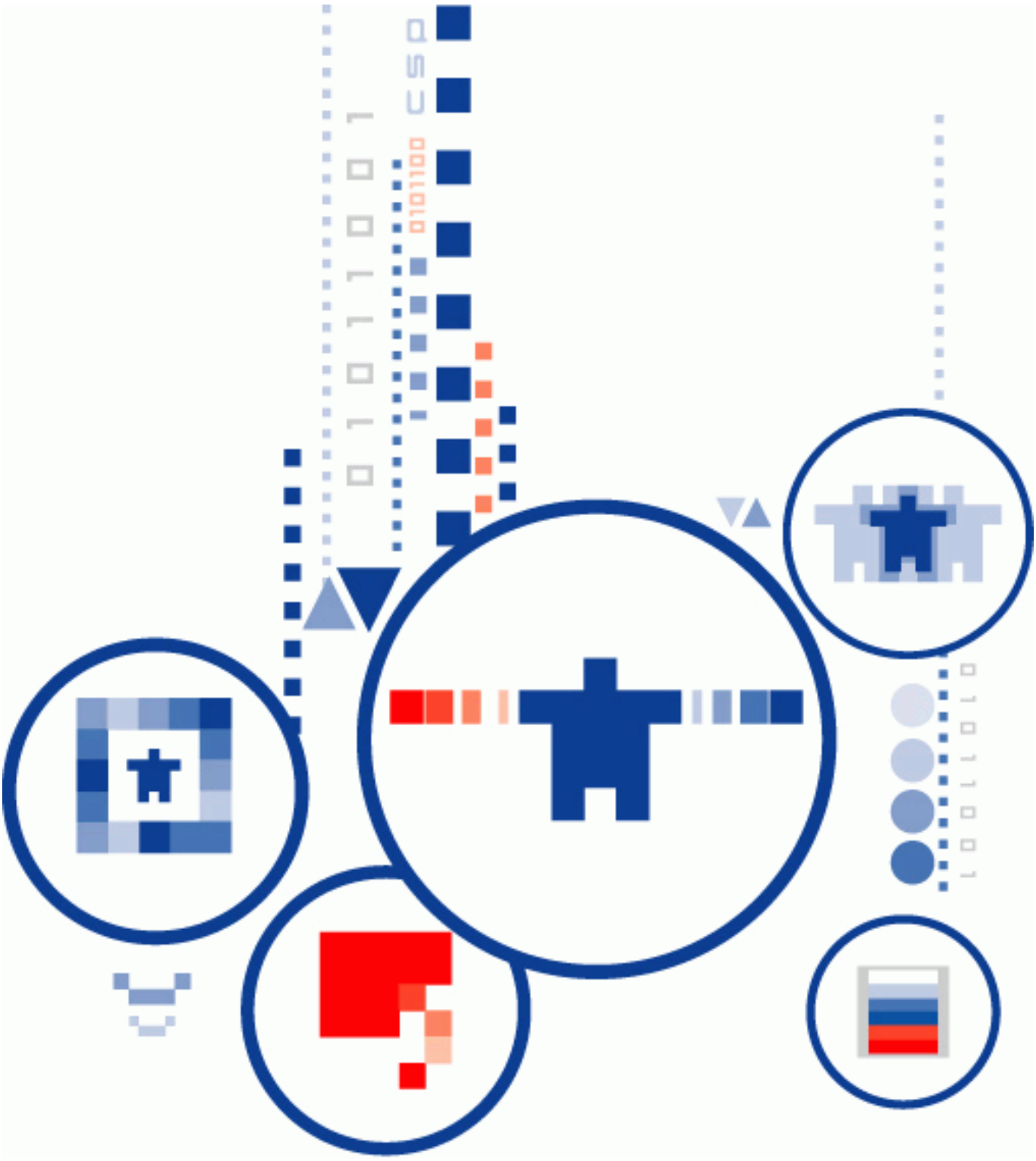
УТВЕРЖДЁН
ЖТЯИ.00074-01 90 02-ЛУ

ЖТЯИ.00074-01 90 02



КриптоПро IPsec

Версия 1.0

Руководство администратора безопасности

АННОТАЦИЯ

Настоящий документ содержит описание особенностей и вариантов использования программного комплекса КриптоПро IPsec, предназначенного для защиты данных передаваемых в IP-сетях.

В настоящем документе описаны особенности применения КриптоПро IPsec для:

- Защиты VPN;
- Защиты соединения site-to-site VPN;
- Организации изоляции домена;

на базе ключевых систем:

- PSK;
- Сертификаты.

Документ предназначен для администраторов как руководство по установке и конфигурации КриптоПро IPsec.

Сценарии пошаговой настройки вариантов использования КриптоПро IPsec, в том числе для МЭ, приводятся в приложении.

Информация о разработчике КриптоПро IPsec:

ООО «КРИПТО-ПРО»,
127018, г. Москва, ул. Сущевский вал, д. 16, стр.5
Телефон: (495) 780-48-20
Факс: (495) 780-48-20
Сайт: www.cryptopro.ru
Почта: info@cryptopro.ru

СОДЕРЖАНИЕ

1. Назначение

КриптоПро IPsec предназначен для обеспечения:

- аутентичности сторон взаимодействия, указанных в политике IPsec (правилах IPsec), при использовании совместно с МЭ;
- конфиденциальности и аутентичности передаваемой по VPN или ЛВС конфиденциальной информации в режиме мандатного шифрования без применения дополнительных МЭ;
- конфиденциальности и аутентичности передаваемой по VPN или ЛВС конфиденциальной информации между некоторыми, выделенными, сторонами взаимодействия при встраивании в состав МЭ или приложений;
- аутентичности сторон голосовых или видеоконференций, в которых нет обмена конфиденциальной информации.

Использование КриптоПро IPsec для обеспечения конфиденциальности голосовых или видеоконференций без проведения дополнительных исследований запрещается.

Встраивание КриптоПро IPsec в МЭ или в другие защищаемые информационные системы должно производиться в соответствии с Положением ПКЗ-2005 организациями, имеющими лицензию на право проведения таких работ.

При встраивании КриптоПро IPsec в прикладные системы необходимо проводить оценку влияния аппаратных, программно-аппаратных и программных средств сети (системы) конфиденциальной связи, совместно с которыми предполагается штатное функционирование СКЗИ, на выполнение предъявленных к СКЗИ требований в следующих случаях:

- Если информация, обрабатываемая СКЗИ, подлежит защите в соответствии с законодательством Российской Федерации;
- При организации защиты информации, обрабатываемой СКЗИ, в федеральных органах исполнительной власти, органах исполнительной власти субъектов Российской Федерации;
- При организации криптографической защиты информации, обрабатываемой СКЗИ, в организациях независимо от их организационно-правовой формы и формы собственности при выполнении ими заказов на поставку товаров, выполнение работ или оказание услуг для государственных нужд.

Указанную оценку необходимо проводить по ТЗ, согласованному с 8 Центром ФСБ России.

2. Требования к системному ПО

КриптоПро IPsec функционирует в следующих ОС:

- Microsoft ® Windows Server ® 2003 архитектуры x86;
- Microsoft Windows XP архитектуры x86;
- Microsoft Windows 7 архитектуры x86 и x64;
- Microsoft Windows Vista ® архитектуры x86 и x64;
- Microsoft Windows Server 2008 x86 и x64;
- Microsoft Windows Server 2008 R2.

КриптоПро IPsec используется совместно с СКЗИ КриптоПро CSP v.3.6, ЖТЯИ.00050-03.

3. Введение

Для защиты данных, передаваемых по открытым каналам связи, принято использовать так называемую технологию защищенного канала, в котором должны быть обеспечены:

- взаимная аутентификация взаимодействующих сторон;
- конфиденциальность передаваемых данных;
- целостность передаваемых данных с защитой от повторов.

Защищенный канал может быть реализован путем организации виртуальной частной сети (Virtual Private Network, VPN). Суть подхода состоит в том, чтобы внутри открытой сети, доступ к которой не ограничен различным категориям пользователей, создать собственную, изолированную, доверенную среду обмена данными. В этой среде смогут работать только допущенные пользователи, а для остальных пользователей трафик защищенного канала будет представлен непонятным набором данных, из которого, без обладания секретной ключевой составляющей (см. Раздел 5 «Ключевая система»), доступной только доверенным пользователям, выделить защищаемую информацию за приемлемое время практически невозможно.

Среди наиболее распространенных VPN протоколов можно выделить L2TP/IPSec и SSTP. Не рекомендуется использовать протокол PPTP для защиты сети, т.к., на сегодняшний день, он не отвечает минимальным требованиям безопасности.

КриптоПро IPsec позволяет создавать защищенные каналы передачи данных в IP-сетях с использованием шифрования. В зависимости от решаемых задач, данный продукт может быть использован в составе уже имеющихся решений, в новой инфраструктуре, на отдельных машинах или в составе всех защищаемых объектов сети. КриптоПро IPsec предназначен для установки на сетевые объекты, такие как межсетевые экраны, сервера удаленного доступа, контроллеры домена, а также на компьютеры пользователей домена и удаленных пользователей, которые работают под управлением поддерживаемых ОС (см. Раздел 2 «Требования к системному ПО»).

