак "*" в конце атрибута конфигурационного файла означает, что значения данного атрибута представлены в виде списка. Если знак "*" не установлен, то предполагается, что вместо списка будет использовано только одно значение или одна ссылка.

15.3. Заголовок конфигурации

Заголовок конфигурации представляет собой структуру, описывающую общие параметры CSP VPN Server. В конфигурации должна быть только одна структура данного типа. Этой структуре имя не присваивается.

<u>Имя структуры</u>	GlobalParameters
<u>Атрибуты</u>	Title
	Version
	Type
	Serial
	StartOfValidity
	EndOfValidity
	CRLHandlingMode
	LDAPLogMessageLevel
	SystemLogMessageLevel
	PolicyLogMessageLevel
	CertificatesLogMessageLevel

Пример:

```
GlobalParameters (  
    Title = "Moon host LSP"  
    Version = "2.1"  
    Serial = "0000000100000000E00000001"  
    CRLHandlingMode = DISABLE  
    LDAPLogMessageLevel = INFO  
    SystemLogMessageLevel = INFO  
    PolicyLogMessageLevel = INFO  
    CertificatesLogMessageLevel = INFO  
)
```

Атрибут Title

Атрибут Title предназначен для краткого описания конфигурации (имя конфигурации).

<u>Синтаксис</u>	Title = СТРОКА
<u>Значение</u>	строка произвольного содержания
<u>Значение по умолчанию</u>	пустая строка

Атрибут Version

Атрибут Version определяет версию спецификации конфигурации.

<u>Синтаксис</u>	Version = СТРОКА
<u>Значение</u>	строка вида [0-9].[0-9]
<u>Значение по умолчанию</u>	пустая строка.

Атрибут Type

Атрибут Type специфицирует тип конфигурации, который определяет действия агента при ее активизации.

<u>Синтаксис</u>	Type = PERMANENT TEMPORARY
<u>Значения</u>	PERMANENT – после успешной активизации конфигурации она сохраняется в базе данных Продукта, если она была активизирована из файла. При следующем запуске Продукта конфигурация будет автоматически активизирована из базы данных Продукта. TEMPORARY – после успешной активизации, конфигурация не сохраняется в базе данных и используется только в текущем сеансе работы Продукта.
<u>Значение по умолчанию</u>	PERMANENT.

Атрибут Serial

Атрибут Serial определяет уникальный серийный номер конфигурации.

<u>Синтаксис</u>	Serial = СТРОКА
<u>Значение</u>	строка содержит шестнадцатеричное представление серийного номера конфигурации
<u>Значение по умолчанию</u>	пустая строка

Атрибут StartOfValidity

Атрибут StartOfValidity определяет момент времени, до которого конфигурация не может быть активизирована.

<u>Синтаксис</u>	StartOfValidity = ДАТА
<u>Значение</u>	01/1/0000 – 31/12/9999
<u>Значение по умолчанию</u>	ограничения отсутствуют на активизацию конфигурации

Атрибут EndOfValidity

Атрибут EndOfValidity определяет момент времени, после которого конфигурация не может быть активизирована.

<u>Синтаксис</u>	EndOfValidity = ДАТА
<u>Значение</u>	01/1/0000 – 31/12/9999
<u>Значение по умолчанию</u>	ограничения отсутствуют на активизацию конфигурации

Атрибут CRLHandlingMode

Атрибут CRLHandlingMode определяет режим обработки списка отозванных сертификатов (CRL).

<u>Синтаксис</u>	CRLHandlingMode = DISABLE OPTIONAL BEST_EFFORT ENABLE
<u>Значения</u>	DISABLE – при проверке сертификата CRL не обрабатывается OPTIONAL – при проверке сертификата CRL используется только в случае, если он был предустановлен в базу Продукта или получен (и обработан) в процессе IKE обмена и является действующим BEST_EFFORT – при проверке сертификата CRL используется только в том случае, если он является действующим, если это не так, то CRL может быть получен посредством протокола LDAP (агент смотрит адрес LDAP-сервера сначала в поле CDP сертификата, а затем ищет структуру LDAPSettings). Если CRL получить не удалось – сертификат принимается. ENABLE – при проверке сертификата обязателен действующий CRL, если это не так, то CRL может быть получен посредством протокола LDAP. Если CRL получить не удалось – сертификат не принимается.
<u>Значение по умолчанию</u>	ENABLE.

Атрибут LDAPLogMessageLevel

Атрибут LDAPLogMessageLevel задает текущий уровень детализации протоколирования для событий, связанных с доступом к LDAP-серверу.

Синтаксис

```
LDAPLogMessageLevel =  DEBUG |  
                        INFO |  
                        NOTICE |  
                        WARNING |  
                        ERR |  
                        CRIT |  
                        ALERT|  
                        EMERG
```

Значения уровни детализации протоколирования определены в RFC 3164³.

Значение по умолчанию

Если этот атрибут не указан или не загружена конфигурация, то действуют общие настройки. Общий уровень протоколирования для всех событий устанавливается опцией [-s в утилите make inst.exe](#). Если общий уровень не менялся, то он имеет значение DEBUG.

Атрибут SystemLogMessageLevel

Атрибут SystemLogMessageLevel задает текущий уровень детализации протоколирования для системных событий.

Синтаксис

```
SystemLogMessageLevel =  DEBUG |  
                        INFO |  
                        NOTICE |  
                        WARNING |  
                        ERR |  
                        CRIT |  
                        ALERT|  
                        EMERG
```

Значения уровни детализации протоколирования определены в RFC 3164.

Значение по умолчанию

Если этот атрибут не указан или не загружена конфигурация, то действуют общие настройки. Общий уровень протоколирования для всех событий устанавливается опцией [-s в утилите make inst.exe](#). Если общий уровень не менялся, то он имеет значение DEBUG.

³ RFC 3164: The BSD syslog Protocol

Атрибут PolicyLogMessageLevel

Атрибут PolicyLogMessageLevel задает текущий уровень детализации протоколирования для событий, связанных с применением локальной политики.

Синтаксис

```
PolicyLogMessageLevel =  DEBUG |  
                        INFO |  
                        NOTICE |  
                        WARNING |  
                        ERR |  
                        CRIT |  
                        ALERT|  
                        EMERG
```

Значения уровни детализации протоколирования определены в RFC 3164.

Значение по умолчанию

Если этот атрибут не указан или не загружена конфигурация, то действуют общие настройки. Общий уровень протоколирования для всех событий устанавливается опцией [-s в утилите make inst.exe](#). Если общий уровень не менялся, то он имеет значение DEBUG.

Атрибут CertificatesLogMessageLevel

Атрибут CertificatesLogMessageLevel задает текущий уровень детализации протоколирования для событий, связанных с получением, обработкой сертификатов и их сохранением их в базе данных Продукта.

Синтаксис

```
CertificatesLogMessageLevel =  DEBUG |  
                              INFO |  
                              NOTICE |  
                              WARNING |  
                              ERR |  
                              CRIT |  
                              ALERT|  
                              EMERG
```

Значения уровни детализации протоколирования определены в RFC 3164.

Значение по умолчанию

Если этот атрибут не указан или не загружена конфигурация, то действуют общие настройки. Общий уровень протоколирования для всех событий устанавливается опцией [-s в утилите make inst.exe](#). Если общий уровень не менялся, то он имеет значение DEBUG.

15.4. Структура LDAPSettings

Структура LDAPSettings задает настройки протокола LDAP, который используется для получения сертификатов и списков отозванных сертификатов (CRL). В конфигурации может присутствовать только одна структура данного типа. Этой структуре имя не присваивается.

В случае отсутствия структуры:

- получение сертификатов посредством протокола LDAP невозможно
- если атрибут [CRLHandlingMode](#) структуры [GlobalParameters](#) имеет значение ENABLE или BEST_EFFORT, то CRL может быть получен посредством протокола LDAP только при наличии в сертификате, для которого производится проверка подписи, расширения CDP (CRL Distribution Point) с адресом LDAP-сервера.

<u>Имя структуры</u>	LDAPSettings
<u>Атрибуты</u>	Server
	Port
	SearchBase
	ConnectTimeout
	ResponseTimeout
	HoldConnectTimeout
	DropConnectTimeout

Атрибут Server

Атрибут Server задает адрес LDAP-сервера, к которому производится запрос на поиск сертификатов. Указанный в этом атрибуте адрес используется, если сертификат, для которого производится проверка подписи, не содержит расширение CDP (CRL Distribution Point) с адресом LDAP-сервера либо в этом поле прописанный путь к LDAP-серверу является неполным и тогда добавляются данные из этой структуры.

Сначала делается попытка установить соединение по LDAP версии 2. Если эта попытка завершается с ошибкой LDAP_PROTOCOL_ERROR (наиболее вероятная причина - не поддерживается версия 2), то повторяется попытка установить соединение по LDAP версии 3.

Для прохождения LDAP-пакетов до каждого используемого агентом LDAP-сервера в политике необходимо задать фильтр вида:

```
FilteringRule PassLdapTraffic(
    PeerIPFilter = FilterEntry(
        IPAddress = <LDAP-server IP-address from CRL Distribution
Points extension>
        ProtocolID = 6
        Port = <LDAP-server port>
    )
    LocalIPFilter = FilterEntry(
        IPAddress = LOCAL_IP_ADDRESSES
        ProtocolID = 6
    )
    RefuseTCPPeerInit = TRUE
    Action = [PASS]
)
```

<u>Синтаксис</u>	Server = IP
<u>Значения</u>	IP - адрес

<u>Значение по умолчанию</u>	LDAP –сервер не указан. Поведение агента аналогично случаю отсутствия структуры LDAPSettings в политике.
------------------------------	--

Атрибут Port

Атрибут Port задает порт LDAP-сервера. Если атрибут Server не задан или расширение сертификата CRL Distribution Point содержит адрес LDAP-сервера, то данный атрибут игнорируется.

<u>Синтаксис</u>	Port = ЦЕЛОЕ32
<u>Значения</u>	Целое число из диапазона 1..65535
<u>Значение по умолчанию</u>	389.

Атрибут SearchBase

Атрибут SearchBase задает имя (Distinguished Name, DN) корневого X.500-объекта, в поддереве которого производится поиск сертификатов и CRL на LDAP-сервере. Указанное имя дополняет запрос, созданный на основе имени из сертификата или CRL, позволяя находить соответствующий X.500-объект в случае, когда исходное имя в запросе является частью имени этого объекта. Для запроса на основе URL данное имя не используется.

<u>Синтаксис</u>	SearchBase = СТРОКА
<u>Значения</u>	строковое представление DN в соответствии с RFC2253. Относительные имена (Relative Distinguished Name, RDN) указываются в порядке от объекта к корню.
<u>Значение по умолчанию</u>	поиск производится по имени, полученному из сертификата или CRL.

Атрибут ConnectTimeout

Атрибут ConnectTimeOut позволяет ограничить время (в секундах) создания TCP-соединения с LDAP-сервером.

<u>Синтаксис</u>	ConnectTimeOut = ЦЕЛОЕ32
<u>Значение</u>	Целое число из диапазона 1..6000
<u>Значение по умолчанию</u>	не устанавливается, что приводит к тому, что время создания TCP-соединения с LDAP-сервером ограничивается установленным для ОС временем создания TCP-соединения.
<u>Примечание:</u>	Если в момент обращения к LDAP-серверу устройство, на котором он установлен, недоступно, то процесс создания TCP-соединения может занимать продолжительное время (до 3 минут, зависит от ОС). По этой причине могут наблюдаться внешние признаки зависания агента и это может служить причиной неудачной попытки создания соединения.

Атрибут ResponseTimeout

Поиск посредством протокола LDAP может занимать достаточно продолжительное время, оно зависит от многих факторов, в том числе от масштаба запроса и характеристик канала передачи данных. Данный атрибут позволяет ограничить время (в секундах), в течение которого ожидается ответ от LDAP-сервера на единичный запрос.

<u>Синтаксис</u>	ResponseTimeOut = ЦЕЛОЕ32
<u>Значение</u>	Целое число из диапазона 2..6000
<u>Значение по умолчанию</u>	200

Атрибут HoldConnectTimeout

Атрибут HoldConnectTimeout устанавливает период времени, в течение которого держится установленное соединение к серверу на случай, если придет к нему повторный запрос.

<u>Синтаксис</u>	HoldConnectTimeOut = ЦЕЛОЕ32
<u>Значение</u>	Целое число из диапазона 0..6000 При значении 0 после обмена с LDAP-сервером соединение с ним сразу закрывается. В виду наличия погрешности в одну секунду не рекомендуется выставлять значение в 1 секунду, поскольку это может привести в некоторых случаях к немедленному закрытию соединения и к избыточному открытию нового соединения.
<u>Значение по умолчанию</u>	60

Атрибут DropConnectTimeout

Атрибут DropConnectTimeout устанавливает период времени, начиная с первой неудачной попытки создания соединения с LDAP-сервером, в течение которого новые попытки создания соединения с ним игнорируются.

<u>Синтаксис</u>	DropConnectTimeOut = ЦЕЛОЕ32
<u>Значение</u>	Целое число из диапазона 0..6000 При значении 0 в случае неудачной попытки установления соединения с LDAP-сервером новые попытки не игнорируются. В виду наличия погрешности в одну секунду не рекомендуется выставлять значение в 1 секунду, поскольку это может привести в некоторых случаях к избыточным попыткам создания соединения.
<u>Значение по умолчанию</u>	5.

Пример

Пусть сертификат партнера имеет Subject = "cn=candy,ou=nomadic".

Для поиска такого сертификата на LDAP-сервере (Active Directory -Рисунок 78), необходимо указать атрибут SearchBase:

```
LDAPSettings (  
    Server = 10.1.1.1
```



```

SearchBase="ou=scenario10,ou=QA,ou=GINS,dc=qamsca,dc=ginsoftware,
dc=ru"
)

```

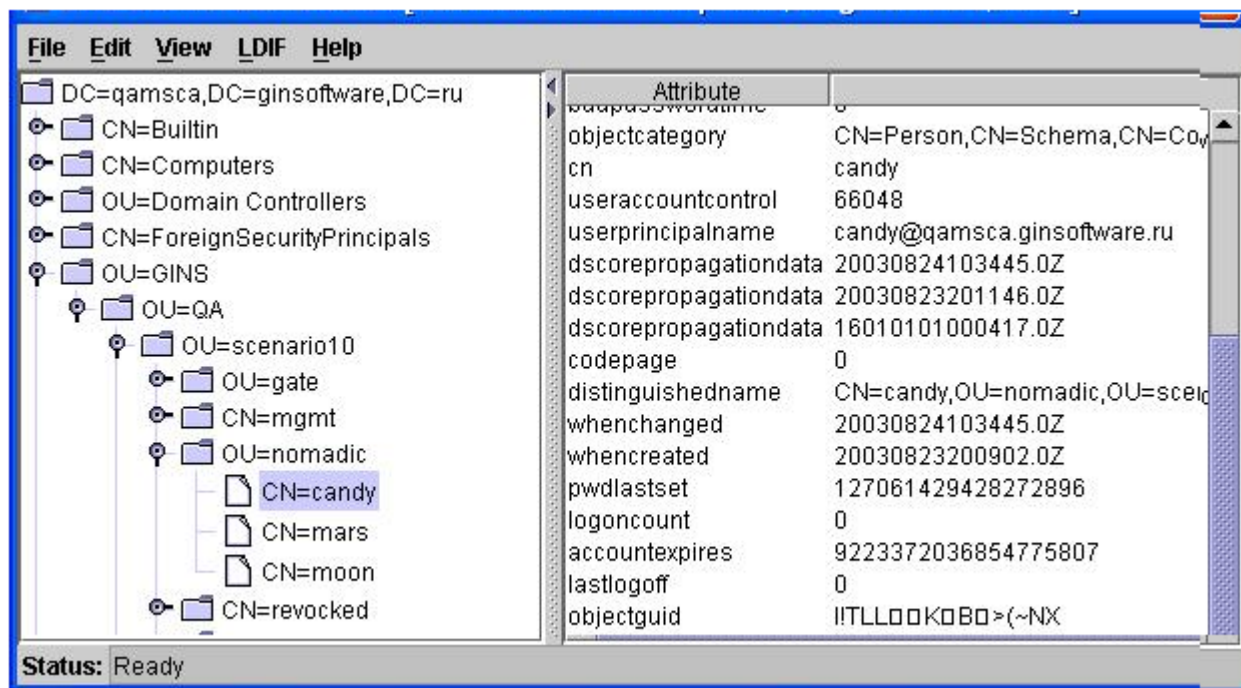


Рисунок 78

15.5. Структура IKEParameters

Структура IKEParameters описывает глобальные настройки протокола IKE. В конфигурации должна быть только одна структура данного типа. Этой структуре имя не присваивается.

<u>Имя структуры</u>	IKEParameters
<u>Атрибуты</u>	SendRetries
	RetryTimeBase
	RetryTimeMax
	SessionTimeMax
	InitiatorSessionsMax
	ResponderSessionsMax
	BlacklogSessionsMax
	BlacklogSilentSessions
	BlacklogSessionsMin
	BlacklogRelaxTime

Логику используемого механизма IKE-ретрансмиссий смотрите в разделе 13.5.1 [“Обработка пакетов - ретрансмиссии”](#).

Атрибут SendRetries

Атрибут SendRetries устанавливает число попыток отправки IKE-пакетов партнеру.

<u>Синтаксис</u>	SendRetries = ЦЕЛОЕ32
<u>Значения</u>	Целое число из диапазона 1..30
<u>Значение по умолчанию</u>	5.

Атрибут RetryTimeBase

Атрибут RetryTimeBase позволяет установить начальный интервал в секундах между повторными попытками отправки IKE-пакетов партнеру. Если ответ не получен в течение начального интервала, то запрос посылается повторно и интервал между повторными попытками увеличивается в два раза. Этот интервал увеличивается в два раза до тех пор, пока:

- не будет получен ответ или
- значение интервала RetryTimeBase не достигнет значения RetryTimeMax (повторные попытки будут продолжаться с интервалом RetryTimeMax) и количество попыток не достигнет значения SendRetries.

<u>Синтаксис</u>	RetryTimeBase = ЦЕЛОЕ32
<u>Значения</u>	Целое число из диапазона 1...5
<u>Значение по умолчанию</u>	1.

Атрибут RetryTimeMax

Атрибут RetryTimeMax позволяет установить максимальный интервал в секундах между повторными попытками отправки IKE-пакетов партнеру. Если выставленное значение этого атрибута меньше, чем RetryTimeBase, то при загрузке конфигурации атрибуту RetryTimeMax присваивается значение RetryTimeBase.

<u>Синтаксис</u>	RetryTimeMax = ЦЕЛОЕ32
<u>Значения</u>	Целое число из диапазона 1...60
<u>Значение по умолчанию</u>	30.

Атрибут SACreationTimeMax

Атрибут SACreationTimeMax ограничивает время (в секундах) на каждую сессию IKE. При использовании ruToken значение этого атрибута должно быть больше 120 секунд.

<u>Синтаксис</u>	SACreationTimeMax = ЦЕЛОЕ32
<u>Значения</u>	Целое число из диапазона 10...300
<u>Значение по умолчанию</u>	60.

Атрибут InitiatorSessionsMax

Атрибут InitiatorSessionsMax устанавливает максимально допустимое количество одновременно иницируемых IKE-сессий для всех партнеров.

<u>Синтаксис</u>	InitiatorSessionsMax = ЦЕЛОЕ32
<u>Значение</u>	число из диапазона 1-10000
<u>Значение по умолчанию</u>	30.

Атрибут ResponderSessionsMax

Атрибут ResponderSessionsMax определяет максимально допустимое количество одновременных обменов, проводимых VPN-устройством с одним неаутентифицированным партнером, в качестве ответчика. С таким партнером нет ни одного ISAKMP SA. Как только создается хотя бы один ISAKMP SA, данный атрибут ResponderSessionsMax перестает действовать.

<u>Синтаксис</u>	ResponderSessionsMax = ЦЕЛОЕ32
<u>Значения</u>	Целое число из диапазона 1..20
<u>Значение по умолчанию</u>	20.

Атрибут BlacklogSessionsMax

"Черный список" предназначен для защиты от DoS-атак (Denial of Service –отказ от обслуживания). "Черный список" минимизирует обработку IKE-пакетов от партнеров, находящихся в "черном списке". В случае первой неуспешной IKE-сессии, инициированной со стороны партнера, партнер сразу же заносится в "черный список". BlacklogSessionsMax устанавливает число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером, только что попавшим в "черный список". При каждом следующем неудачном завершении IKE обмена число разрешенных одновременных IKE обменов для данного партнера снижается вдвое с округлением в меньшую сторону, вплоть до полного запрещения IKE трафика с данным партнером.

Примечание: как только партнер заносится в "черный список", для него текущее значение разрешенных одновременно проводимых IKE обменов не только начинает уменьшаться в два раза после каждого неуспешного завершения обмена, но и увеличиваться на единицу по истечении каждого интервала времени BlacklogRelaxTime (описанного далее).

Синтаксис BlacklogSessionsMax = ЦЕЛОЕ32

Значения Целое число из диапазона 0..($2^{32}-1$).

Если значение равно 0, то "черный список" не используется⁴.

Если значение BlacklogSessionsMax больше или равно ResponderSessionsMax, то атрибуту BlacklogSessionsMax присваивается значение ResponderSessionsMax-1.

Значение по умолчанию 16.

Атрибут BlacklogSessionsMin

Атрибут BlacklogSessionsMin позволяет установить минимальное число разрешенных одновременных IKE обменов, инициируемых неаутентифицированным партнером, находящимся в "черном списке".

Синтаксис BlacklogSessionsMin = ЦЕЛОЕ32

Значения Целое число из диапазона 0..($2^{32}-1$)

Если это значение больше, чем BlacklogSessionsMax, то атрибуту BlacklogSessionsMin присваивается значение BlacklogSessionsMax.

Значение по умолчанию 0 – нет ограничения снизу на активные обмены с партнером, находящимся в "черном списке".

⁴ При загрузке конфигурации с *отключенным* "черным списком" вся статистическая информация о "плохих" партнерах сбрасывается. Если же "черный список" *включен*, то к уже имеющейся накопленной статистике применяются новые параметры настроек "черного списка".

Атрибут BlacklogSilentSessions

Атрибут BlacklogSilentSessions позволяет установить число активных обменов, инициированных партнером, находящимся в "черном списке", по достижении которого VPN-устройство перестает информировать партнера о причине отказа в создании IKE-контекста (ISAKMP SA).

Синтаксис BlacklogSilentSessions = ЦЕЛОЕ32

Значения Целое число из диапазона $0..(2^{32}-1)$

Если это значение больше, чем BlacklogSessionsMax, то атрибуту BlacklogSilentSessions присваивается значение BlacklogSessionsMax.

Значение по умолчанию 4.

Атрибут BlacklogRelaxTime

Атрибут BlacklogRelaxTime устанавливает интервал времени (в секундах) релаксации "черного списка".

- За указанный период времени число разрешенных одновременных IKE обменов для каждого партнера, находящегося в "черном списке", увеличивается на единицу. По истечении следующего такого же интервала времени, текущие значения разрешенных одновременно проводимых IKE обменов для каждого партнера опять увеличивается на единицу и т.д. Этот интервал времени отсчитывается с момента последней загрузки конфигурации.
- Как только текущее значение разрешенных одновременно проводимых партнером IKE обменов начинает превышать значение BlacklogSessionsMax, такой партнер исключается из "черного списка".

Синтаксис BlacklogRelaxTime = ЦЕЛОЕ32

Значения Целое число из диапазона $0..(2^{32}-1)$.

0 – бесконечное время (партнер попадает в "черный список" навсегда).

Значение по умолчанию 120

Примечание: помимо механизма релаксации, партнер также может быть исключен из "черного списка" в следующих случаях:

при перезапуске сервиса

при загрузке конфигурации с отключенным "черным списком" (с атрибутом BlacklogSessionsMax = 0)

при инициации IKE обмена со стороны локального VPN устройства с целью установления ISAKMP (IPSec) соединения⁵

если партнеру удалось установить ISAKMP (IPSec) соединение с локальным VPN устройством, и тем самым партнер был успешно аутентифицирован.

⁵ В данном случае считается, что локальное VPN устройство потенциально доверяет партнеру, с которым оно хочет установить соединение, и информация, накопленная в "черном списке", для такого партнера сбрасывается.

15.5.1. Обработка пакетов – ретрансмиссии

1. Используемый механизм IKE-ретрансмиссий находится в общей концепции, согласно которой инициатор, исходя из наличия собственных ресурсов, проявляет настойчивость и добивается чего-то от ответчика, а ответчик, во первых, не доверяет инициатору насколько это возможно, во-вторых, по-максимуму бережет собственные ресурсы.
 - Инициатор, в большинстве случаев, являясь активной стороной, посылает очередной пакет IKE-обмена и затем перепосылает его (в соответствии с настройками ретрансмиссий – атрибуты [SendRetries](#), [RetryTimeBase](#) и [RetryTimeMax](#)) до тех пор, пока не получит ответный пакет от ответчика.
 - Таким образом, инициатор выполняет работу за двоих:
 - если исходящий от инициатора пакет не дошел до ответчика, то ответчик его не обрабатывает и, соответственно, никак не ответит инициатору. Но исходящий пакет инициатором может быть перепослан (возможно, с n-ой попытки), ответчик его получит, обработает и отошлёт ответ
 - если же проблема возникла на обратном пути (т.е. пакет от ответчика потерялся на пути к инициатору), то для инициатора эта ситуация детектируется точно так же, как и первая - то есть инициатор ответного пакета ждал, но за отведенный timeout так и не дождался. Тогда инициатор перепосылает свой последний исходящий пакет, ответчик снова его получает, распознает его как совпадающий с последним пакетом от инициатора, т.е. ретрансмиссию, и в ответ перепосылает свой последний пакет.
2. События для перепосылки:
 - для стороны, выполняющей активную роль в ретрансмиссиях, событием для перепосылки своего последнего пакета является таймер и отсутствие ответа от партнера
 - для пассивной стороны событием для перепосылки своего последнего пакета является получение ретрансмиссии от партнера.
3. В сценариях IKE, в которых ответчик обрабатывает последний пакет (Aggressive Mode и Quick Mode без поддержки Commit Bit), ответчик становится активной стороной при ожидании последнего пакета обмена. В этих случаях инициатор уже не может выполнять активную роль, так как он в любом случае по сценарию не получает ответный пакет.

15.6. Структура SNMPPollSettings

Структура задает настройки для выдачи информации по запросу SNMP-менеджера. В конфигурации должна быть только одна структура данного типа. Этой структуре имя не присваивается.

<u>Имя структуры</u>	SNMPPollSettings
<u>Атрибуты</u>	LocalIPAddress Port ReadCommunity SysLocation SysContact

Атрибут LocalIPAddress

Атрибут LocalIPAddress задаёт локальный IPv4-адрес, на который можно получать запросы от SNMP-менеджера.

<u>Синтаксис</u>	LocalIPAddress = IP ANY
<u>Значения</u>	IP –адрес – любой из локальных IP-адресов ANY – все локальные IP-адреса
<u>Значение по умолчанию</u>	ANY

Атрибут Port

Атрибут Port задаёт порт, на который можно получать SNMP-запросы.

<u>Синтаксис</u>	Port = ЦЕЛОЕ32
<u>Значение</u>	целое число из диапазона 1..65535
<u>Значение по умолчанию</u>	161.

Атрибут ReadCommunity

Атрибут ReadCommunity играет роль пароля при аутентификации сообщений SNMP и разрешает SNMP-менеджеру чтение статистики из базы управления SNMP-агента.

<u>Синтаксис</u>	ReadCommunity = СТРОКА
<u>Значение</u>	произвольный формат
<u>Значение по умолчанию</u>	не существует, атрибут обязательный.

Атрибут SysLocation

Атрибут SysLocation содержит информацию о физическом расположении SNMP-агента.

Синтаксис SysLocation = СТРОКА

Значение произвольный формат, например "Building 3/Room 214"

Значение по умолчанию пустая строка.

Атрибут SysContact

Атрибут SysContact содержит информацию о контактном лице, ответственном за работу SNMP-агента.

*

Синтаксис SysContact = СТРОКА

Значение произвольный формат, например e-mail, телефон и т.д.

Значение по умолчанию пустая строка.

15.7. Структура SNMPTrapSettings

Структура задает настройки для выдачи агентом сообщений менеджеру о возникшем прерывании в виде SNMP-трапов. В конфигурации должна быть только одна структура данного типа. Этой структуре имя не присваивается. При отсутствии этой структуры трап-сообщения не высылаются.

Имя структуры SNMPTrapSettings

Атрибуты Receivers

Атрибут Receivers

Атрибут Receivers задаёт список получателей SNMP-трапов и дополнительные настройки.

Синтаксис Receivers* = [TrapReceiver](#)

Значение по умолчанию не существует, атрибут обязательный.

15.8. Структура TrapReceiver

Структура описывает одного получателя SNMP-трапов и дополнительные настройки для трапов, отсылаемых на него.

<u>Имя структуры</u>	Trapreceiver
<u>Атрибуты</u>	IPAddress
	Port
	Community
	Version
	SNMPv1AgentAddress

Атрибут IPAddress

Атрибут IPAddress описывает IP-адрес получателя SNMP-трапов.

<u>Синтаксис</u>	IPAddress = IP
<u>Значение</u>	IP- адрес
<u>Значение по умолчанию</u>	не существует, атрибут обязательный.

Атрибут Port

Атрибут Port задает UDP-порт, на который SNMP-менеджеру будут высылаться трап-сообщения.

<u>Синтаксис</u>	Port = ЦЕЛОЕ32
<u>Значение</u>	целое число из диапазона 1..65535.
<u>Значение по умолчанию</u>	162.

Атрибут Community

Атрибут Community играет роль идентификатора отправителя трап-сообщения.

<u>Синтаксис</u>	Community = СТРОКА
<u>Значение</u>	произвольный формат
<u>Значение по умолчанию</u>	не существует, атрибут обязательный.

Атрибут Version

Атрибут Version указывает версию SNMP, в которой формируются трап-сообщения.

<u>Синтаксис</u>	Version = V1 V2C
<u>Значение</u>	V1 – SNMP версии 1 V2C – SNMP версии 2с
<u>Значение по умолчанию</u>	V1.

Атрибут SNMPv1AgentAddress

Атрибут SNMPv1AgentAddress задает IP-адрес источника трап-сообщения, который прописывается в поле Agent address внутри SNMP-пакета. Этот атрибут указывается только для Version = V1.

<u>Синтаксис</u>	SNMPv1AgentAddress = IP
<u>Значение</u>	IP- адрес
<u>Значение по умолчанию</u>	0.0.0.0.

15.9. Структура SyslogSettings

В конфигурации может присутствовать только один экземпляр этой структуры, поэтому этой структуре не может быть присвоено имя.

Структура SyslogSettings задает текущие настройки для SYSLOG-клиента. Структура SyslogSettings также позволяет отключить использование протокола SYSLOG.

Если активной является DDP (политика по умолчанию) или в LSP отсутствует структура SyslogSettings, то действуют локальные настройки, выставляемые в утилите make_inst.exe и записываемые в файл syslog.ini.

<u>Имя структуры</u>	SyslogSettings
<u>Атрибут</u>	Server
	Facility

Атрибут Server

Атрибут Server задает адрес SYSLOG-сервера.

<u>Синтаксис</u>	Server = IP NO_SYSLOG
<u>Значение</u>	IP – одиночный IP-адрес. Указание адреса 0.0.0.0 аналогично указанию константы NO_SYSLOG, которая приводит к отключению использования протокола SYSLOG. При указании адреса 127.0.0.1 сообщения посылаются на локальный хост. NO_SYSLOG – указание этой константы отключает использование протокола SYSLOG.
<u>Значение по умолчанию</u>	не существует, атрибут обязательный.

Атрибут Facility

Атрибут Facility позволяет задать источник сообщений протокола SYSLOG.

<u>Синтаксис</u>	Facility = СТОКА
<u>Значение</u>	LOG_KERN – система ядра LOG_USER – пользовательские программы LOG_MAIL – почтовая система LOG_DAEMON – прочие процессы LOG_AUTH – система авторизации и безопасности LOG_SYSLOG – производятся самим SYSLOG LOG_LPR – подсистема печати LOG_NEWS – подсистема сетевых сообщений LOG_UUCP – подсистема UUCP LOG_CRON – системные часы LOG_AUTHPRIV LOG_FTP LOG_NTP LOG_AUDIT LOG_ALERT LOG_CRON2

LOG_LOCAL0
LOG_LOCAL1
LOG_LOCAL2
LOG_LOCAL3
LOG_LOCAL4
LOG_LOCAL5
LOG_LOCAL6
LOG_LOCAL7 – значение по умолчанию

Значение по умолчанию LOG_LOCAL7.

15.10. Структура RoutingTable

Структура RoutingTable описывает таблицу маршрутизации. Таблица содержит записи, необходимые для работоспособности конфигурации, успешное добавление которых в таблицу проверяется на момент загрузки конфигурации.

Если таблица содержит записи, которые уже присутствуют в системной таблице маршрутизации, то загрузка конфигурации будет продолжена остановлена с соответствующей диагностикой.

При отгрузке конфигурации из системной таблицы маршрутизации будут удалены все указанные в конфигурации записи маршрутизации, которые могли существовать и до загрузки этой конфигурации (например, добавленные командой `route add`).

В конфигурации допускается только один экземпляр этой структуры. Этой структуре не может быть присвоено имя.

Имя структуры RoutingTable

Атрибуты Routes

Атрибут Routes

Атрибут Routes содержит список записей таблицы маршрутизации.

Синтаксис Routes* = [Route](#)

Значение по умолчанию не существует, атрибут обязательный.

15.11. Структура Route

Структура Route описывает одну запись (маршрут) в таблице маршрутизации.

<u>Имя структуры</u>	Route
<u>Атрибуты</u>	Destination
	Gateway
	NetworkInterface
	Metric

Атрибут Destination

Атрибут Destination задает адрес назначения (получателя) пакета.

<u>Синтаксис</u>	Destination = IP IP/ЦЕЛОЕ32
<u>Значение</u>	IP –адрес IP/ЦЕЛОЕ32 – IP-адрес с маской подсети Для указания маршрута, который будет использоваться по умолчанию, IP-адрес и маска подсети должны иметь значение 0.0.0.0/ 0.

Маршрут по умолчанию – маршрут, по которому будет отправлен пакет, если IP-адрес назначения, указанный в заголовке пакета, не совпадает ни с одним адресом назначения в таблице маршрутизации.

Значение по умолчанию отсутствует, атрибут обязательный.

Атрибут Gateway

Атрибут Gateway задает IP-адрес устройства, на который нужно передать пакет для продвижения его к получателю пакета. Атрибут Gateway должен отсутствовать при наличии атрибута [NetworkInterface](#).

<u>Синтаксис</u>	Gateway = IP
<u>Значение</u>	IP –адрес
<u>Значение по умолчанию</u>	используется значение из атрибута NetworkInterface.

Атрибут NetworkInterface

Атрибут NetworkInterface указывает имя выходного интерфейса, на который нужно передать пакет для продвижения его к получателю пакета.. Атрибут NetworkInterface должен отсутствовать при наличии атрибута [Gateway](#).

<u>Синтаксис</u>	NetworkInterface = СТОКА
<u>Значение</u>	имя интерфейса
<u>Значение по умолчанию</u>	используется значение из атрибута Gateway.

Атрибут Metric

Использовать этот атрибут не рекомендуется, так как в разных ОС имеет разный смысл и будет проигнорирован.

Атрибут Metric задает метрику маршрута. В качестве метрики маршрута может использоваться любой показатель: длину маршрута, число промежуточных маршрутизаторов, надежность, задержка, затраты на передачу и др.

Синтаксис Metric = ЦЕЛОЕ32

Значение Целое число из диапазона 1..255

Значение по умолчанию 1.

15.12. Правила пакетной фильтрации. Структура FilteringRule

Правила пакетной фильтрации содержат условия срабатывания правила и те действия, которые необходимо произвести с пакетом, в случае попадания пакета под правило.

Порядок перечисления правил фильтрации существенен, так как правила срабатывают в прямом порядке перечисления в конфигурации.

При получении TCP/IP пакета просматриваются правила в порядке указания в локальной политике (конфигурации) и сравниваются параметры заголовка пакета, относящиеся к удаленному IP-хосту, до нахождения первого подходящего правила. Если правило не найдено – пакет уничтожается.

Правило считается подходящим, если в структуре FilteringRule в атрибутах PeerIPFilter и LocalIPFilter указаны параметры, совпадающие с параметрами в TCP/IP заголовке пакетов.

В случае исходящих пакетов параметры в атрибуте LocalIPFilter сравниваются с адресом источника пакета. Параметры в атрибуте PeerIPFilter сравниваются с адресом получателя пакета.

Для входящих пакетов параметры в атрибуте LocalIPFilter сравниваются с адресом получателя пакета. Параметры в атрибуте PeerIPFilter сравниваются с адресом источника пакета.

Структура FilterEntry формирует условие срабатывания конкретного правила пакетной фильтрации для партнеров по взаимодействию.