Возможно применение КриптоПро IPsec в 3-х базовых сценариях:

- «точка-сеть» («точка-точка», «подключение удаленного доступа», «client-to-site»), когда клиент подключается к серверу удаленного доступа, связь между которым и локальной сетью назначения идет через сеть общего доступа (см. Рисунок 1, Рисунок 2);
- «сеть-сеть» («маршрутизатор-маршрутизатор», «site-to-site»), когда две (или более) доверенные сети обмениваются внутренними данными через общедоступную, сеть (например, «Интернет»), но при этом риск, связанный с нарушением конфиденциальности передаваемых данных, их подмены, искажения сводится к допустимому минимуму (см. Рисунок 3, Рисунок 4);
- «изоляция группы» компьютеров или всего домена в локальной сети (см. Рисунок 5).

VPN-подключение типа «точка-сеть» дает пользователям возможность получать доступ к сетевым ресурсам своей организации с использованием общедоступной сети передачи данных. При этом, реальная инфраструктура общедоступной сети не имеет никакого значения, так как передача данных организована подобно тому, как если бы они передавались по выделенному (т.е. недоступному посторонним лицам, частному) каналу (см. Рисунок 1, Рисунок 2).

Рисунок 1 Client-to-Site

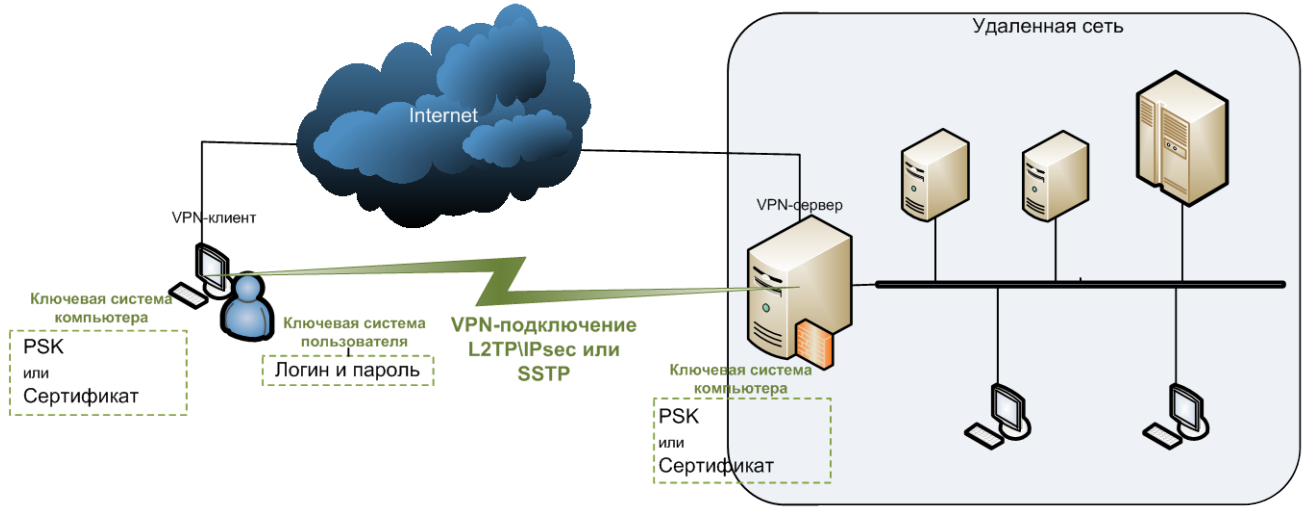
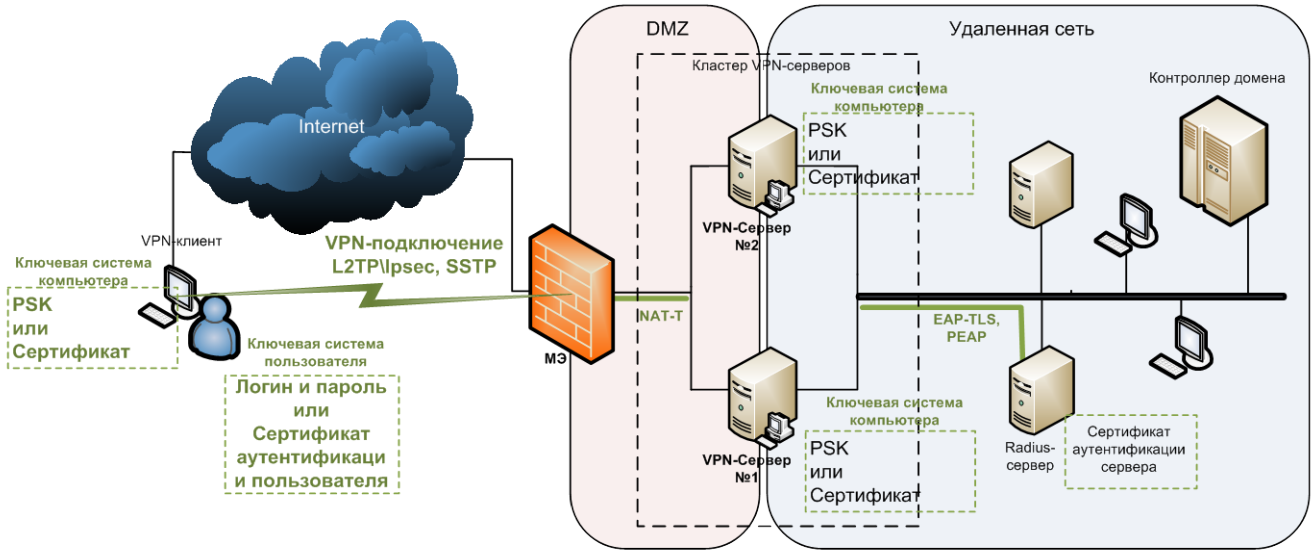


Рисунок 2 Client-to-Site 2



При соединении типа «сеть-сеть» протоколы безопасности применяются только к пакетам, выходящим из локальной сети, и прекращают свое действие при входе пакета в другую удаленную локальную сеть, т.е. внутри локальных сетей пакеты не защищены (не зашифрованы, не содержат данных для проверки целостности). При таком соединении один VPN-сервер обеспечивает маршрутизируемое подключение к сети, к которой прикреплен другой VPN-сервер. Сервер, инициирующий VPN-соединение, т.е. по сути VPN-клиент, проходит проверку подлинности на отвечающем сервере (VPN-сервере), а затем уже отвечающий сервер проходит проверку подлинности на вызывающем сервере с целью обеспечения взаимной проверки подлинности взаимодействующих сторон (см. Рисунок 3, Рисунок 4).

Рисунок 3 Site-to-Site

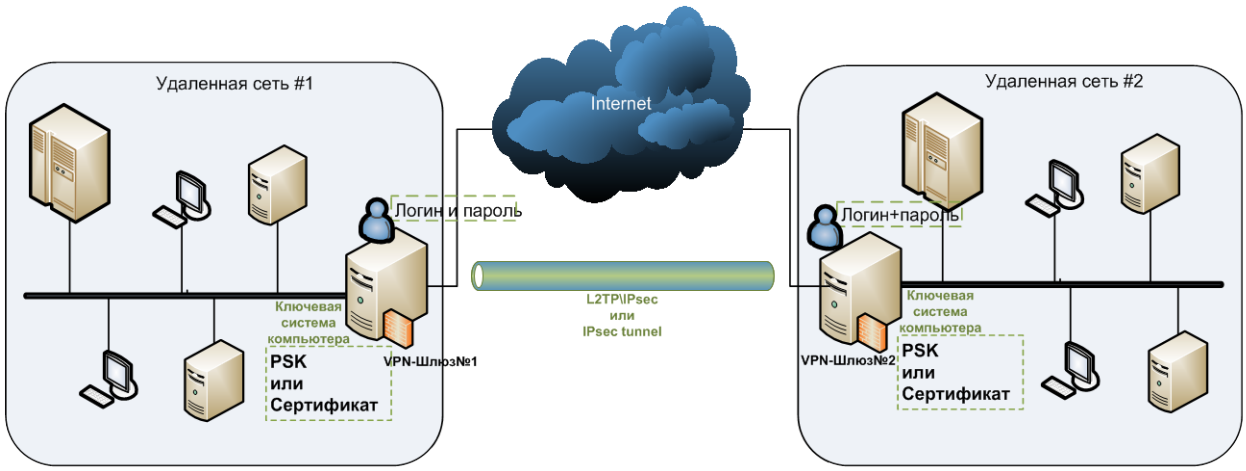
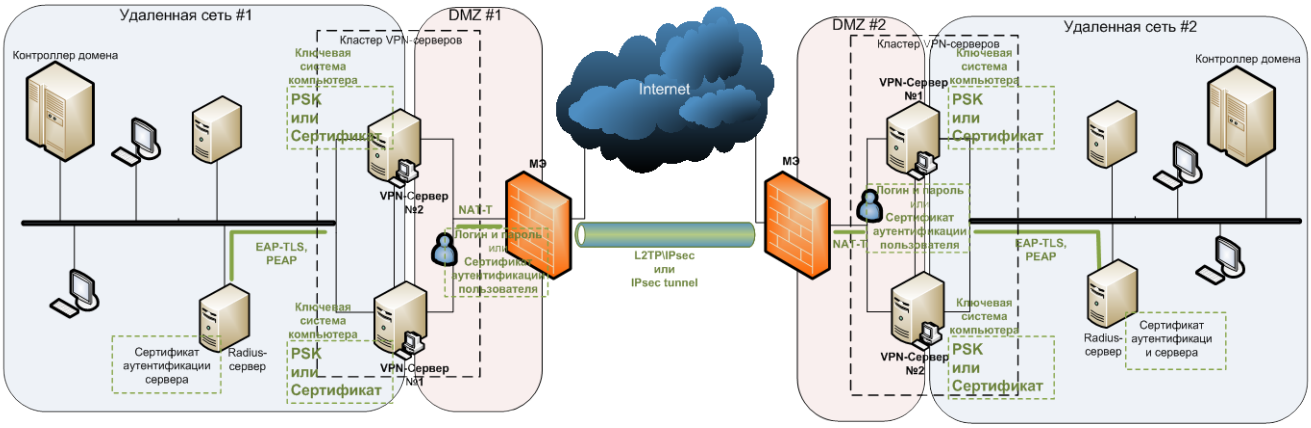
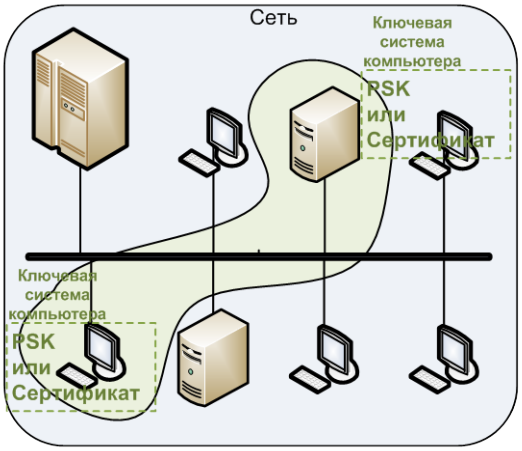


Рисунок 4 Site-to-Site 2



Кроме того, КриптоПро IPsec поддерживает **Правила** и **Политики IPsec**, что позволяет сегментировать локальную сеть на изолированные логические сети с разными уровнями безопасности. Можно в имеющейся физической сети создать логическую, в которой компьютеры будут использовать общий набор правил и политик безопасного обмена данными (см. Рисунок 5).

Рисунок 5 Политики и правила IP-безопасности



С точки зрения правила, любой IP пакет, подходящий по совокупности критериев (фильтров) к данному правилу, должен быть обработан. Есть 3 варианта обработки: применить IPsec к пакету, заблокировать или пропустить пакет. Таким образом, существует возможность управлять тем или иным типом трафика с помощью настройки правил, что в результате позволяет защищать с помощью IPsec необходимый диапазон IP пакетов.

Перечисленные выше сценарии применения КриптоПро IPsec основаны на низкоуровневом («сетевой уровень» №3 модели OSI) протоколе IPsec. Что исключает необходимость внесения изменений в топологию сети и в существующие приложения.

IPsec можно условно разделить на три группы протоколов. Первая, **IKE**, отвечает за согласование параметров и выработку ключевой информации, работает в режиме пользователя на транспортном уровне, использует для транспорта протокол UDP порт 500 (4500 в случае NAT-Traversal). Вторая группа, протоколы **ESP** и **AH**, обеспечивает защиту непосредственно передаваемых данных, на основе параметров и ключей, полученных на этапе работы IKE, работает в режиме ядра на сетевом уровне. Протокол IKE содержит две фазы работы. **Фаза 1** предназначена для организации основы для дальнейшего взаимодействия, она согласует параметры работы протокола IKE, вырабатывает ключевой материал криптографической защиты данных вложений и обеспечивает аутентификацию сторон (основанием подлинности может быть сертификат или PSK, см ниже). После того как стороны подтвердили свою подлинность, фаза 1 считается завершенной. **Фаза 2** создается на основе фазы 1 и предназначена для выработки согласованных параметров и новой ключевой информации для протоколов ESP и AH, завершается созданием IPsec SA. На основе одной фазы 1, может быть создано несколько фаз 2. Одна успешно завершенная фаза 2 создает, по умолчанию, две IPsec SA (для входящих и исходящих пакетов), они содержат весь необходимый набор правил и криптографических ключей для обработки пакетов в рамках протоколов ESP и AH. Третья группа протоколов **L2TP** и EAP-TLS, PEAP обеспечивает контроль регламента подключаемого к сети клиента (пользователя).

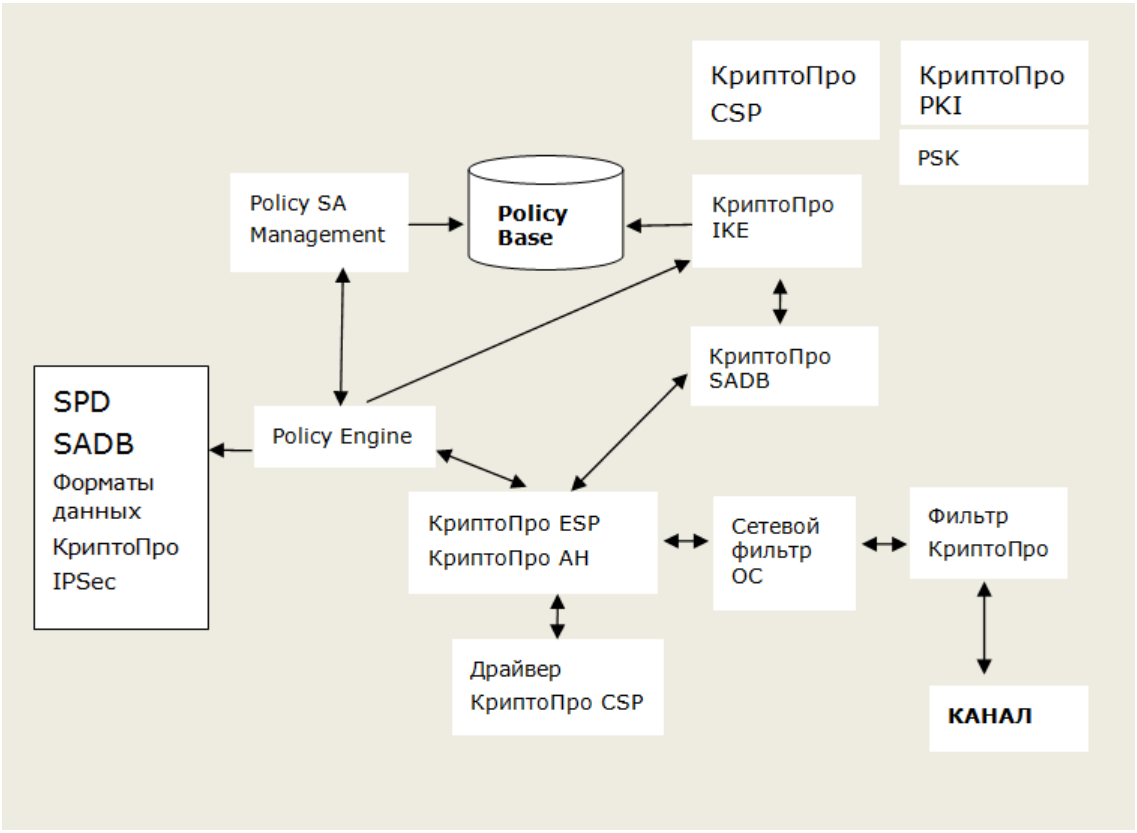
Соединение по IPsec — это безопасное соединение типа точка-точка. Поэтому для установки соединения по IPsec между любыми двумя участниками должны быть успешно пройдены IKE фазы 1 и 2 для выработки актуальных IPsec SA. После этого, фаза 1 переходит в режим ожидания, фаза 2 считается завершенной и освобождается с появлением IPsec SA. Пока IPsec SA актуальны, соединение по IPsec может быть использовано. С течением времени и трафика, IPsec SA могут утратить актуальность (ключи требуют периодического обновление), обновление IPsec SA происходит автоматически при повторном прохождении новой IKE фазы 2 или полного цикла 1 и 2 фазы IKE, аналогичного начальному. При появлении нового участника в обмене, каждый должен установить с ним отдельное соединение по IPsec, описанным выше образом.

Важно помнить, что соединение по IPsec является инструментом защиты канала, как только канал установлен, дальнейшая логика работы в канале зависит от используемых приложений и протоколов транспортного и других уровней взаимодействия.

4. Структура

Структуру КриптоПро IPsec следует представлять как надстройку над механизмами реализации IPsec в ОС. Рисунок 6 изображает схему взаимодействия компонентов КриптоПро IPsec с компонентами ОС. Все компоненты, за исключением фильтра КриптоПро, встроены в реализацию IPsec ОС и обеспечивают выполнение расширенного функционала. Фильтр КриптоПро находится на канальном уровне и обеспечивает дополнительный контроль корректности применения шифрования. В случае применения режима мандатного шифрования фильтр также обеспечивает блокировку выхода в канал всех незашифрованных пакетов (исключением являются пакеты базовых сетевых служб, таких как DHCP, DNS, а также пакеты IKE и UDP порт 4500 для работы IPsec в режиме NAT-Traversal).

Рисунок 6 Схема взаимодействия компонентов КриптоПро IPsec и ОС



5. Ключевая система

Под ключевой системой КриптоПро IPsec понимается совокупность данных, необходимых для аутентификации участника, устанавливающего соединение по IPsec. В это понятие входит: сертификаты компьютера и пользователя, PSK, имя пользователя и пароль. Ключевая система в зависимости от вариантов использования может представлять собой ограниченный набор, например, только сертификат компьютера или только PSK. Для корректного функционирования ключевой системы требуется обеспечить каждому участника обмена соответствующие механизмы получения, хранения, обновления, исключения, удаления ключевого материала. Для сертификатов это обеспечивается внедренной инфраструктурой открытых ключей. Для PSK — утилита genpsk и организационные методы. Для имени пользователя и пароля — администрирование учетных записей пользователей в ОС.