Имя структуры	FilteringRule
Атрибуты	PeerIPFilter
	LocalIPFilter
	NetworkInterfaces
	RefuseTCPPeerInit
	Action

Схематическое представление взаимосвязей структуры FilteringRule:

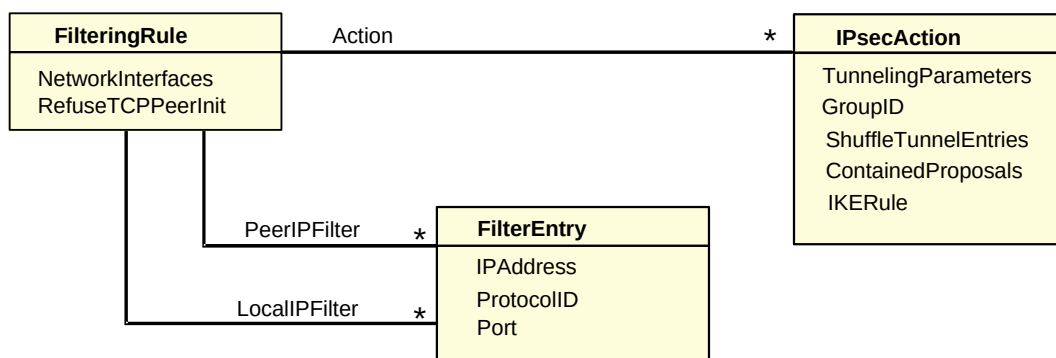


Рисунок 79

Атрибут PeerIPFilter

Атрибут PeerIPFilter описывает параметры удаленного хоста, которые

- в случае выходящих пакетов будут сравниваться с адресом получателя пакета
- в случае входящих пакетов будут сравниваться с адресом источника пакета.

Этот атрибут представляет собой список структур FilterEntry.

Синтаксис PeerIPFilter* = FilterEntry

Значение по умолчанию весь сетевой трафик.

Атрибут LocalIPFilter

Атрибут LocalIPFilter описывает параметры защищаемого хоста, а также защищаемых подсетей, которые:

- в случае выходящих пакетов будут сравниваться с адресом источника пакета
- в случае входящих пакетов будут сравниваться с адресом получателя пакета.

Этот атрибут представляет собой список структур FilterEntry.

Синтаксис LocalIPFilter* = FilterEntry

Значение по умолчанию весь локальный и транзитный трафик.

Атрибут NetworkInterfaces

Атрибут NetworkInterfaces задает список сетевых интерфейсов, на которые могут приходить пакеты от партнера (с которых могут уходить пакеты партнеру).

Синтаксис NetworkInterfaces* = СТРОКА

Значения Список логических имен сетевых интерфейсов. Интерфейсы должны быть указаны в кавычках (кроме служебного слова ANY).

Значение по умолчанию ANY – задействуются все интерфейсы.

Атрибут RefuseTCPPeerInit

Атрибут RefuseTCPPeerInit задает блокировку входящих TCP-соединений; используется как дополнительное ограничение к действию.

Синтаксис RefuseTCPPeerInit* = **TRUE | FALSE**

Значения TRUE – уничтожается первый входящий TCP-пакет соединения, в результате отвергаются все TCP-соединения, инициированные извне

FALSE – не производится никаких дополнительных действий

Значение по умолчанию FALSE

Атрибут Action

Атрибут Action описывает варианты действий, допускаемых VPN-устройством по взаимодействию с удаленным хостом.

Синтаксис Action *= ([IPsecAction](#) [, IPsecActionN]) | (DROP) | (PASS)

Значение

Действия формируются в виде списка цепочек из правил создания SA:

- в списке не должно быть одинаковых цепочек
- в списке вместо цепочки могут использоваться зарезервированные слова PASS или DROP. При этом:
 - определяется действие, которое будет применено к пакету, подпадающему под это правило пакетной фильтрации, при отсутствии соответствующего SA
 - в списке допускается только одна цепочка заданная таким образом
 - порядок указания такой цепочки в списке не имеет значения
- если в цепочке указано более одного правила, то все они, кроме последнего, должны иметь непустой атрибут [TunnelingParameters](#)..

Например,

[IPsecAction1] [IPsecAction2, IPsecAction3] [IPsecAction4] [PASS] [IPsecAction5]

Создание SA

Если устройство является инициатором соединения, то трафик будет обрабатываться в соответствии с первой цепочкой списка.

Если устройство является ответчиком, то правило обработки трафика выбирается путем сравнения каждой цепочки этого списка с каждой цепочкой своего списка и выбирается первая совпавшая цепочка.

Обработка трафика

Если выбранная цепочка состоит из двух правил [IPsecAction1, IPsecAction2] или более, то:

исходящий трафик вначале обрабатывается контекстом, созданным по правилу IPsecAction2, а затем контекстом, созданным по правилу IPsecAction1

для входящего трафика порядок применения контекстов обратный: вначале трафик обрабатывается контекстом, созданным по правилу IPsecAction1, а затем – IPsecAction2.

Значение по умолчанию (DROP)

15.13. Структура FilterEntry

Структура FilterEntry описывает параметры IP-заголовка пакета. Структура FilterEntry формирует условие срабатывания конкретного правила пакетной фильтрации.

<u>Имя структуры</u>	FilterEntry
<u>Атрибуты</u>	IPAddress
	ProtocolID
	Port

Атрибут IPAddress

Атрибут IPAddress описывает набор IPv4 адресов, диапазонов адресов и/или подсетей,, конкретного правила (FilteringRule) для сетевого объекта.

<u>Синтаксис</u>	IPAddress *= IP IP..IP IP/ЦЕЛОЕ32 LOCAL_IP_ADDRESSES
<u>Значения</u>	AddressPool – множество адресов IKECFG пула IP-адрес IP..IP – диапазон IP-адресов IP/ЦЕЛОЕ32 – IP-адрес с маской LOCAL_IP_ADDRESSES – все локальные адреса устройства
<u>Значение по умолчанию</u>	всевозможные IP-адреса.

Атрибут ProtocolID

Атрибут ProtocolID описывает протокол или диапазон протоколов конкретного правила (FilteringRule).

<u>Синтаксис</u>	ProtocolID *= ЦЕЛОЕ32 ЦЕЛОЕ32..ЦЕЛОЕ32
<u>Значение</u>	целое число из диапазона 0..255. Значение 0 означает все сетевые протоколы.
<u>Значение по умолчанию</u>	все протоколы.

Атрибут Port

Атрибут Port описывает список идентификаторов портов для указанных протоколов объекта. Если атрибут ProtocolID отсутствует, то указанные порты будут применяться и к TCP(6) и к UDP(17).

<u>Синтаксис</u>	Port *= ЦЕЛОЕ32 ЦЕЛОЕ32..ЦЕЛОЕ32
<u>Значение</u>	целое число из диапазона 0..65535. Значение 0 означает все порты для указанных протоколов.
<u>Значение по умолчанию</u>	все порты.

15.14. Структура IPsecAction

Структура IPsecAction задает правило создания контекста соединения для протоколов семейства IPSec. Этой структуре может быть присвоено имя.

<u>Имя структуры</u>	IPsecAction
<u>Атрибуты</u>	TunnelingParameters ShuffleTunnelEntries CryptoContextsPerIPsecSA GroupID ContainedProposals IKERule NoPathMTUDiscovery NoSmoothRekeying

Структура IPsecAction:

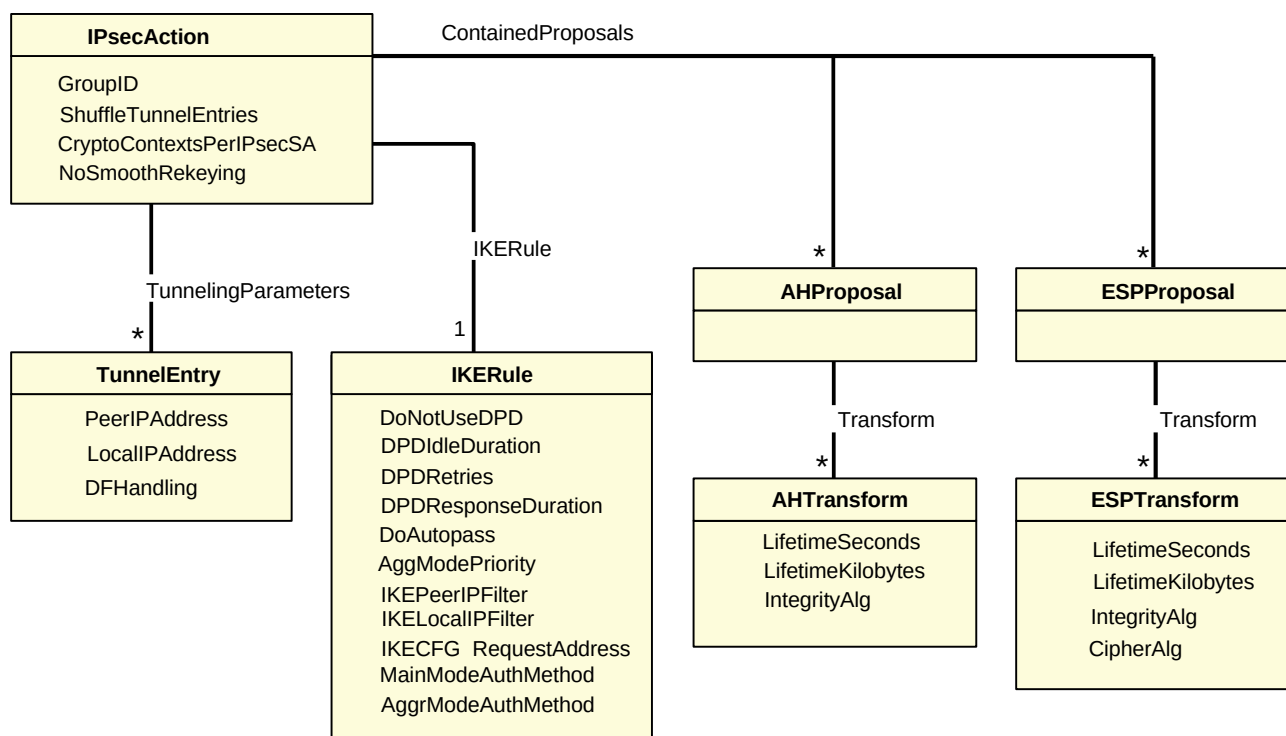


Рисунок 80

Атрибут TunnelingParameters

Атрибут TunnelingParameters описывает параметры внешнего IP-заголовка пакета, который добавляется в туннельном режиме IPsec. Если в TunnelingParameters указано более одного элемента, то элементы используются как альтернативные партнеры. Если не удалось установить IPsec-туннель с партнером, то производится попытка установить туннель со следующим партнером в списке, и так далее до окончания списка.

Синтаксис TunnelingParameters* = [TunnelEntry](#)

Значение по умолчанию используется транспортный режим.

Предупреждение: если между партнерами обнаружен NAT, то создавать соединение в транспортном режиме нельзя.

Атрибут ShuffleTunnelEntries

Атрибут ShuffleTunnelEntries задает порядок применения структур [TunnelEntry](#) в атрибуте TunnelingParameters. Атрибут ShuffleTunnelEntries игнорируется, если атрибут TunnelingParameters не задан.

Синтаксис ShuffleTunnelEntries = TRUE | FALSE

Значения TRUE – при загрузке конфигурации туннели в списке TunnelingParameters перемешиваются случайным образом

FALSE – при загрузке конфигурации туннели в списке TunnelingParameters применяются в порядке перечисления

Значение по умолчанию FALSE

Атрибут CryptoContextsPerIPSecSA

Атрибут CryptoContextsPerIPSecSA задает количество открываемых криптографических контекстов на один IPsec SA, созданный по этому правилу IPsecAction. Если данный атрибут не указан в правиле, то количество контекстов задается параметром из файла agent.ini DefaultCryptoContextsPerIPSecSA. Наличие нескольких криптографических контекстов позволяет распараллелить обработку пакетов одним IPsec SA.

Синтаксис CryptoContextsPerIPSecSA = ЦЕЛОЕ32

Значения Целое число из диапазона 1..128.

Значение по умолчанию 1.

Атрибут IKERule

Атрибут IKERule является ссылкой на правило создания контекста соединения для ISAKMP-инициатора.

Синтаксис IKERule = [IKERule](#)

Значение по умолчанию не существует, атрибут обязательный.

Атрибут GroupID

Атрибут GroupID задает параметры получения ключевого материала. Если список не пуст, то для инициатора соединения ключевой материал всегда задаётся согласно первому компоненту списка. Для ответчика присланное предложение инициатора сравнивается последовательно со всеми элементами списка.

Синтаксис GroupID* = MODP_768, MODP_1024, MODP_1536

Значения MODP_768 – длина ключа 768 бит – группа 1
MODP_1024 – длина ключа 1024 бита - группа 2
MODP_1536 – длина ключа 1536 бит - группа 5

Значение по умолчанию ключевой материал заимствуется из первой фазы IKE.

Атрибут ContainedProposals

Каждая из структур AHProposal и ESPProposal содержит список вариантов преобразований (transforms). Структуры AHProposal и ESPProposal могут группироваться, позволяя обрабатывать трафик комбинацией протоколов AH и ESP.

Атрибут ContainedProposals содержит список единичных структур AHProposal и ESPProposal или их пар в порядке убывания приоритета.

Синтаксис ContainedProposals *= Proposal

Proposal *= (AHProposal [, ESPProposal]) | ESPProposal

Число элементов списка неограничено. Все элементы списка должны быть различными.

Один элемент списка содержит до двух преобразований с различными протоколами.

Если элемент списка содержит AHProposal и ESPProposal, то они должны следовать в указанном порядке.

Инициатор соединения посылает партнеру все варианты параметров защиты соединения, указанные в атрибуте ContainedProposals, с целью их согласования во время второй фазы IKE –сессии.

Ответная сторона присланные предложения инициатора соединения последовательно сравнивает с каждым элементом своего списка предложений и выбирает первое совпавшее. При переборе более приоритетным является список на стороне ответчика.

Параметры преобразований и комбинация протоколов AH и ESP определяют качество защиты соединения.

Запись (ah1, esp1), (esp2), (ah3) означает, что рассматриваются варианты контекстов: либо связка (ah1, esp1), либо proposal esp2, либо proposal ah3.

Значение по умолчанию не существует, атрибут обязательный.

Пример

```
ContainedProposals *=  
(ipsec_ah_md5, ipsec_esp_des3), (ipsec_ah_md5, ipsec_esp_idea)  
(* (AH(MD5) и ESP(DES3) или AH(MD5) и ESP(IDEA) *)
```

```
ContainedProposals *=  
(ipsec_ah_md5, ipsec_esp_des3), (ipsec_ah_md5)  
  (* (AH(MD5) и ESP(DES3) или AH(MD5) *)  
  
ESPProposal ipsec_esp_idea(  
  Transform *= ESPTransform(  
    CipherAlg = "IDEA-CBC"  
  )  
)  
AHProposal ipsec_ah_md5(  
  Transform *= AHTransform(  
    IntegrityAlg* = "MD5-H96-HMAC"  
  )  
)  
ESPProposal ipsec_esp_des3(  
  Transform *= ESPTransform(  
    CipherAlg = "DES3-K168-CBC"  
  )  
)
```

Атрибут NoSmoothRekeying

Атрибут NoSmoothRekeying задает режим "мягкой" смены ключевого материала.

Синтаксис

NoSmoothRekeying = **TRUE | FALSE**

Значения

TRUE – заблаговременная смена ключевого материала (rekeying) не проводится. При отсутствии подходящего IPSec соединения, новый IPSec SA создается только по запросу из ядра – при наличии исходящего IP-пакета, либо по инициативе партнера. В результате, во время создания нового IPSec SA IP-трафик приостанавливается, а при интенсивном трафике возможна потеря пакетов.

FALSE – заблаговременно, незадолго до окончания действия IPSec соединения, на его основе (с теми же параметрами) проводится IKE-сессия (Quick Mode) по созданию нового IPSec SA – rekeying. Rekeying не проводится, если за время существования старого SA под его защитой не было никакого трафика.⁶

Значение по умолчанию FALSE

⁶Для проведения rekeying-а необходимо, чтобы время жизни обновляемого соединения было существенно больше времени, которое отводится на проведение IKE-сессии.

15.15. Структура TunnelEntry

Структура TunnelEntry описывает параметры внешнего IP-заголовка пакета при использовании туннельного режима IPsec.

<u>Имя структуры</u>	TunnelEntry
<u>Атрибуты</u>	PeerIPAddress LocalIPAddress DFHandling

Атрибут PeerIPAddress

Атрибут PeerIPAddress описывает туннельный адрес. Этот адрес используется для двух целей – адрес получателя во внешнем IP-заголовке и адрес IKE-партнера, если последний не задан явно.

Синтаксис PeerIPAddress = IP

Значение по умолчанию

если туннельный адрес используется как адрес получателя во внешнем IP заголовке, то

для исходящего пакета берется адрес IKE партнера

если туннельный адрес используется как адрес IKE партнера:

для исходящего пакета берется адрес из IP пакетов, вызвавших создание соединения

для входящего пакета – принимается любой адрес

Атрибут LocalIPAddress

Атрибут LocalIPAddress описывает туннельный адрес локального VPN-устройства.

Синтаксис LocalIPAddress = IP

Значение по умолчанию для исходящего пакета - любой из адресов сетевого интерфейса, с которого отправляется пакет.

Атрибут DFHandling

Атрибут DFHandling задает алгоритм формирования DF (Don't Fragment) бита внешнего IP-заголовка для туннельного режима IPsec.

Синтаксис DFHandling = **COPY** | **SET** | **CLEAR**

Значения COPY - копировать DF бит из внутреннего заголовка во внешний заголовок

SET - всегда устанавливать DF бит внешнего заголовка в 1

CLEAR – всегда сбрасывать DF бит внешнего заголовка в 0.

Значение по умолчанию COPY.

Пример структуры IPsecAction

```
IPsecAction tunnel_ipsec_des_md5_action(  
    TunnelingParameters *= TunnelEntry(  
        PeerIPAddress = 192.168.2.1  
        DFHandling = CLEAR  
    )  
  
    IKERule = ike_r  
    GroupID *= MODP_768, MODP_1024  
    ContainedProposals *= (ipsec_ah_md5, ipsec_esp_des),  
(ipsec_esp_des_md5)  
)  
  
ESPProposal ipsec_esp_des(  
    Transform *= ESPTransform(  
        CipherAlg *= "DES-CBC"  
    )  
)  
  
AHProposal ipsec_ah_md5(  
    Transform *= AHTransform(  
        IntegrityAlg *= "MD5-H96-HMAC"  
    )  
)  
  
ESPProposal ipsec_esp_des_md5(  
    Transform *= ESPTransform(  
        CipherAlg *= "DES-CBC"  
        IntegrityAlg *= "MD5-H96-HMAC"  
    )  
)  
)
```

15.16. Структуры AHProposal и ESPProposal

Структура AHProposal задает список криптографических преобразований (transforms) протокола AH в порядке убывания приоритета, которые допускаются для обработки трафика. Трафик – количество килобайт данных, обработанных данным контекстом.

Структура ESPProposal определяет список преобразований (transforms) протокола ESP в порядке убывания приоритета, которые допускаются для обработки специфицированного трафика.

Имя структуры AHProposal

Атрибуты Transform

Имя структуры ESPProposal

Атрибуты Transform

Атрибут Transform

Атрибут Transform задает список возможных групп параметров протокола AH (для структуры AHProposal) или ESP (для структуры ESPProposal), необходимых для создания SA, расположенных в порядке убывания их приоритета.

Синтаксис Transform *= [AHTransform](#) # для структуры AHProposal

Transform *= [ESPTransform](#) # для структуры ESPProposal

Должен присутствовать хотя бы один трансформ.

Значение по умолчанию не существует, атрибут обязательный.

15.17. Структура AHTransform

Структура AHTransform задает параметры контекста (SA) AH.

<u>Имя</u>	AHTransform
<u>Атрибуты</u>	LifetimeSeconds
	LifetimeKilobytes
	IntegrityAlg

Атрибут LifetimeSeconds

Атрибут LifetimeSeconds задает максимальное время существования контекста (SA) AH (в секундах).⁷

<u>Синтаксис</u>	LifetimeSeconds = ЦЕЛОЕ32
<u>Значение</u>	число из диапазона 1.. 4 294 967 295.
<u>Значение по умолчанию</u>	28800 (8 часов).

Атрибут LifetimeKilobytes

Атрибут LifetimeKilobytes задает максимальное ограничение по трафику на действие контекста в килобайтах. Трафик – количество килобайт данных, обработанных данным контекстом.⁸

<u>Синтаксис</u>	LifetimeKilobytes = ЦЕЛОЕ32
<u>Значение</u>	число из диапазона 1.. 4 294 967 295.
<u>Значение по умолчанию</u>	нет ограничений на действие SA.

Атрибут IntegrityAlg

Атрибут IntegrityAlg задает набор предлагаемых/допустимых алгоритмов проверки целостности в рамках создаваемого контекста. Список должен содержать хотя бы один элемент.

Рекомендуется указывать не список алгоритмов, а только один алгоритм проверки целостности пакета.

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько алгоритмов (их комбинацию) проверки целостности, то используйте альтернативный подход: в атрибуте Transform

⁷ В случае использования связок (AH+ESP) в качестве элементов списка_ContainedProposals структуры IPsecAction, соответствующие значения в AH- и ESP- трансформациях уравниваются в меньшую сторону.

⁸ В случае использования связок (AH+ESP) в качестве элементов списка_ContainedProposals структуры IPsecAction, соответствующие значения в AH- и ESP- трансформациях уравниваются в меньшую сторону.

структуры AHProposal укажите список структур AHTransform, а в каждой структуре AHTransform задайте только один алгоритм проверки целостности.

Синтаксис

IntegrityAlg* = СТРОКА

Значение

Возможные значения:

"MD5-H96-KPDK" - Keyed MD5

"MD5-H96-HMAC" - HMAC MD5 (96 бит)

"SHA1-H96-HMAC" - HMAC SHA-1 (96 бит)

"GR341194CPRO1-H96-HMAC-254" – реализация ГОСТ Р 34.11-94 (96 бит)

"GR341194CPRO1-H96-HMAC-254" – реализация ГОСТ Р 34.11-94 (96 бит)

Значение по умолчанию

не существует, атрибут обязательный.

15.18. Структура ESPTransform

Структура ESPTransform задает параметры контекста (SA) ESP.

<u>Имя</u>	ESPTransform
<u>Атрибуты</u>	LifetimeSeconds LifetimeKilobytes CipherAlg IntegrityAlg

Атрибут LifetimeSeconds

Атрибут LifetimeSeconds задает максимальное время существования контекста в секундах.⁹

<u>Синтаксис</u>	LifetimeSeconds = ЦЕЛОЕ32
<u>Значение</u>	Целое число из диапазона 1.. 4 294 967 295.
<u>Значение по умолчанию</u>	28800 (8 часов).

Атрибут LifetimeKilobytes

Атрибут LifetimeKilobytes задает максимальное ограничение по трафику на действие контекста в килобайтах. Трафик – количество килобайт данных, обработанных данным контекстом.¹⁰

<u>Синтаксис</u>	LifetimeKilobytes = ЦЕЛОЕ32
<u>Значение</u>	Целое число из диапазона 1.. 4 294 967 295.
<u>Значение по умолчанию</u>	нет ограничений на действие SA.

Атрибут CipherAlg

Атрибут CipherAlg задает набор предлагаемых/допустимых алгоритмов шифрования трафика в рамках создаваемого контекста. Список должен содержать хотя бы один элемент.

Рекомендуется указывать не список алгоритмов, а только один алгоритм шифрования трафика.

⁹ В случае использования связок (AH+ESP) в качестве элементов списка_ContainedProposals структуры IPsecAction, соответствующие значения в AH- и ESP- трансформх уравниваются в меньшую сторону

¹⁰ В случае использования связок (AH+ESP) в качестве элементов списка_ContainedProposals структуры IPsecAction, соответствующие значения в AH- и ESP- трансформх уравниваются в меньшую сторону

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько алгоритмов шифрования, то используйте альтернативный подход: в атрибуте Transform структуры ESPProposal укажите список структур ESPTransform, а в каждой структуре ESPTransform задайте только один алгоритм шифрования.

Синтаксис

CipherAlg* = СТРОКА

Значение

Возможные значения:

"NULL" – NULL (данные не шифруются)

"DES-CBC_IV64" - DES в режиме CBC с явным IV длиной 64 бита

"DES-CBC_IV32" - DES в режиме CBC с явным IV длиной 32 бита

"DES-CBC" - DES в режиме CBC

"DES3-K168-CBC" - DES3 в режиме CBC

"IDEA-CBC" - IDEA в режиме CBC

"AES-K128-CBC" - AES в режиме CBC с длиной ключа 128

"AES-K192-CBC" - AES в режиме CBC с длиной ключа 192

"AES-K256-CBC" - AES в режиме CBC с длиной ключа 256

"G2814789CPRO1-K256-CBC-254" – реализация ГОСТ 28147-89 в режиме CBC

Значение по умолчанию

не существует, атрибут обязательный.

Атрибут IntegrityAlg

Атрибут IntegrityAlg задает набор предлагаемых/допустимых алгоритмов проверки целостности пакета в рамках создаваемого контекста. Список должен содержать хотя бы один элемент.

Рекомендуется указывать не список алгоритмов, а только один алгоритм проверки целостности пакета.

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько алгоритмов проверки целостности (их комбинацию), то используйте альтернативный подход: в атрибуте Transform структуры ESPProposal укажите список структур ESPTransform, а в каждой структуре ESPTransform задайте только один алгоритм проверки целостности пакета.

Синтаксис

IntegrityAlg* = СТРОКА

Значение

Возможные значения:

"MD5-H96-KPDK" - Keyed MD5

"MD5-H96-HMAC" - HMAC MD5 (96 бит)

"SHA1-H96-HMAC" - HMAC SHA-1 (96 бит)

"GR341194CPRO1-H96-HMAC-65534" – реализация ГОСТ Р 34.11-94 (96 бит)

<u>Значение по умолчанию</u>	при отсутствии в связке контекстов компонента AHProposal, список должен содержать хотя бы один элемент. Иначе функциональность проверки целостности пакетов возлагается на протокол AH.
------------------------------	---

Пример структуры ESPProposal

```
ESPTransform esp_trf_01(  
    LifetimeSeconds = 28800  
    LifetimeKilobytes = 4608000  
    CipherAlg      *= "G2814789CPRO1-K256-CBC-254"  
    IntegrityAlg   *= "GR341194CPRO1-H96-HMAC-65534"  
)  
ESPTransform esp_trf_02(  
    LifetimeSeconds = 28800  
    LifetimeKilobytes = 4608000  
    CipherAlg      *= "G2814789CPRO1-K256-CBC-254"  
    IntegrityAlg   *= "MD5-H96-HMAC"  
)  
ESPTransform esp_trf_03(  
    LifetimeSeconds = 28800  
    LifetimeKilobytes = 4608000  
    CipherAlg      *= "G2814789CPRO1-K256-CBC-254"  
    IntegrityAlg   *= "SHA1-H96-HMAC"  
)  
ESPProposal ESP_1(  
    Transform *= esp_trf_01, esp_trf_02, esp_trf_03  
)
```


15.19. Структура IKERule

Структура IKERule описывает правило создания контекста соединения для протокола IKE.

Имя структуры	IKERule
Атрибуты	IKEPeerIPFilter IKELocalIPFilter DoNotUseDPD DPDIIdleDuration DPDResponseDuration DPDRetries IKECFGRequestAddress DoAutopass AggrModeAuthMethod MainModeAuthMethod AggrModePriority Transform

Схематическое представление структуры IKERule и структур, на которые ссылаются атрибуты IKERule:

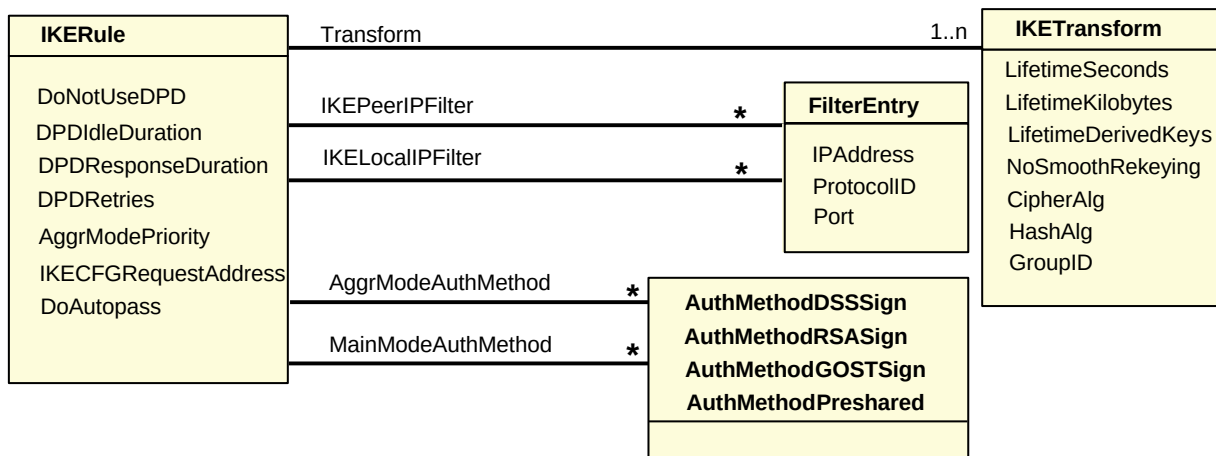


Рисунок 81

Атрибут IKEPeerIPFilter

Атрибут IKEPeerIPFilter описывает список допустимых IP-адресов партнера, при которых применяется данное правило.

Этот атрибут используется VPN-устройством, выступающим в роли ответчика IKE-сессии, при проверке UDP-заголовка первого (входящего) пакета.

Для VPN-устройства, выступающего в роли инициатора создания IKE-сессии, этот атрибут игнорируется.

Синтаксис

IKEPeerIPFilter* = [FilterEntry](#)

Значения

В качестве элементов списка могут использоваться структуры [FilterEntry](#), используемые в [FilteringRule](#), либо самостоятельные структуры [FilterEntry](#). При этом для каждого элемента:

адрес: учитываются все единичные IP-адреса и диапазоны. При наличии хотя бы одного элемента без IP-адресов, принимается логика проверки IP-адреса IKE-партнера по умолчанию.

значения протоколов игнорируются. При анализе входящего ISAKMP-пакета в качестве протокола всегда подразумевается UDP.

значения портов игнорируются. При анализе входящего ISAKMP-пакета допускаются любые порты партнера.

Значение по умолчанию

При проверке IP-адреса IKE-партнера учитываются все возможные значения IP-адресов, используемых в структурах [TunnelEntry](#) в списках [TunnelingParameters](#) всех возможных структур [IPsecAction](#), которые в свою очередь используют текущее правило [IKERule](#). Если в какой-либо из таких структур [TunnelEntry](#) не задано поле PeerIPAddress, то данное правило [IKERule](#) может быть использовано с любым партнером.

Если в структурах [IPsecAction](#) атрибут [TunnelingParameters](#) отсутствует (работает транспортный режим), то IP-адрес IKE-партнера проверяется по атрибуту [PeerIPFilter](#) всех структур [FilteringRule](#), в которых используется данное правило [IPsecAction](#).

Атрибут IKELocalIPFilter

Атрибут IKELocalIPFilter описывает список допустимых локальных IP-адресов, при которых применяется данное правило.

Этот атрибут используется VPN-устройством, выступающим в роли ответчика IKE-сессии, при проверке UDP-заголовка первого (входящего) пакета.

Для VPN-устройства, выступающего в роли инициатора создания IKE-сессии, этот атрибут игнорируется.

Синтаксис

IKELocalIPFilter* = [FilterEntry](#)

Значения

В качестве элементов списка могут использоваться структуры [FilterEntry](#), используемые в [FilteringRule](#), либо самостоятельные структуры [FilterEntry](#). При этом для каждого элемента:

значения портов игнорируются. При анализе входящего ISAKMP-пакета допускаются следующие локальные порты:

4500 (используется для NAT Traversal).

Значение по умолчанию

Атрибут DoNotUseDPD

Атрибут DoNotUseDPD задает режим использования протокола DPD (Dead Peer Detection).

Синтаксис

Значение

FALSE – использовать протокол DPD

Значение по умолчанию

Атрибут DPIdleDuration

Атрибут `DPDIdleDuration` задает допустимый период времени отсутствия входящего трафика от партнера, по истечении которого, при наличии исходящего трафика, активируется DPD-сессия. Если атрибут `DoNotUseDPD = TRUE`, то атрибут `DPDIdleDuration` игнорируется.

Синтаксис

Значение

Значение по умолчанию

Атрибут DPDResponseDuration

Атрибут `DPDResponseDuration` задает время ожидания ответа от партнера на `DPD` запрос в секундах. Если атрибут `DoNotUseDPD` = `TRUE`, то атрибут `DPDResponseDuration` игнорируется.

Синтаксис

Значение

Значение по умолчанию

Атрибут DPDRetries

Атрибут DPDRetries задает число попыток провести DPD обмен. Если все попытки закончились неудачей, защищенное соединение (IKE-контекст) считается "мертвым", и производится попытка создать его заново. Если атрибут DoNotUseDPD = TRUE, то атрибут DPDRetries игнорируется.

Синтаксис DPDRetries = ЦЕЛОЕ32

Значение 1..10

Значение по умолчанию 3.

Атрибут IKECFGRequestAddress

Атрибут IKECFGRequestAddress задает режим работы IKECFG-клиента.

Синтаксис IKECFGRequestAddress = **TRUE** | **FALSE**

Значение TRUE – агент является активным IKECFG-клиентом, т.е. агент инициирует отправку запроса на получение внутреннего IP-адреса у партнера сразу после создания IKE SA. Возможны следующие варианты дальнейшей работы агента:

Состояние партнера		Дальнейшие действия агента
Партнер является IKECFG-сервером	Успешно выделен IP-адрес из IKECFG-пула	а) Иницируется вторая фаза IKE б) Полученный адрес будет использован в качестве локального для пакетов, которые будут обрабатываться IPSec SA, созданными на основе исходного IKE SA (включая его потомков – rekeying).
	Выдача адреса невозможна в ходе текущей IKECFG-сессии	Иницируется вторая фаза создания соединения, в ходе которой может быть инициирована новая IKECFG-сессия со стороны партнера для выдачи IP-адреса.
	Ошибка выдачи адреса (например, пул адресов исчерпан)	Создание соединения будет остановлено.
Партнер не является IKECFG-сервером		Иницируется вторая фаза создания соединения.

FALSE - агент является пассивным IKECFG-клиентом, т.е. IKECFG-сессия может быть проведена только по инициативе партнера, если он является IKECFG –сервером.

Значение по умолчанию FALSE

Атрибут DoAutopass

Атрибут DoAutopass задает автоматическую генерацию фильтра для пропускания ISAKMP-трафика.

<u>Синтаксис</u>	DoAutopass = TRUE FALSE
<u>Значение</u>	TRUE: автоматически пропускать ISAKMP-пакеты, соответствующие атрибутам IKEPeerIPFilter и IKELocalIPFilter при отсутствии IP-адреса в атрибуте IKEPeerIPFilter, IP-адреса для построения фильтра берутся из атрибута TunnelingParameters всех структур IPsecAction, ссылающихся на данное правило IKE для структур IPsecAction, ссылающихся на данное правило IKE, в которых атрибут TunnelingParameters отсутствует, IP-адреса берутся из атрибутов PeerIPFilter, LocalIPFilter всех структур FilteringRule, имеющих ссылки на такие IPsecAction FALSE: не пропускать автоматически ISAKMP-трафик. Правило фильтрации (Filtering Rule) с действием PASS должно быть задано явно (вручную) для пропускания ISAKMP-трафика.
<u>Значение по умолчанию</u>	FALSE.

Атрибут AggrModeAuthMethod

Атрибут AggrModeAuthMethod содержит список структур, определяющих способ и параметры аутентификации в агрессивном режиме IKE. В списке не должно быть задано двух одинаковых методов аутентификации.

<u>Примечание:</u>	Хотя бы один из атрибутов AggrModeAuthMethod или MainModeAuthMethod должен быть задан.
<u>Синтаксис</u>	AggrModeAuthMethod* = AuthMethodDSSSign AuthMethodRSASign FuthMethodGOSTSign AuthMethodPreshared
<u>Значение</u>	AuthMethodDSSSign - Аутентификация DSA подписью AuthMethodRSASign - Аутентификация RSA подписью AuthMethodGOSTSign - Аутентификация при помощи подписи алгоритмом ГОСТ34.10 AuthMethodPreshared - Аутентификация при помощи предустановленного ключа.
<u>Значение по умолчанию</u>	При отсутствии MainModeAuthMethod атрибут является обязательным. При наличии атрибута MainModeAuthMethod Aggressive Mode не проводится.

Атрибут MainModeAuthMethod

Атрибут MainModeAuthMethod содержит список структур, определяющих способ и параметры аутентификации в основном режиме IKE. В списке не должно быть задано двух одинаковых методов аутентификации.

<u>Примечание:</u>	Хотя бы одно из атрибутов AggrModeAuthMethod или MainModeAuthMethod должен быть задан.
<u>Синтаксис</u>	MainModeAuthMethod* = AuthMethodDSSSign AuthMethodRSASign FuthMethodGOSTSign AuthMethodPreshared
<u>Значение</u>	AuthMethodDSSSign - Аутентификация DSA подписью AuthMethodRSASign - Аутентификация RSA подписью AuthMethodGOSTSign - Аутентификация при помощи подписи алгоритмом ГОСТ3410 AuthMethodPreshared - Аутентификация при помощи предустановленного ключа.
<u>Значение по умолчанию</u>	При отсутствии атрибута AggrModeAuthMethod атрибут является обязательным. При наличии атрибута AggrModeAuthMethod Main Mode не проводится.

Атрибут AggrModePriority

AggrModePriority задает режим использования Aggressive Mode. Атрибут используется только для инициатора в случае, если заданы значения MainModeAuthMethod и AggrModeAuthMethod одновременно. Атрибут игнорируется, если задан только один режим (Main Mode или Aggressive Mode)

<u>Синтаксис</u>	AggrModePriority = TRUE FALSE
<u>Значение</u>	TRUE – Aggressive Mode является более приоритетным, инициатор начинает первую фазу IKE в "агрессивном" режиме. FALSE – Main Mode является более приоритетным, то инициатор начинает первую фазу IKE в "основном" режиме.
<u>Значение по умолчанию</u>	FALSE.

Атрибут Transform

Атрибут Transform задает список допустимых групп параметров протокола ISAKMP для создания SA. Количество элементов списка не ограничено.