Использование того или иного варианта ключевой системы зависит от выбора реализуемого варианта использования. Следует различать сертификат компьютера и пользователя. Пользователь аутентифицируется по **UPN** из Расширения сертификата Subject Alternative Name (SAN) – OID 2.5.29.17, а компьютер по **DNS-имени.**

Вариант использования VPN предполагает несколько вариантов ключевых систем. Первый вариант (рекомендуется): наличие сертификата компьютера и сертификата пользователя, допустимо объединение сертификатов в один сертификат двойного назначения компьютера-пользователя. Сертификат компьютера необходим для аутентификации в рамках IKE, сертификат пользователя для аутентификации пользователя на удаленном сервере. В этом варианте, серверу необходимо иметь только сертификат компьютера. При этом инфраструктура открытых ключей (ИОК) должна находиться как внутри сети, так и снаружи. Второй вариант (возможен): использование PSK и учетной записи пользователя (символьные имя пользователя и пароль). В этом случае, PSK используется для аутентификации в рамках IKE, имя пользователя и пароль для аутентификации пользователя на удаленном сервере. В случае использования PSK для аутентификации машин пользователя в рамках IKE, требуются дополнительные организационные меры защиты в случае стационарных компьютеров. В случае мобильных компьютеров, данный вариант не рекомендуется к использованию, ввиду повышенной вероятности компрометации PSK.

Вариант использования Site-to-site VPN предполагает использование PSK и учетных записей серверов (символьные имя пользователя и пароль). Так как данный вариант использует соединение по IPsec исключительно между серверами, то, как правило, не требуются дополнительные организационные меры по предотвращению НСД, и сервера находятся в оперативном доступе администратора. Таким образом, достаточно пройти процедуру аутентификации по PSK в рамках IKE и аутентификацию по имени пользователя и паролю сервера инициатора на удаленном сервере. Ввиду обоснованной простоты, данная ключевая система рекомендуется к использованию при Site-to-site VPN.

Вариант использования Изоляция домена предполагает использование инфраструктуры открытых ключей внутри домена. В этом варианте, все участники домена должны иметь сертификат компьютера для аутентификации в рамках IKE, аутентификация в домене происходит штатными средствами данного домена и не включается в требования к ключевой системе КриптоПро IPsec.

5.1. Pre-Shared Key

Генерация, распространение, плановая схема и действия при компрометации PSK определяются установленным регламентом.

Для генерации КриптоПро PSK применяется утилита Genpsk. Утилита реализована в виде исполняемого файла «genpsk.exe». Для ее запуска, после установки КриптоПро IPsec, необходимо выполнить следующую команду:

[путь]genpsk [<команда> [<опции>]]

-путь – путь к месторасположению программы (по умолчанию "%Program-Files%\Crypto Pro\IPsec\");

-genpsk – имя исполняемого файла;

-команда – одна из допустимых команд:

-f GenPSK – генерация PSK;

-f CreateBasePSK – генерация закрытого ключа;

-f DeleteBasePSK – удаление закрытого ключа;

-f chkpsk – проверка PSK;

-опции – параметры команды;

Для формирования PSK запуск утилиты производится с параметром **-f GenPSK**:

[-f GenPSK] [-n <PSKId>] [-D <NetName>] [-d <FilePath>] [-v <Version>] [-P <PrintType>] [-S <on/off>] [-m <PSK time to live>] [-N <Statoins List>]

-n <PSKId> -Идентификатор PSK

-D <NetName> -Имя сети связи (направления связи). Кроме того, используется как заголовок при печати ключей

-d <FilePath> -Путь к файлам результирующих списков ключей. Должен завершаться символом '/'. полные имена файлов: FilePath|NetName_0, FilePath|NetName_1. Если отсутствует, то печать в файлы не производится

-v <Version> -Версия PSK. Если не задан, то в качестве версии используется случайное число

-P <PrintType> -Форма вывода на печать:

- по признаку "Net" осуществляется печать PSK в двух частях;
- по признаку "CMAK" - единым массивом.

-S <on/off> -Если установлен, то производится выдача на экран

-m <PSK time to live> **-**Срок действия PSK в месяцах (не более 6 месяцев)

-N <Statoins List> **-**Список узлов связи

Пример:

genpsk -D TestNet -n 02.06.11 -v 2 -m 6 -f GenPSK -P CMAK -S -N ForOffice ForClient

02.06.11,ForOffice,FPH90HEKY2WDWPR1W2VLAZD603C1

02.06.11,ForClient,UKUX0QYGM52EPPEPG5HZ09URUU41

PSK действительны до 01.12.11

Для создания PSK может быть использован контейнер закрытого ключа. Применение контейнер упрощает генерацию и сохраняет возможность расширения списка PSK без перегенерации всех PSK.

[-f GenPSK] [-n <PSKId>] [-D <NetName>] [-d <FilePath>] [-v <Version>] [-P <PrintType>] [-S <on/off>] [-m <time to live>] [-k <Container>] [-p <PIN>] [-N <Statoins List>]

-k <Container> -Имя ключевого контейнера, использующегося как хранилище ключа

-p <PIN> -Пароль (PIN) на ключевой контейнер

Пример:

genpsk -D TestNet -n 02.06.11 -f GenPSK -k MainCont -p 123456 -m 6 -P CMAK -S -N ForOffice ForClient

02.06.11,ForOffice,DH8BPT8XA40HYCX8FXPM87FWRM5H
02.06.11,ForClient,GAAYM6ETF10ZUC2Z9LQFWRVD3TBH

PSK действительны до 01.12.11

Для создания контейнера закрытого ключа, Genpsk запускается с параметром **–f CreateBasePSK:**

[-f CreateBasePSK] [-k <Container>] [-p <PIN>] [-m <time to live>]

-k <Container> - Имя ключевого контейнера, использующегося как хранилище ключа;

-p <PIN> -Пароль (PIN) на ключевой контейнер;

Пример:

genpsk -D TestNet -n 02.06.11 -f CreateBasePSK -k MainCont -p 123456 -m 6

Для удаления контейнера закрытого ключа, Genpsk запускается с параметром **–f DeleteBasePSK**

[-f DeleteBasePSK] [-k <Container>] [-p <PIN>] [-m <time to live>]

Пример:

genpsk -f DeleteBasePSK -k MainCont -p 123456

Для проверки PSK Genpsk нужно запустить с параметром **–f chkpsk**

[-f chkpsk] [-n <PSKId>] [-D <NetName>] [-v <Version>] [-K < checking PSK>] [-N <Statoins List>]

-K < checking PSK> **-**Значение проверяемого PSK;

Пример:

genpsk -n 02.06.11 -D TestNet -v 2 -f chkpsk -K FPH90HEKY2WDWPR1W2VLAZD603C1 -N ForOffice

PSK FPH90HEKY2WDWPR1W2VLAZD603C1 OK, TTL_EXPIRED: UTC Fri Dec 01 00:00:00 2011

5.2. Сертификаты открытого ключа

Запрос, выпуск, распространение, плановая схема сертификатов и действия при компрометации определяются установленными регламентами ИОК (УЦ) в ИС.

Все сертификаты должны соответствовать стандарту X.509, кроме того, в зависимости от назначения к сертификату предъявляются дополнительные требования.

Сертификаты IPsec (аутентификация компьютера в IKE) должны удовлетворять следующим требованиям:

- находиться в личном хранилище **компьютера** с привязкой к закрытому ключу (см. Рисунок 7);

- быть действительными (см. Рисунок 8);
- содержать назначение «**IKE-посредник IP-безопасности**» (1.3.6.1.5.5.8.2.2) (см. Рисунок 9);
- содержать назначение ключа («Key Usage» OID 2.5.29.15) «Цифровая подпись» (см. Рисунок 10);
- содержать открытый ключ ГОСТ Р 34.10-2001, для которого имеется соответствующий контейнер закрытого ключа **компьютера** с кэшированным паролем или без пароля (см. Рисунок 11);
- содержать **«Дополнительное имя субъекта»** (2.5.29.17) -> DNS со значением FQDN (Fully Qualified Domain Name) компьютера.

Сертификаты могут применяться при проверке подлинности **пользователя** в VPN-подключениях, с использованием протоколов EAP-TLS, PEAP. В зависимости от типа проверки подлинности, настроенного для метода проверки подлинности, сертификаты используются для проверки подлинности клиента и сервера или только сервера.

Сертификаты аутентификации клиента должны удовлетворять следующим требованиям:

- находиться в личном хранилище **пользователя** с привязкой к закрытому ключу;
- быть действительными;
- содержать назначение **«Проверка подлинности клиента»** (1.3.6.1.5.5.7.3.2);
- содержать назначение ключа («Key Usage» OID 2.5.29.15) «Цифровая подпись» (см. Рисунок 10);
- содержать открытый ключ ГОСТ Р 34.10-2001, для которого имеется соответствующий контейнер закрытого ключа **пользователя** с кэшированным паролем или без пароля;
- содержать расширение **«Дополнительное имя субъекта»** (2.5.29.17) со значением основного имени пользователя (UPN, User Principal Name) (см Рисунок 12).

Сертификаты аутентификации сервера должны удовлетворять следующим требованиям:

- находиться в личном хранилище **компьютера** с привязкой к закрытому ключу компьютера;
- быть действительны;
- содержать назначение **«Проверка подлинности сервера»** (1.3.6.1.5.5.7.3.1);
- содержать назначение ключа («Key Usage» OID 2.5.29.15) «Цифровая подпись» (см. Рисунок 10);
- содержать открытый ключ ГОСТ Р 34.10-2001, для которого имеется соответствующий контейнер закрытого ключа **компьютера** с кэшированным паролем или без пароля;
- содержать расширение **«Общее имя»** (2.5.4.3) или **«Дополнительное имя субъекта»** (2.5.29.17) -> DNS со значением FQDN (Fully Qualified Domain Name) сервера (см. Рисунок 13) .

Возможно использование смарт-карт для хранения ключей аутентификации пользователя.

Сертификаты аутентификации по смарт-карте должны удовлетворять следующим требованиям:

- находиться в контейнере по умолчанию на одной из поддерживаемых КриптоПро CSP смарт-карте подключенной к поддерживаемому считывателю;
- быть действительны;
- содержать назначение **«Вход со смарт-картой»** (1.3.6.1.4.1.311.20.2.2.);

- содержать назначение ключа («Key Usage» OID 2.5.29.15) «Цифровая подпись» (см. Рисунок 10);
- содержать открытый ключ ГОСТ Р 34.10-2001;
- содержать расширение **«Дополнительное имя субъекта»** (2.5.29.17) со значением UPN пользователя.

При использовании одного сертификат для разных назначений требования к нему совмещаются.

Рисунок 7 Сертификат в личном хранилище компьютера

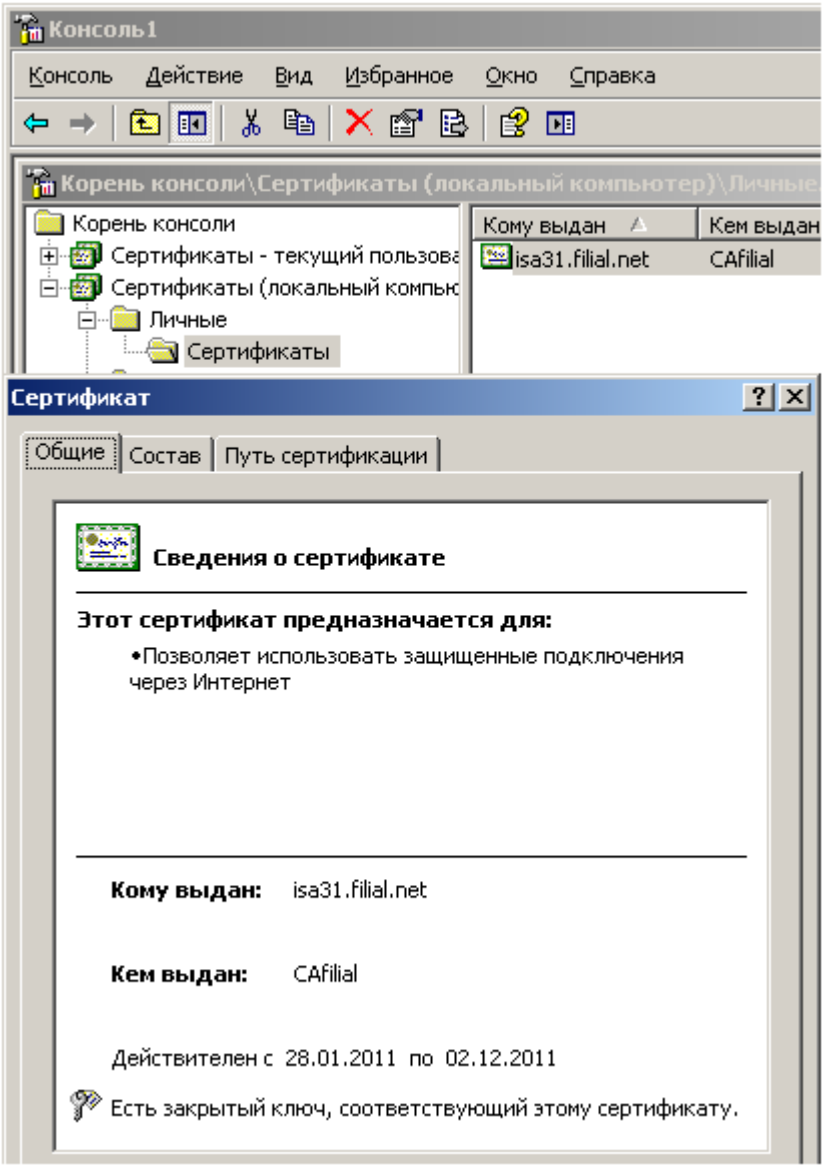


Рисунок 8 Действительный сертификат

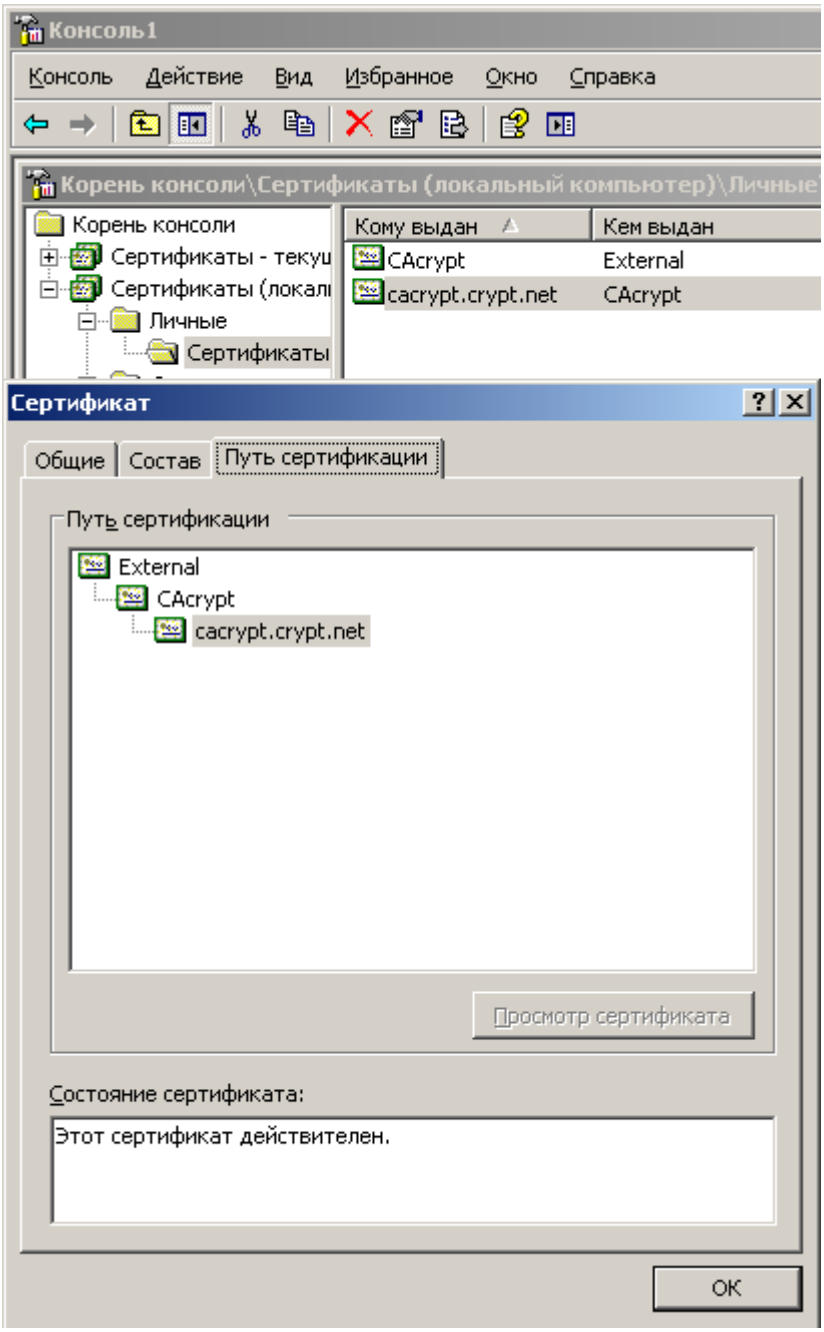


Рисунок 9 Сертификата IPsec «Улучшенный ключ»