<u>Синтаксис</u>	Transform* = <u>IKETransform</u>
<u>Значение по умолчанию</u>	не существует, атрибут обязательный.

15.20. Структура IKETransform

Структура IKETransform задает набор параметров, необходимых для создания ISAKMP SA.

<u>Имя структуры</u>	IKETransform
<u>Атрибуты</u>	LifetimeSeconds LifetimeKilobytes LifetimeDerivedKeys NoSmoothRekeying CipherAlg HashAlg GroupID

Атрибут LifetimeSeconds

Атрибут LifetimeSeconds задает время существования IKE- контекста (в секундах).

Синтаксис LifetimeSeconds = ЦЕЛОЕ32

Значение Целое число из диапазона 1 .. 4 294 967 295.

Значение по умолчанию нет ограничений на действие SA.

Для совместимости IOS-партнером (Cisco) нужно всегда указывать в своем предложении атрибут LifetimeSeconds - время жизни в секундах и высылать IOS-партнеру. В противном случае, IOS будет пытаться поместить в принятое предложение новый атрибут – время жизни SA по времени, которое IOS-ом будет установлено для создаваемого SA. Это является неприемлемым для агента и CSP VPN Gate, будучи партнером IOS, прекращает у становление соединения.

Атрибут LifetimeKilobytes

Атрибут LifetimeKilobytes задает максимальное ограничение по трафику на действие контекста в килобайтах.

Синтаксис LifetimeKilobytes = ЦЕЛОЕ32

Значение Целое число из диапазона 1 .. 4 294 967 295.

Значение по умолчанию нет ограничений на действие SA.

Атрибут LifetimeDerivedKeys

Атрибут LifetimeDerivedKeys задает ограничение по числу IPsec SA (числу успешных Quick Mode - QM), которые можно сделать с использованием одного IKE-контекста.

Синтаксис LifetimeDerivedKeys = ЦЕЛОЕ32

Значение Целое число из диапазона 1 .. 4 294 967 295.

Значение по умолчанию нет ограничений на действие SA по числу созданных под его защитой IPsec SA.

Атрибут NoSmoothRekeying

Атрибут NoSmoothRekeying задает режим "мягкой" смены ключевого материала.

<u>Синтаксис</u>	NoSmoothRekeying = TRUE FALSE
<u>Значение</u>	TRUE -заблаговременная смена ключевого материала (rekeying) не проводится. При отсутствии подходящего ISAKMP SA, новый ISAKMP SA создаётся только по запросу из ядра на создание IPsec SA – при наличии исходящего IP-пакета, либо по инициативе партнера. В результате процесс создания IPsec SA существенно задерживается FALSE - заблаговременно, незадолго до окончания действия ISAKMP SA, на его основе (по тем же правилам и с теми же Identity) проводится IKE-сессия по созданию нового ISAKMP SA - rekeying. Rekeying не проводится, если за время существования старого SA под его защитой не было никакого трафика¹¹
<u>Значение по умолчанию</u>	FALSE

Атрибут CipherAlg

Атрибут CipherAlg задает набор предлагаемых/допустимых алгоритмов шифрования для ISAKMP.

Рекомендуется указывать не список алгоритмов, а только один алгоритм шифрования.

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько алгоритмов шифрования (их комбинацию), то используйте альтернативный подход: в атрибуте Transform структуры IKERule укажите список структур IKETransform, а в каждой структуре IKETransform задайте только один алгоритм шифрования (см. [Пример структуры IKERule](#)).

<u>Синтаксис</u>	CipherAlg* = СТРОКА
<u>Значение</u>	возможные значения: "DES-CBC" - DES в режиме CBC "IDEA-CBC" - IDEA в режиме CBC "DES3-K168-CBC" - DES3 в режиме CBC "AES-K128-CBC" - AES в режиме CBC с длиной ключа 128 "AES-K192-CBC" - AES в режиме CBC с длиной ключа 192 "AES-K256-CBC" - AES в режиме CBC с длиной ключа 256 "G2814789CPRO1-K256-CBC-65534" – реализация ГОСТ 28147-89 в режиме CBC
<u>Значение по умолчанию</u>	не существует, атрибут обязательный, список должен содержать хотя бы один элемент.

¹¹ Для проведения rekeying необходимо, чтобы время жизни обновляемого соединения было существенно больше времени, которое отводится на проведение IKE-сессии.

Атрибут HashAlg

Атрибут HashAlg задает набор предлагаемых/допустимых алгоритмов вычисления хэша для ISAKMP.

Рекомендуется указывать не список алгоритмов, а только один алгоритм хэширования.

Если же указан список алгоритмов и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько алгоритмов хэширования, то используйте альтернативный подход: в атрибуте Transform структуры IKERule укажите список структур IKETransform, а в каждой структуре IKETransform задайте только один алгоритм хэширования (см. [Пример структуры IKERule](#)).

<u>Синтаксис</u>	HashAlg* = СТРОКА
<u>Значение</u>	"MD5"
	"SHA1"
	"GR341194CPRO1-65534" – реализация ГОСТ Р 34.11-94
<u>Значение по умолчанию</u>	не существует, атрибут обязательный, список должен содержать хотя бы один элемент.

Атрибут GroupID

Атрибут GroupID описывает предлагаемые/допустимые Oakley группы.

Рекомендуется указывать не список Oakley-групп, а только одну группу.

Если же указан список Oakley-групп и Агент является инициатором соединения, то будет использоваться только первый элемент списка.

Если же существует необходимость задать несколько Oakley-групп, то используйте альтернативный подход: в атрибуте Transform структуры IKERule укажите список структур IKETransform, а в каждой структуре IKETransform задайте только одну группу (см. [Пример структуры IKERule](#) – MainMode).

При использовании атрибута GroupID для Aggressive Mode число предлагаемых Oakley групп должно быть равно единице. Это связано с тем, что в Aggressive Mode вычисление ключевых пар в соответствии с предлагаемой Oakley-группой производится сразу, не дожидаясь ответа от партнера.

<u>Синтаксис</u>	GroupID* = MODP_768, MODP_1024, MODP_1536
<u>Значение</u>	MODP_768 – стандартная Oakley-группа с длиной ключа 768 бит – группа 1
	MODP_1024 – стандартная Oakley-группа с длиной ключа 1024 бита-группа 2
	MODP_1536 – стандартная Oakley-группа с длиной ключа 1536 бит - группа 5
<u>Значение по умолчанию</u>	не существует, атрибут обязательный, список должен содержать хотя бы один элемент.

Примечание

Стоит отметить, что в правиле IKE (IKERule) предоставление партнеру выбора различных Oakley-групп возможно только в основном режиме IKE (MainMode). Если правило IKE предусматривает агрессивный режим (присутствует структура

AggrModeAuthMethod), то в этом правиле IKERule во всех структурах IKETransform атрибут GroupID должен иметь только одно значение и оно должно быть одинаковым во всех структурах IKETransform, т.е. должна быть указана одна и та же группа.

В ряде случаев это приводит к потере гибкости конфигурации CSP VPN Gate и, следовательно, к применению не рекомендуется.

Пример структуры IKERule

```
IKETransform ike_trf_01(  
    LifetimeSeconds = 28800  
    CipherAlg      *= "G2814789CPR01-K256-CBC-65534"  
    HashAlg       *= "GR341194CPR01-65534"  
    GroupID       *= MODP_1536  
)  
IKETransform ike_trf_02(  
    LifetimeSeconds = 28800  
    CipherAlg      *= "DES-CBC"  
    HashAlg       *= "GR341194CPR01-65534"  
    GroupID       *= MODP_1024  
)  
IKETransform ike_trf_03(  
    LifetimeSeconds = 28800  
    CipherAlg      *= "AES-K128-CBC"  
    HashAlg       *= "GR341194CPR01-65534"  
    GroupID       *= MODP_768  
)  
IKERule ike_rule(  
    DoNotUseDPD = FALSE  
    DPDIdleDuration = 60  
    DPDResponseDuration = 5  
    DPDRetries = 3  
    MainModeAuthMethod *= auth_method_01  
    Transform *= ike_trf_01,ike_trf_02,ike_trf_03  
    DoAutopass = TRUE  
)
```

15.21. Структуры для аутентификации

Схема данных структур AuthMethodDSSSign, AuthMethodRSASign, AuthMethodGOSTSign, AuthMethodPreshared, описывающих идентификационную информацию, предполагаемую к использованию при создании IKE контекста соединения, представлена на рисунке ниже.

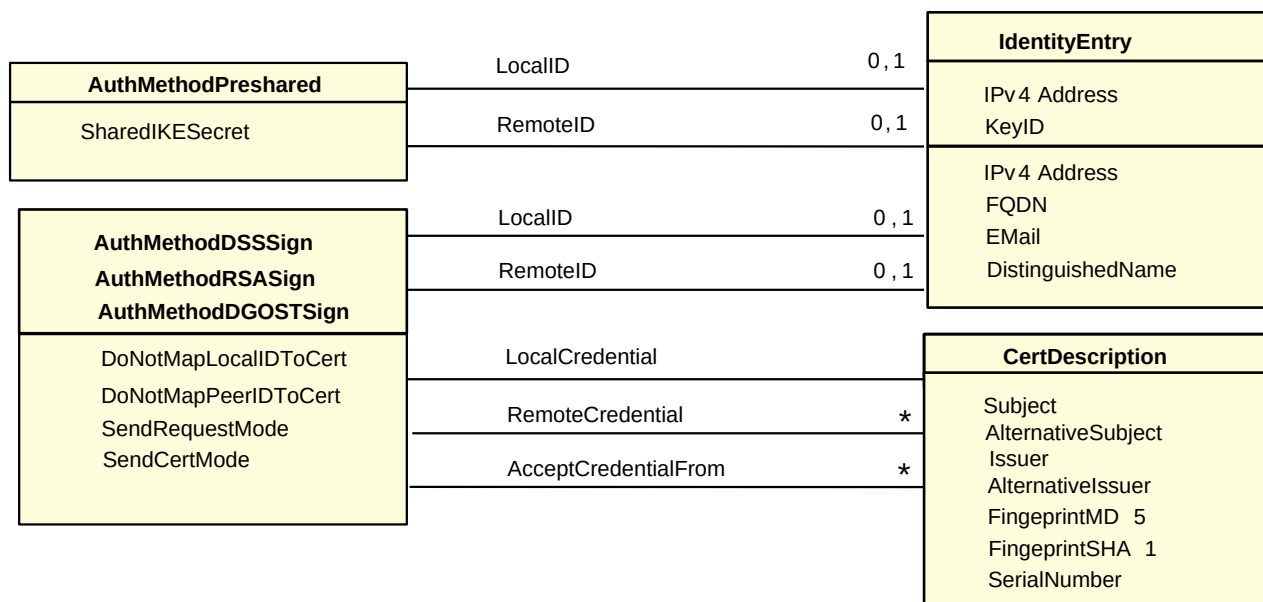


Рисунок 82

15.22. Структуры AuthMethodDSSSign, AuthMethodRSASign, AuthMethodGOSTSign

Указанная структура задает аутентификационную информацию при использовании сертификатов. Алгоритм (RSA, DSA, GOST), указанный в названии структуры, является криптографическим алгоритмом аутентификации сторон.

AuthMethodDSSSign – аутентификация DSS подписью

AuthMethodRSASign – аутентификация RSA подписью

AuthMethodGOSTSign - аутентификация при помощи подписи алгоритмом ГОСТ3410-94 или ГОСТ3410-2001.

<u>Имя структур</u>	AuthMethodDSSSign AuthMethodRSASign AuthMethodGOSTSign
<u>Атрибуты</u>	LocalID RemoteID LocalCredential RemoteCredential AcceptCredentialFrom DoNotMapLocalIDToCert DoNotMapRemoteIDToCert SendRequestMode SendCertMode

Атрибут LocalID

Атрибут LocalID задает идентификационную информацию данного VPN-устройства.

Синтаксис LocalID = IdentityEntry

В структуре IdentityEntry допускается задание одного значения одному из идентификаторов типа IPv4Address, FQDN, Email, DistinguishedName.

При задании значения атрибуту DistinguishedName использование в строке Subject зарезервированного слова TEMPLATE недопустимо.

При задании значения атрибуту IPv4Address использование диапазона IP-адресов недопустимо.

Если значение задано зарезервированным словом USER_SPECIFIC_DATA, то в качестве идентификатора будет использовано соответствующее значение из локального сертификата. Если в сертификате соответствующее значение отсутствует, то ISAKMP-сессия будет прервана.

Значение по умолчанию первый IP-адрес сетевого интерфейса, с которого отсылаются ISAKMP-пакеты партнеру.

Атрибут RemoteID

Атрибут RemoteID задает требования к идентификационной информации партнера.

Синтаксис RemoteID = [IdentityEntry](#)

В структуре IdentityEntry допускается задание нескольких идентификаторов типа [IPv4Address](#), [FQDN](#), [EMail](#), [DistinguishedName](#).

Значение по умолчанию принимается любой ID партнера.

Атрибут LocalCredential

Атрибут LocalCredential задает требуемые характеристики сертификата данного VPN-устройства. В случае использования аутентификации на алгоритме ГОСТ Р 3410 локальный сертификат используется, если его секретный ключ доступен.

Синтаксис LocalCredential = [CertDescription](#)

Значение по умолчанию требования отсутствуют. Используется первый локальный сертификат.

Атрибут RemoteCredential

Атрибут RemoteCredential задает требуемые характеристики сертификата партнера по взаимодействию.

Синтаксис RemoteCredential* = [CertDescription](#)

Значение по умолчанию требования отсутствуют, допускается любой сертификат.

Атрибут AcceptCredentialFrom

Атрибут AcceptCredentialFrom задает требуемые характеристики CA-сертификата, удостоверяющего подлинность сертификата партнера.

Синтаксис AcceptCredentialFrom* = [CertDescription](#)

Значение по умолчанию используется любой из тех CA, которому мы доверяем.

Атрибут DoNotMapLocalIDToCert

Атрибут DoNotMapLocalIDToCert задает режим использования локального идентификатора при поиске локального сертификата.

Синтаксис

DoNotMapLocalIDToCert = **TRUE** | **FALSE**

Значение

TRUE – при поиске локального сертификата используются описания сертификатов, указанные в атрибуте LocalCredential. Значение атрибута LocalID игнорируется

FALSE - при поиске локального сертификата используется список CertDescription. Каждый элемент этого списка является объединением атрибута LocalID (используется первое значение) и CertDescription из атрибута LocalCredential. Объединение строится по следующим правилам:

если LocalID задан зарезервированным словом USER_SPECIFIC_DATA, то результирующий CertDescription совпадает с исходным CertDescription из атрибута LocalCredential.

если LocalID задан типом DistinguishedName, то:

если в исходном CertDescription задано поле Subject, то множество его атрибутов должно являться подмножеством атрибутов значения LocalID. Если это условие не выполняется, то соединение не установится

результирующий CertDescription получается заменой или добавлением значения поля Subject из LocalID в исходном CertDescription

если LocalID задан типом, отличным от DistinguishedName, то:

если в исходном CertDescription задано поле такого же типа, то их значения должны совпадать. Если это не выполняется, то соединение не установится

результирующий CertDescription получается добавлением значения LocalID в исходный CertDescription.

Значение по умолчанию **FALSE**

Атрибут DoNotMapRemoteIDToCert

Атрибут DoNotMapRemoteIDToCert задает режим использования идентификатора партнера при поиске его сертификата.

Синтаксис

DoNotMapRemoteIDToCert = **TRUE** | **FALSE**

Значение

TRUE – при поиске сертификата партнера используются описания сертификатов, указанные в атрибуте RemoteCredential, значение атрибута RemoteID игнорируется

FALSE – при поиске сертификата партнера используется список CertDescription. Каждый элемент этого списка является объединением присланного идентификатора партнера и CertDescription из атрибута RemoteCredential. Правила объединения совпадают с ранее описанными правилами в атрибуте DoNotMapLocalIDToCert.

Значение по умолчанию **FALSE**.

Атрибут SendRequestMode

Атрибут SendRequestMode определяет логику отсылки запроса на сертификат партнера.

Синтаксис

SendRequestMode = **AUTO | NEVER | ALWAYS**

Значение

AUTO – запрос высылается, если возможный сертификат партнера отсутствует

NEVER – запрос не высылается

ALWAYS – запрос высылается всегда

Значение по умолчанию AUTO

Атрибут SendCertMode

Атрибут SendCertMode определяет логику отсылки локального сертификата в процессе первой фазы IKE на запрос партнера. В своем запросе партнер может и указать какому CA сертификату он доверяет. Если такой сертификат не найден, то он не отправляется.

Синтаксис

SendCertMode = **AUTO | NEVER | ALWAYS | CHAIN**

Значение

AUTO – автоматически определяется, когда необходима отсылка локального сертификата партнеру:

если партнер не прислал запроса, то сертификат не отправляется

если партнер прислал запрос и соответствующий сертификат был найден, то партнеру высылается либо сертификат либо найденная цепочка сертификатов

если партнер прислал запрос и этот запрос не был удовлетворен, то сертификат не высылается.

NEVER – сертификат не высылается

ALWAYS – сертификат высылается всегда

CHAIN - сертификат высылается всегда, причем в составе с цепочкой доверительных CA:

Имеется ввиду цепочка сертификатов, построенная от локального сертификата до CA, который удовлетворяет описанию, присланному партнером в запросе. В общем случае это CA, удовлетворяющий запросу партнера, произвольное количество промежуточных CA и локальный сертификат.

Значение по умолчанию AUTO.

15.23. Структура AuthMethodPreshared

Структура AuthMethodPreshared задает аутентификационную информацию при использовании предустановленных (Preshared) ключей.

<u>Имя структуры</u>	AuthMethodPreshared
<u>Атрибуты</u>	LocalID
	RemoteID
	SharedIKESecret

Атрибут LocalID

Атрибут LocalID задает идентификационную информацию данного VPN-устройства. В структуре IdentityEntry допускается задание только одного идентификатора с одним значением.

При задании значения атрибуту IPv4Address использование диапазона IP-адресов недопустимо.

Использование зарезервированного слова USER_SPECIFIC_DATA недопустимо.

Синтаксис LocalID = [IdentityEntry](#)

Значение по умолчанию локальный IP-адрес из IKE-пакета.

Атрибут RemoteID

Атрибут RemoteID задает требования к идентификационной информации партнера. В структуре IdentityEntry допускается задание нескольких идентификаторов разных типов.

Синтаксис RemoteID = [IdentityEntry](#)

Значение по умолчанию принимается любой ID партнера.

Атрибут SharedIKESecret

Атрибут SharedIKESecret определяет ссылку на предустановленный секретный ключ.

В атрибуте указывается имя предустановленного (Preshared) ключа, хранимого в базе данных Продукта.

Синтаксис SharedIKESecret = СТРОКА

Значение имя предустановленного (Preshared) ключа.

Значение по умолчанию не существует, атрибут обязательный.

15.24. Структура IdentityEntry

Структура IdentityEntry описывает идентификационную информацию. Варианты задания этой структуры приведены в описаниях структур [AuthMethodPreshared](#) и [AuthMethod{DSS|RSA|GOST}Sign](#).

<u>Имя структуры</u>	IdentityEntry
<u>Атрибуты</u>	IPv4Address - IPv4 адрес FQDN - FQDN хоста EMail - EMail пользователя DistinguishedName - DN в формате X509Subject KeyID - Идентификатор ключа

Если структура IdentityEntry используется определенным методом аутентификации, то атрибуты, не соответствующие данному методу, игнорируются. Атрибуты, используемые для определенных методов аутентификации:

- AuthMethodPreshared
 - IPv4Address
 - KeyID
- AuthMethod{DSS|RSA|GOST}Sign
 - IPv4Address
 - FQDN
 - EMail
 - DistinguishedName.

Атрибут IPv4Address

Атрибут IPv4Address задает описание идентификатора по указанным IP-адресам.

<u>Синтаксис</u>	для данного VPN устройства: IPv4Address = IP USER_SPECIFIC_DATA для партнера: IPv4Address*=IP IP..IP IP/ЦЕЛОЕ32 USER_SPECIFIC_DATA
<u>Значения</u>	для данного VPN устройства: IP- один IP-адрес для партнера: IP – список IP-адресов IP..IP – список диапазонов IP-адресов IP/ЦЕЛОЕ32 – список подсетей с IP-адресом и маской

Если задано значение **USER_SPECIFIC_DATA**, то берется первый IP-адрес из расширения **Subject Alternative Name** локального сертификата, используемого для подписи. Если IP-адрес в сертификате отсутствует, то соединение не создается.

Если заданы диапазоны IP-адресов либо подсети, то это означает, что принимается любой Identity типа IP-адрес, если значение IP, присланное партнером в таком Identity, попадает в указанный диапазон, либо подсеть.

Значение по умолчанию используются другие атрибуты.

Атрибут FQDN

Атрибут FQDN (Fully Qualified Domain Name – полностью определенное доменное имя) задает описание идентификатора хоста по указанным DNS именам.

Синтаксис

FQDN* = СТРОКА | **USER_SPECIFIC_DATA**

Значения

для AuthMethodPreshared – атрибут игнорируется;

для AuthMethod{DSS|RSA|GOST}Sign:

строки вида "host.domain". Шаблоны не допускаются.

если задано значение **USER_SPECIFIC_DATA**, то при проверке/отсылке Identity используется поле **DNS** расширения **Subject Alternative Name** соответствующего сертификата, используемого соответственно для проверки/формирования подписи.

Значение по умолчанию используются другие атрибуты.

Атрибут EMail

Атрибут EMail задает описание идентификатора конечного устройства по указанным Email-адресам.

Синтаксис

Email* = СТРОКА | **USER_SPECIFIC_DATA**

Значения

для AuthMethodPreshared – атрибут игнорируется

для AuthMethod{DSS|RSA|GOST}Sign:

строки вида "user@host.domain". Шаблоны не допускаются.

если задано значение **USER_SPECIFIC_DATA**, то при проверке/отсылке Identity используется поле **EMail** расширения **Subject Alternative Name** сертификата, используемого соответственно для проверки/формирования подписи.

Значение по умолчанию используются другие атрибуты.

Атрибут DistinguishedName

Атрибут DistinguishedName задает описание идентификатора по указанным DN (уникальное имя в формате X509Subject.).

<u>Синтаксис</u>	DistinguishedName* = CertDescription USER_SPECIFIC_DATA
<u>Значения</u>	для AuthMethodPreshared – атрибут игнорируется для AuthMethod{DSS RSA GOST}Sign: в каждой структуре CertDescription допускается использовать только поле Subject если задано значение USER_SPECIFIC_DATA, то при проверке/отсылке Identity используется полное описание раздела Subject Name сертификата, используемого соответственно для проверки/формирования подписи.
<u>Значение по умолчанию</u>	используются другие атрибуты

Атрибут KeyID

Атрибут KeyID задает описание Identity по указанным идентификаторам Preshared ключей.

<u>Синтаксис</u>	KeyID* = СТРОКА
<u>Значение</u>	строка, содержащая шестнадцатеричное представление идентификаторов ключей. Для AuthMethodPreshared: рекомендуется при составлении идентификатора ключа использовать шестнадцатеричное представление только печатных символов без пробела: Именно такое ограничение существует при формировании конфигурации IOS. шаблоны не допускаются. Для AuthMethod{ DSS RSA GOST}Sign - атрибут игнорируется.
<u>Значение по умолчанию</u>	используются другие атрибуты.

Пример

```
AuthMethodPreshared auth_key (  
    RemoteID = IdentityEntry(  
        IPv4Address *= 192.168.13.117, 192.168.13.118  
    )  
    SharedIKESecret = "cskey"  
)
```

15.25. Структура CertDescription

Структура CertDescription используется для задания собственного идентификатора и идентификатора партнера, для задания характеристик локального сертификата и сертификата партнера.

Для задания СТРОКИ в атрибутах этой структуры смотрите формат DN в разделе ["Формат задания DistinguishedName в LSP"](#).

<u>Имя структуры</u>	CertDescription
<u>Атрибуты</u>	Subject
	AlternativeSubject
	Issuer
	AlternativeIssuer
	FingerprintMD5
	FingerprintSHA1
	SerialNumber

Атрибут Subject

Атрибут Subject задает значение/шаблон поля Subject сертификата.

<u>Синтаксис</u>	Subject* = TEMPLATE COMPLETE , СТРОКА
<u>Значение</u>	TEMPLATE – флаг, при котором указанная строка представляет собой незаконченное значение поля Subject сертификата. При поиске и сравнении, поле Subject сертификата должно содержать указанную строку COMPLETE – флаг, при котором указанная строка представляет собой законченное значение поля Subject сертификата. При поиске и сравнении поле Subject сертификата должно совпадать с указанным множеством атрибутов и их значениями (с точностью до порядка указания в сертификате) в строке.
<u>Предупреждение:</u>	DN в строке должен быть задан точно также, как он задан в сертификате: необходимо строго соблюдать количество пробелов и регистр символов.
<u>Значение по умолчанию</u>	если задана строка, но опущен флаг TEMPLATE или COMPLETE, то по умолчанию он равен COMPLETE; если не задана строка, то поле Subject сертификата принимает любые значения.

Пример: Допустимые варианты:

```
Subject* = TEMPLATE, "ou=eng"
Subject* = "ou=eng", TEMPLATE
Subject* = COMPLETE, "c=RU,o=co.,ou=eng,cn=engineer"
Subject* = "c=RU, o=co, ou=eng, cn=engineer"

Недопустимые варианты:
Subject *= TEMPLATE, "ou=eng", COMPLETE
Subject *= "ou=eng", "ou=qa"
```

Атрибут AlternativeSubject

Атрибут AlternativeSubject задает значение/шаблон Alternative Subject Extension сертификата.

Синтаксис AlternativeSubject = СТРОКА

Значение по умолчанию любое значение Alternative Subject Extension сертификата.

Атрибут Issuer

Атрибут Issuer задает значение/шаблон поля Issuer сертификата.

Синтаксис Issuer* = **TEMPLATE | COMPLETE**, СТРОКА

Значение TEMPLATE – флаг, при котором указанная строка представляет собой незаконченное значение поля Issuer сертификата. При поиске и сравнении, поле Issuer сертификата должно содержать указанную строку.

COMPLETE – флаг, при котором указанная строка представляет собой законченное значение поля Issuer сертификата. При поиске и сравнении, поле Issuer сертификата должно совпадать с указанным множеством атрибутов и их значениями (с точностью до порядка указания в сертификате) в строке.

Предупреждение: DN в строке должен быть задан точно также, как он задан в сертификате: необходимо строго соблюдать количество пробелов и регистр символов.

Значение по умолчанию
если задана строка, но опущен флаг TEMPLATE или COMPLETE, то по умолчанию он равен COMPLETE;
если не задана строка, то поле Issuer сертификата принимает любые значения.

Атрибут AlternativeIssuer

Атрибут AlternativeIssuer задает значение/шаблон Alternative Issuer Extension сертификата.

Синтаксис AlternativeIssuer = СТРОКА

Значение по умолчанию любое значение Alternative Issuer Extension сертификата.

Атрибут FingerprintMD5

Атрибут FingerprintMD5 задает значение хеш-функции алгоритма MD5 по бинарному представлению сертификата.

Синтаксис FingerprintMD5 = СТРОКА

Значение шестнадцатеричная запись значения хэш-функции, длина строки должна быть равна 32 символам.

Значение по умолчанию любое значение хэш-функции.

Атрибут FingerprintSHA1

Атрибут FingerprintSHA1 задает значение хеш-функции алгоритма SHA1 по бинарному представлению сертификата.

<u>Синтаксис</u>	FingerprintSHA1 = СТРОКА
<u>Значение</u>	шестнадцатеричная запись значения хэш-функции, длина строки должна быть равна 40 символам.
<u>Значение по умолчанию</u>	любое значение хэш-функции.

Атрибут SerialNumber

Атрибут SerialNumber задает значение серийного номера сертификата.

<u>Синтаксис</u>	SerialNumber = СТРОКА
<u>Значение</u>	шестнадцатеричная запись серийного номера.
<u>Значение по умолчанию</u>	любое значение серийного номера.

Пример

```
RemoteCredential* = CertDescription(  
    Issuer* = COMPLETE, " CN=S-Terra CenterCA, O=S-Terra, L=Moscow,  
                        C=RU"  
    Subject* = TEMPLATE, "CN=S-Terra, OU=QA"  
    AlternativeSubject = "EMAIL=inform@s-terra.com,  
                        DNS= tester.s-terra.com, IP =10.10.10.10"  
    SerialNumber = "567A99991E1F"  
)
```

15.26. Формат задания DistinguishedName (GeneralNames) в LSP

Текстовое представление DN

Текстовое представление DistinguishedName (GeneralNames), далее просто имени, задается в соответствии с RFC2253:

```
distinguishedName = [name]; may be empty string

name  name-component *("," name-component)

name-component = attributeTypeAndValue *("+" attributeTypeAndValue)

attributeTypeAndValue = attributeType "=" attributeValue

attributeType = (ALPHA 1*keychar) / oid
keychar = ALPHA / DIGIT / "-"

oid = 1*DIGIT *("." 1*DIGIT)

attributeValue = string

string = *( stringchar / pair )
        / "#" hexstring
        / QUOTATION *( quotechar / pair ) QUOTATION; only from v2

quotechar = <any character except "\" or QUOTATION >

special = "," / "=" / "+" / "<" / ">" / "#" / ";"

pair = "\" ( special / "\" / QUOTATION / hexpair )
stringchar = <any character except one of special, "\" or QUOTATION>

hexstring = 1*hexpair
hexpair = hexchar hexchar

hexchar = DIGIT / "A" / "B" / "C" / "D" / "E" / "F"
         / "a" / "b" / "c" / "d" / "e" / "f"

ALPHA = <any ASCII alphabetic character>; (decimal 65-90 and 97-122)
DIGIT = <any ASCII decimal digit> ; (decimal 48-57)
QUOTATION = <the ASCII double quotation mark character '"' decimal 34>
```

Дополнения и отступления от RFC2253

В Агенте версии 3.0 имеются следующие дополнения и отступления от RFC2253:

- символ "/" является разделителем компонент имени, т.е. допустим следующий синтаксис:

```
name = name-component *("/" name-component)
```
- для того, чтобы использовать этот символ как значащий, перед ним необходимо ввести символ "/" (эскейп-символ).
- распознаются следующие сокращения типов атрибутов (attributeType) DistinguishedName:

X.500 Attribute Type	Сокращение
countryName	C
stateName	ST
localityName	L
organizationName	O
organizationalUnitName	OU
commonName	CN
title	T
surname	SN
givenName	GN
initials	I
streetAddress	STREET
nameQualifier	NQ
generationQualifier	GQ
userid	UID
domainComponent	DC

- регистр, в котором записано сокращение, не имеет значения.
- Строковое задание GeneralNames сведено к синтаксису, описанному в RFC2253. Распознаются следующие сокращения типов атрибутов имени GeneralNames:

Тип атрибута	Сокращение
otherName	OTHERNAME
rfc822Name	EMAIL
dNSName	DNS
directoryName	DN
uniformResourceIdentifier	URI
iPAddress	IP
registeredID	RID

- регистр, в котором записано сокращение, не имеет значения
- задание атрибутов x400Address и ediPartyName в строковом представлении не поддерживается.
- Согласно RFC2253 символы ''' (кавычки) и \' (back-slash) являются служебными. Согласно [описанию Терминального символа СТРОКА](#), при задании любого строкового значения в LSP указанные символы так же используются как служебные. Поэтому:
 - каждая отдельно стоящая кавычка в строковом представлении должна быть дополнена слева символом ' \' в LSP
 - каждое сочетание ' \' в строковом представлении должно быть дополнено слева ' \\' в LSP.

Примеры

Имя в сертификате	Строковое представление	В LSP
O=Sergey, Danila and company	O=Sergey\, Danila and company	Subject="O=Sergey\, Danila and company"
O=JSC "Horns and hoofs"	O=JSC \"Horns and hoofs\"	Subject="O=JSC \\\\"Horns and hoofs\\\""
CN=Device#4	CN="Device#4"	Subject="CN=\"Device#4\""

15.27. Работа с сертификатами в LSP

Отсылка локального сертификата

Для отсылки локального сертификата партнеру по IKE в LSP-конфигурации необходимо:

- в структуре [AuthMethodGOSTSign](#) задать атрибут [SendCertMode](#) со значением:
 - ALWAYS – всегда отсылать локальный сертификат
 - CHAIN – всегда отсылать локальный сертификат, CA сертификат и промежуточные CA сертификаты.

Получение сертификата партнера

Сертификат партнера можно получить либо по протоколу IKE, либо по протоколу LDAP.

Сначала агент пытается получить сертификат партнера по IKE, если партнер не прислал сертификат, а прислал только свой идентификатор. Агент по этому идентификатору ищет сертификат партнера сначала в своей базе Продукта, если не нашел, то продолжает поиск на LDAP-сервере.

Получение сертификата партнера по IKE

Для получения сертификата партнера по IKE в LSP-конфигурации нужно:

- в структуре [AuthMethodGOSTSign](#) задать атрибут [SendRequestMode](#) со значением ALWAYS – всегда запрашивать сертификат партнера
- в конфигурации партнера в структуре AuthMethodGOSTSign задать атрибут [SendCertMode](#) со значением:
 - ALWAYS – высылать сертификат
 - CHAIN – высылать локальный сертификат, CA сертификат с цепочкой промежуточных CA.

Получение сертификата партнера по LDAP

В этом случае партнер присылает свой идентификатор, а агент по Subject будет искать сертификат партнера на LDAP-сервере. Для прохождения LDAP-пакетов до LDAP-сервера необходимо в LSP-конфигурации задать соответствующий фильтр:

- задать структуру [LDAPSettings](#) с IP-адресом LDAP-сервера:
 - если прислан идентификатор типа DN:
 - агент по Subject ищет сертификат партнера сначала в своей базе Продукта, а затем на LDAP-сервере
 - если прислан идентификатор другого типа:
 - для получения Subject в локальной конфигурации задаются атрибуты [RemoteID](#), [RemoteCredential](#), [DoNotMapRemoteIDToCert](#)
 - если DoNotMapPeerIDToCert = TRUE, то Subject будет состояться из RemoteCredential
 - если DoNotMapPeerIDToCert = FALSE, то Subject будет состояться из RemoteCredential и RemoteID.

- по составленному Subject агент ищет сертификат партнера сначала в своей базе Продукта, а затем на LDAP-сервере.

Проверка сертификата по CRL

Для проверки сертификата партнера по CRL в LSP-конфигурации нужно:

- в структуре GlobalParameters задать атрибут [CRLHandlingMode](#), при значениях этого атрибута:
 - optional – используется действующий CRL из базы Продукта
 - enable и best_effort – действующий CRL может быть получен по LDAP.

Для получения CRL с LDAP-сервера сначала проверяется поле CDP в проверяемом сертификате, если поле CDP отсутствует, то в конфигурации должна быть задана структура [LDAPSettings](#) с адресом LDAP-сервера. В базу Продукта с LDAP-сервера загружается действующий CRL и по нему проверяется сертификат партнера.

Для прохождения LDAP-пакетов до LDAP-сервера необходимо в политике задать соответствующий фильтр.

15.28. Пример локальной политики безопасности

Сценарий 1

Пример локальной политики безопасности для CSP VPN Server при удаленном доступе к серверу 192.168.16.1 в подсети 192.168.16.0/24 по протоколу http. Трафик между CSP VPN Server и шлюзом безопасности (CSP VPN Gate) защищен VPN-туннелем, построенным на основе протокола ESP. Кроме того, правила фильтрации не разрешают CSP VPN Server доступ к другим ресурсам сети. Аутентификация взаимодействующих сторон осуществляется на основе сертификатов. На внешнем интерфейсе шлюза безопасности защита трафика снимается, к Application Server идет незащищенный трафик.

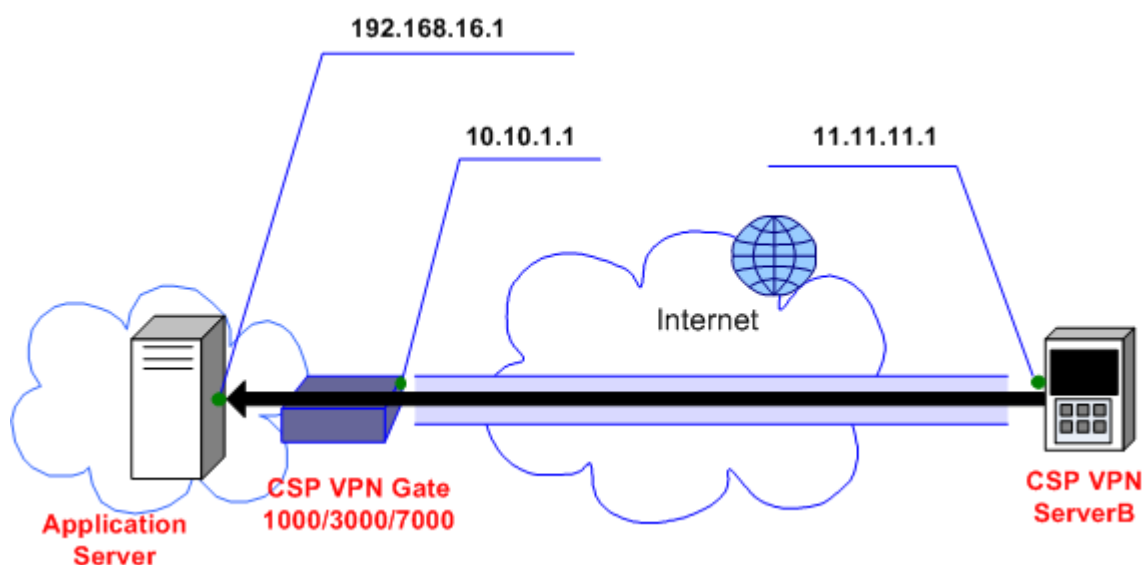
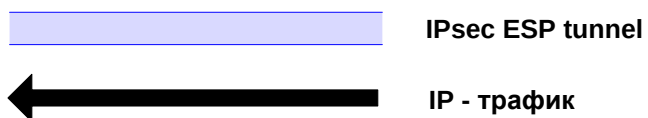


Рисунок 83

Условные обозначения:



```
GlobalParameters (
    Title = "LSP for Server's remote access to Subnet to
    Application Server"
    Version = "2.1"
    IKEInitiatorSessionMax=100
)
FilteringRule Server_Subnet_Server(
    LocalIPFilter* = FilterEntry(
        IPAddress *= 11.11.11.1
        ProtocolID = 6
    )
)
```

```
)
PeerIPFilter* = FilterEntry(
    IPAddress *= 192.168.16.1
    ProtocolID = 6
    Port =80
)
Action* = ( Server_Gate )
)
IPsecAction Server_Gate(
    TunnelingParameters* = TunnelEntry(
        LocalIPAddress = 11.11.11.1
        PeerIPAddress = 10.10.1.1
        DFHandling=COPY
    )
    ContainedProposals* = (ESP_Server_Gate)
    IKERule = IKE_Server_Gate
)
ESPProposal ESP_Server_Gate(
    Transform* = ESPTransform(
        IntegrityAlg* = "GR341194CPR01-H96-HMAC-254"
        CipherAlg *= "G2814789CPR01-K256-CBC-254"
        LifetimeSeconds = 3600
    )
)
IKERule IKE_Server_Gate(
    Transform* = IKETransform(
        CipherAlg* = "G2814789CPR01-K256-CBC-65534"
        HashAlg* = "GR341194CPR01-65534"
        GroupID* = MODP_768
        LifetimeSeconds = 86400
        LifetimeKilobytes = 4608000
        LifetimeDerivedKeys =10000
    )
    AggrModeAuthMethod* = auth_cert
    MainModeAuthMethod* = auth_cert
    DoAutopass = TRUE
)
AuthMethodGOSTSign auth_cert(
    LocalID = IdentityEntry( DistinguishedName* =
        USER_SPECIFIC_DATA
    )
    RemoteCredential* = CertDescription(
        Issuer* = COMPLETE, "C=RU,O=S-Terra,OU=QA,CN=S-Terra"
        SerialNumber = "3aaa4bbb"
        Subject* = TEMPLATE, "C=RU,O=S-Terra"
        AlternativeIssuer = "EMAIL=information@s-terra.com"
        AlternativeSubject = "IP = 11.11.11.1"
    )
    AcceptCredentialFrom* = CertDescription(
        Issuer* = COMPLETE, "C=RU,O=S-Terra,OU=Devel,
        CN=S-Terra_CA"
        SerialNumber = "3aaa4bbb"
        AlternativeSubject = "DNS= tester.s-terra.com"
    )
    SendRequestMode = ALWAYS
    SendCertMode = ALWAYS
)
```

16. Специализированные команды

Для настройки некоторых параметров Продукта предназначены команды интерфейса командной строки, имеющие специализированный синтаксис. Эти команды описаны в данном разделе.

Специализированные команды применяются в области настройки сетевых интерфейсов, в процедурах, связанных с сертификатами, предустановленными ключами, LSP, DDP и пр.

Специализированные команды выполняются в рамках соответствующих программных утилит.

Перечень программных утилит, входящих в состав Продукта CSP VPN Server:

[cert_mgr.exe](#)
[key_mgr.exe](#)
[lsp_mgr.exe](#)
[if_mgr.exe](#)
[dp_mgr.exe](#)
[log_mgr.exe](#)
[sa_show.exe](#)
[klogview.exe](#)

Все эти утилиты расположены в каталоге C:\Program Files\CSP VPN Server.

В операционной системе Microsoft® Windows запуск описанных ниже команд можно производить из консоли типа FAR.

При запуске команд из консоли изначально следует установить путь к папке, в которую распакованы утилиты.

В качестве примера приведены варианты выполнения команды `cert_mgr show`:

```
C:\Program Files\CSP VPN Server>cert_mgr show
```

В приведенных ниже примерах не указан путь к папке, в которую распакованы файлы программных утилит.

16.1. cert_mgr show

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

Синтаксис

```
cert_mgr show [-f CERT_FILE [-p C_PWD]] [-i BJ_INDEX_1] ..  
[-i OBJ_INDEX_N]
```

-f CERT_FILE	Путь к файлу с сертификатами и CRL. Если данная опция не указана, то будут показаны сертификаты из базы Продукта.
-p C_PWD	Пароль к файлу с сертификатами и CRL.
-i OBJ_INDEX_N	Индекс объекта (сертификата и CRL) в файле или в базе Продукта. Если при написании команды указан путь к файлу, то индекс будет определять номер искомого сертификата (CRL) в файле. Если же путь к файлу не указан, то этот индекс будет применяться к базе Продукта сертификатов и CRL.

Значение по умолчанию значение по умолчанию отсутствует

Рекомендации по использованию

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

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

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

Пример

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

```
cert_mgr show
```

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

16.2. cert_mgr import

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

Синтаксис

```
cert_mgr import -f CERT_FILE [-p C_PWD] [-i OBJ_INDEX01]
[-t | [-kc CONTAINER_NAME [-kcp CONTAINER_PWD] [-kf KEY_FILE [-kfp
KEY_FILE_PWD]]]
...
...
[-i OBJ_INDEX0N] [-t | (-kc CONTAINER_NAME [-kcp CONTAINER_PWD]
[-kf KEY_FILE [-kfp KEY_FILE_PWD]])]
```

- f CERT_FILE Путь к файлу с сертификатами и/или CRL
- p C_PWD Пароль к файлу с сертификатами или CRL. Необязательный параметр. Используется только для доступа к файлам, защищенным паролем.
- i OBJ_INDEXN Индекс объекта (сертификата или CRL) в файле или базе Продукта. Если при написании команды указан путь к файлу, то индекс будет определять номер искомого сертификата (CRL) в файле (при импорте одного сертификата (CRL) данный параметр можно не указывать, он будет равен 1). При импорте сертификата из файла, содержащего один сертификат, в качестве индекса следует указывать 1. Индекс задается в виде целого десятичного числа. В качестве индекса нельзя указывать 0.
- t импортируемому сертификату присваивается статус "trusted". При использовании этой опции запрещается использование опций -kc, -kcp и -kf, kfp. Запрещается использовать эту опцию при импорте CRL.

Для получения уникального имени контейнера с секретным ключом воспользуйтесь СКЗИ "КриптоПро CSP 2.0"(относится только к "КриптоПро"). Уникальное имя контейнера нужно заключить в двойные кавычки. См. Пример.

- kc CONTAINER_NAME (для "Сигнал-КОМ") Путь к контейнеру с секретным ключом, служебной и ключевой информацией. Контейнер реализован в виде каталога файловой системы. Не может использоваться, если ранее введена опция -t.
- kcp CONTAINER_PWD (для "Сигнал-КОМ") Пароль к контейнеру с секретным ключом, служебной и ключевой информацией. Необязательный параметр. Используется, если контейнер защищен паролем.
- kf KEY_FILE (для "Сигнал-КОМ"). Путь к файлу с секретным ключом импортируемого сертификата. Необязательный параметр. Не может использоваться, если ранее введена опция -t.
- kfp K_FILE_PWD (для "Сигнал-КОМ") Пароль к файлу с секретным ключом импортируемого сертификата. Необязательный параметр. Используется, если файл с секретным ключом защищен паролем.

Значение по умолчанию значение по умолчанию отсутствует.

Рекомендации по использованию

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

Пример

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

```
cert_mgr import -f c:\certs\test.pfx -p password
-t -i 1 -i 2
1 OK O=S-Terra,CN=CA Cert
2 OK O= S-Terra,CN=Technological Cert
```

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

```
cert_mgr import -f c:\certs\ca.cer -t
```

Импорт локального сертификата в базу Продукта:

```
cert_mgr import -f c:\crts\user01.cer -kc c:\cont\cont01 -kcp 1111
-kf a:\user01.key -kfp 2222
```


16.3. cert_mgr create

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

Синтаксис

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

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

Значение по умолчанию

По умолчанию используется RSA алгоритм и ключ длиной 512 бит

Рекомендации по использованию

Используйте данную команду для создания запроса на сертификат.

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

Пример

Ниже приведен пример создания запроса на локальный сертификат:

```
cert_mgr create -subj O=S-Terra,CN=LocalCert -RSA -1024 -dns  
local.s-terra.com -f c:\certs\local_cert
```

16.4. cert_mgr remove

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

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

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для удаления сертификатов из базы Продукта.

Удалять можно как один, так и несколько сертификатов.

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

Для того чтобы ознакомиться с сертификатами, хранящимися в базе данных и выяснить номера (индексы) под какими они хранятся в базе Продукта, используйте команду [cert_mgr show](#).

С помощью этой команды из базы Продукта нельзя удалять CRL. Если в тексте команды будет указан номер (индекс) CRL, то будет выведено сообщение об ошибке.

Пример

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

```
cert_mgr remove -i 1 -i 2 -i 3
1 OK O=S-Terra,CN=Technological Cert
2 OK O=S-Terra,CN=CA Cert
User error: Certificate index 3 exceeds number of certificates in
base
```

16.5. cert_mgr check

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

Синтаксис `cert_mgr check [-i OBJ_INDEX01] [-i OBJ_INDEX02] ...`

`[-i OBJ_INDEX0N]` порядковые номера интересующих сертификатов.

Значение по умолчанию значение по умолчанию отсутствует

Рекомендации по использованию

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

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

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

16.6. key_mgr show

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

Синтаксис `key_mgr show`

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации

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

При выполнении этой команды будут выводиться следующие данные:

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

Пример

Ниже приведен пример выполнения команды `key_mgr show`:

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

16.7. key_mgr import

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

Синтаксис `key_mgr import -n KEY_NAME -f KEY_FILE`

`-n KEY_NAME` имя предопределенного ключа.

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации

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

Пример

Ниже приведен пример импорта предопределенного ключа:

```
key_mgr.exe import -f c:\certs\key1 -n key1 -f key2 -n key2name -f  
key3 -n key3name
```

```
OK key1name
```

```
OK key2name
```

```
OK key3name
```

16.8. key_mgr remove

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

Синтаксис `key_mgr remove -n KEY_NAME`

`-n KEY_NAME` имя предопределенного ключа.

Значение по умолчанию Значение по умолчанию отсутствует

Рекомендации

Используйте данную команду для удаления предопределенных ключей из базы Продукта.

Пример

Ниже приведен пример удаления предопределенного ключа:

```
key_mgr remove -n keylname
OK keylname
```

16.9. lsp_mgr show

Команда `lsp_mgr show` предназначена для просмотра локальной политики безопасности (конфигурации).

Синтаксис `lsp_mgr show`

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра действующей конфигурации, хранящейся в базе Продукта.

При просмотре конфигурацию можно сохранить в файле, например `current.lsp`, командой

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

отредактировать в текстовом редакторе, например Notepad, и сохранить.

Пример

Ниже приведен пример вывода действующей конфигурации:

```
lsp_mgr show
```

```
GlobalParameters (
    Title = "This LSP was automatically generated by CSP
VPN Server AdminTool (sc) at 2007.03.13 17:56:37"
    Version = "2.1"
    CRLHandlingMode = BEST_EFFORT
)
LDAPSettings (
    ResponseTimeout = 200
    HoldConnectTimeout = 60
    DropConnectTimeout = 5
)
IdentityEntry auth_identity_01(
)
AuthMethodPreshared auth_method_01(
    SharedIKESecret = "gfg"
    LocalID = auth_identity_01
)
```

16.10. lsp_mgr load

Команда `lsp_mgr load` предназначена для загрузки конфигурации из файла в базу Продукта.

Синтаксис `lsp_mgr load -f LSP_FILE`

- f LSP_FILE путь к файлу конфигурации

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Если политика безопасности написана в виде текстового конфигурационного файла, то для загрузки ее в базу Продукта используйте команду `lsp_mgr load..`

Пример

Ниже приведен пример загрузки конфигурации из файла в базу Продукта:

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


16.11. lsp_mgr unload

Команда `lsp_mgr unload` предназначена для выгрузки активной конфигурации в базу Продукта и загрузки политики DDP.

Синтаксис `lsp_mgr unload`

Команда не имеет аргументов и ключей

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для выгрузки активной конфигурации в базу Продукта. При выгрузке конфигурации начинает действовать политика драйвера по умолчанию - DDP, которая задается командой [dp_mgr set](#). При этой политике пакеты либо все пропускаются, но не обрабатываются либо пропускаются только по DHCP.

Пример

Ниже приведен пример выгрузки активной конфигурации в базу Продукта:

```
lsp_mgr unload
Operation completed successfully
```

16.12. lsp_mgr reload

Команда `lsp_mgr reload` предназначена для перезагрузки конфигурации, помеченной как активная в базе Продукта, если она была отгружена командой `lsp_mgr unload`.

Синтаксис `lsp_mgr reload`

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для перезагрузки активной конфигурации.

Пример

Ниже приведен пример перезагрузки активной конфигурации из базы Продукта:

```
lsp_mgr reload
LSP is reloaded successfully.
```

16.13. if_mgr show

Команда `if_mgr show` предназначена для просмотра параметров защищаемых сетевых интерфейсов.

Синтаксис `if_mgr show`

Команда не имеет аргументов и ключей

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра параметров защищаемых сетевых интерфейсов.

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

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

Сетевые интерфейсы, которые не относятся к ethernet интерфейсам, показываются под именем NDISWANIP. Такие виртуальные интерфейсы в основном являются PPP интерфейсами. При отсутствии соединения (подключения) IP-адрес и маска такого интерфейса не показывается.

Пример

Ниже приведен пример выполнения команды `if_mgr show`:

```
if_mgr show
```

```
1) Network Interface Logical name pptp
1) Network Interface Physical name NDISWANIP
IP - 10.0.2.11, MASK - 255.255.255.255
2) Network Interface Logical name eth0
2) Network Interface Physical name {E52C3675-62ED-4E43-A9F4-
3A529E1426DA}
IP - 10.10.1.2, MASK - 255.255.255.0
```

16.14. if_mgr add

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

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

<code>-a IP_ADDR</code>	IP-адрес защищаемого сетевого интерфейса
<code>-n PHYSICAL_NAME</code>	физическое имя защищаемого интерфейса
<code>-l LOGICAL_NAME</code>	логическое имя, присваиваемое защищаемому интерфейсу

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

Если во время инсталляции CSP VPN Server какой-либо интерфейс был отключен, а после инсталляции его включили, то на нем будет работать политика DDP. Для задания на этом интерфейсе такой же политики, как и на остальных интерфейсах, выполните команду `if_mgr add` для регистрации этого интерфейса в Продукте.

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

Сетевые интерфейсы, не относящиеся к ethernet интерфейсам, регистрируйте с физическим именем NDISWANIP.

Пример

Ниже приведен пример выполнения команды `if_mgr add`:

```
if_mgr add -a 10.0.19.2 -l int1
Saving hardware interface 10.0.19.2 as int1
```

16.15. if_mgr remove

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

Синтаксис `if_mgr remove -l LOGICAL_NAME`

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для удаления из базы Продукта записей о защищаемых сетевых интерфейсах.

Пример

Ниже приведен пример выполнения удаления записи о защищаемом сетевом интерфейсе с логическим именем `int1`:

```
if_mgr remove -l int1
Removing the network interface... int1
```

16.16. dp_mgr show

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

<code>passall</code>	пропускать весь трафик
<code>passdhcp</code>	пропускать пакеты только по протоколу DHCP. Трафик DHCP пропускается для настройки TCP/IP стека по протоколу DHCP.

Синтаксис `dp_mgr show`

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра текущих настроек политики безопасности.

Default Driver Policy действует в следующих случаях:

- при старте Продукта до загрузки конфигурации
- при незагрузке локальной политики безопасности из-за какой-либо ошибки
- при отсутствии LSP в базе Продукта
- при выгрузке LSP командой [lsp_mgr unload](#).

Пример

Ниже приведен пример выполнения команды `dp_mgr show`:

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

16.17. dp_mgr set

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

Default Driver Policy (DDP) – политика драйвера по умолчанию, описана в команде [dp_mgr show](#)

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

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для настройки параметров политики по умолчанию.

Пример

Ниже приведен пример выполнения команды `dp_mgr set`:

```
dp_mgr set -ddp passall
Default driver policy is wrote to db successfully
```

16.18. log_mgr set

Команда `log_mgr set` предназначена для настройки общего уровня протоколирования событий.

Синтаксис `log_mgr set -l SEVERITY_LEVEL`

`-l SEVERITY_LEVEL` уровень протоколирования событий. Устанавливается одно из возможных значений:

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

Общий уровень лога действует тогда, когда не задан уровень лога для разных событий.

Пример

Ниже приведен пример выполнения команды `log_mgr set`:

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


16.19. log_mgr show

Команда `log_mgr show` предназначена для просмотра текущего уровня протоколирования событий.

Синтаксис `log_mgr show`

Данная команда не имеет аргументов и ключей.

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для ознакомления с настройкой уровня протоколирования событий.

Пример

Ниже приведен пример выполнения команды `log_mgr show`:

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

16.20. sa_show

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

Синтаксис `sa_show [-e]`

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

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

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

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

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

При указании ключа `-e` выводится полная информация:

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

Пример

Ниже приведен пример выполнения команды `sa_show -e`:

```
IKE sessions: 0 initiated, 0 responded
```

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

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

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

16.21. klogview

Утилита `klogview` предназначена для просмотра сообщений, выдаваемых системой протоколирования IPsec-драйвера.

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

- `-l` ожидать сообщения из ядра и выводить их по мере поступления. Эта опция принимается по-умолчанию, если не задана опция `-m`.
- `-t` печатать дату и время вывода сообщения
- `-T` печатать относительное время, когда произошло событие. Время выводится в секундах относительно предыдущего события, показанного данным экземпляром утилиты. Например, значение 10.353245 – это 10 секунд и 353245 микросекунд. Максимальная точность – наносекунды, но реальная погрешность зависит от аппаратной платформы и операционной системы. Значение, выдаваемое с первым сообщением, отображает абсолютное значение часов, которые используются для вычисления относительного времени. Это либо время со старта системы, либо время относительно какой-то даты, принятой в данной системе за точку отсчета.
- `-p ts_precision` количество знаков долей секунд, используемых при печати относительного времени события (`-T`).
- `-f event_mask` задать фильтр событий для данного экземпляра утилиты. Возможные события описаны в таблице.
- `-m event_mask` задать фильтр событий по-умолчанию. Заданное значение используется, если не указана опция `-f`.
- `-h` вывести краткую информацию об использовании утилиты.

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

Группа событий	Код	Описание
drop	2	Уничтожение пакета. Выводится непосредственно перед уничтожением какого-либо пакета. Сообщение содержит краткий текст, поясняющий причину уничтожения и информацию из IP-заголовка пакета. В некоторых случаях IP-заголовок может быть испорчен к моменту вывода сообщения, тогда в сообщении допускаются нулевые или любые другие случайные адреса.
pass	1	Пропуск пакета. Выводится непосредственно перед отсылкой какого-либо пакета. Сообщение содержит краткий текст, поясняющий действия, которые были произведены над пакетом.
sa_minor	8	Некоторые внутренние события, происходящие с IPsec - контекстом. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста.

Группа событий	Код	Описание
sa_major	4	Взаимодействия между IPsec-драйвером и приложением, касающиеся изменения состояния IPsec-контекстов. Сообщения содержат номер контекста (ID), который можно увидеть из сообщения о загрузке контекста.
sa_trace	16	Сообщения выводятся перед попыткой применения к пакету IPsec-контекста.
sa_errors	32	Ошибки, связанные с неуспешным применением IPsec-контекста к пакету.
filt_trace	64	Выводится имя и индекс правила фильтрации, если такое для пакета найдено.

Нужный набор событий (`event_mask`) можно указать двумя способами:

- сложением кодов групп событий (см. в таблице)

Пример:

```
klogview -f 0x43
или
klogview -f 67
```

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

Пример:

```
klogview -f drop,pass,filt_trace
```

Значение по умолчанию Значение по умолчанию отсутствует.

Рекомендации по использованию

Используйте данную команду для просмотра сообщений, выдаваемых системой протоколирования.

Сообщения, выводимые утилитой

Сообщения, выводимые утилитой, формируются на основе данных, присылаемых из IPsec-драйвера. Структура большинства сообщений определяется строкой формата¹², получаемой из IPsec-драйвера (см. [Примеры сообщений](#)).

Специальные сообщения, выводимые утилитой:

*** N messages lost ***

выводится, если утилита не успевает обрабатывать сообщения и N сообщений поретяны.

no format string

в сообщении отсутствует строка формата¹³.

<error: .в выводимом сообщении

несоответствие строки формата параметрам сообщения¹⁴.

¹² Строка формата по смыслу и стилю похожа на форматную строку в printf.

¹³ Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.

¹⁴ Это не является нормальной ситуацией, просьба сообщать разработчикам о подобных проявлениях.

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

16.21.1. События группы pass и drop

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

Формат сообщения (в порядке следования):

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

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

Примеры сообщений группы pass

Пакет обработан по правилу фильтрации с действием PASS:

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

Пакет был обработан по IPsec-правилу:

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

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

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

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

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

Примеры сообщений группы drop

Сообщения, связанные с некорректными данными заголовков пакета:

IP-заголовок испорчен:

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

TCP/UDP заголовок испорчен:

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

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

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

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

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

Испорчен ESP или АН заголовок:

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

Может выводиться при внутренних ошибках работы клиентской стороны IKEcfg:

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

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

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

Пакет уничтожен в соответствии с [RefuseTCPPeerInit](#), выставленном в правиле фильтрации:

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

Сообщения о подпадании пакета под правило с действием DROP:

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

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

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

Открытый пакет подпадает под правило фильтрации с IPsec-действием:

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

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

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

Ошибки IPsec:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: SA 33:
decapsulation error 5: integrity verification failed
out packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped: SA
33: encapsulation error 4: sequence number wrapped
```

Возможны следующие ошибки

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

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

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

Ограничение на обработку транзитного трафика:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
decapsulated packet is not local (not a security gateway)
```

Ограничение на обработку транзитного трафика только при вложенном IPsec:

```
in packet 2.3.4.5:12->3.4.3.3:14, proto 6, if eth0, dropped:
decapsulated ipsec packet is not local (not a security gateway)
```

Очередь пакетов, ожидающая создания IPsec SA bundle переполнена:

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

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

¹⁵ Это является внутренней ошибкой, просьба сообщать разработчикам.


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

Внутренние ошибки, о которых просьба сообщать разработчикам:

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

Другие сообщения:

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

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

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

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

16.21.2. События группы `filt_trace`

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

Пример сообщения:

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

16.21.3. События группы `sa_minor`, `sa_major`

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

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

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

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

Примеры сообщений группы `sa_major`

Превышено ограничение SA по трафику:

```
SA 55 expired
```

Пора начинать rekeying SA (пройден барьер по трафику):

requesting rekeying for SA 33

SA нигде не используются и должны быть удалены:

requesting to remove SA: 44,45

Сообщения о загрузке новых SA:

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

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

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

- Расшифровка type:

51 - AH
50 - ESP

- Расшифровка некоторых¹⁶ битов flags:

0x1 - входящий

- Расшифровка битов ipsec flags:

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

Загрузка связки SA (SA bundle):

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

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

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

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

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

disabled SA 33

Удаление SA:

removed SA 33

Удаление ранее заблокированного SA:

removed dead SA 33

Другие сообщения:

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

¹⁶ Остальные значения флагов не предназначены для интерпретации пользователями.

Сообщения, возникающие при ошибочном/странном¹⁷ поведении Продукта:

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

Примеры сообщений группы sa_minor¹⁸:

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

16.21.4. События группы sa_trace

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

Примеры сообщений:

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

16.21.5. События группы sa_error

Сообщения этой группы выводят дополнительную информацию о специфических ошибках IPsec.

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

Пример сообщения:

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

¹⁷ Просьба сообщать разработчикам о возникновении одной из перечисленных ошибок.

¹⁸ Сообщения данного раздела предназначены для внутреннего использования. Расшифровка пользователям ПродуктПродукта не предоставляется.

16.22. Сообщения об ошибках

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

Если в тексте полученного сообщения присутствует фраза "Internal error:", то обращайтесь в службу поддержки по адресу support@s-terra.com.

Утилита cert_mgr

	Текст сообщения	Описание проблемы
1	User error: no source file specified	Не указан путь к файлу (cert_mgr ... -f)
2	FILENAME unable to open file	Ошибка при открытии файла
3	Internal error: No memory	Нет свободной оперативной памяти
4	User error. No password specified to open FILENAME	Не задан пароль доступа к файлу
5	FILENAME wrong password PASSWORD	Неверный пароль
6	User error. No password specified	Не указан пароль (cert_mgr-p)
7	Internal error. Unable obtain certs from DB	Не удастся получить сертификаты из базы продукта
8	User error: no number specified\n	Не указан индекс сертификата (cert_mgr -i)
9	User error: NUMBER exceeds number of objects	Указанный индекс превышает количество объектов в базе продукта
10	User error. No subject	Не зада Subject сертификата
11	User error: Key KEY1 is not compatible with key KEY2	Несовместимость ключей
12	User error: Key KEY is useless	Задан лишний параметр
13	User error: Key KEY is used twice	Повторное использование ключа
14	User error: Unable remove. Base is empty	Попытка удаления сертификата из пустой базы продукта
15	Internal error:Unable remove object from base	Неудачная попытка удаления объекта из базы продукта
16	User Error. Missing parameter	Пропущен параметр
17	User Error. No file name specified	Не указано имя файла
18	Internal error. Storage error.	Ошибка при открытии хранилища
19	User error: INDEX exceeds number of objects in NAME	Ошибка указания индекса объекта
20	User error: Container name is not specified	Не указано имя контейнера
21	User error: CRL can not be removed from base	CRL не может быть удален из базы продукта
22	User error: Object index INDEX exceeds number of certificates and CRLs in base	Объекта с указанным индексом не существует
23	User Error. Missing index of object to be removed from base. Specify 'i' key and index	Не указан индекс объекта

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

Утилита key_mgr

	Текст сообщения	Описание проблемы
1	Internal error: No memory to open file FILENAME	Нет свободной оперативной памяти, необходимой для открытия файла
2	User error: Key file no specified	Не указан файл с ключом
3	User error: Key name no specified	Не указано имя ключа
4	Internal error. Unable to append key into base KEYNAME	Ошибка при попытке импорта ключа в базу продукта
5	Error: unable to remove key from db	Ошибка при попытке удаления ключа из базы продукта

Утилита lsp_mgr

	Текст сообщения	Описание проблемы
1	FILENAME unable to open file	Ошибка при попытке открыть файл
2	Internal error: Unable to set LSP as active	Не удалось сделать политику LSP. текущей
3	Internal error: No memory to open file	Нет свободной оперативной памяти,

	Текст сообщения	Описание проблемы
	FILENAME	необходимой для открытия файла
4	Internal error: unrecognized error	Внутренняя ошибка
5	Internal error: Unable to load lsp from base	Не удалось загрузить LSP из базы продукта
6	LSP loading error	Ошибка при загрузке LSP

Утилита lf_mgr

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

Утилита dp_mgr

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

Утилита log_mgr

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

17. Протоколирование событий

Продукт использует протокол Syslog для отправки сообщений о протоколируемых событиях. Настройка Syslog-клиента производится администратором при подготовке инсталляционного пакета для конечного устройства.

Настройка Syslog-клиента для протоколирования событий осуществляется в конфигурационном файле (LSP) или утилите `make_inst.exe`. Администратор определяет IP-адрес хоста, на который будут посылаться сообщения о событиях, уровень важности сообщений и источник сообщений.

В конфигурационном файле производятся текущие настройки Syslog, а в утилите `make_inst.exe` – общие настройки Syslog.

17.1. Текущие настройки

В конфигурационном файле текущие настройки для Syslog-клиента осуществляются в двух структурах. В [структуре GlobalParameters](#) устанавливаются текущие уровни лога протоколируемых событий, разделенных на четыре раздела:

- [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.

В структуре [SyslogSettings](#) задается адрес Syslog-сервера, на который посылаются сообщения, и источник сообщений. В этой же структуре можно отключить использование протокола Syslog.

17.2. Общие настройки

Задание общих настроек Syslog-клиента осуществляется в [утилите make_inst.exe](#). В опции `-s` задается общий уровень лога для всех протоколируемых событий. В опции `-t` указывается IP-адрес сервера, на который будут посылаться сообщения о протоколируемых событиях. В опции `-y` указывается источник сообщений.

17.3. Действие текущих и общих настроек

Общие настройки вступают в действие при отсутствии загруженной локальной политики безопасности (когда действует Default Driver Policy) или отсутствии текущих настроек.

Текущие настройки отсутствуют, если в структуре [GlobalParameters](#) нет настроек лога для разных событий и структура [SyslogSettings](#) отсутствует.

Если заданы текущий уровень лога протоколирования событий и общий уровень, то протоколирование будет происходить по уровню лога для разных событий.

17.4. Получение лога в Windows

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

17.5. Настройки Syslog сервера для получения лога в Solaris

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

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

```
local0.debug      /var/admin/message
```

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

```
local2.notice     /var/admin/message
```

Подробнее о файле `/etc/syslog.conf` смотрите документацию Solaris.

После изменения конфигурации надо перезагрузить syslog:

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

Изложенная информация относится как к протоколированию событий от VPN-сервиса на данном компьютере, так и к SYSLOG-пакетам, пришедшим извне (в том числе от Windows-агентов).

17.6. 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.

Выдаваемые сообщения и описание событий по этим сообщениям представлены в таблицах 3-7.

Сообщения уровня ERROR

Таблица 3

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Локальный сертификат непригоден	ERR	CERT	Searching local certificate failed. Reason: %s ¹⁹ . Subject: %s Issuer: %s SN: %s
2	Секретный ключ локального сертификата недоступен	ERR	CERT	Local certificate '%{1}s' is invalid: private key %{2}s%{3}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
3	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
3	Секретный ключ не соответствует локальному сертификату. Это возможно только после установки ОСИ	ERR	CERT	Local certificate '%{1}s' is invalid: private key %{2}s%{3}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
5	Неуспешная попытка установить соединение в качестве инициатора	ERR	POLICY	Connection request FAILED, Reason: %s ²⁰ , ip: %s, protocol: %s ²¹ , IKERule: "%s", IPsecAction: "%s", FilteringRule: "%s" ²² , Stopped at: %s ²³
6	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

¹⁹ revoked | expired | not verified²⁰ Session timeout | Invalid packet | No proposal chosen | Invalid ID | Authentication failed | Internal error²¹ ISAKMP либо IPsec²² Если на момент вывода сообщения сведения о правилах ISAKMP, IPsec либо о фильтре отсутствуют, то соответствующие сведения не выводятся²³ Дополнительные сведения об операции, на которой прервался процесс установления соединения

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
7	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' %{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
8	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-я 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)
9	Ошибка при добавлении записи в таблицу маршрутизации	ERR	SYSTEM	Failed to add routing: %{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-я 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.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
10	Ошибка при удалении записи из таблицы маршрутизации	ERR	SYSTEM	Failed to delete routing: %{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-я 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.
11	Неудачная попытка доступа Пользователя к Агенту	ERR	SYSTEM	User login failed

Сообщения уровня WARNING

Таблица 4

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	В файле x509conv.ini указана неподдерживаемая кодировка	WARNING	CERT	Unsupported encoding “%{1}s” has been specified in x509conv.ini, “%{2}s” will be used %{1}s – неподдерживаемая кодировка %{2}s – кодировка, которая будет использована для соответствующего ASN.1-типа
2	В файле x509conv.ini указан неизвестный параметр	WARNING	CERT	Unexpected parameter “%{1}s” has been specified in x509conv.ini, ignored %{1}s – имя неизвестного параметра
3	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. %{1}s – строковое представление поля Subject сертификата

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
4	LDAP запрос {1} закончился неудачей. Причина: {2}	WARNING	LDAP	LDAP request failed. Reason: %s ²⁴ . Request: “%{1}s”.
5	Неуспешная попытка установить соединение в качестве ответчика	WARNING	POLICY	Incoming connection request FAILED, Reason: %s ²⁵ , ip: %s, protocol: %s ²⁶ , IKERule: “%s”, IPsecAction: “%s” ²⁷ , FilteringRule: “%s” ²⁸ , Stopped at: %s
6	Значение параметра DefaultCryptoContextsPerIPSecSA задано неверно	WARNING	POLICY	DefaultCryptoContextsPerIPSecSA in “agent.ini” is not valid (must be from 1 to 128), %s will be used instead. %s – значение, которое будет использовано для параметра DefaultCryptoContextsPerIPSecSA
7	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 трансформы в правиле	WARNING	POLICY	WARNING: IKERule ‘%s’, line %s: in Aggressive Mode initiator will use %s only. %s – название выбранной группы, по которой будет работать Агент в качестве инициатора в Aggressive Mode. %s – имя IKERule, для которого выведена эта диагностика %s – строка, на которой располагается IKERule.

Сообщения уровня NOTICE

Таблица 5

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Результат LDAP запроса {1} – объекты не найдены	NOTICE	LDAP	LDAP request result: NOT FOUND. Request: “%{1}s”.

²⁴ 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

²⁵ Session timeout | Limit of %u responded sessions achieved | Invalid packet | No proposal chosen | No rule chosen | Invalid ID | Authentication failed | Internal error²⁶ ISAKMP либо IPsec²⁷ Если на момент вывода сообщения правило ISAKMP, либо IPsec не выбрано, то сведения о нём не выводятся²⁸ Если на момент вывода сообщения сведения о правилах ISAKMP, IPsec либо о фильтре отсутствуют, то соответствующие сведения не выводятся

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
2	Результат LDAP запроса {1} – найдено {2} объектов	NOTICE	LDAP	LDAP request result: %{2}s object(s) found. Request: “%{1}s”.
3	Присвоен IP-адрес из удалённого IKE-CFG пула	NOTICE	POLICY	VPN ip-address %s obtained, Partner: %s:%d ²⁹
4	Партнёру присвоен IP-адрес из IKE-CFG пула	NOTICE	POLICY	VPN ip-address %s assigned to external host Partner: %s:%d ³⁰
5	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 ³¹
6	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 ³²
7	Старт сервиса	NOTICE	SYSTEM	Service started, version %s
8	Остановка сервиса	NOTICE	SYSTEM	Service stopped
9	Доступ Пользователя к Агенту	NOTICE	SYSTEM	User logged in
10	Отключение доступа Пользователя к Агенту	NOTICE	SYSTEM	User logged out

²⁹ ip:port³⁰ ip:port³¹ ip:port³² ip:port

Таблица 6

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	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 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 состоялось соединение
2	Получен ISAKMP-пакет от партнера, с которым запрещен IKE-трафик ³³	INFO	POLICY	Inbound IKE packet dropped, Reason: Access denied, Partner: %s:%d ³⁴

³³ 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 unsuccessfully 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.

³⁴ ip:port

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
3	Заккрытие 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 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.

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
4	IPSec-соединение не установилось из-за превышения количества, разрешенного лицензией	INFO	POLICY	Unable to establish connection: resources exceeded
5	Информация о лицензии Продукта	INFO	SYSTEM	Product licence: product code: %s, customer code: %s, license number: %n, license code: %s

Сообщения уровня DEBUG

Таблица 7

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
1	Не найден сертификат партнёра	DEBUG	CERT	Searching peer certificate failed. Reason: not found. Search template: %s
2	Найден непригодный сертификат партнёра	DEBUG	CERT	Searching peer certificate failed. Reason: %s ³⁵ . Subject: %s Issuer: %s SN: %s
3	Выбран сертификат партнёра	DEBUG	CERT	Use peer certificate: Subject: %s Issuer: %s SN: %s
4	Сформирован LDAP запрос {1}	DEBUG	LDAP	LDAP request: "%{1}s" ³⁶ .
5	LDAP запрос {1} проигнорирован: не задан LDAP сервер	DEBUG	LDAP	LDAP request ignored: there is no LDAP server available. Request: "%{1}s".
6	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 filter "%s" – название фильтра, под который попал пакет.

³⁵ revoked | expired | not verified³⁶ 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
7	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
8	Создание ISAKMP SA	DEBUG	POLICY	ISAKMP connection [%u] established, Partner: %s:%d ³⁷ , Identity: %s, IKERule: “%s”
9	Удаление ISAKMP SA	DEBUG	POLICY	ISAKMP connection [%u] closed, Partner: %s:%d ³⁸ , Identity: %s, bytes sent/received: %d / %d, Exchanges passed: %d
10	Обнаружение устройства NAT	DEBUG	POLICY	NAT detected on ... ³⁹ side, Partner: %s:%d ⁴⁰
11	Proposals высланы партнёру	DEBUG	POLICY	(Phase I):⁴¹ Sending IKE proposals. Rule “%s”: Auth: %s Transform #1: Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: % Transform #2: ..
				(Phase II):⁴² 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:

³⁷ ip:port³⁸ ip:port³⁹ local | remote⁴⁰ ip:port⁴¹ Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются⁴² Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
12	Партнёр прислал набор proposals	DEBUG	POLICY	(Phase I): ⁴³ IKE proposals received. Transform #1: Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: %s Transform #2:
				(Phase II): ⁴⁴ 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
13	Проверка proposal для правила	DEBUG	POLICY	Check proposal #0%u, Protocol %s ⁴⁵ , Transform #%u for Rule "%s". Result: %s ⁴⁶ , attribute: %s ⁴⁷
14	Выбран proposal	DEBUG	POLICY	(Phase I): ⁴⁸ ISAKMP proposal selected. Auth: %s, Hash: %s, Cipher: %s, Group: %s, Life Time: %s, Life Traffic: %s
				(Phase II): ⁴⁹ IPSec proposal selected. Mode: %s ⁵⁰ , Group: %s, AH Integrity: %s, ESP Integrity: %s, Cipher: %s, Life Time: %s, Life Traffic: %s
15	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

⁴³ Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются⁴⁴ Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются⁴⁵ ISAKMP | AH | ESP⁴⁶ Not matched | OK⁴⁷ Authentication method | Hash | Cipher | Oakley group | Integrity | mode – только для не совпавших proposals⁴⁸ Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются⁴⁹ Если отдельные структуры, либо атрибуты отсутствуют, то они не протоколируются⁵⁰ Transport | Tunnel

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
16	Недоступен выбранный Preshared ключ	DEBUG	POLICY	Preshared key "%{1}s" not found, где: %{1}s – Идентификатор выбранного ключа, указанный в LSP
17	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
18	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
19	Информация об используемом локальном IKE-Identity	DEBUG	POLICY	[ISAKMP]: Sending identity "%s" to partner <ip:port>
20	Информация об IKE-Identity, присланным партнером	DEBUG	POLICY	[ISAKMP]: Identity "%s" is received from partner <ip:port>
21	Информация о сообщении (IKE-Notification), присланном партнером	DEBUG	POLICY	[ISAKMP]: Notification [%s ⁵¹] has been received for Exchange <%u ⁵² >: %s ⁵³

⁵¹ Согласно списку п. 3.14.1 в RFC 2408 и п. 4.6.3 в RFC 2407.