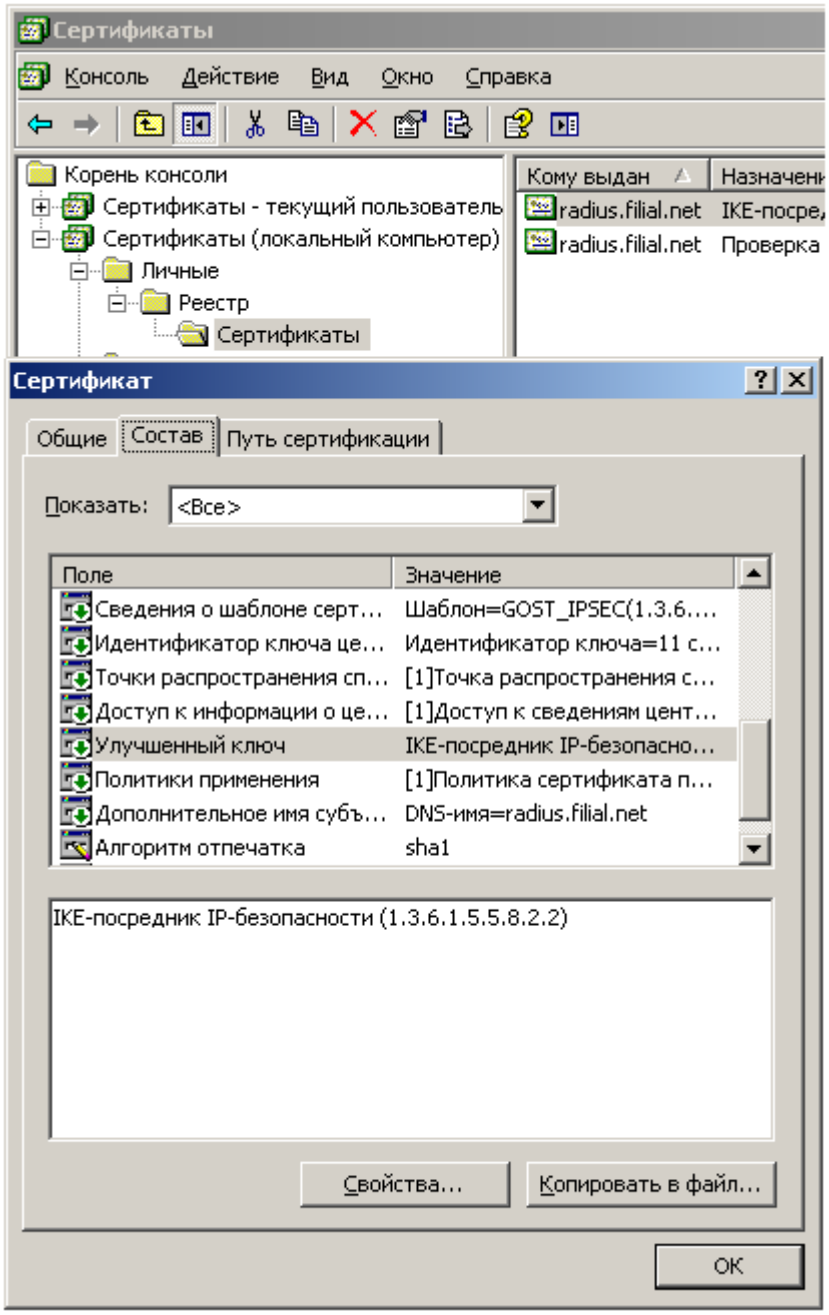


Рисунок 10 Сертификата IPsec «Использование ключа»

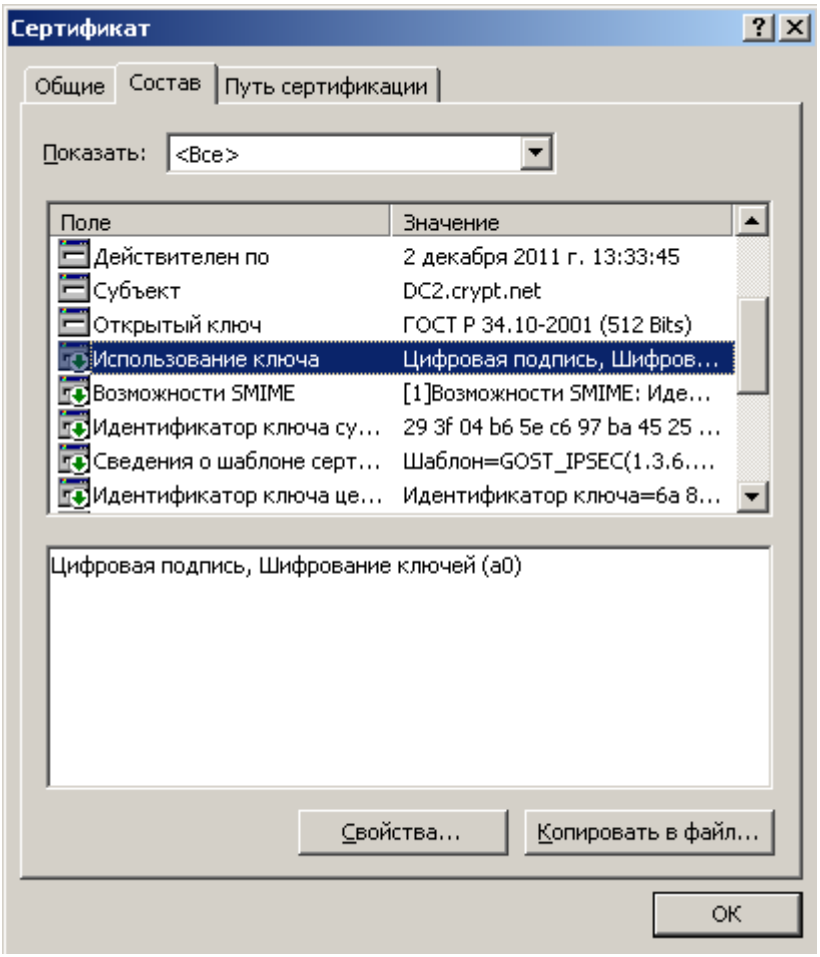


Рисунок 11 Кэширование пароля на контейнер закрытого ключа

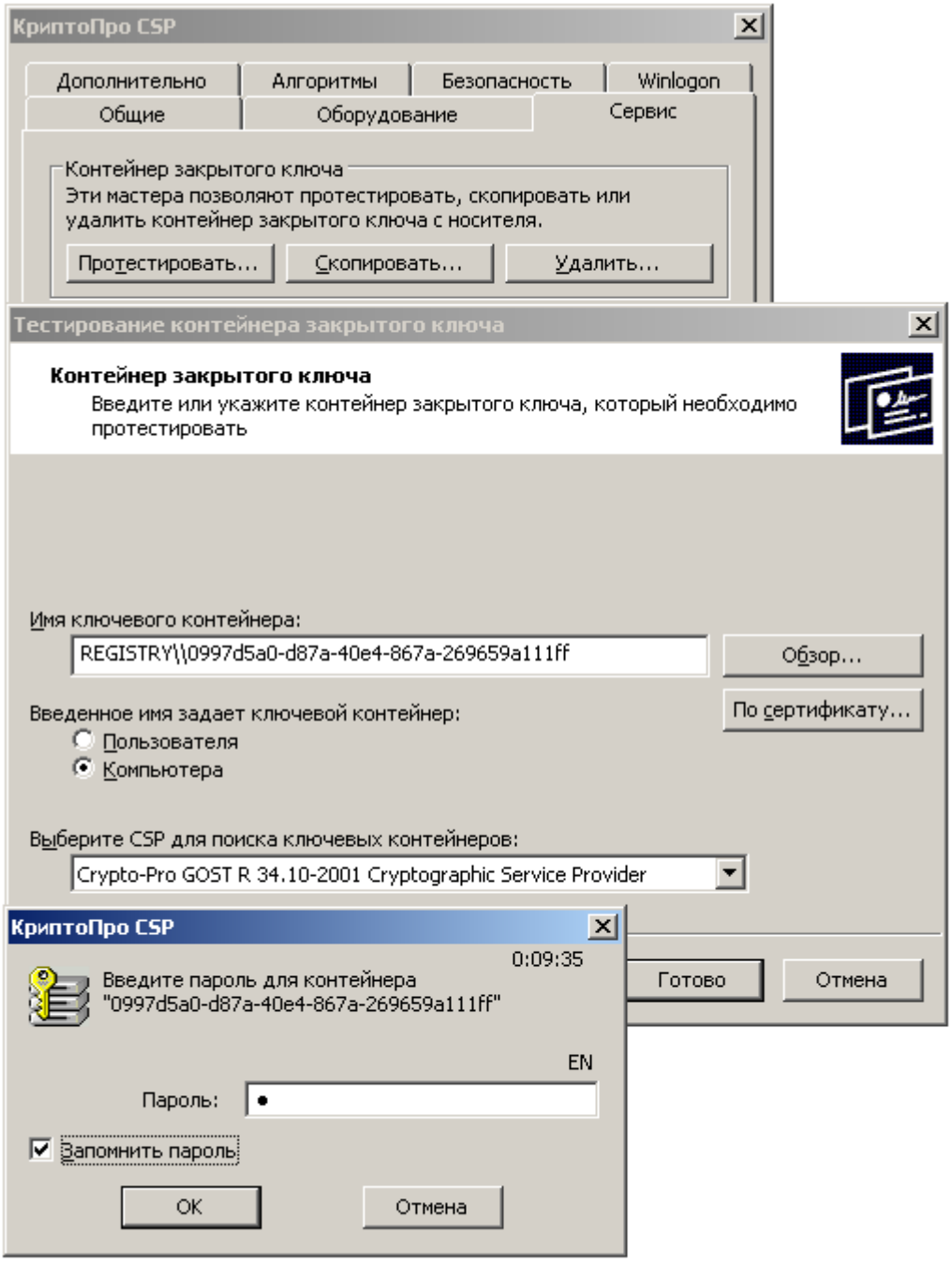


Рисунок 12 Сертификат клиента «Дополнительное имя субъекта»