⁵² Номер-идентификатор IKE-обмена.

⁵³ 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

	Описание события	Уровень важности	Раздел	Шаблоны сообщений
22	Инициированный IKE-обмен завершился с ошибкой	DEBUG	POLICY	[ISAKMP]: Connection request FAILED. %s где: %s – дополнительная доступная информация о несостоявшемся обмене: причина аварийного завершения ⁵⁴ (см. Таблица 8) стек выполняемых операций (см. Таблица 9) сведения о партнере: <ip:port>, IKE-Identity ⁵⁵
23	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 ⁵⁶ (см. Таблица 8) стек выполняемых операций (см. Таблица 9) сведения о партнере: <ip:port>, IKE-Identity ⁵⁷
24	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

⁵⁴ 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.

⁵⁵ IKE Identity указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.

⁵⁶ 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.

⁵⁷ IKE Identity указывается только в случаях, когда в пределах данного IKE-обмена такая информация доступна.

17.6.1. Список ошибок протокола ISAKMP

(см. [пункты 22 и 23](#) Таблица 7)

Таблица 8

	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 дополнительной настройки 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 Authentication method
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

	Описание ошибки	Запись об ошибке в строке сообщения
18	Партнер прислал IKE-пакет с неправильной структурой, либо пакет не удалось правильно расшифровать	Invalid packet (invalid structure).

17.6.2. Список выполняемых действий по протоколу ISAKMP

(см. [пункты 22 и 23](#) Таблица 7)

Таблица 9

	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
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
19	Вычисление хэша для обнаружения устройства NAT	Calculate NAT Discovery payload

	Описание действия	Информация в строке сообщения
20	Вычисление общего ключа	Calculate Shared Key
21	Вычисление инициализационного вектора	Calculate InitVector
22	Определение метода аутентификации	Detect Authentication Method
23	Проверка локального сертификата для метода аутентификации с использованием сертификатов	Authentication uses Certificates: Check for Local Certificates
24	Проверка метода аутентификации, предложенного партнером, на соответствие текущей политике безопасности	Check Authentication Method
25	Выбор метода аутентификации	Choose Authentication 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 дополнительной настройки ISAKMP-соединения (XAuth, IKE-CFG, и т.п.)	Determine IKE configuration method

	Описание действия	Информация в строке сообщения
38	Распознавание команды дополнительной настройки 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 ⁵⁸
42	Проверка структуры компонента IKE-пакета	Analyse payload structure %s ⁵⁹
43	Формирование компонента IKE-пакета	Form payload %s ⁶⁰
44	Заполнение блока данных указанного компонента IKE-пакета	Fill payload %s ⁶¹
45	Проверка содержимого компонента IKE-пакета	Check %s ⁶²
46	Вычисление хэша – содержимого указанного компонента	Calculate %s ⁶³
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]

⁵⁸ Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

⁵⁹ Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

⁶⁰ Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

⁶¹ Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

⁶² Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

⁶³ Название компонента (payload type) – согласно разделам 3.4 – 3.16 RFC 2408

	Описание действия	Информация в строке сообщения
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]
64	Выполнение шага сценария продолжения формирования 1-го пакета IKE Aggressive Mode для аутентификации 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 действия	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]
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)]

	Описание действия	Информация в строке сообщения
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]
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]

	Описание действия	Информация в строке сообщения
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]

18. Мониторинг

Продукт должен накапливать статистику, характеризующую его работу и обрабатываемый сетевой трафик. Для этого администратор при подготовке инсталляционного пакета для конечного устройства производит настройку SNMP-агента.

А SNMP-менеджер имеет возможность удаленно запрашивать у SNMP-агента накопленную статистику - содержимое базы данных агента.

Настройка SNMP-агента в LSP для выдачи статистики и база данных MIB, которую он поддерживает, описана в разделе ["Выдача статистики"](#).

SNMP-агент может посылать SNMP-менеджеру сообщения о некоторых значимых событиях в виде трап-сообщений. Настройка SNMP-агента в LSP для отсылки трап-сообщений и список этих сообщений описаны в разделе ["Трап-сообщения"](#).

CSP VPN Server поддерживает протоколы обмена SNMPv1 и SNMPv2c для сбора статистики и мониторинга.

В качестве SNMP-менеджера могут быть использованы:

- программный Продукт CiscoWorks Monitoring Center for Performance 2.0.2, который входит в состав комплекта CiscoWorks VMS 2.3.
- бесплатная утилита NET-SNMP (<http://www.net-snmp.org/>) , которая является простейшим SNMP-менеджером. При работе с SNMP-агентом нужно указывать версию SNMP –v 1 или – v 2c.

18.1. Выдача статистики

SNMP-менеджер инициирует запрос на значения одной или нескольких переменных, который посылает SNMP-агенту. SNMP-агент, отвечая на запрос, возвращает значения одной или нескольких переменных.

В конфигурационном файле LSP задание настроек SNMP-агента для выдачи статистики SNMP-менеджеру осуществляется [структурой SNMPollSettings](#). В этой структуре указывается IP-адрес и порт, на который можно получать запросы от SNMP-менеджера, строку, играющую роль пароля при аутентификации сообщений, информация о размещении SNMP-агента и контактном лице.

База данных MIB, поддерживаемая SNMP-агентом, разделена на группы. В приведенной ниже таблице перечислены переменные из стандартной группы system, глобальной статистики IKE и IPsec, и MIB.

Примечание 1: при принудительном перезапуске сервиса IKE-статистика сбрасывается и начинает считаться со старта Агента. IPsec-статистика считается со старта компьютера и при принудительном перезапуске сервиса не сбрасывается.

Примечание 2: в IKE-статистике при подсчете трафика учитывается только количество байт в ISAKMP-пакете. У Cisco же в IKE-статистике учитываются данные из IP-заголовка, UDP-заголовка и Ethernet-заголовка пакета.

Таблица 10

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
Статистика по стандартной группе System и специфичным константным значениям				
sysDescr	1.3.6.1.2.1.1.1.0	DisplayString	Текстовое описание сетевого объекта. Строка вида "CSP VPN Gate 2.2.<build>"	RFC1213-MIB
sysObjectID	1.3.6.1.2.1.1.2.0	OID	Идентификатор фирмы-производителя (внутри поддерева 1.3.6.1.4.1): 1.3.6.1.4.1.9.1.467(cisco2611XM из CISCO-PRODUCTS-MIB)	RFC1213-MIB
sysUpTime	1.3.6.1.2.1.1.3.0	TimeTicks	The time (in hundredths of a second) since the network management portion of the system was last re-initialized. Время в сотых долях секунды с момента последней загрузки системы	RFC1213-MIB
sysContact	1.3.6.1.2.1.1.4.0	DisplayString	Имя контактной персоны и способ контакта	RFC1213-MIB
sysName	1.3.6.1.2.1.1.5.0	DisplayString	Полное имя домена <hostname>.<domain-name>	RFC1213-MIB
sysLocation	1.3.6.1.2.1.1.6.0	DisplayString	Физическое местоположение агента	RFC1213-MIB
sysServices	1.3.6.1.2.1.1.7.0	int32	Значение, которое характеризует сервисы, предоставляемые узлом. Это значение есть сумма номеров уровней модели OSI в зависимости от того, какие сервисы поддерживаются: 0x01 (физический), 0x02 (канальный), 0x04 (сетевой), 0x08 (точка-точка), 0x40 (прикладной). Например, если поддерживается IP уровень (маршрутизация) и транспортный уровень (точка-точка), то значение sysServices есть сумма 4 и 8. 78 (c2611XM)	RFC1213-MIB
chassisType	1.3.6.1.4.1.9.3.6.1.0	int32	335 (c2611XM)	OLD-CISCO-CHASSIS-MIB
cipSecMibLevel	1.3.6.1.4.1.9.9.171.1.1.1.0	int32	The level of the IPsec MIB 1	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
snmpSetSerialNo	1.3.6.1.6.3.1.1.6.1.0	int32	<An advisory lock used to allow several cooperating SNMPv2 entities, all acting in a manager role, to coordinate their use of the SNMPv2 set operation. Используется как значение, которое ограничивает сверху Cisco-specific значения. Фактически является неформальным обозначением конца MIB-а. Служит для предотвращения возможных коллизий при обработке GET-NEXT операций. 0	SNMPv2-MIB
ciscoImageString	1.3.6.1.4.1.9.9.25.1.1.1.2.<i>	DisplayString	<The string of this entry.> (описание таблицы – <A table provides content information describing the executing IOS image.>). Выдаются данные для агента: 1: "CW_BEGIN\$csp-vpn\$" 2: "CW_IMAGE\$C2600-CSP-VPN\$" 3: "CW_FAMILY\$C2600\$" 4: "CW_FEATURE\$IP FIREWALL 2 PLUS 3DES\$" 5: "CW_VERSION\$12.2(13)T5, \$" 6: "CW_MEDIA\$RAM\$" 7: "CW_SYSDSCR\$CSP VPN {Gate Server Client} <major>.<minor>.<build>\$"" 8: "CW_MAGIC\$" 9: "CW_END\$csp-vpn\$"	CISCO-IMAGE-MIB
Глобальная IKE-статистика				
cikeGlobalActiveTunnels	1.3.6.1.4.1.9.9.171.1.2.1.1.0	uint32	<The number of currently active IPsec Phase-1 IKE Tunnels> Все существующие на данный момент активные ISAKMP SA.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalPreviousTunnels	1.3.6.1.4.1.9.9.171.1.2.1.2.0	uint32	<The total number of previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInOctets	1.3.6.1.4.1.9.9.171.1.2.1.3.0	uint32	<The total number of octets received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество байт, принятых в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalInPkts	1.3.6.1.4.1.9.9.171.1.2.1.4.0	uint32	<The total number of packets received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов, принятых в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInDropPkts	1.3.6.1.4.1.9.9.171.1.2.1.5.0	uint32	<The total number of packets which were dropped during receive processing by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов, отвергнутых в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2Exchgs	1.3.6.1.4.1.9.9.171.1.2.1.7.0	uint32	<The total number of IPsec Phase-2 exchanges received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество успешных Quick Modes в качестве респондера.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2ExchgInvalids	1.3.6.1.4.1.9.9.171.1.2.1.8.0	uint32	<The total number of IPsec Phase-2 exchanges which were received and found to be invalid by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий по созданию IPSec соединений, инициированных партнёрами, не состоявшихся по причине ошибки обмена.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2ExchgRejects	1.3.6.1.4.1.9.9.171.1.2.1.9.0	uint32	<The total number of IPsec Phase-2 exchanges which were received and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий по созданию IPSec соединений, инициированных партнёрами, которые не состоялись по причине рассогласования политик безопасности.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutOctets	1.3.6.1.4.1.9.9.171.1.2.1.11.0	uint32	<The total number of octets sent by all currently and previously active and IPsec Phase-1 IKE Tunnels> Количество байт, высланных в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalOutPkts	1.3.6.1.4.1.9.9.171.1.2.1.12.0	uint32	<The total number of packets sent by all currently and previously active and IPsec Phase-1 Tunnels> Количество ISAKMP-пакетов, высланных в течение всех IKE-сессий с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutDropPkts	1.3.6.1.4.1.9.9.171.1.2.1.13.0	uint32	<The total number of packets which were dropped during send processing by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов в течение всех IKE-сессий с момента старта Агента, которые были готовы к отсылке, но по каким-то причинам не были отосланы	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2Exchgs	1.3.6.1.4.1.9.9.171.1.2.1.15.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество успешных Quick Modes в качестве инициатора.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2ExchgInvalids	1.3.6.1.4.1.9.9.171.1.2.1.16.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent and found to be invalid by all currently and previously active IPsec Phase-1 Tunnels> Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявшихся по причине ошибки обмена.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2ExchgRejects	1.3.6.1.4.1.9.9.171.1.2.1.17.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявшихся по причине рассогласования политик безопасности.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInitTunnels	1.3.6.1.4.1.9.9.171.1.2.1.19.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were locally initiated> Количество созданных ISAKMP SA в качестве инициатора (т.е. по инициативе локальной стороны).	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInitTunnelFails	1.3.6.1.4.1.9.9.171.1.2.1.20.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were locally initiated and failed to activate> Количество инициированных сессий по созданию ISAKMP SA, завершившиеся неудачей	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalRespTunnelFails	1.3.6.1.4.1.9.9.171.1.2.1.21.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were remotely initiated and failed to activate> Количество сессий по созданию ISAKMP SA, инициированных партнёрами, которые завершились неудачей	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalAuthFails	1.3.6.1.4.1.9.9.171.1.2.1.23.0	uint32	<The total number of authentications which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Количество неудачных сессий по созданию ISAKMP SA, в которых не прошла аутентификация	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalDecryptFails	1.3.6.1.4.1.9.9.171.1.2.1.24.0	uint32	<The total number of decryptations which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий, не состоявшихся по причине ошибки расшифрования пакета.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalHashValidFails	1.3.6.1.4.1.9.9.171.1.2.1.25.0	uint32	<The total number of hash validations which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Количество неудачных операций по проверке значения хэш-функции во всех IKE сессиях	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalNoSaFails	1.3.6.1.4.1.9.9.171.1.2.1.26.0	uint32	<The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий, не состоявшихся по причине отсутствия ISAKMP соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
Глобальная IPsec-статистика				
cipSecGlobalActiveTunnels	1.3.6.1.4.1.9.9.171.1.3.1.1.0	uint32	<The total number of currently active IPsec Phase-2 Tunnels> Количество существующих на данный момент IPSec соединений.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalPreviousTunnels	1.3.6.1.4.1.9.9.171.1.3.1.2.0	uint32	<The total number of previously active IPsec Phase-2 Tunnels> Количество IPSec SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cipSecGlobalInOctets	1.3.6.1.4.1.9.9.171.1.3.1.3.0	uint32	<The total number of octets received by all current and previous IPsec Phase-2 Tunnels. This value is accumulated BEFORE determining whether or not the packet should be decompressed. See also cipSecGlobalInOctWraps for the number of times this counter has wrapped> Количество байт, принятых под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInOctWraps	1.3.6.1.4.1.9.9.171.1.3.1.5.0	uint32	<The number of times the global octets received counter (cipSecGlobalInOctets) has wrapped> Количество переполнений счетчика cipSecGlobalInOctets.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInPkts	1.3.6.1.4.1.9.9.171.1.3.1.9.0	uint32	<The total number of packets received by all current and previous IPsec Phase-2 Tunnels> Количество пакетов, принятых под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDrops	1.3.6.1.4.1.9.9.171.1.3.1.10.0	uint32	<The total number of packets dropped during receive processing by all current and previous IPsec Phase-2 Tunnels. This count does NOT include packets dropped due to Anti-Replay processing> Общее количество всех входящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения (Кроме проигнорированных по Anti-Replay).	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInReplayDrops	1.3.6.1.4.1.9.9.171.1.3.1.11.0	uint32	<The total number of packets dropped during receive processing due to Anti-Replay processing by all current and previous IPsec Phase-2 Tunnels> Общее количество всех входящих пакетов, отвергнутых локальным устройством посредством механизма Anti-Replay, при задействовании IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInAuthFails	1.3.6.1.4.1.9.9.171.1.3.1.13.0	uint32	<The total number of inbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество всех неудачных входящих аутентификаций по IPsec соединениям.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cipSecGlobalInDecrypts	1.3.6.1.4.1.9.9.171.1.3.1.14.0	uint32	<The total number of inbound decryption's performed by all current and previous IPsec Phase-2 Tunnels> То же самое значение, что и cipSecGlobalInPkts.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDecryptFails	1.3.6.1.4.1.9.9.171.1.3.1.15.0	uint32	<The total number of inbound decryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество входящих пакетов, которые были неудачно расшифрованы IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutOctets	1.3.6.1.4.1.9.9.171.1.3.1.16.0	uint32	<The total number of octets sent by all current and previous IPsec Phase-2 Tunnels. This value is accumulated AFTER determining whether or not the packet should be compressed. See also cipSecGlobalOutOctWraps for the number of times this counter has wrapped> Количество байт, отосланных под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutOctWraps	1.3.6.1.4.1.9.9.171.1.3.1.18.0	uint32	<The number of times the global octets sent counter (cipSecGlobalOutOctets) has wrapped> Количество переполнений счетчика cipSecGlobalOutOctets.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutPkts	1.3.6.1.4.1.9.9.171.1.3.1.22.0	uint32	<The total number of packets sent by all current and previous IPsec Phase-2 Tunnels> Количество пакетов, отосланных под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutDrops	1.3.6.1.4.1.9.9.171.1.3.1.23.0	uint32	<The total number of packets dropped during send processing by all current and previous IPsec Phase-2 Tunnels> Общее количество всех исходящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutAuthFails	1.3.6.1.4.1.9.9.171.1.3.1.25.0	uint32	<The total number of outbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество всех неудачных исходящих аутентификаций по IPsec соединениям.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cipSecGlobalOutEncrypts	1.3.6.1.4.1.9.9.171.1.3.1.26.0	uint32	<The total number of outbound encryption's performed by all current and previous IPsec Phase-2 Tunnels> Тоже самое значение, что и cipSecGlobalOutPkts.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutEncryptFails	1.3.6.1.4.1.9.9.171.1.3.1.27.0	uint32	<The total number of outbound encryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество исходящих пакетов, которые были неудачно зашифрованы IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalNoSaFails	1.3.6.1.4.1.9.9.171.1.3.1.29.0	uint32	<The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-2 Tunnels> Общее количество обменов, не состоявшихся по причине отсутствия IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
Interfaces-статистика				
ifPhysAddress	1.3.6.1.2.1.2.2.1.6.<ifIndex>	Octet string	<The interface's address at the protocol layer immediately `below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.> MAC-адрес данного интерфейса. Индекс для данного значения берется из ipAdEntIfIndex.<ip>	RFC1213-MIB
ifIndex	1.3.6.1.2.1.2.2.1.1.<ifIndex>	int32	<A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization> ifIndex – индекс интерфейса, находится в диапазоне между 1 и ifNumber (ifNumber - число сетевых интерфейсов)	RFC1213-MIB
IP - статистика				
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1.<ip>	IpAddress	<The IP address to which this entry's addressing information pertains.> Собственно сам <ip> (совпадает с индексом значения)	IP-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3.<ip>	IpAddress	<The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.> Маска адреса.	IP-MIB
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2.<ip>	int32	<The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.> Индексом переменной является IP-адрес устройства. Значением – индекс интерфейса (в таблице ifTable), который содержит данный адрес.	IP-MIB
CPU, Memory - статистика				
cpmCPUTotal5sec	1.3.6.1.4.1.9.9.109.1.1.1.1.3.1	uint32 (1..100)	<The overall CPU busy percentage in the last 5 second period. This object obsoletes the busyPer object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5secRev which has the changed range of value (0..100).> Загрузка процессора за последние 5 секунд.	CISCO-PROCESS-MIB
cpmCPUTotal5secRev	1.3.6.1.4.1.9.9.109.1.1.1.1.6.1	uint32 (0..100)	<The overall CPU busy percentage in the last 5 second period. This object deprecates the object cpmCPUTotal5sec and increases the value range to (0..100). This object is deprecated by cpmCPUTotalMonInterval> Загрузка процессора за последние 5 секунд. Отличается от cpmCPUTotal5sec допустимыми пределами.	CISCO-PROCESS-MIB
cpmCPUTotal1min	1.3.6.1.4.1.9.9.109.1.1.1.1.4.1	uint32 (1..100)	<The overall CPU busy percentage in the last 1 minute period. This object obsoletes the avgBusy1 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal1minRev which has the changed range of value (0..100).> Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1minRev допустимыми пределами.	CISCO-PROCESS-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7.1	uint32 (0..100)	<The overall CPU busy percentage in the last 1 minute period. This object deprecates the object cpmCPUTotal1min and increases the value range to (0..100).> Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1min допустимыми пределами.	CISCO-PROCESS-MIB
cpmCPUTotal5min	1.3.6.1.4.1.9.9.109.1.1.1.1.5.1	uint32 (1..100)	<The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5minRev which has the changed range of value (0..100).> Средняя загрузка процессора за последние 5 минут (в процентах).	CISCO-PROCESS-MIB
cpmCPUTotal5minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.8.1	uint32 (0..100)	<The overall CPU busy percentage in the last 5 minute period. This object deprecates the object cpmCPUTotal5min and increases the value range to (0..100).> Загрузка процессора за последние 5 минут. Отличается от cpmCPUTotal5min допустимыми пределами.	CISCO-PROCESS-MIB
ciscoMemoryPoolUsed	1.3.6.1.4.1.9.9.48.1.1.1.5.1	uint32	<Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.> Рассматривается как таблица из одного элемента (с индексом 1), которая задает общее количество используемой физической памяти.	CISCO-MEMORY-POOL-MIB
ciscoMemoryPoolFree	1.3.6.1.4.1.9.9.48.1.1.1.6.1	uint32	<Indicates the number of bytes from the memory pool that are currently unused on the managed device. Note that the sum of ciscoMemoryPoolUsed and ciscoMemoryPoolFree is the total amount of memory in the pool> Общее количество свободной физической памяти.	CISCO-MEMORY-POOL-MIB

18.2. Трап-сообщения

SNMP- агент посылает трап-сообщения о некоторых значимых событиях SNMP – менеджеру.

В конфигурационном файле LSP задание настроек SNMP-агента для отправки трап - сообщений осуществляется в структурах [SNMPTrapSettings](#) и [TrapReceiver](#). В этих структурах указывается IP-адрес и порт, на который отсылаются сообщения SNMP-менеджеру, идентификатор и IP-адрес отправителя трап-сообщения, версия SNMP, в которой формируются трап-сообщения.

В приведенной ниже таблице перечислены реализованные трапы и переменные, которые высылаются SNMP-менеджеру, и описание трапов.

Таблица 11

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
cikeSysFailure	1.3.6.1.4.1.9.9.1 71.2 3 1.3.6.1.4.1.9.9.1 71.2.0.3	cikePeerLocalAddr – адрес local peer cikePeerRemoteAddr – адрес remote peer Оба значения – табличные.	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences an internal or system capacity error.> Сигнализация о внутренней ошибке или исчерпании ресурсов при обработке IKE.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeCertCrlFailure	1.3.6.1.4.1.9.9.1 71.2 4 1.3.6.1.4.1.9.9.1 71.2.0.4	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a Certificate or a Certificate Revoke List (CRL) related error.> Ошибка, связанная с сертификатами или CRL.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeProtocolFailure	1.3.6.1.4.1.9.9.1 71.2 5 1.3.6.1.4.1.9.9.1 71.2.0.5	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a protocol related error.> Ошибка, связанная с обработкой протокола IKE: Authentication error (в ситуациях, не попадающих под cikeCertCrlFailure) BlackLog	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeNoSa	1.3.6.1.4.1.9.9.1 71.2 6 1.3.6.1.4.1.9.9.1 71.2.0.6	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a non-existent security association error.> Приход IKE-пакетов на несуществующий SA (Invalid cookie).	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecSetUpFailure	1.3.6.1.4.1.9.9.1 71.2 10 1.3.6.1.4.1.9.9.1 71.2.0.10	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the setup for an IPsec Phase-2 Tunnel fails.> По тем или иным причинам не удалось создать IPsec SA (при	CISCO-IPSEC-FLOW-MONITOR-MIB

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
			существующем IKE SA). <u>Примечание:</u> этот трап отсылается только при появлении ошибки во время проведения IKE-сессии и тем партнером, на котором случилась ошибка. Если создание соединения прекращено по другим причинам – остановка сервиса, перезагрузка LSP, delete payload, получение нотификации о том, что партнер по своей инициативе прекратил создание соединения, timeout и др., то локальное устройство трап не отсылает. В этом состоит отличие нашего агента от IOS, где трапы отсылаются с обоих партнеров при любой неуспешной сессии по созданию IPsec соединения.	
cipSecTunnel Start	1.3.6.1.4.1.9.9.1 71.7 7 1.3.6.1.4.1.9.9.1 71.2.0.7	cipSecTunLifeTime cipSecTunLifeSize Табличные значения.	<This notification is generated when an IPsec Phase-2 Tunnel becomes active.> Успешное создание туннеля.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecTunnel Stop	1.3.6.1.4.1.9.9.1 71.8 8 1.3.6.1.4.1.9.9.1 71.2.0.8	cipSecTunActiveTime Табличное значение	<This notification is generated when an IPsec Phase-2 Tunnel becomes inactive.> Уничтожение созданного туннеля (по разным причинам).	CISCO-IPSEC-FLOW-MONITOR-MIB
cipsTooMany SAs	1.3.6.1.4.1.9.10. 62.2 7 1.3.6.1.4.1.9.10. 62.2.0.7	cipsMaxSAs – максимальное количество IPsec SAs. Если не существует предела – 0.	<This trap is generated when a new SA is attempted to be setup while the number of currently active SAs equals the maximum configurable. The variables are: cipsMaxSAs> Отказ от создания SA по причине достигнутого максимального количества SA, указанного в лицензии. В переменной прописывается максимальное количество SA из лицензии.	CISCO-IPSEC-MIB
ciscoConfigManEvent	1.3.6.1.4.1.9.9.4 3.2 1 1.3.6.1.4.1.9.9.4 3.2.0.1	ccmHistoryEventCommandSource = { commandLine(1), snmp(2) } ccmHistoryEventConfigSource = { erase(1), commandSource(2) , running(3), startup(4), local(5), networkTftp(6),	<Notification of a configuration management event as recorded in ccmHistoryEventTable.> Всегда ccmHistoryEventCommandSource=1 Несколько вариантов: 1 При вызове lsp_mgr show или cs_console show run: ccmHistoryEventConfigSource=2 ccmHistoryEventConfigDestinatio	CISCO-CONFIG-MAN-MIB

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
		networkRcp(7) } ccmHistoryEventConfigDestination = { erase(1), commandSource(2), running(3), startup(4), local(5), networkTftp(6), networkRcp(7) } Табличные значения. Индекс – целое число, начинающееся с единицы. Инкрементируется при каждой посылке трапа данного типа.	n=2 <u>Примечание:</u> аналогично реакции Cisco на команду show run 2 При успешной загрузке LSP: ccmHistoryEventConfigSource=2 ccmHistoryEventConfigDestination=3 <u>Примечание:</u> аналогично реакции Cisco на команду configure terminal. Для стартовой загрузки LSP надо задать ccmHistoryEventConfigSource = 4 3 При отгрузке LSP (по разным причинам): ccmHistoryEventConfigSource=1 ccmHistoryEventConfigDestination=3	

19. Приложение

[Утилита make inst.exe](#)

[Сообщения об ошибках утилиты make inst](#)

[Создание сертификата конечного устройства](#)

[Установка "Signal-COM CSP"](#)

[Установка и настройка Удостоверяющего Центра. Создание СА сертификата](#)

[Установка "Admin-PKI"](#)

[Создание ключевой пары и запроса на сертификат конечного устройства](#)

[Создание сертификата конечного устройства.](#)

19.1. Утилита make_inst.exe

Вызов утилиты `make_inst.exe` должен происходить из каталога административного пакета. В противном случае будет выдано сообщение об ошибке. Утилита имеет обязательные опции и необязательные, которые заключены в квадратные скобки.

make_inst.exe -o SFX_file_path -l LSP_file_path

при использовании Preshared_Key указываются опции:

```
-kn Preshared_key_name
{-kv Preshared_key_val | -kvf file_path_Preshared_key_val}
```

при использовании сертификата указываются опции:

```
-c CA_file_path
-u USER_cert_file_path
-uc USER_cert_container_name
-kf Secret_Key_Path
[-skp Secret_Key_Password] | [skpf file_path_Secret_Key_Password]
[-up USER_cert_container_password] |
[-ufp file_path_USER_cert_container_password]
```

при копировании контейнера и файла с секретным ключом на конечном устройстве указываются опции:

```
[-cs Source_USER_cert_container_name]
[-cp Source_USER_cert_container_password] |
[-cfp file_path_Source_USER_cert_container_password]
[-kfs Source_Secret_Key_Path]
```

при проверке соответствия сертификата конечного устройства и его секретного ключа, проводимой на компьютере администратора, указываются опции:

```
[-chksecret {on | off}] (default: off)
[-uac USER_cert_container_name_ADMIN]
[-uap USER_cert_container_password_ADMIN] |
[-uafp file_path_USER_cert_container_password_ADMIN]
[-kaf Secret_Key_Path_ADMIN]
```

при копировании контейнера в инсталляционный файл указывается опция (а также опции проверки):

```
[-ucpkgcopy {on | off}] (default: off)
```

локальные настройки:

```
[-q {basic | normal | silent}] (default: basic)
[-d {passall | passdhcp}] (default: passall)
[-s {emerg | alert | crit | err | warning | notice | info | debug}]
(default: notice)
[-t <SYSLOG_server_IP>] (default: 127.0.0.1)
[-y <log_facility>] (default: log_local7)
[-a "<Additional_cmd_msiexec_params>"] (/l* log_file.txt /i)
[-lic <license_file_path>]
[-rngc {new | exist | copy | usecert | pkgcopy}]
[-rngn RNG_Container]
[-rngs Source_RNG_Container]
[-rnga RNG_Container_ADMIN]
```

где:

-o SFX_file_path
SFX_file_path - имя создаваемого инсталляционного SFX-файла. Обязательная опция. Имя файла подразумевает и путь к этому файлу.
-l LSP_file_path
LSP_file_path - имя файла, содержащего LSP. Имеет текстовый формат. Обязательная опция.
-kn Preshared_key_name
Preshared_key_name - имя предустановленного ключа. Обязательная опция, если используются Preshared ключи. Может быть задано несколько таких ключей (см. Примечание 1). Preshared ключи или сертификаты обязательно должны быть заданы. Можно задавать и то, и другое.
-kv Preshared_key_val
Preshared_key_val - Preshared ключ. Например, -kv 12345 или -kv "Test preshared key". (кавычки в ключ не входят). Может быть задано несколько таких ключей (см. Примечание 1).
-kvf file_path_Preshared_key_val
file_path_Preshared_key_val - имя файла, содержащего Preshared ключ на компьютере администратора. Если используется Preshared ключ, то обязательно должна быть задана опция -kv либо -kvf. Может быть задано несколько таких ключей (см. Примечание 1).
-c CA_file_path
CA_file_path - имя файла с CA-сертификатом на компьютере администратора. Обязательная опция, если используются сертификаты.
-u USER_cert_file_path
USER_cert_file_path - имя файла с локальным сертификатом конечного устройства на компьютере администратора. Обязательный параметр, если используются сертификаты.
-uc USER_cert_container_name
USER_cert_container_name - имя контейнера с секретным ключом локального сертификата на конечном устройстве (см. Примечание 2). Здесь же указывается и носитель информации, на котором хранится контейнер. Не больше 60 символов. Обязательная опция, если используются сертификаты. Например, "C:\Containers\container1" (См. Примечание 3 об именах контейнеров).
-up USER_cert_container_password
USER_cert_container_password - пароль к контейнеру. Не больше 40 символов. Параметр актуален, если не задана опция -ufp. Различается ситуация, когда отсутствует пароль (опция не задана) и когда пароль пустой (задано -up "").

-ufp file_path_USER_cert_container_password
file_path_USER_cert_container_password - имя файла на компьютере администратора, содержащего пароль к контейнеру. Не больше 40 символов. Пароль читается из файла как текстовая строка. Если файл содержит несколько строк, то читается только первая строка (воспринимается как пароль).
-skp Secret_Key_Password
Secret_Key_Password - пароль к секретному ключу. Различается ситуация, когда пароль отсутствует (опция не задана) и когда пароль - пустой (задано -skp "").
-skpf file_path_USER_cert_container_password
file_path_USER_cert_container_password - имя файла на компьютере администратора, содержащего пароль к файлу с секретным ключом. Пароль читается из файла как текстовая строка. Если файл содержит несколько строк, то читается только первая строка и воспринимается как пароль.
-chksecret {on off}
включение/выключение (on off) - проверки соответствия сертификата конечного устройства и секретного ключа. По умолчанию - значение off. Такая проверка осуществляется на компьютере администратора и возможна только при наличии на нем контейнера с секретным ключом либо контейнера и файла с секретным ключом. Для проведения проверки указываются опции uac, uafp, kaf (если секретный ключ не в контейнере).
-ucpkgcopy {on off}
включение/выключение (on off) копирования контейнера в инсталляционный файл. Если копирование включено, то контейнер, заданный в опции -uac, копируется в инсталляционный файл. При инсталляции на конечное устройство, данный контейнер копируется в контейнер, указанный в опции -uc. По умолчанию - значение off.
-uac USER_cert_container_name_ADMIN
USER_cert_container_name_ADMIN - имя контейнера на компьютере администратора для проведения проверки. Эта опция используется только при включенной опции -chksecret. При проверке происходит импортирование файла с секретным ключом из контейнера с данным именем в инсталляционный пакет, если секретный ключ расположен по стандартному варианту, т.е. находится в контейнере. В противном случае, кроме опции -uac задается еще опция -kaf для указания местоположения секретного ключа.
-uap USER_cert_container_password_ADMIN
USER_cert_container_password_ADMIN - пароль к контейнеру с именем, указанным в опции -uac, на компьютере администратора.
-uafp file_path_USER_cert_container_password_ADMIN
file_path_USER_cert_container_password_ADMIN - имя файла на компьютере администратора, в котором записан пароль к контейнеру, указанному в опции -uac.

-kaf Secret_Key_Path_ADMIN

Secret_Key_Path_ADMIN - имя файла с секретным ключом на компьютере администратора. Если задана эта опция, то кроме проверки происходит еще импортирование секретного ключа из данного файла в инсталляционный пакет. Если эта опция не задана, делается попытка взять секретный ключ из контейнера, заданного в опции -uac. Если опция -uac также не задана, либо в контейнере нет валидного секретного ключа, то секретный ключ не импортируется в инсталляционный пакет. Вместо этого указываются опции -kf либо -uc для секретного ключа на конечном устройстве.

-cs Source_USER_cert_container_name

при указании этой опции при запуске инсталляционного файла на конечном устройстве будет производиться копирование контейнера с именем Source_USER_cert_container_name, размещенного на конечном устройстве (например, дискете), в контейнер с именем USER_cert_container_name, которое указано в опции -uc, если контейнер содержит секретный ключ. Если секретный ключ находится в отдельном файле на конечном устройстве (например, дискете), то для копирования ключа нужно указать опцию -kfs. Опция -cs задается, если используется сертификат. Если опция не задана, то копирование контейнера не производится. Копирование контейнера с точки зрения администратора описано в разделе "Копирование контейнера при инсталляции".

-cp Source_USER_cert_container_password

Source_USER_cert_container_password - пароль к контейнеру с именем, указанным в опции -cs, который будет копироваться при инсталляции. Если пароль отсутствует, то опция -cp не задается, если пароль пустой, то задается -cp "".

-cfp file_path_Source_USER_cert_container_password

file_path_Source_USER_cert_container_password – имя файла, в котором записан пароль к контейнеру, указанному в опции -cs.

-kfs Source_Secret_Key_Path

при указании этой опции при установке инсталляционного пакета будет производиться копирование файла с секретным ключом с именем Source_Secret_Key_Path, расположенного на конечном устройстве (например, дискете), в файл с именем, указанным в опции -kf. Эта опция используется, если файл с секретным ключом расположен вне контейнера. **Ограничение:** происходит простое копирование файла, поэтому нельзя использовать эту опцию, если секретный ключ расположен на токене.

-q {basic | normal | silent}

тип инсталляции:

- **basic** – неинтерактивная установка с запросом на инсталляцию. Вариант по умолчанию.
- **normal** – интерактивная установка (в диалоговом режиме) с демонстрацией Лицензии и другими окнами.
- **silent** – неинтерактивная установка без запросов. Стартует сразу после запуска EXE-файла без дополнительных запросов.

-d {passall | passdhcp}

Default Driver Policy:

- passall. – пропускать все. Вариант по умолчанию
- passdhcp – ничего не пропускать, кроме DHCP.

-s log_severity

log_severity = {EMERG|ALERT|CRIT|ERR|WARNING|NOTICE|INFO|DEBUG}

По умолчанию – NOTICE. Опция задает общий уровень важности протоколируемых событий, ее использование описано в главе ["Протоколирование событий"](#).

-t SYSLOG_server_IP

SYSLOG_server_IP - IP-адрес SYSLOG сервера, на который будут посылаться сообщения о протоколируемых событиях. По умолчанию – 127.0.0.1 (сообщения будут присылаться на локальный хост).

-y log_facility

log_facility = log_local 0-7. По умолчанию – log_local7.

-a "Additional_cmd_msiexec_params"

"Additional_cmd_msiexec_params" – дополнительные параметры запуска WinInstaller. Например, альтернативная инсталляционная папка, настройки лога Windows Installer и т.п. Эти параметры можно посмотреть по ссылке http://msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/command_line_options.asp

Например, для протоколирования событий в файл C:\log_client1.txt при инсталляции CSP VPN Server нужно выставить опцию -a /l* C:\log_client1.txt /i

Эту опцию рекомендуется указать, если выбирается тип инсталляции silent.

Можно задать максимальное время (в секундах), которое необходимо для инициализации VPN сервиса (vpnsvc) для CSP VPN Server - указывается параметр MAX_SERVICE_START_TIMEOUT и его значение, например, MAX_SERVICE_START_TIMEOUT=45. Максимальное значение – 600 секунд. Значение по умолчанию - 30 секунд.

-lic license_file_path

license_file_path - имя файла с Лицензией на CSP VPN Server на компьютере администратора. Эта опция обязательна для режимов инсталляции basic и silent. Для режима normal эта опция необязательна:

- если ее задать, то при установке Продукта вопросы о Лицензии задаваться не будут
- если ее не задать, то при установке Продукта появится стандартное окно для ввода Лицензии.

В текстовом файле данные Лицензии должны быть записаны в виде:

```
[license]
CustomerCode=NNNN
ProductCode=SERVERB/SERVER
LicenseNumber=NNNN
LicenseCode=NNNNNNNN
```

-rngc {new | exist | copy | usecert | pkgcopy}

вариант выбора RNG контейнера, размещенного на конечном устройстве, который содержит информацию для датчика случайных чисел:

- **new** - создать новый RNG контейнер на конечном устройстве
- **exist** - использовать существующий RNG контейнер на конечном устройстве
- **copy** - скопировать из существующего RNG контейнера на конечном устройстве **usecert** – использовать сертификатный контейнер в качестве RNG контейнера на конечном устройстве
- **pkgcopy** – скопировать с компьютера администратора RNG контейнер в инсталляционный файл, а при установке инсталляционного файла скопировать на конечное устройство

Эта опция обязательна для режимов инсталляции **basic** и **silent**.

Для режима **normal** эта опция необязательна:

- если ее задать, то при установке Продукта вопросы об RNG контейнере задаваться не будут
- если не задать – появится окно ввода параметров RNG контейнера.

Если опция **-rndc** задана, то обязательно должна быть задана и опция **-rndn** для всех случаев, кроме **usecert**.

Если выбран вариант **"copy"**, то обязательно должна быть задана опция **-rnds**.

Примечание: RNG контейнер должен храниться на носителе, доступ к которому осуществляется без каких-либо паролей под пользователем **System**. Например, нельзя задавать контейнер на токене или сетевом диске.

-rngn RNG_Container

RNG_Container – имя RNG-контейнера. Эта опция необходима, если задана опция **-rndc**. Если контейнер хранится на файловой системе, то имя контейнера - полный путь к папке с контейнером. Контейнер может быть расположен и на другом носителе, например **eToken** (используется префикс **"etoken"**) или **Touch Memory** (используется префикс **"ibutton"**).

Для указания папки с контейнером может использоваться подстановка **%INSTALLDIR%**, которая обозначает каталог Продукта, включая обратный слэш на конце (по умолчанию **-VPN Client**). Например - **%INSTALLDIR%\rng_container**.

-rngs Source_RNG_Container

Source_RNG_Container – имя исходного RNG контейнера, который будет скопирован. Опция необходима, если задана опция **-rngc "copy"**, в противном случае – неактуальна.

-rnga RNG_Container_Admin

RNG_Container_ADMIN – название исходного RNG контейнера на машине администратора. Необходим, если задана опция **-rngc pkgcopy**, в противном случае неактуален. При включении режима **pkgcopy** RNG контейнер, лежащий на машине администратора, копируется в инсталляционный пакет. При установке на конечное устройство этот RNG контейнер копируется в контейнер, заданный в опции **-rngn**.

Примечание 1:

Если задается несколько предустановленных ключей, то опции с именем ключа и самим ключом (-kn и -kv или -kvf) должны следовать одна за другой, т.е. опции

-kn и -kv (-kvf), расположенные рядом, относятся к одному и тому же предустановленному ключу.

Пример: -kn key1 -kv value1 -kn key2 -kvf file_with_value2.

Пример неправильного задания ключей (два имени и два значения расположены подряд):

-kn key1 -kn key2 -kv value1 -kvf value2 – НЕПРАВИЛЬНО!!!

Примечание 2:

Контейнер содержит служебную и ключевую информацию. Секретный ключ локального сертификата конечного устройства может находиться в этом же контейнере (стандартный вариант) либо в отдельном файле вне контейнера. Если секретный ключ лежит вне контейнера, тогда используется опция - kf.

Примечание 3:

Имя контейнера в файловой системе – это имя папки, например, "C:\Program Files\CSP VPN Server\cert_container".

19.2. Сообщения об ошибках утилиты make_inst.exe

	Сообщение	Пояснение
1	Error: SFX file path is missing	Не задан путь к SFX-файлу
2	Error: CA file path is missing	Не задан путь к CA-сертификату
3	Error: Local certificate file path is missing	Не задан путь к локальному сертификату
4	Error: Container name is missing	Не задано имя контейнера
5	Error: LSP file path is missing	Не задан путь к LSP
6	Error: Container name too long	Имя контейнера слишком длинное
7	Error: Container password too long	Пароль контейнера слишком длинный
8	Error: Wrong install type	Неправильно задан тип инсталляции
9	Error: Wrong Default Driver Policy	Неправильно задана DDP
10	Error: Wrong Logoff Policy	Неправильно задано Logoff policy
11	Error: Wrong Log Severity	Неправильно задана Log Severity
12	Error: Wrong parameter: "..."	Неподдерживаемый параметр
13	Error: temporary directory creation failed	Не удалось создать временную директорию для работы утилиты
14	Error: Key creation failed	Не удалось создать описание контейнера ключа (наиболее вероятная причина – не удалось прочитать файл с паролем).
15	Error: installer files copy failed	Не удалось скопировать файлы инсталлятора
16	Error: CA not found	Не удалось найти файл с CA сертификатом
17	Error: Local certificate not found	Не удалось найти файл с локальным сертификатом
18	Error: LSP not found	Не удалось найти файл с LSP
19	Error: User preferences write failed	Не удалось создать пользовательские настройки
20	Error: Log settings write failed	Не удалось создать настройки лога
21	Error: SFX archive creation failed	Не удалось сформировать SFX-архив
22	Error: Preshared key value not found	Не удалось найти файл со значением Preshared ключа
23	Error: Source container is not applicable	Попытка задать исходный контейнер, когда не используются сертификаты
24	Error: Source and destination containers have the same name	Исходный и рабочий контейнеры имеют одинаковые имена, что не допустимо
25	Error: Certificates or Preshared key should be set	Сертификаты или Preshared ключ должны быть заданы
26	Error: Preshared key name is missing	Не задано имя Preshared ключа
27	Error: Preshared key value is missing	Не задано значение Preshared ключа
28	Error: Preshared key name or value missed	Не задано имя или значение Preshared ключа

	Сообщение	Пояснение
29	Error: Preshared key names should be different	Имена Preshared ключей должны различаться
30	Error: Cannot initialize package settings	Не удастся инициализировать настройки инсталляционного пакета
31	Error: License should be set for non-interactive installation	Лицензия должна быть задана для неинтерактивной инсталляции
32	Error: Product incorrectly installed or damaged	Продукт некорректно установлен или поврежден
33	Error: Unknown RNG initialization choice	Некорректный вариант выбора RNG контейнера
34	Error: Secret key path is missing	Не указан путь к файлу с секретным ключом
35	Error: RNG container parameters should be set for non-interactive installation	Параметры RNG контейнера должны быть заданы для неинтерактивной инсталляции
36	Error: RNG Container is missing	Не задано имя RNG контейнера
37	Error: Source RNG Container is missing	Не задан исходный RNG контейнер
38	Error: Container name on the administrator computer is missing	Отсутствует контейнер на администраторской машине
39	Error: Secret key copy is only applicable with the container copy	Задано копирование секретного ключа, но не задано копирование сертификатного контейнера
40	Error: RNG Container can not be set as certificate container in non-certificate package	RNG контейнер не может быть выставлен как сертификатный контейнер, если не используются сертификаты
41	Error: RNG container name on the administrator computer is missing	Не задано имя RNG контейнера на машине администратора
42	Error: Insertion of RNG container into package failed	Не удалось вставить RNG контейнер в инсталляционный пакет
43	Error: Insertion of certificate container into package failed	Не удалось вставить сертификатный контейнер в инсталляционный пакет
44	Error: RNG Container can not be set as password-protected certificate container. RNG container must not have password.	Сертификатный контейнер, защищенный паролем, не может быть указан в качестве RNG контейнера. RNG контейнер не может быть с паролем.
45	Error: Container password reading from file failed	Не удалось прочитать из файла пароль на контейнер
46	Error: Source container password reading from file failed	Не удалось прочитать из файла пароль на исходный контейнер
47	Error: Container on administrator computer password reading from file failed	Не удалось прочитать из файла пароль на контейнер на машине администратора
48	Error: Secret key password reading from file failed	Не удалось прочитать из файла пароль на секретный ключ
49	Error: Cannot create SFX "<SFX_path>". Error code: <Error_code>[(<Error_description>)]	Не удалось создать SFX-архив по пути <SFX_path>. Номер системной ошибки: <Error_code>. Описание ошибки: <Error_description> (может отсутствовать). См. Примечание

	Сообщение	Пояснение
50	Error: File "<File_Path>" open failed. Error code: <Error_code>[(<Error_description>)]	Не удалось открыть файл по пути <File_path>. Номер системной ошибки: <Error_code>. Описание ошибки: <Error_description> (может отсутствовать). См. Примечание
51	Error: File archiving failed	Произошла ошибка при упаковке файлов.

Примечание:

В сообщениях, в которых фигурируют номер и описание системной ошибки, существуют особенности:

номер системной ошибки – стандартный номер ошибки Windows.

не для всех системных ошибок существуют текстовые описания, поэтому часть с описанием ошибки может отсутствовать.

описание ошибки выводится языком, стандартным для текущего пользователя. Вывод осуществляется в кодировке ANSI.

Это удобно для вывода, перенаправленного в файл или обрабатываемого GUI-программой.

Однако это может вызвать проблемы при работе из окна командной строки, поскольку там по умолчанию используется OEM-кодировка. Соответственно сообщение об ошибке в окне командной строки может оказаться нечитаемым. Исправить данную ситуацию можно одним из следующих способов:

- использовать перенаправление вывода в файл.
- изменить текущую кодовую страницу для окна командной строки:
 - открыть окно командной строки, использующее шрифты True Type (по умолчанию используются точечные шрифты, для которых описываемый метод неприменим). На практике, как правило, в подобных ситуациях используется шрифт Lucida Console.
 - вызвать команду `chcp`, в качестве аргумента которой прописать номер кодировки ANSI для используемого языка. Например в случае русского языка надо задать команду:
 - `chcp 1251`
 - после этого в текущем окне командной строки сообщения об ошибке утилиты `make_inst` будут показываться в читаемом виде.

19.3. Создание сертификата конечного устройства с использованием "Signal-COM CSP"

Для создания сертификата конечного устройства с использованием криптопровайдера "Signal-COM CSP", который можно использовать для работы с Продуктами CSP VPN Agent, опишем план действий:

- установить криптопровайдера "Signal-COM CSP"
- установить и настроить Удостоверяющий Центр (Certification Authority). Мы опишем как установить и настроить Microsoft Certification Authority, и создать CA сертификат
- установить "Admin-PKI", реализующий российские криптографические алгоритмы. Создать ключевую пару и запрос на локальный сертификат конечного устройства.
- создать сертификат конечного устройства.

Приведем подробные инструкции по каждому пункту.

19.3.1. Установка "Signal-COM CSP"

Для выполнения инсталляции необходимо:

- операционная система Windows 2000 Server (или выше)
- программный Продукт "Signal-COM CSP" версии 1.407 (или выше)
- описание криптопровайдера "Signal-COM CSP" можно посмотреть по адресу: http://www.signal-com.ru/ru/prod/crypt/signal_com/
- демо-версию этого Продукта можно запросить по адресу: <http://www.signal-com.ru/ru/demo/csp/index.php>

Запустите инсталляцию из файла `sccsp.exe` и следуйте инструкциям инсталлятора:

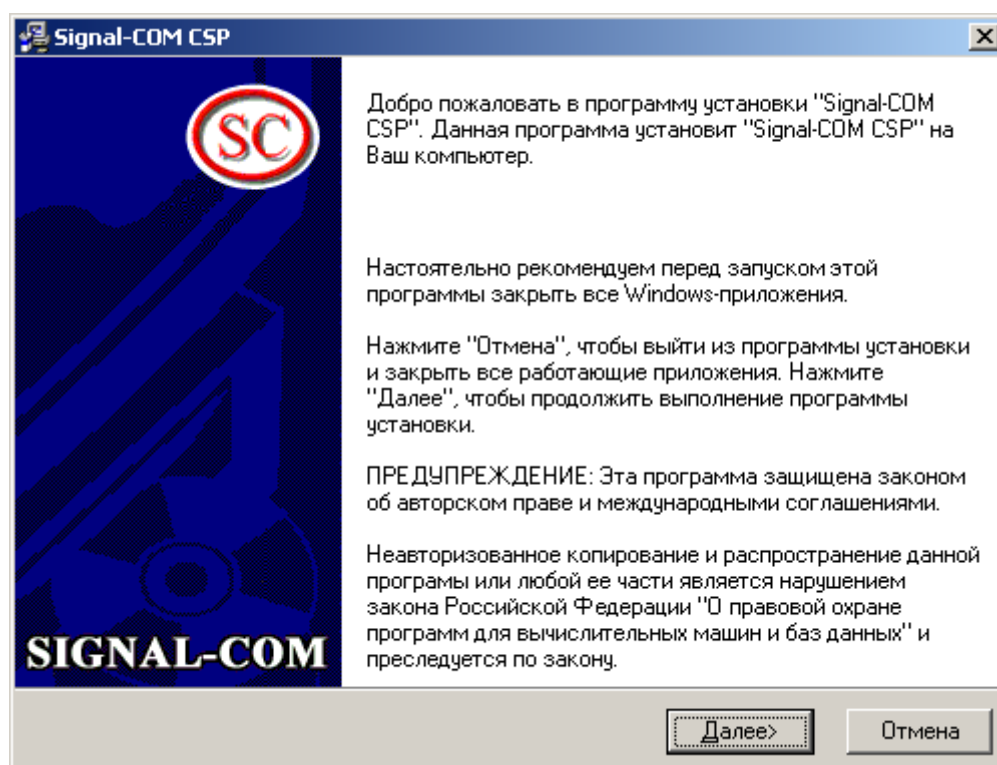


Рисунок 84

Введите требуемую информацию:

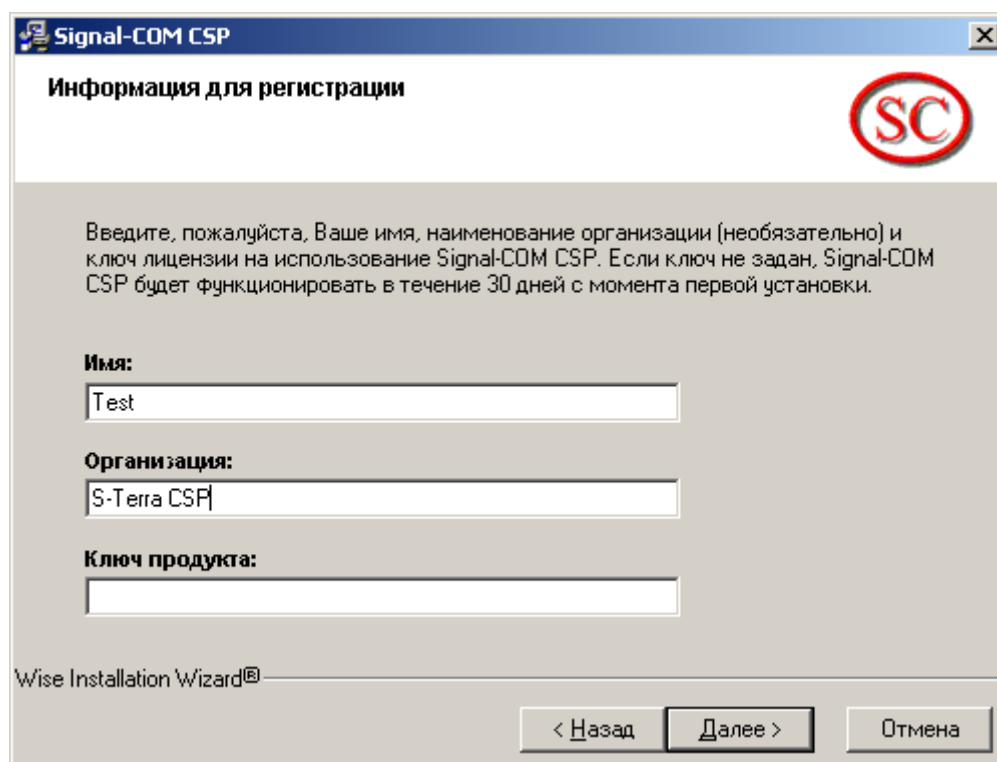


Рисунок 85

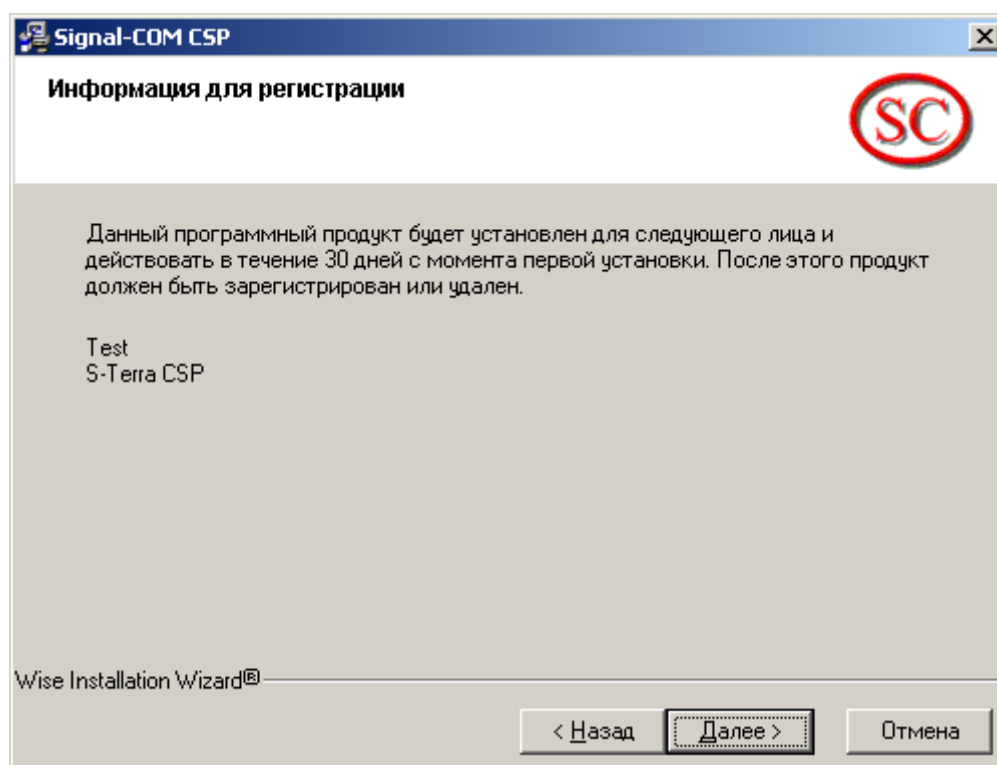


Рисунок 86

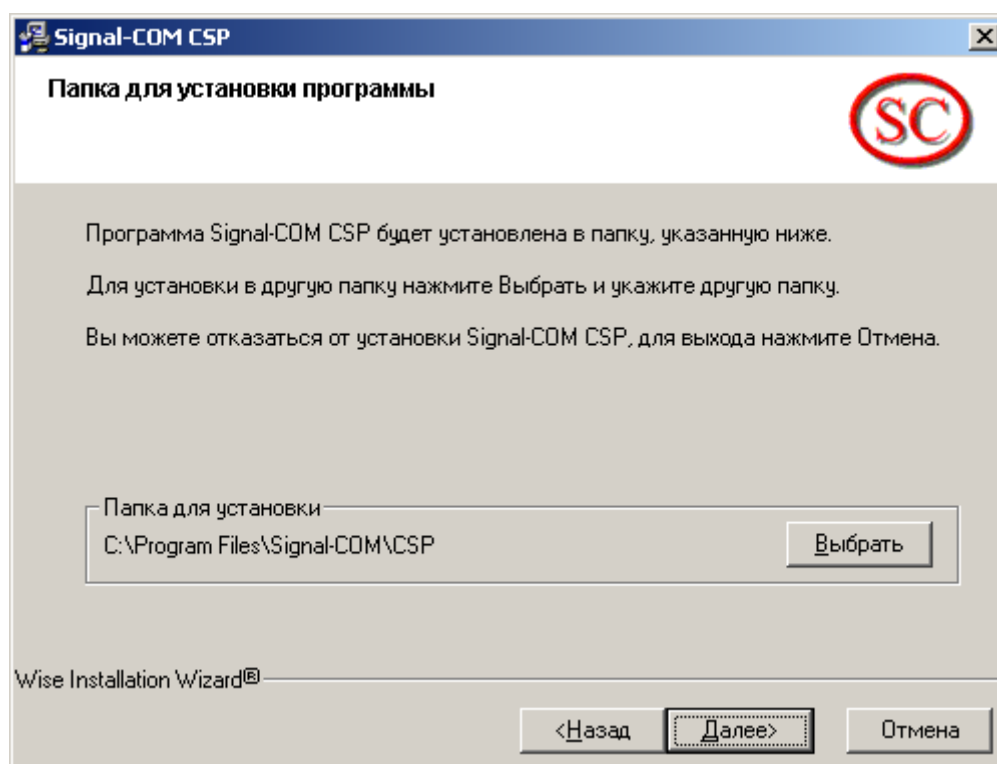


Рисунок 87

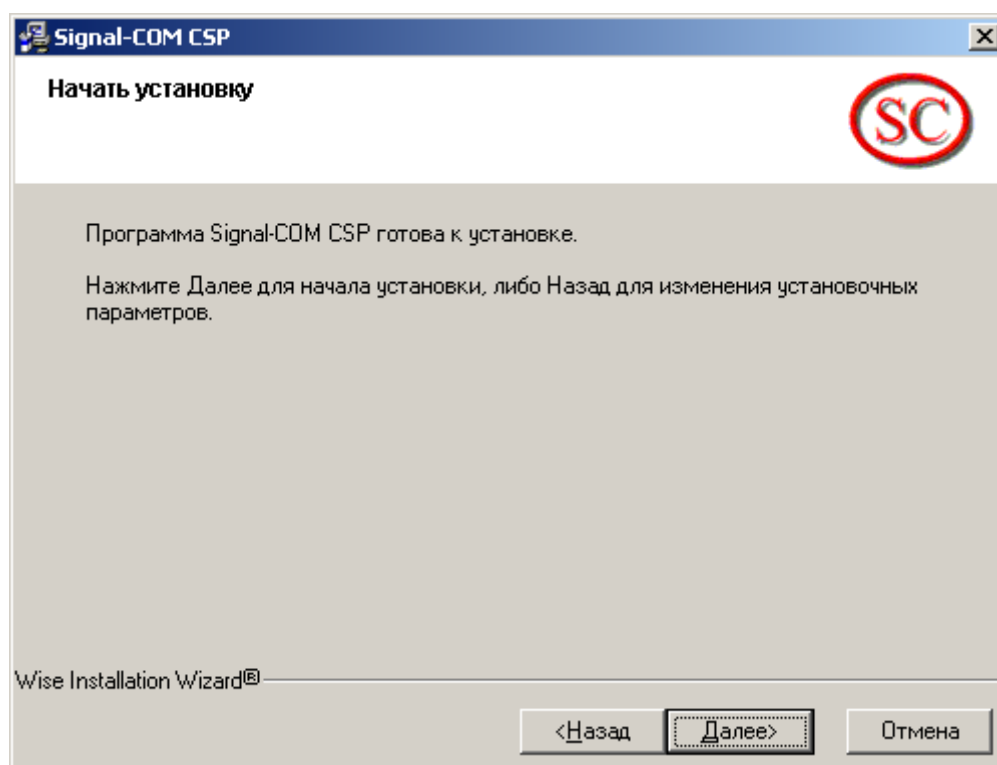


Рисунок 88

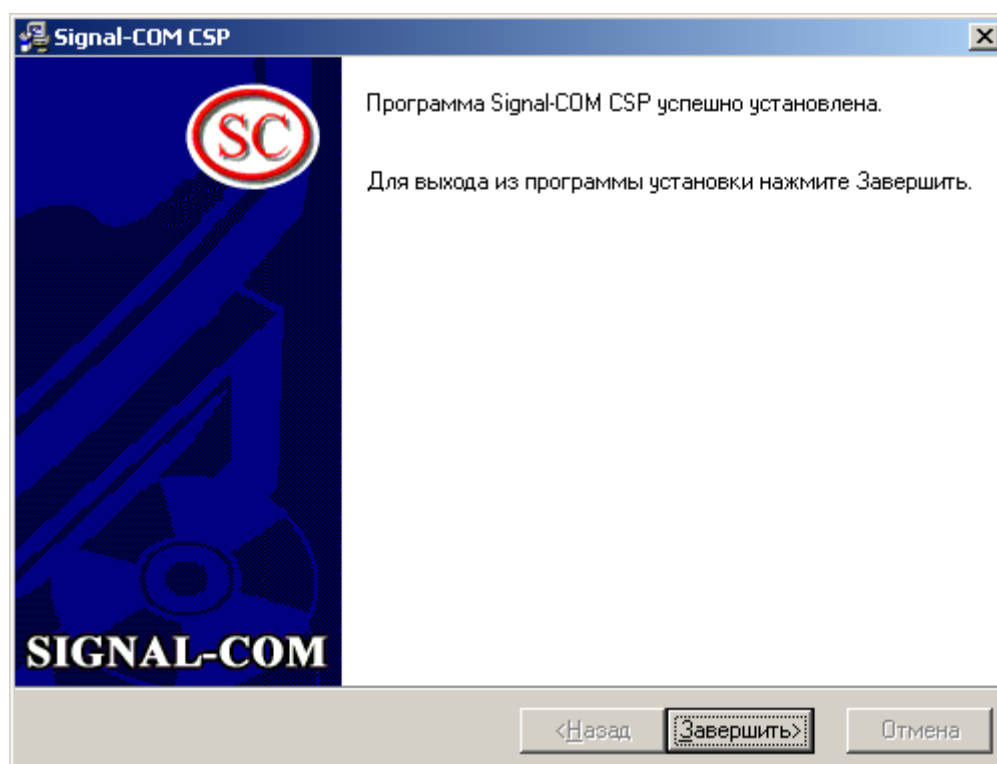


Рисунок 89

Инсталляция криптопровайдера завершена.

19.3.2. Установка и настройка Удостоверяющего Центра. Создание СА сертификата

На компьютере с установленной ОС Windows 2003 Server для инсталляции Удостоверяющего Центра Microsoft Certification Authority выполните следующее:

В окне установки компонент Windows (Start-Settings-Control Panel-Add/Remove Programs-Add/Remove Windows Components) установите флажок Application Server, а нажав на кнопку Details, установите сервисы Internet Information Services (IIS) и ASP.NET. Затем установите флажок Certificate Services и нажмите Next (Рисунок 90).

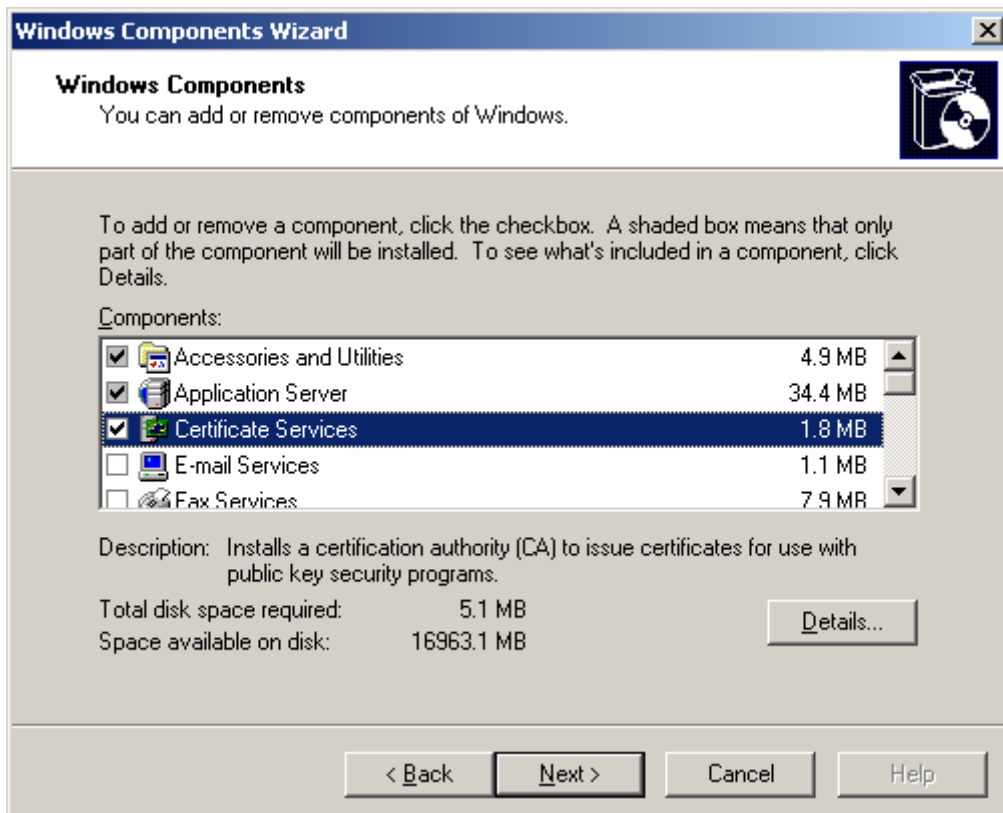


Рисунок 90

Если Certificate Services уже установлен, то его нужно удалить (снять флажок Certificate Services), а потом снова установить.

Перед установкой Certificate Services будет выдано предупреждение (Рисунок 91). Нажмите кнопку Yes.

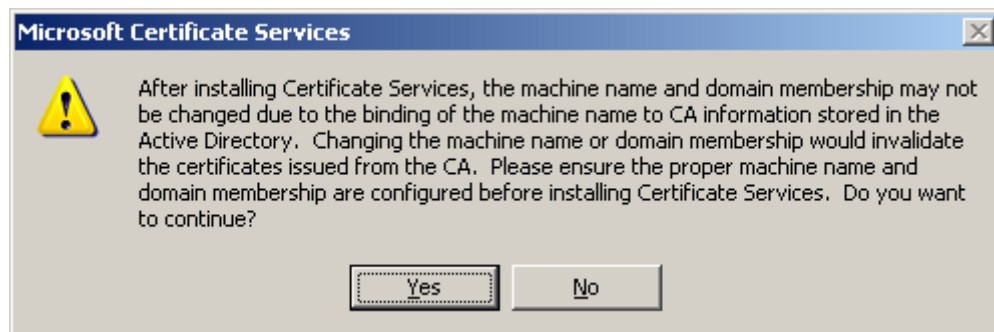


Рисунок 91

В следующем окне (Рисунок 92) выберите Удостоверяющий Центр с корневым CA сертификатом: поставьте переключатель в положение Stand-alone root CA. Установите флажок Use custom settings to generate the key pair and CA certificate и нажмите Next:

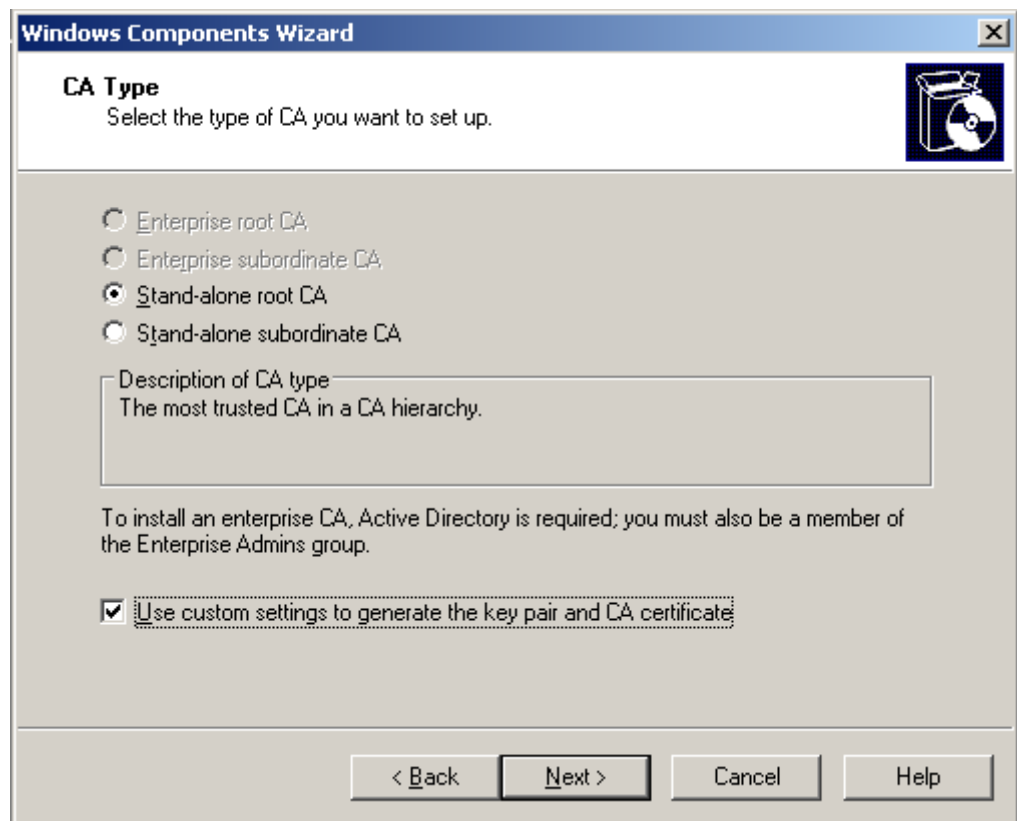


Рисунок 92

В качестве криптопровайдера (Рисунок 93) выберите Signal-COM Enhanced Cryptographic Provider (или Signal-COM Special Cryptographic Provider для использования CryptoPro совместимых алгоритмов) и нажмите Next:

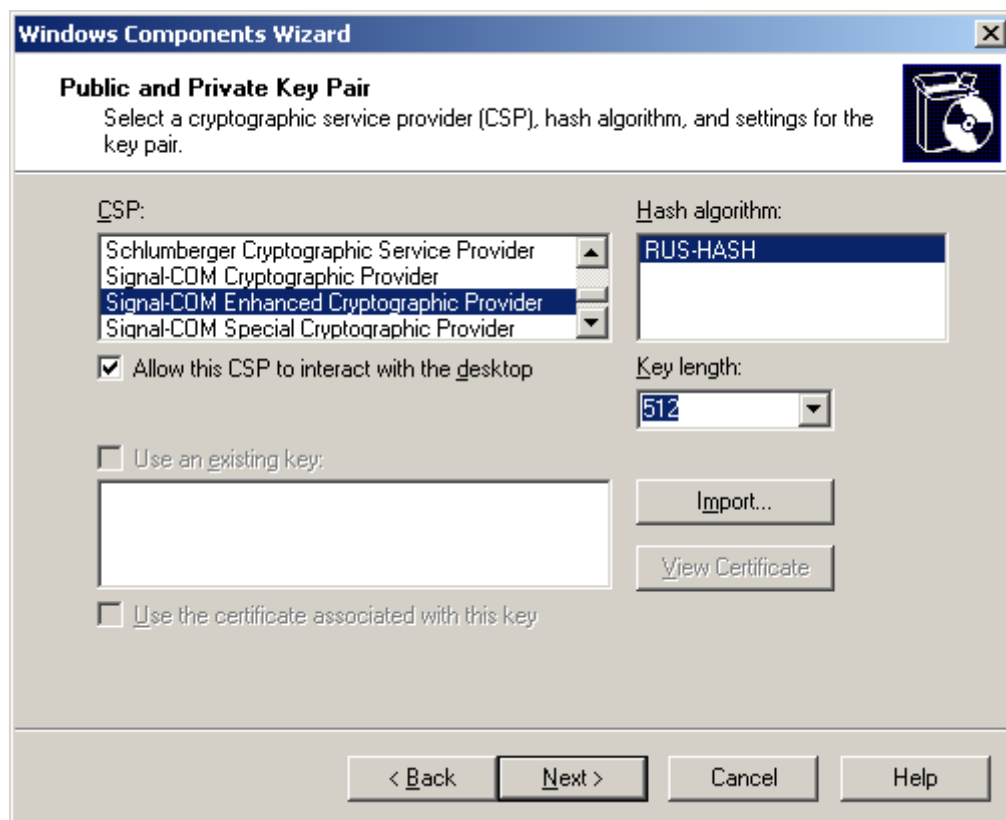


Рисунок 93

Заполните поля для CA сертификата и нажмите Next:

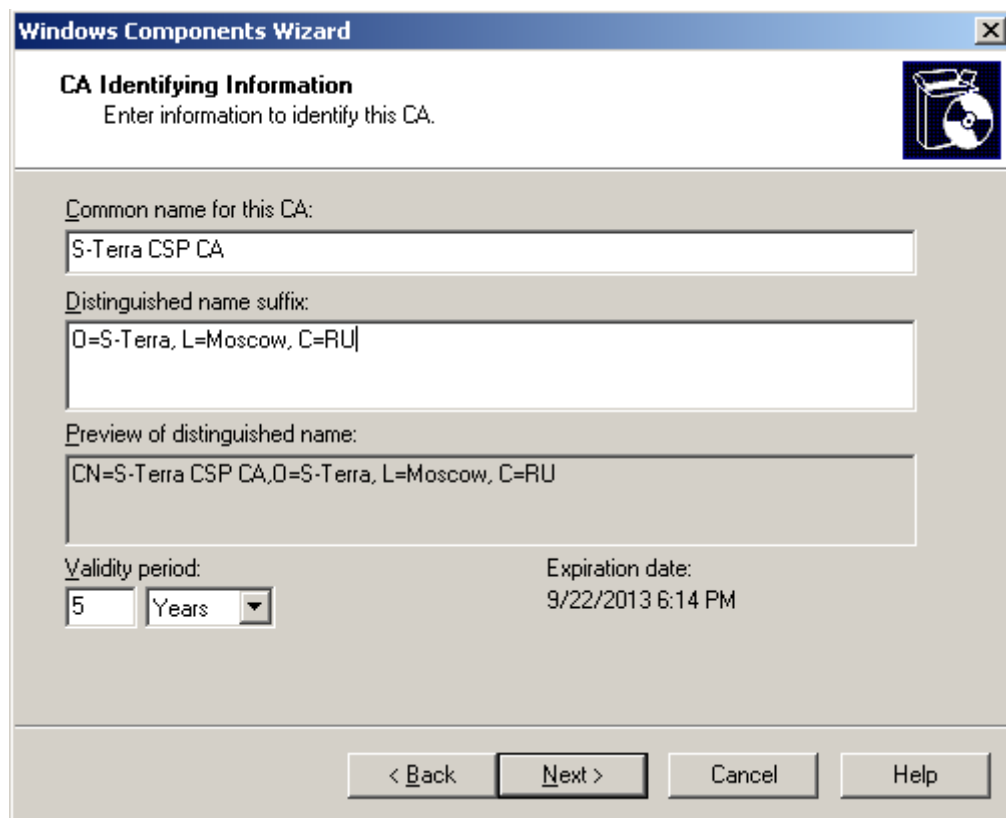


Рисунок 94

Выберите ключевой носитель, на котором будет записан контейнер с секретным ключом для CA сертификата и нажмите OK:

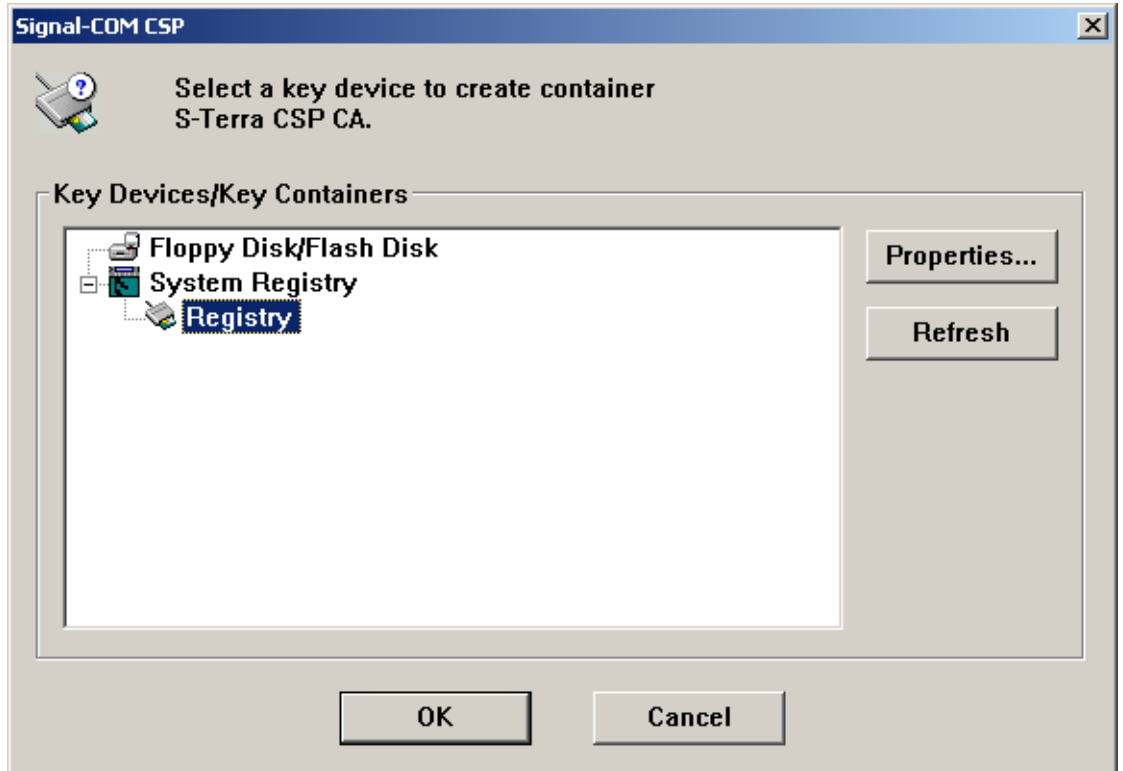


Рисунок 95

Далее происходит генерация ключей для CA сертификата. На вопрос об использовании пароля к ключевому контейнеру нажмите Yes. Пароль рекомендуется, но не обязателен.