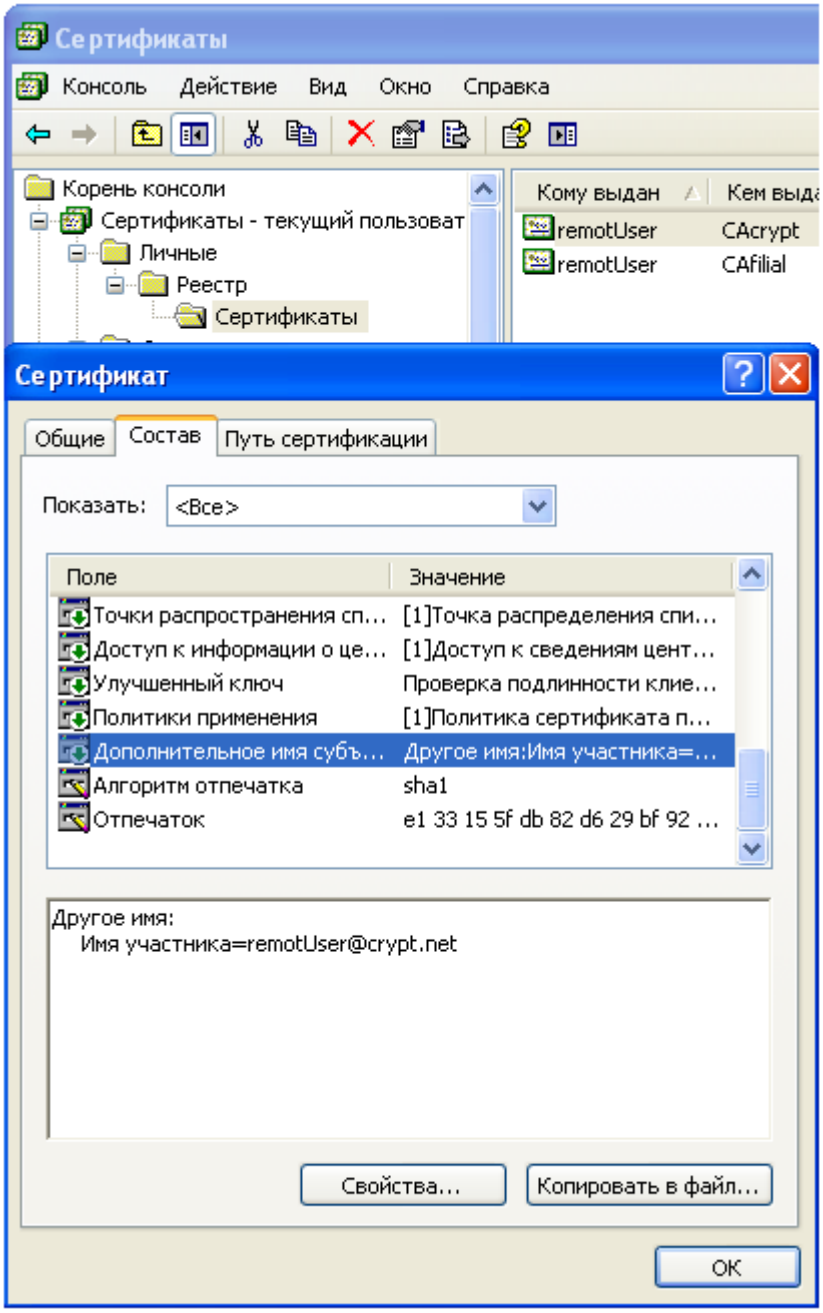
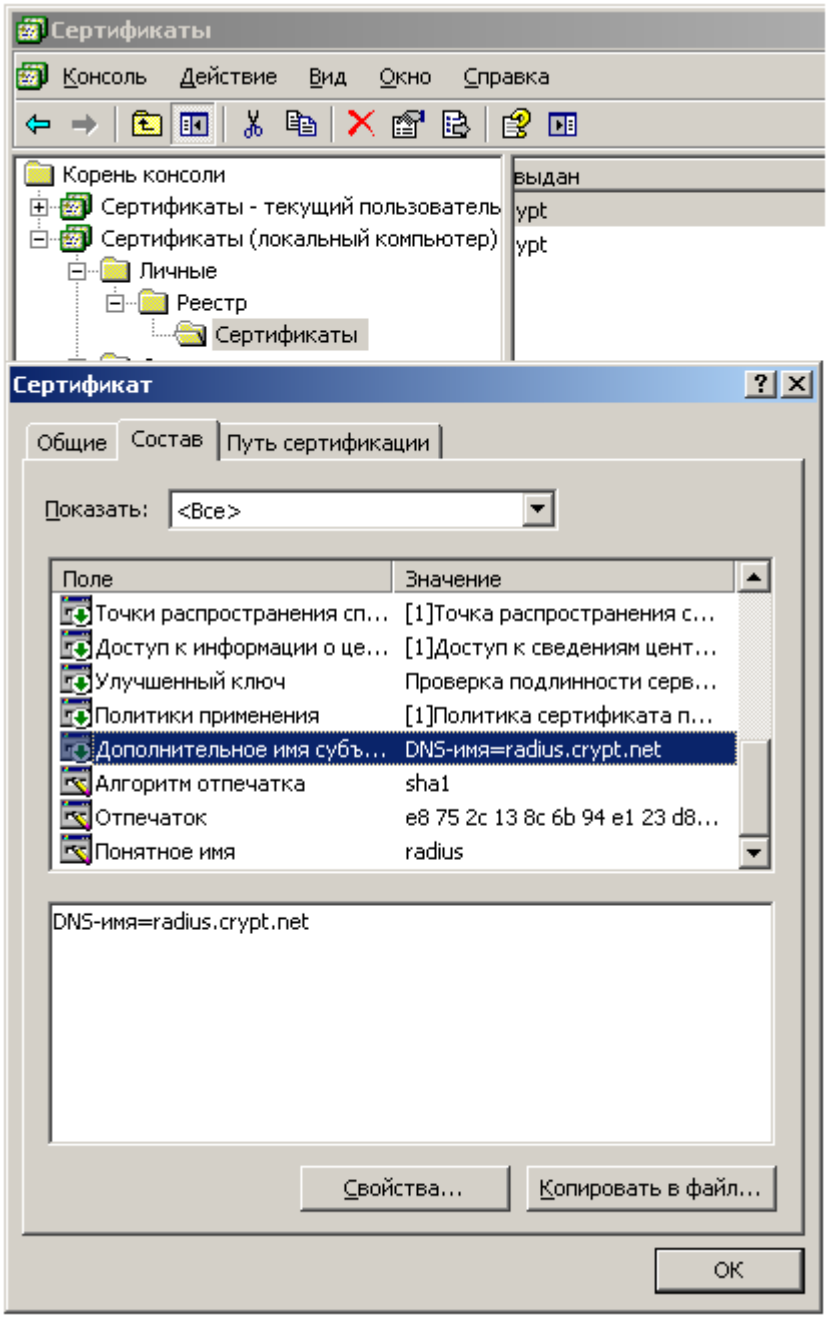


Рисунок 13 Сертификат сервера «Дополнительное имя субъекта»



6. Управление

Управление КриптоПро IPsec включает в себя установку, функции первичной, статической и динамической настройки и мониторинг.

Под первичной настройкой понимается настройка IPsec средствами ОС, не включающей понятия КриптоПро IPsec. Предполагается, что администратор проводит данную настройку самостоятельно, до установки КриптоПро IPsec, на основе знаний об IPsec в ОС.

Статическая настройка является набором неизменяемых при активной работе параметров КриптоПро IPsec, сюда включается набор параметров алгоритмов и способ аутентификации.

Динамическая настройка является набором изменяемых в процессе работы параметров. Сюда включено управление мандатным шифрованием и управление лицензией.

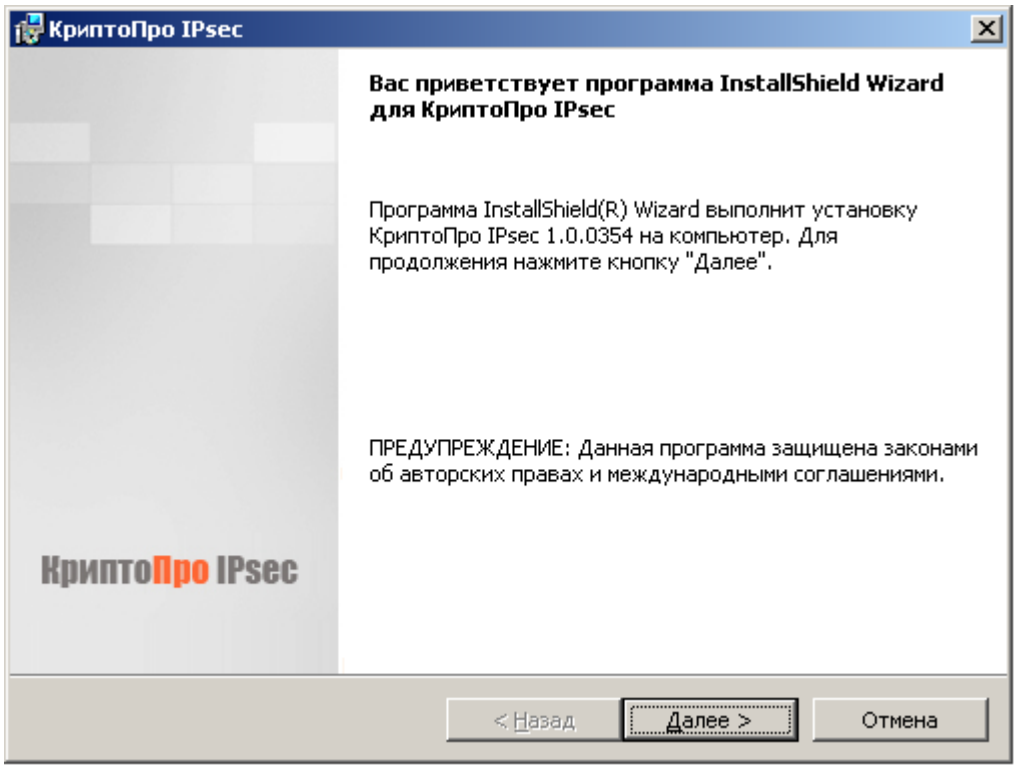
В мониторинг помимо средств мониторинга IPsec в ОС, включено приложение для просмотра общего состояния КриптоПро IPsec, информации об ошибках и состояние соединений КриптоПро IPsec ("%ProgramFiles%\Crypto Pro\IPsec**cp_ipsec_info.exe**").