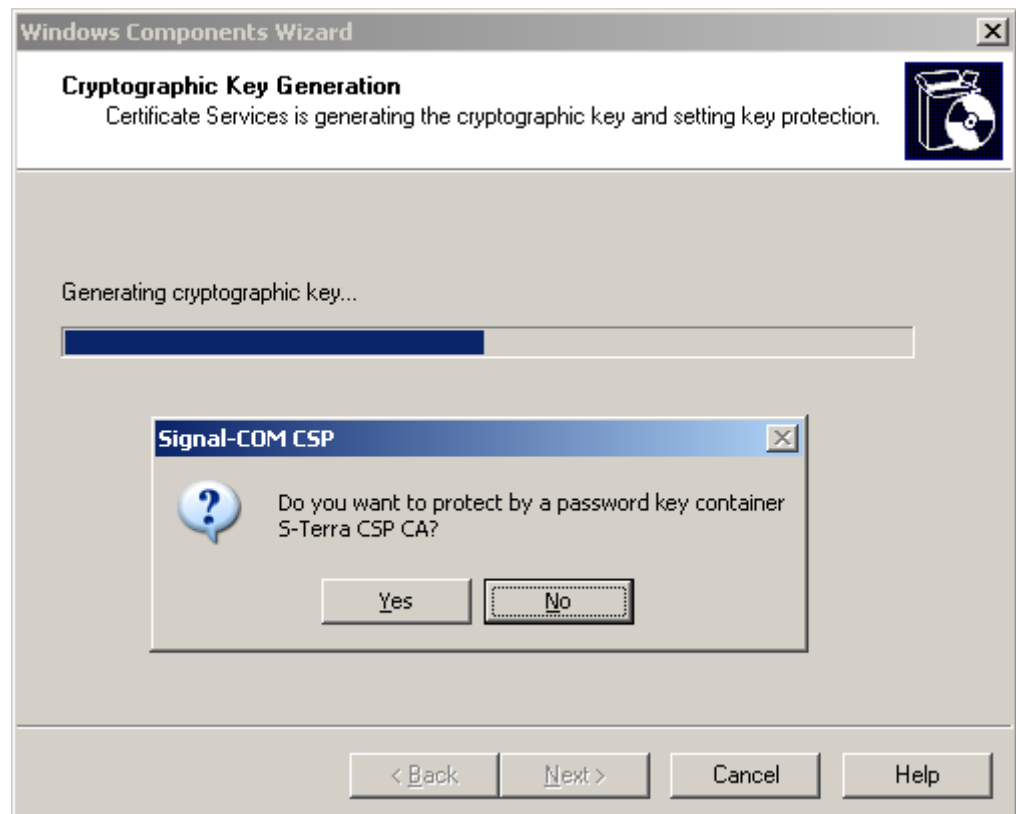


Рисунок 96

Задайте пароль к ключевому контейнеру и нажмите OK:

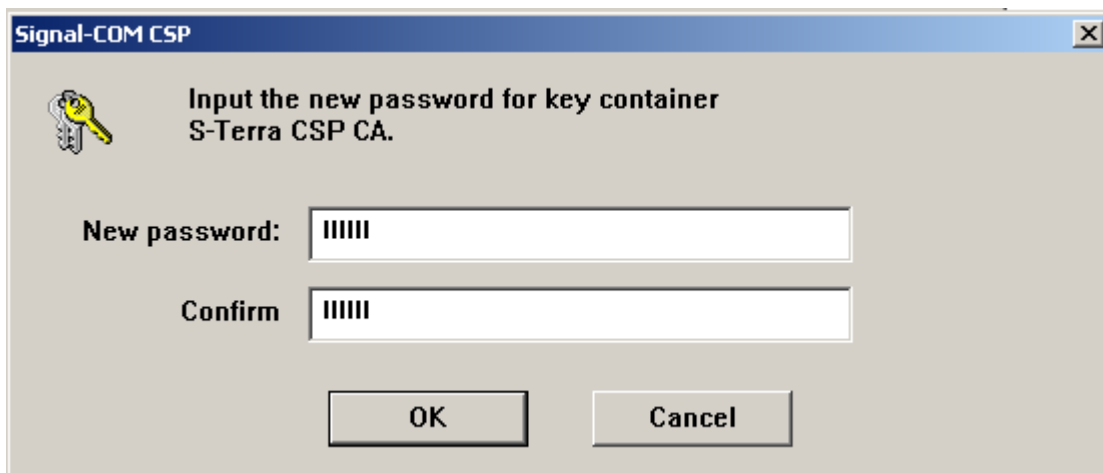


Рисунок 97

Для генератора случайных чисел вводите запрашиваемые символы:

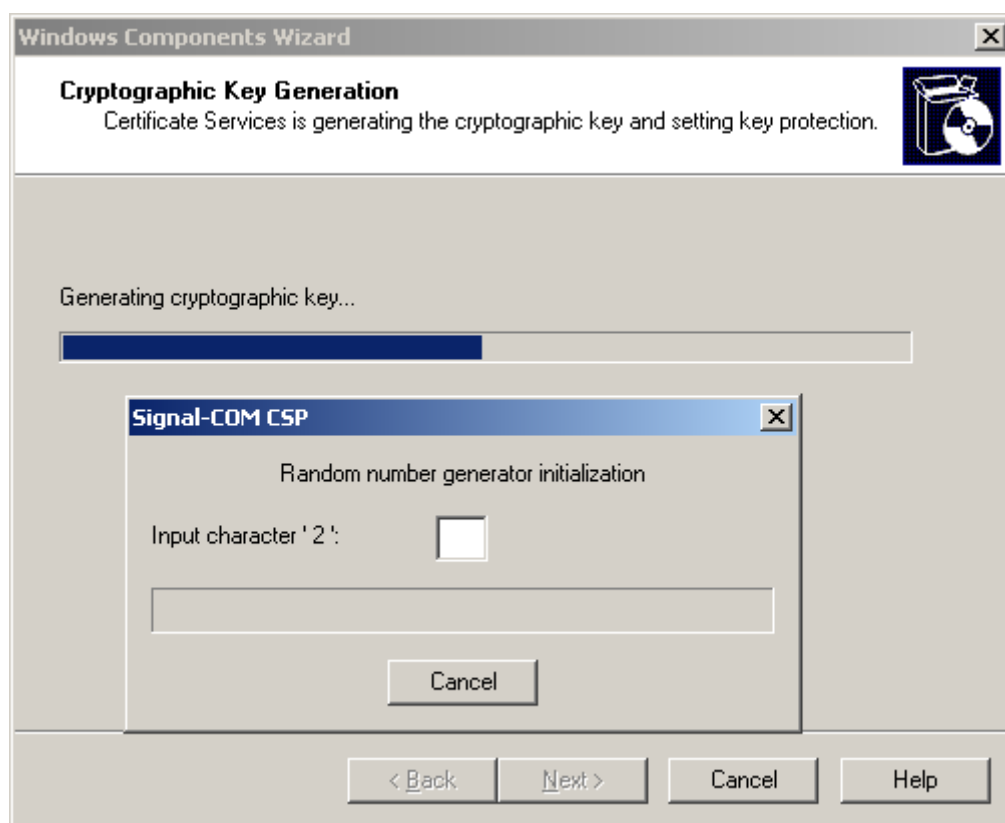


Рисунок 98

Оставьте без изменения установленные пути и нажмите Next (Рисунок 99):

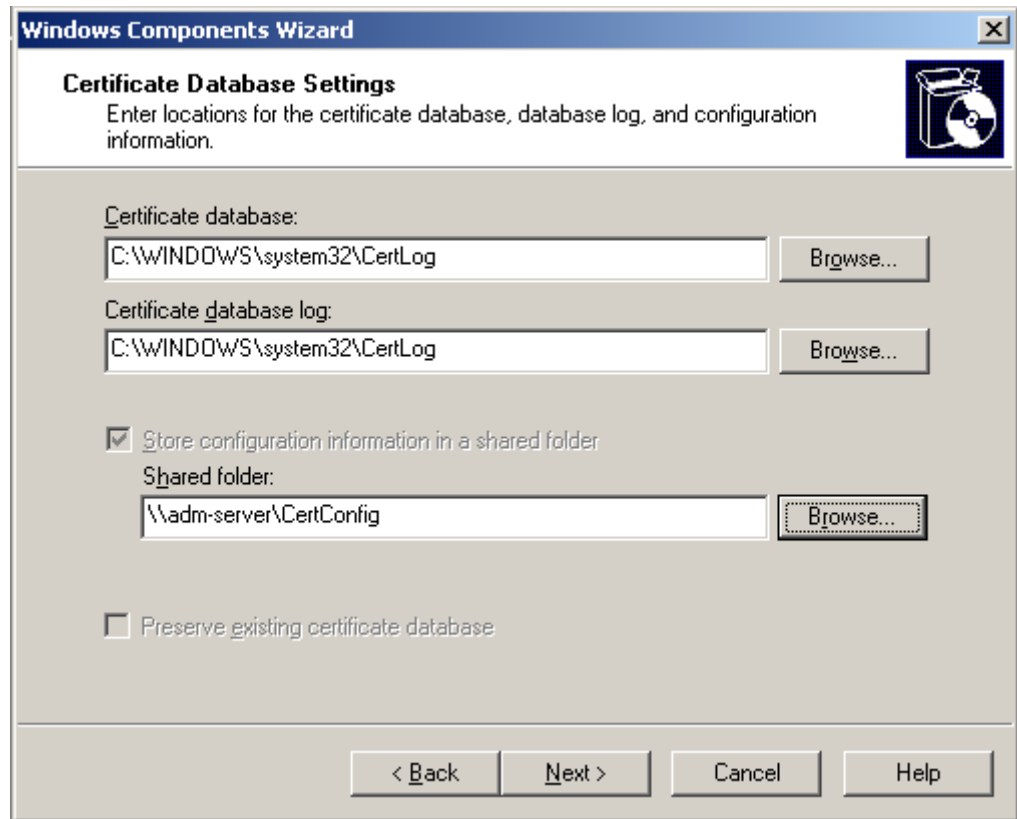


Рисунок 99

Введите еще раз пароль к контейнеру с секретным ключом CA сертификата и нажмите OK:



Рисунок 100

Инсталляция Удостоверяющего Центра завершена, нажмите **Finish**.



Рисунок 101

Для экспортирования СА сертификата в файл войдите в Certificate Authority (Start-Settings-Control Panel-Administrative Tools-Certificate Authority), выберите центр сертификации, а затем Action - Properties:

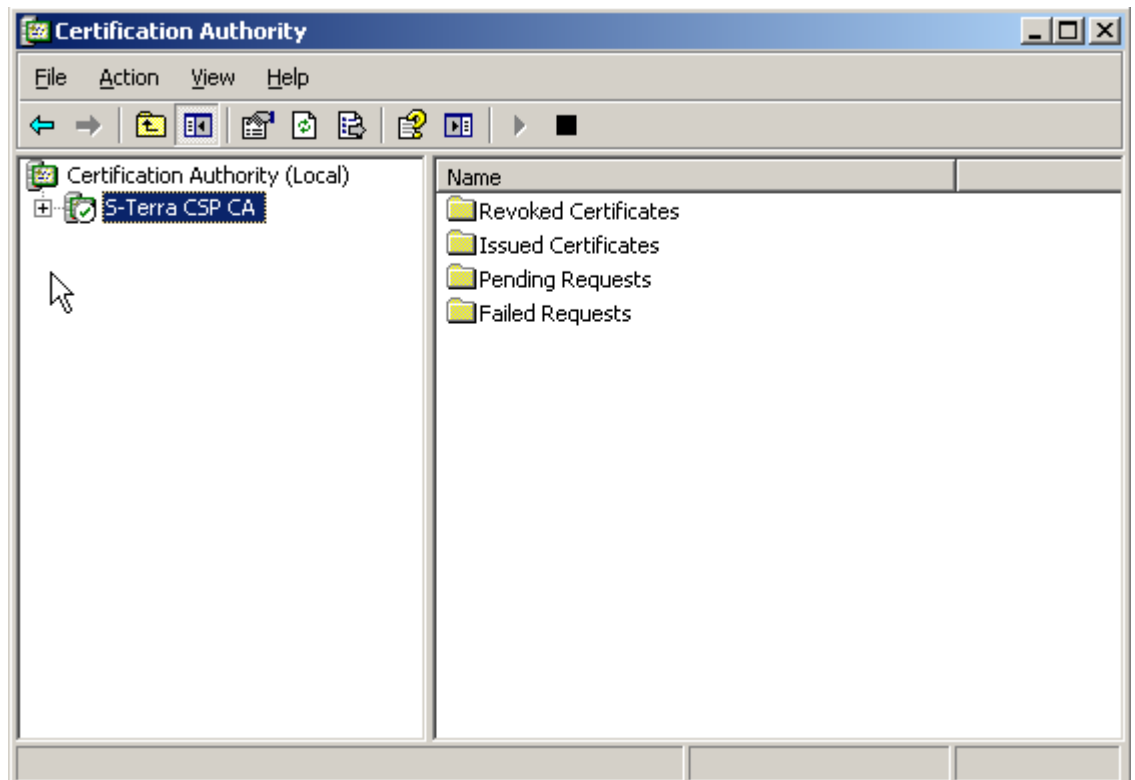


Рисунок 102

Далее во вкладке General нажмите кнопку View Certificate. В окне Certificate выберите вкладку Details (Рисунок 103) и нажмите кнопку Copy to File:

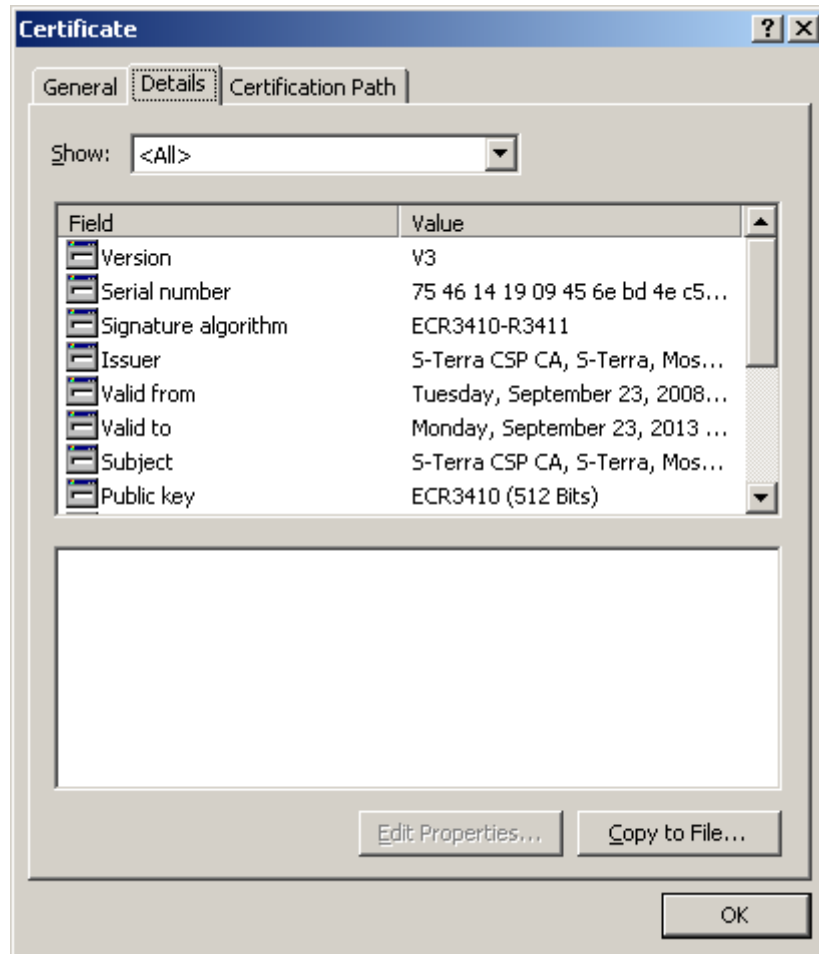


Рисунок 103

Затем в окне визарда **Certificate Export** (Рисунок 104) выберите формат, в котором должен быть экспортирован сертификат.

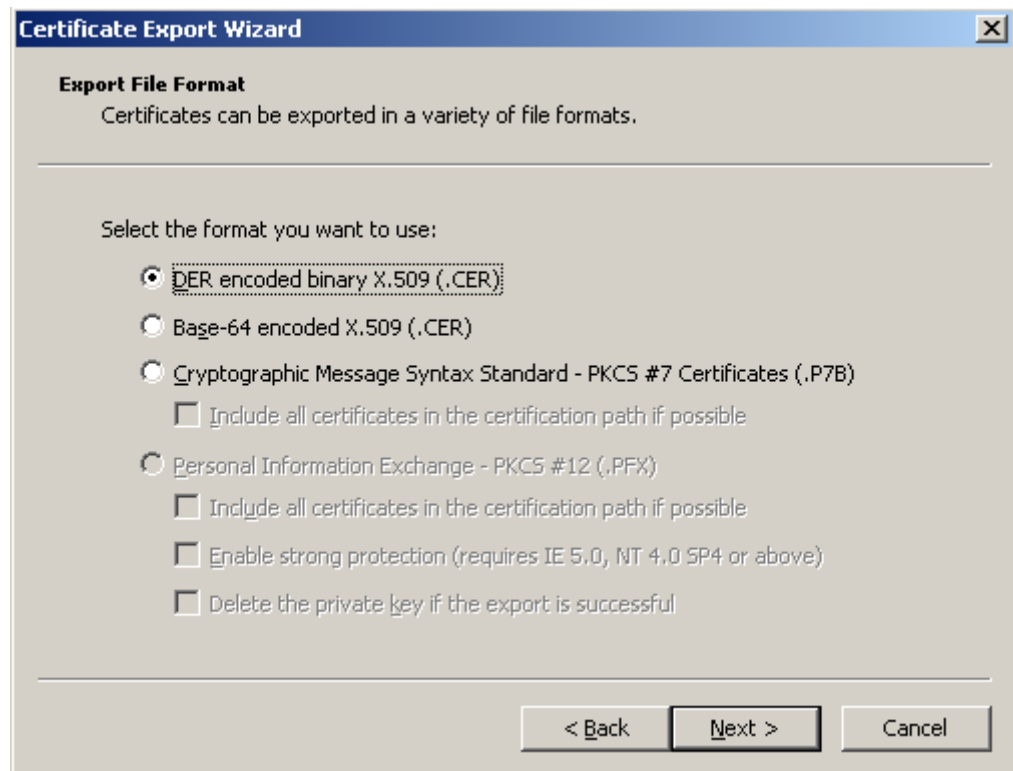


Рисунок 104

Введите имя файла, в который будет экспортирован сертификат.

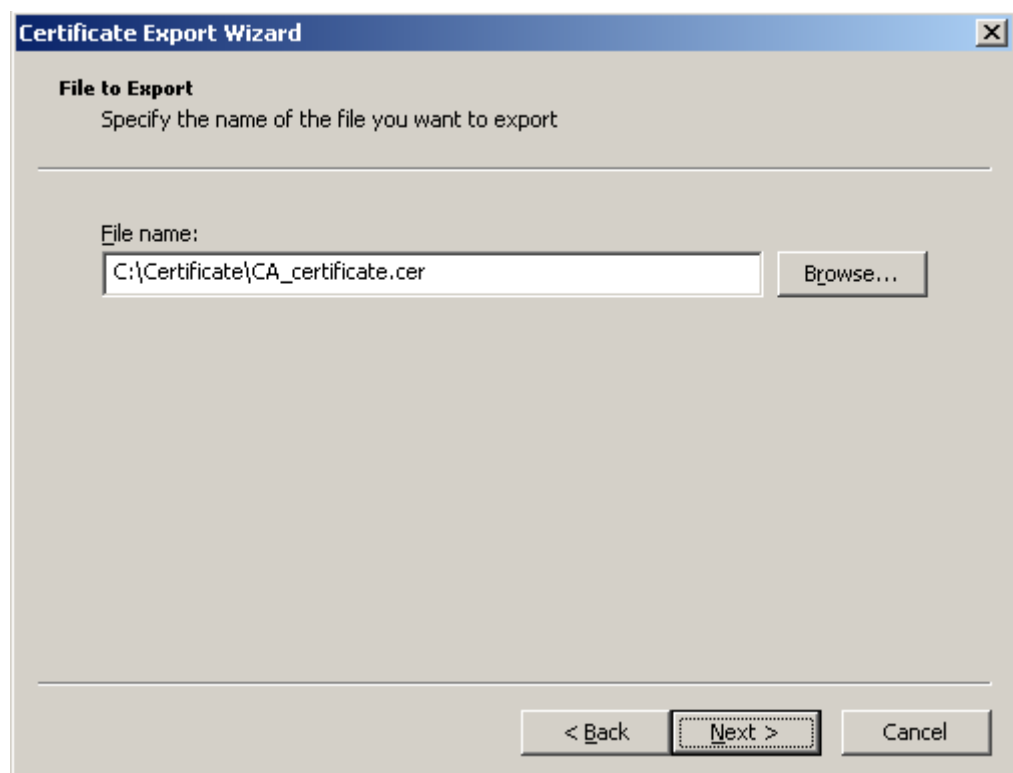


Рисунок 105

Экспортирование CA сертификата в файл завершено, нажмите **Finish**.



Рисунок 106

Закройте окно **Cerificate** (Рисунок 103), нажав кнопку **OK**.

Для автоматического создания подписываемых сертификатов войдите сначала в Certificate Authority (Start-Settings-Control Panel-Administrative Tools-Certificate Authority), выберите центр сертификации, а затем Action - Properties. Далее в окне Properties во вкладке Policy Module нажмите кнопку Properties... В появившемся окне установите флажок Follow the settings in the certificate template, if applicable. Otherwise, automatically issue the certificate и нажмите ОК (Рисунок 107).

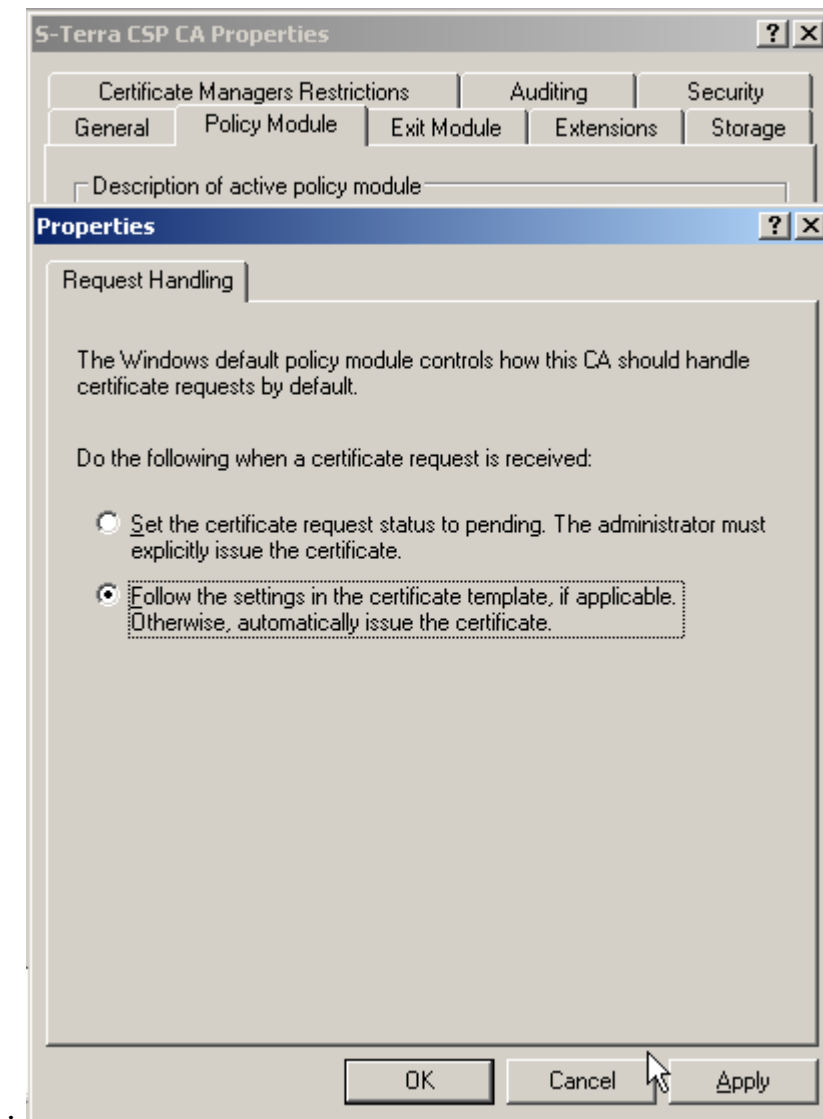


Рисунок 107

Появится предупреждение о необходимости перезапуска сервиса.

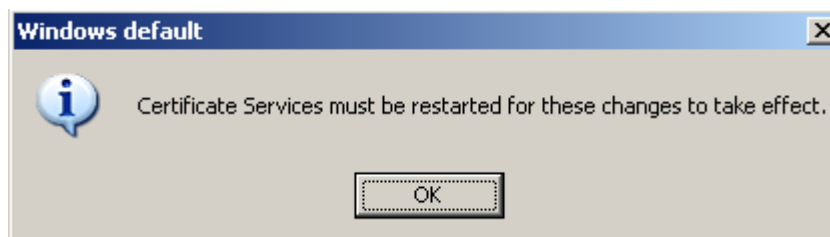


Рисунок 108

В окне Certificate Authority выберите центр сертификации, затем меню Action -- All Tasks -- Stop Service. После остановки сервиса выберите Start Service.

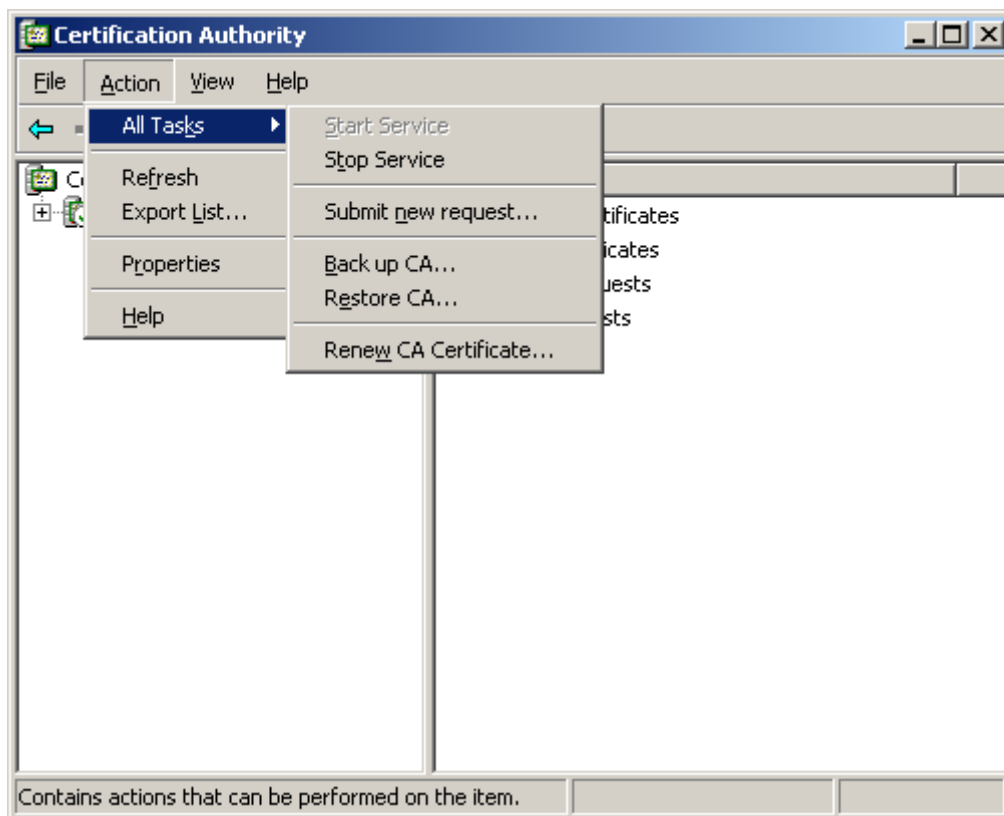


Рисунок 109

На этом создание Удостоверяющего Центра и его CA сертификата закончено.

19.3.3. Установка "Admin-PKI"

Для генерации ключевой пары для сертификата и формирования запроса на сертификат конечного устройства установите программный Продукт Admin-PKI.

Для выполнения инсталляции необходимо:

- операционная система Windows 2000 Server (или выше). Возможно использовать тот же компьютер, на котором установлен Microsoft Certification Authority
- программный Продукт Signal-COM "Admin-PKI" версии 3.1.0.4 (или выше)
- описание "Admin-PKI" можно посмотреть по адресу:
http://www.signal-com.ru/ru/prod/pki/admin_pki/
- демо-версию этого Продукта можно запросить по адресу:
<http://www.signal-com.ru/ru/demo/admin-pki/index.php>

Запустите инсталляцию из файла AdminPKI(trial).exe и следуйте инструкциям инсталлятора:

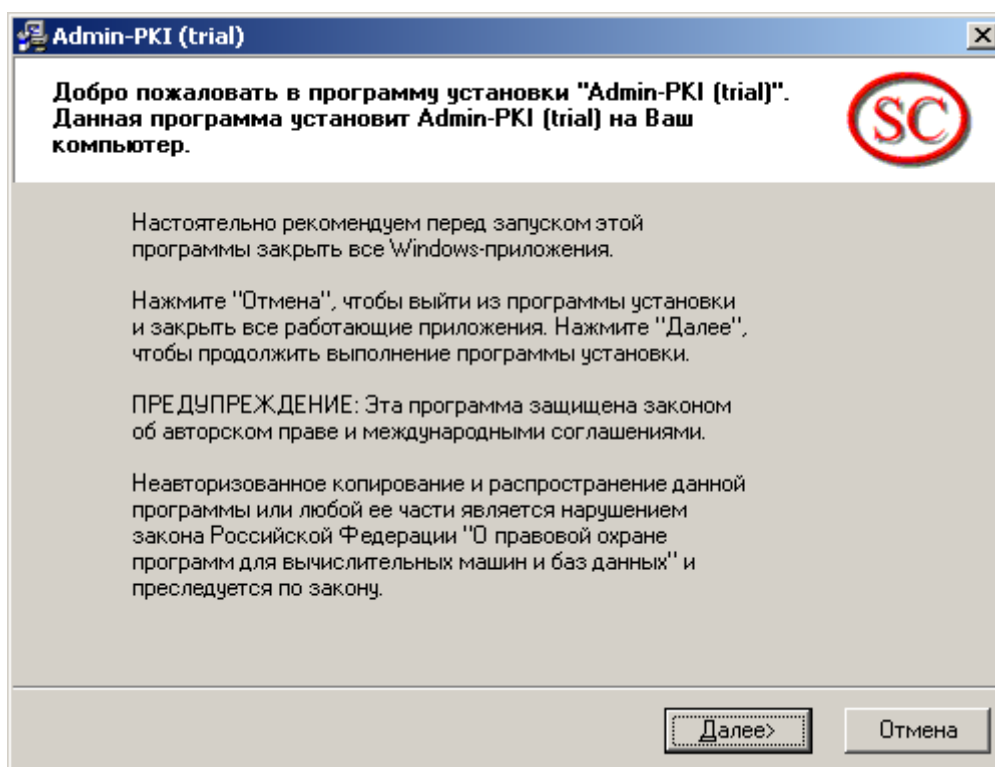


Рисунок 110

В следующих окнах нажимайте кнопку Далее:

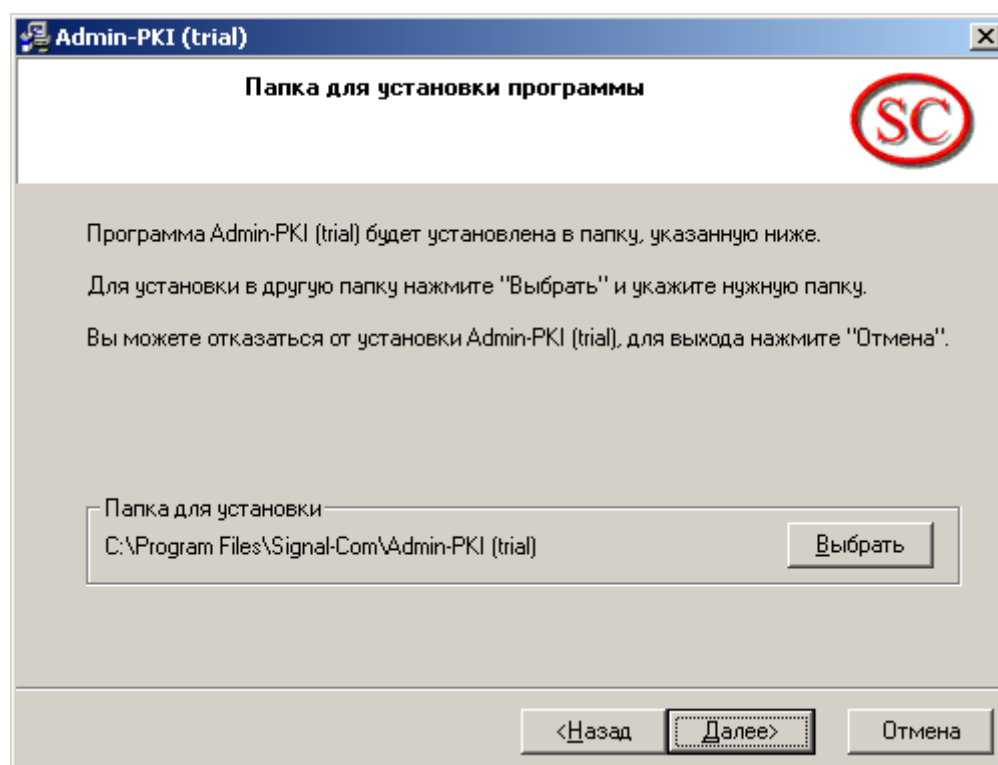


Рисунок 111

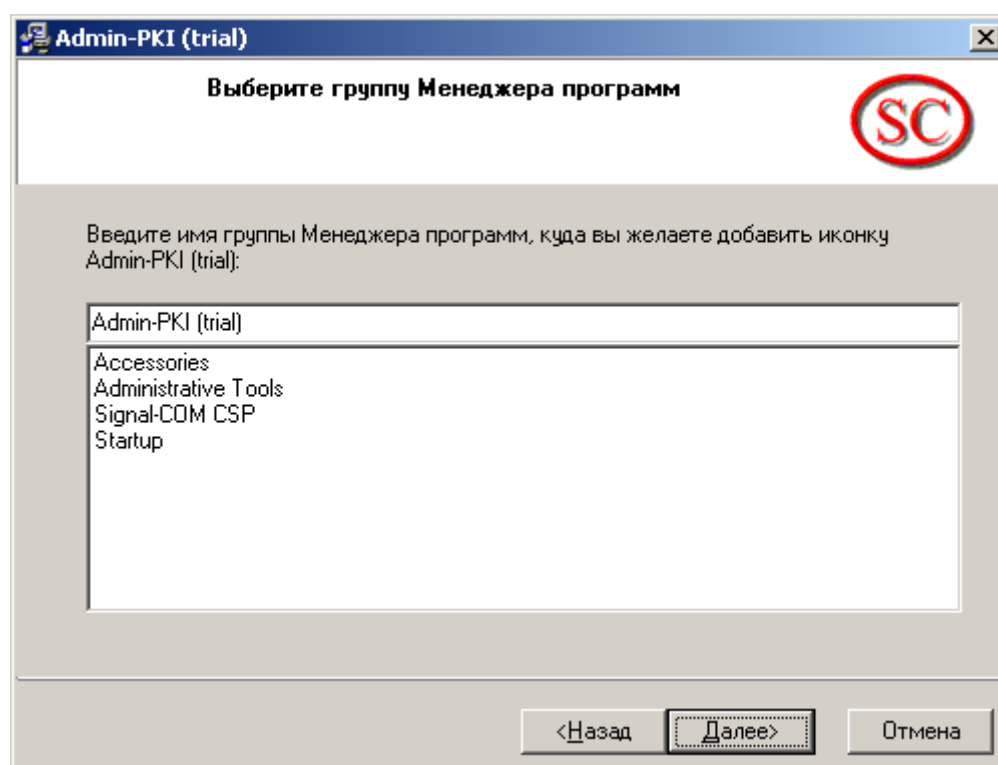


Рисунок 112

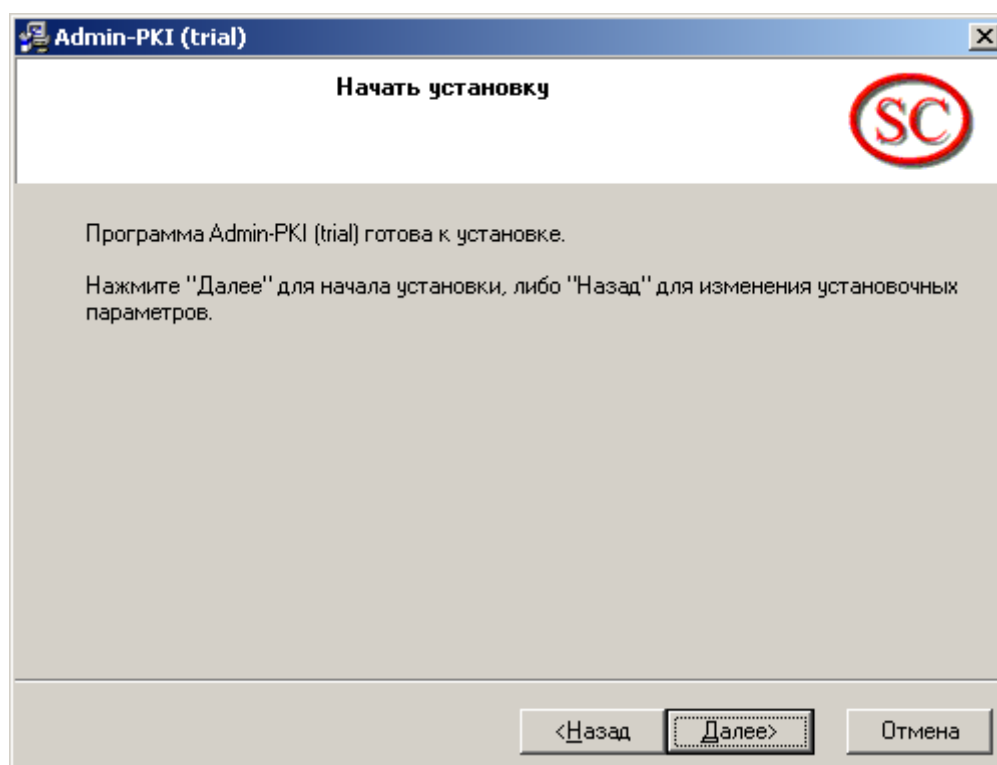


Рисунок 113

Инсталляция завершена, нажмите Завершить.

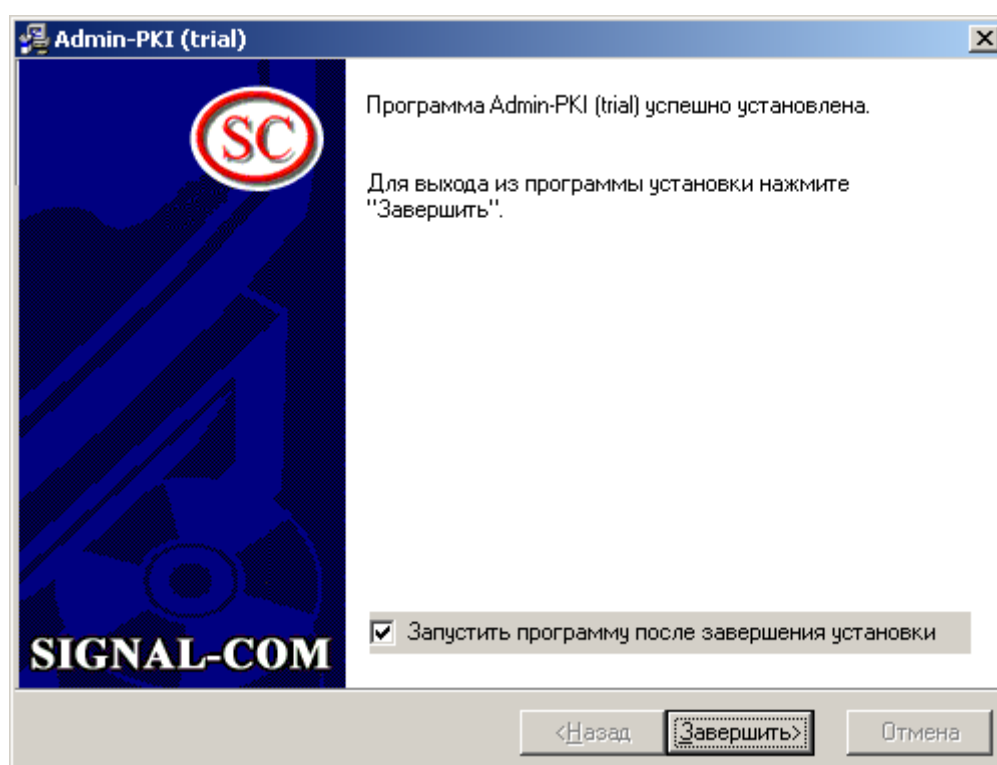


Рисунок 114

19.3.4. Создание ключевой пары и запроса на сертификат конечного устройства

Запустите Admin-PKI (Start -Programs -Admin-PKI (trial)- Admin-PKI (trial) v3). В меню Формирование выберите пункт Генерация ключей:

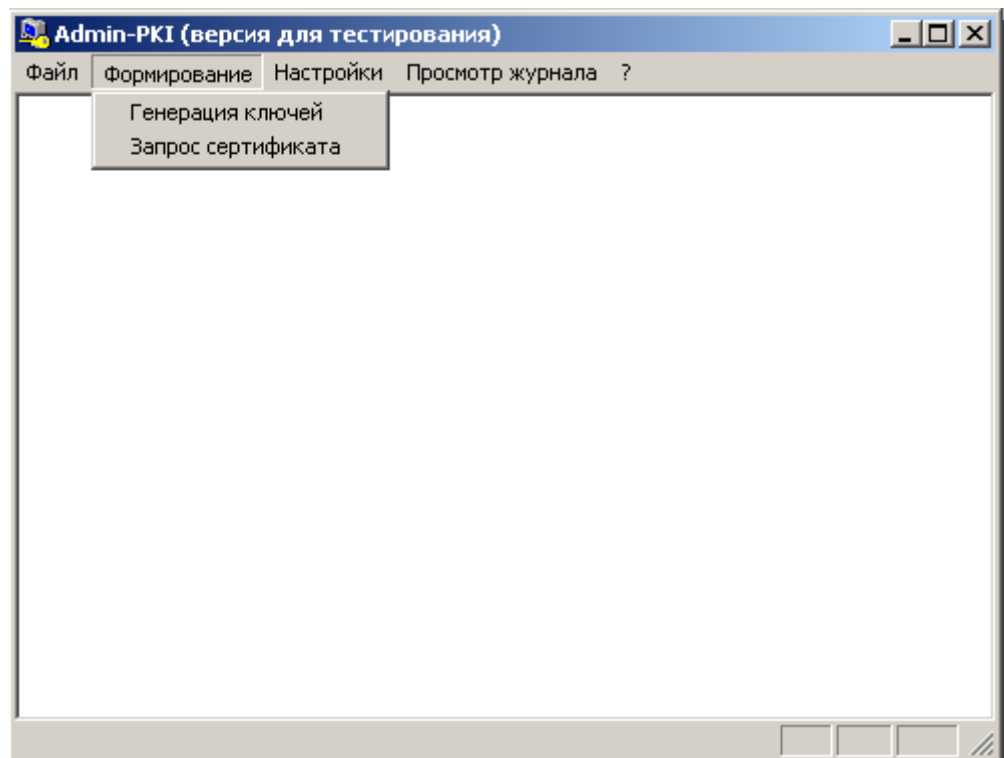


Рисунок 115

В поле Каталог ключевого носителя задайте контейнер в виде каталога.

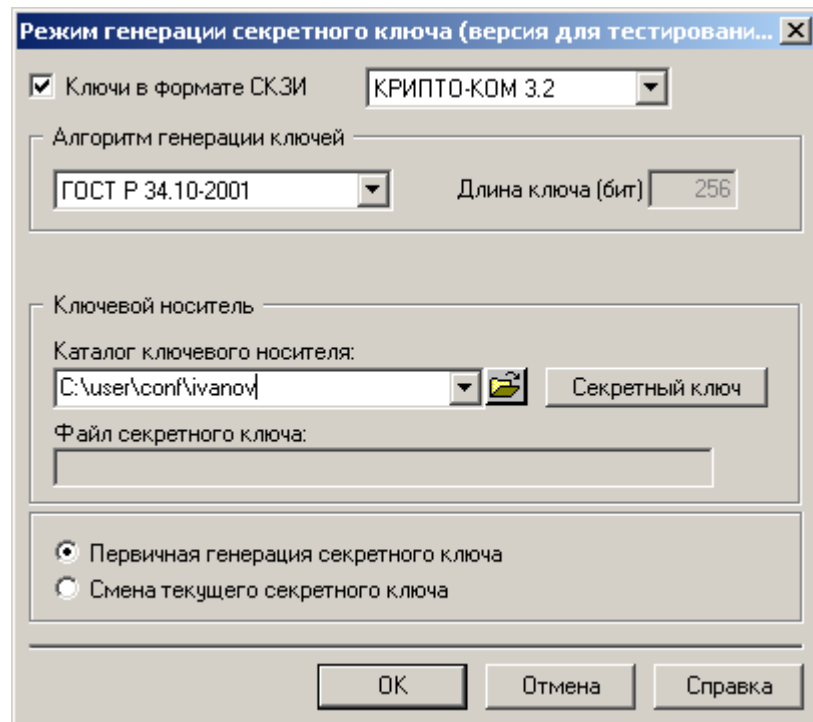


Рисунок 116

Если секретный ключ локального сертификата конечного устройства нужно разместить не в контейнере, а в отдельном файле, то в окне Режим генерации секретного ключа нажмите кнопку Секретный ключ и в окне Файл секретного ключа укажите имя секретного ключа и нажмите ОК:

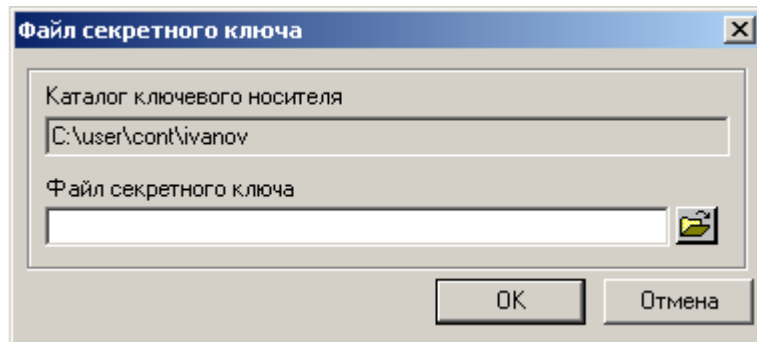


Рисунок 117

На вопрос о задании нового каталога (контейнера) ответьте Yes:

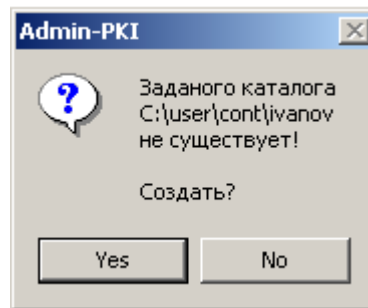


Рисунок 118

Ввести запрашиваемые параметры для сертификата конечного устройства и в поле Файл запроса указать имя файла, в который будет записан запрос на сертификат конечного устройства, и нажать ОК:

Параметры запроса сертификата (версия для тестирования) ? X

☒ Ключи в формате СКЗИ

Каталог ключевого носителя с ключом для формирования запроса
C:\user\cont\ivanov [Folder icon] Секретный ключ

Файл запроса
C:\user\cont\ivanov\request.pem [Folder icon]

Тип запроса
☒ Самоподписанный
☐ Подписанный другим ключом

Каталог ключевого носителя с ключом для подписи запроса
A:\ [Folder icon] Секретный ключ

☐ Сертификат ключа для подписи запроса
[Folder icon]

Кодировка символов в запросе ☐ ANSI ☒ UTF8

Запрашиваемые параметры сертификата

Страна RU (RU для России) [Search...]
Область/Район
Город/Село Moscow
Организация S-Terra
Подразделение devel
Должность
Полное имя Ivanov
E-mail адрес ivanov@s-terra.com

OK Отмена Справка

Рисунок 119

В окне отчета о выполненных операциях нажмите OK:

Admin-PKI X

Процедура генерации ключей СКЗИ и запроса успешно завершена !

Каталог ключевого носителя:
C:\user\cont\ivanov

Файл запроса на сертификат:
C:\user\cont\ivanov\request.pem

Файл запроса необходимо передать на сертификацию.
Работа с новым секретным ключом будет возможна только после получения сертификата.

OK

Рисунок 120

В окне на вопрос о сохранении в буфере обмена запроса на сертификат нажмите Yes:

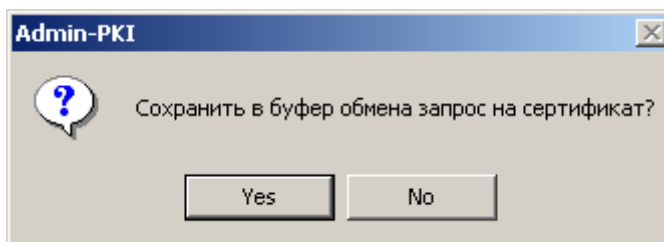


Рисунок 121

На вопрос о передаче запроса на сертификат в Удостоверяющий Центр по E-mail нажмите No:

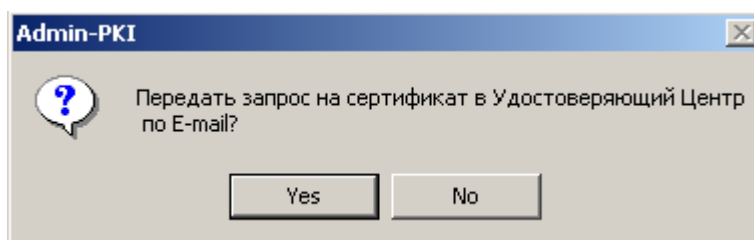


Рисунок 122

На вопрос о передаче запроса на сертификат в Удостоверяющий Центр через Web-интерфейс Удостоверяющего Центра нажмите No:

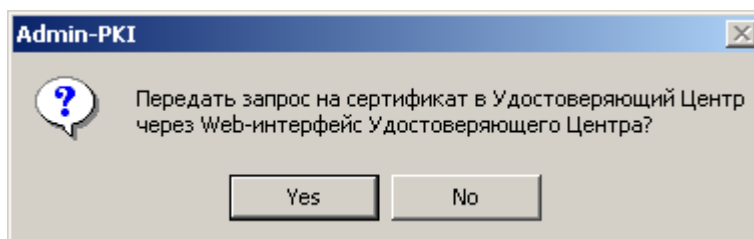


Рисунок 123

На вопрос о распечатке запроса на сертификат нажмите No:

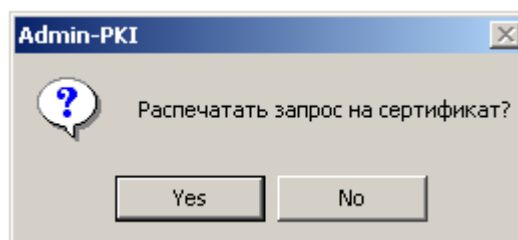


Рисунок 124

После этого Admin-PKI можно закрыть.

Контейнер с ключевой информацией и секретным ключом размещен в указанном Вами каталоге. А запрос на сертификат – в указанном файле. В данном примере:

- каталог контейнера – C:\user\cont\ivanov
- файл запроса на сертификат конечного устройства – C:\user\cont\ivanov\request.pem.

19.3.5. Создание сертификата конечного устройства

Для создания сертификата конечного устройства нужно отослать запрос на сертификат в Удостоверяющий Центр, имеющий CA сертификат, созданный с использованием криптопровайдера Signal-COM CSP. В разделе "[Установка и настройка Удостоверяющего Центра. Создание CA сертификата](#)" мы описали установку и настройку такого УЦ Microsoft Certification Authority и создание для него CA сертификата.

Для отсылки запроса запустите Microsoft Internet Explorer и в поле для ввода URL с префиксом `http://` укажите IP-адрес Удостоверяющего Центра и утилиту `certsrv`. В нашем случае это будет – `http://10.0.34.33/certsrv`.

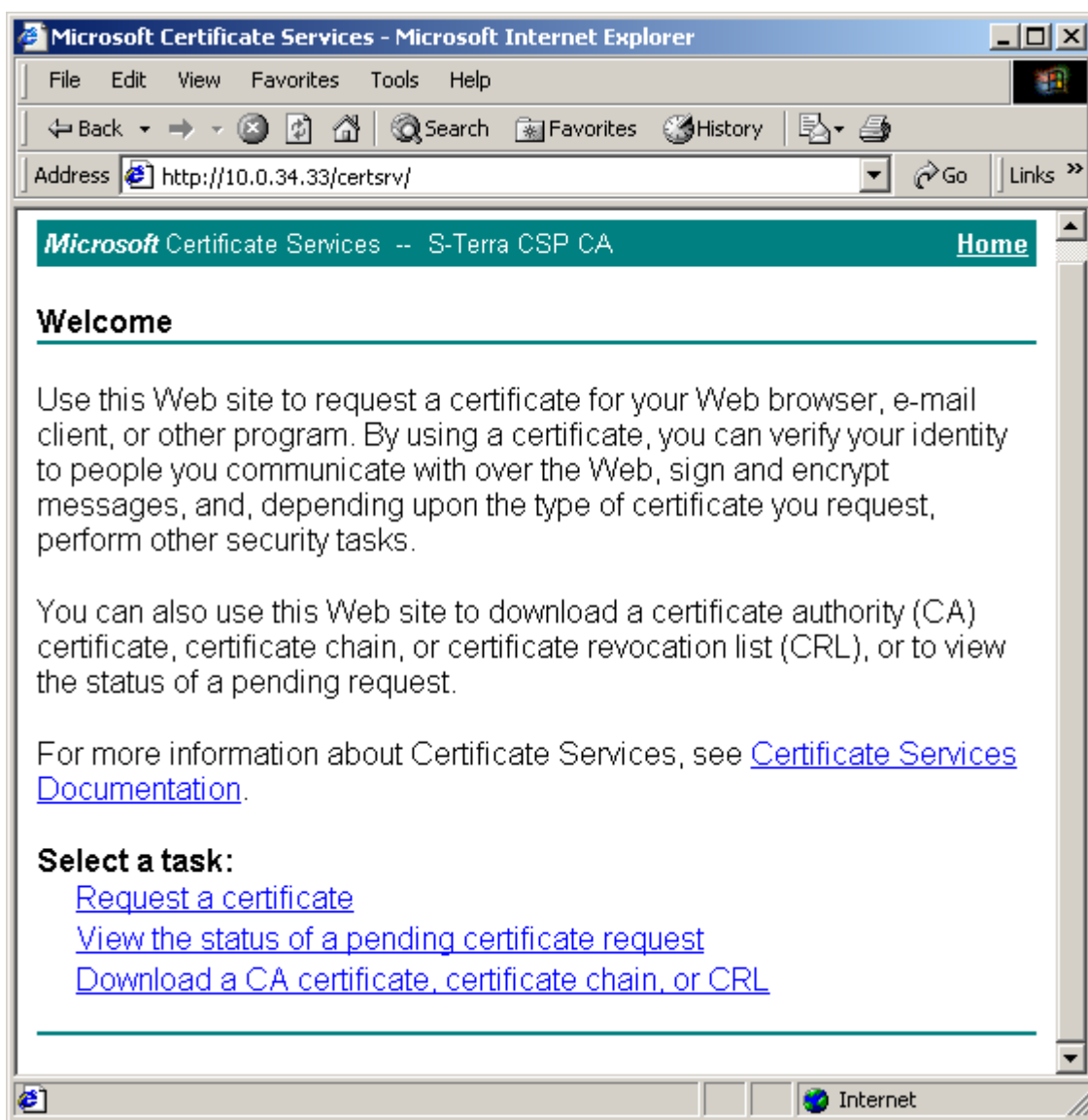


Рисунок 125

В появившемся окне Удостоверяющего Центра выберите задачу –Request a certificate.

Выберите `advanced certificate request` (Рисунок 126):

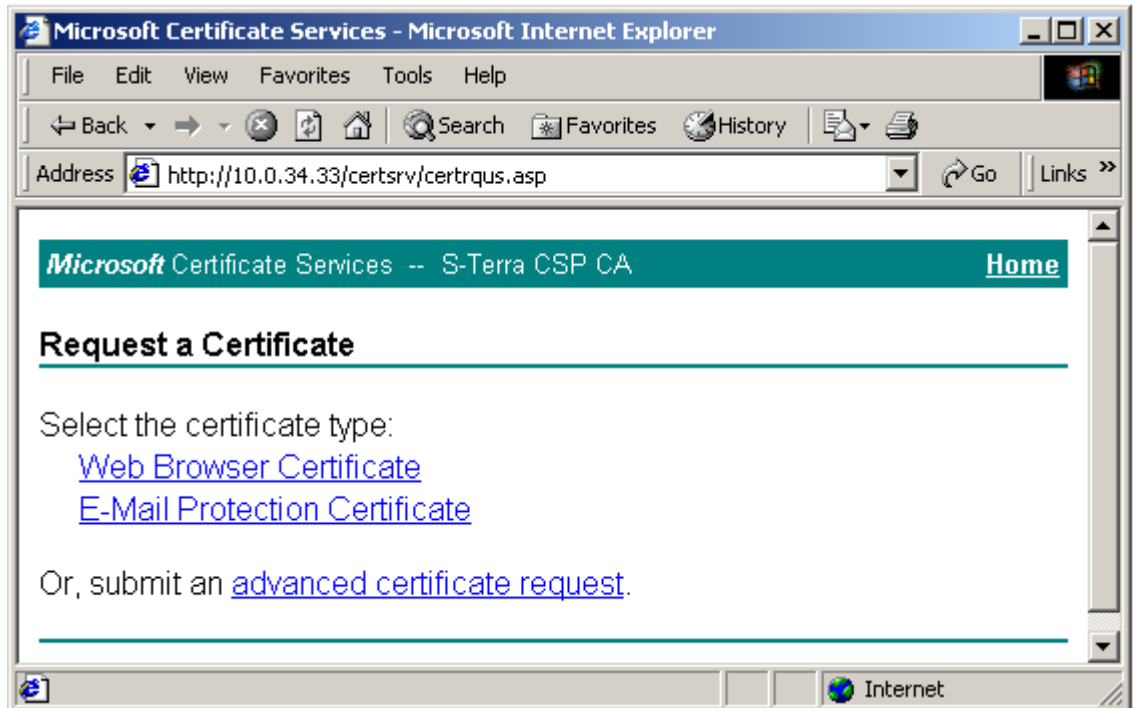


Рисунок 126

Выберите второе предложение `Submit a certificate request...`(Рисунок 127):

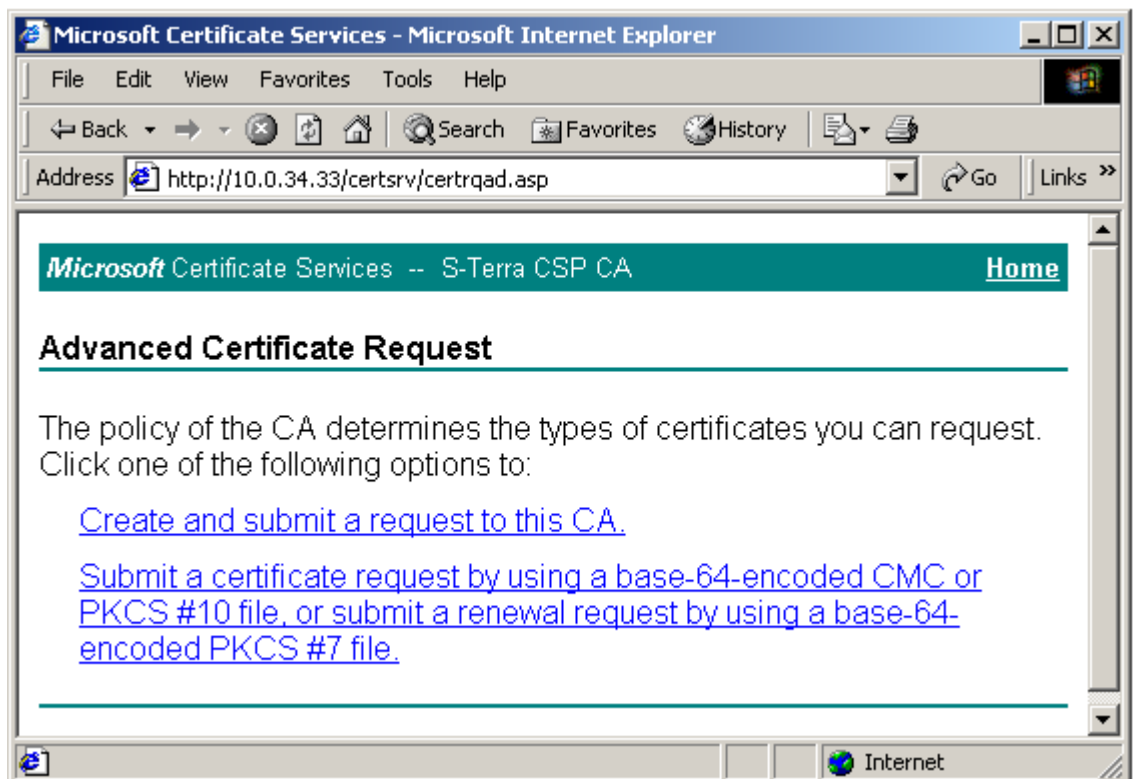


Рисунок 127

Скопируйте из файла запрос на сертификат, описанный и созданный в разделе "[Создание ключевой пары и запроса на сертификат конечного устройства](#)", и вставьте его в поле Saved Request и нажмите Submit (Рисунок 128):

Microsoft Certificate Services -- S-Terra CSP CA [Home](#)

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
jVhXNEFzuGbM5rBF8QXFxvANldxVVfqqC7yHva/W  
z+M2Su3SKUr616AAMA4GCisGAQQBrVkBawIFAANI  
52n03LKQ/aWVqw1A7gRGDaYtJrwCIBIOc1XuY9sq  
PrvNoIqZ  
-----END CERTIFICATE REQUEST-----
```

[Browse for a file to insert.](#)

Additional Attributes:

Attributes:

[Submit >](#)

Рисунок 128

Удостоверяющий Центр издал сертификат конечного устройства по полученному запросу. Выберите формат файла сертификата и нажмите Download CA certificate (Рисунок 129):

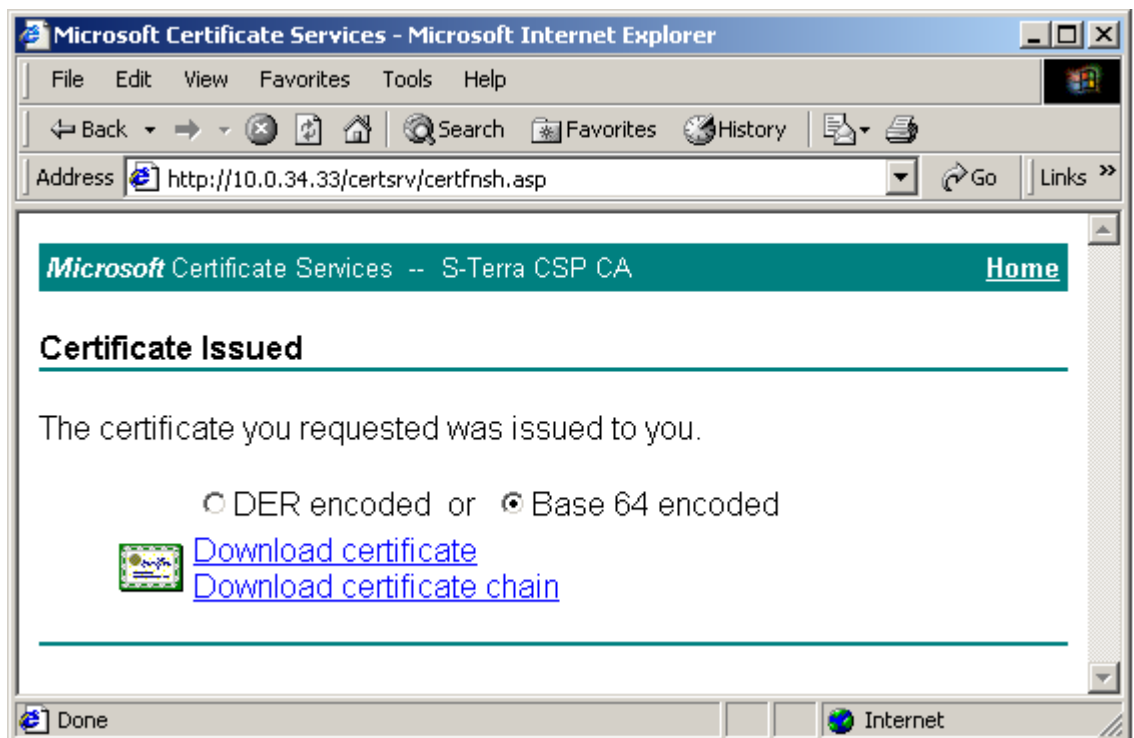


Рисунок 129

Установите переключатель в положение Save this file to disk и нажмите OK:

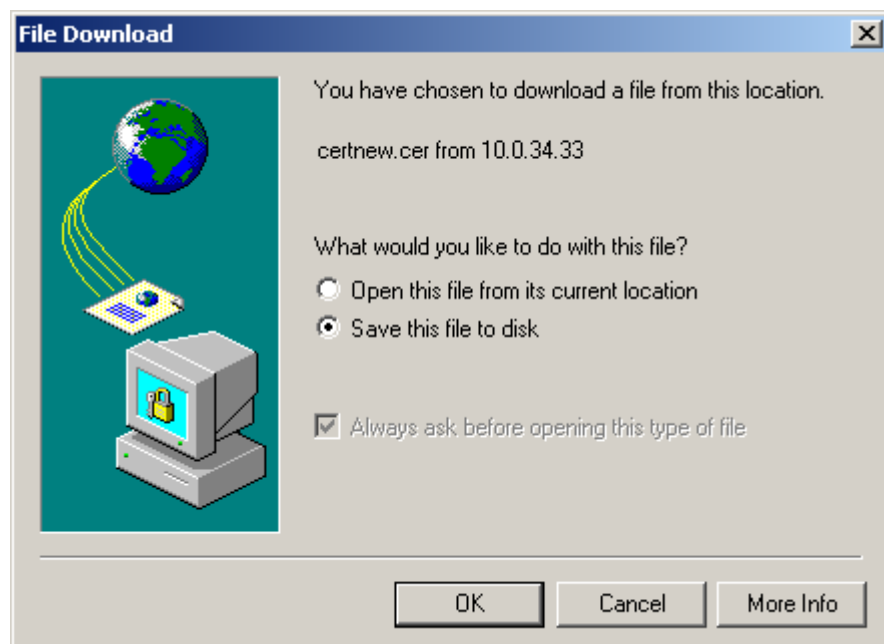


Рисунок 130

Введите имя файла, в который будет записан сертификат конечного устройства и нажмите **Save** (Рисунок 131):

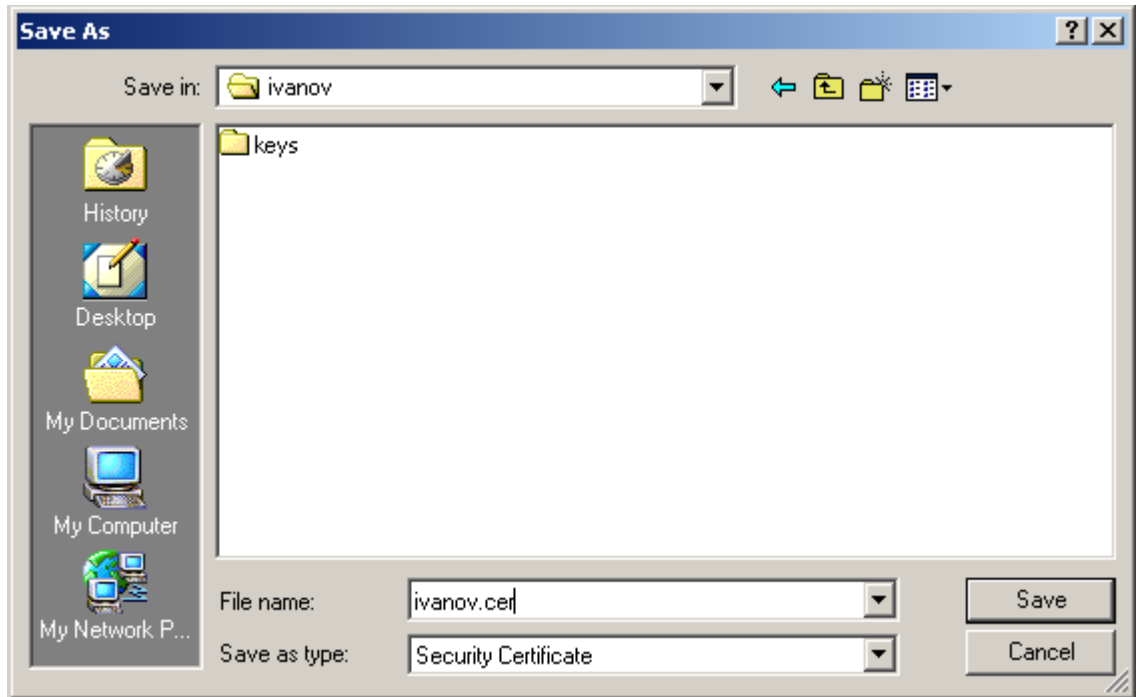


Рисунок 131

В результате всех выполненных действий мы создали СА сертификат и сертификат конечного устройства, и экспортировали их в файлы. Эти сертификаты можно использовать при работе с Продуктами CSP VPN Agent. Секретный ключ сертификата конечного устройства размещен в контейнере – `C:\user\cont\ivanov`. Для удобства и безопасности контейнер с секретным ключом лучше размещать на внешнем ключевом носителе.