7. Установка

7.1. Последовательность шагов по установке КриптоПро IPsec с диска

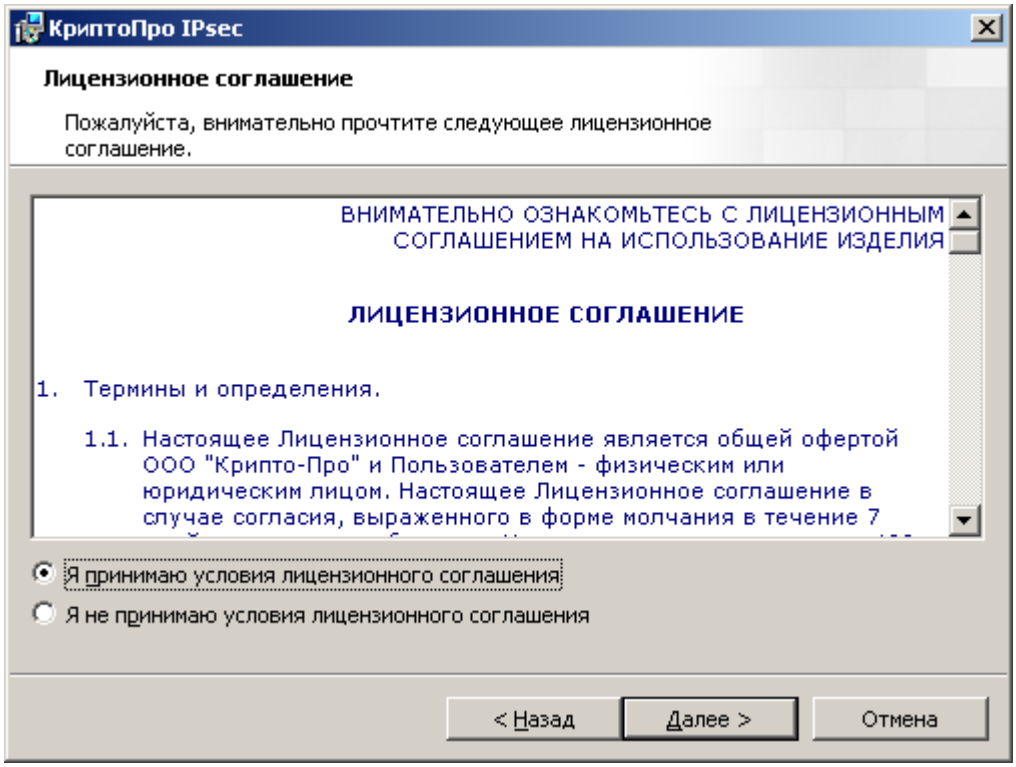
Для того чтобы установить КриптоПро IPsec, запустите установку MSI пакета, расположенного на компакт-диске. После коротких подготовительных процедур на экране появится окно мастера установки (см. Рисунок 14). Нажмите кнопку **Далее**.

Рисунок 14. Мастер установки КриптоПро IPsec



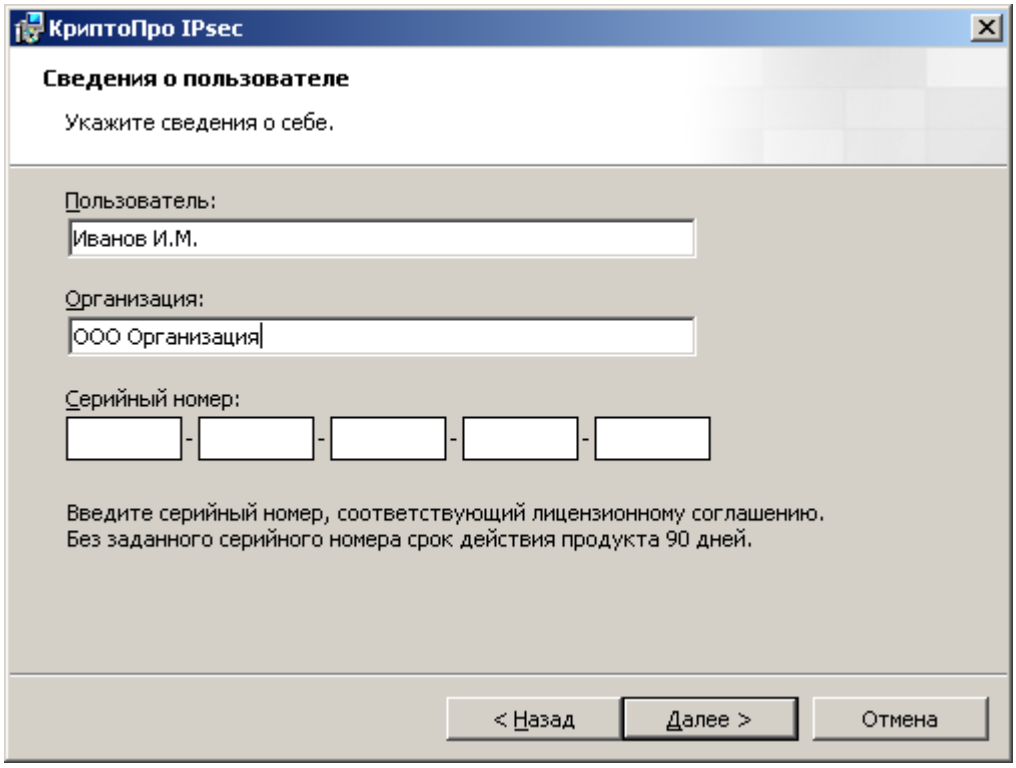
В следующем окне мастера установки ознакомьтесь с лицензионным соглашением на использование КриптоПро IPsec. Если Вы согласны со всеми пунктами соглашения, выделите пункт **Я принимаю условия лицензионного соглашения**, и нажмите **Далее** (см. Рисунок 15).

Рисунок 15. Лицензионное соглашение на использование КриптоПро IPsec



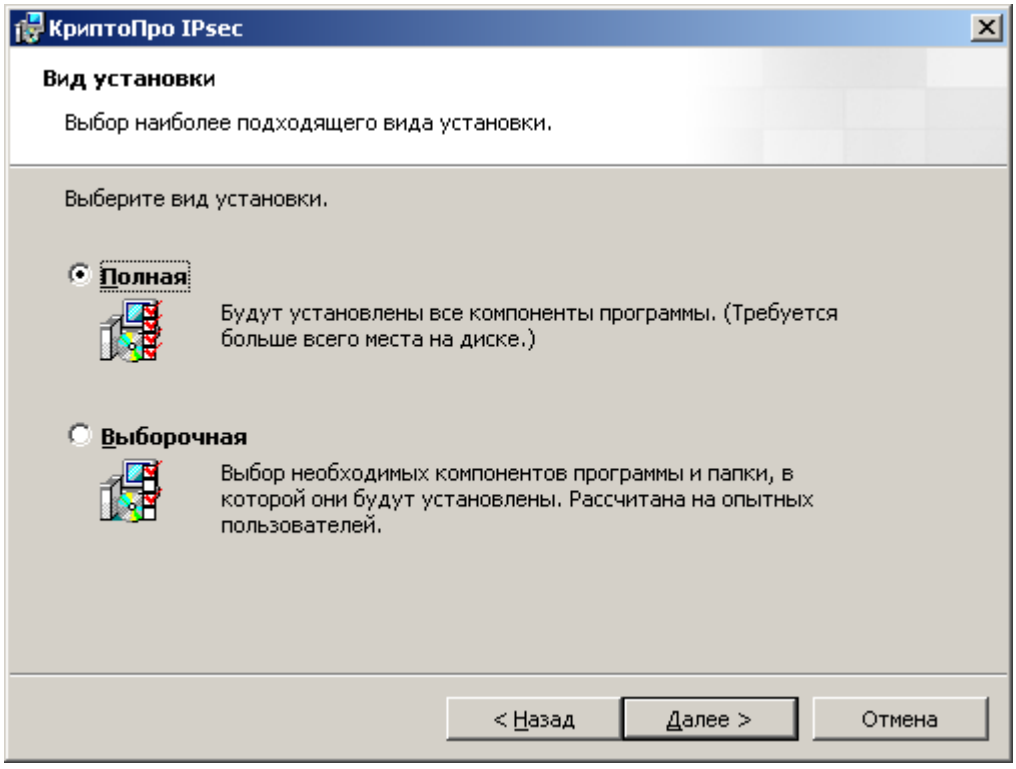
Следующим шагом необходимо ввести информацию о пользователе, производящем установку, и серийный номер лицензии на использование КриптоПро IPsec (см. Рисунок 16). Поле серийного номера можно оставить пустым, тогда продукт будет работать в демонстрационном режиме в течение 90 дней.

Рисунок 16. Сведения о пользователе КриптоПро IPsec



После нажатия кнопки **Далее** программа установки отобразит диалоговое окно (см. Рисунок 17), где необходимо выбрать вид установки. КриптоПро IPsec определяет два вида установки: полная и выборочная. Использование выборочной установки позволяет сменить папку для установки.

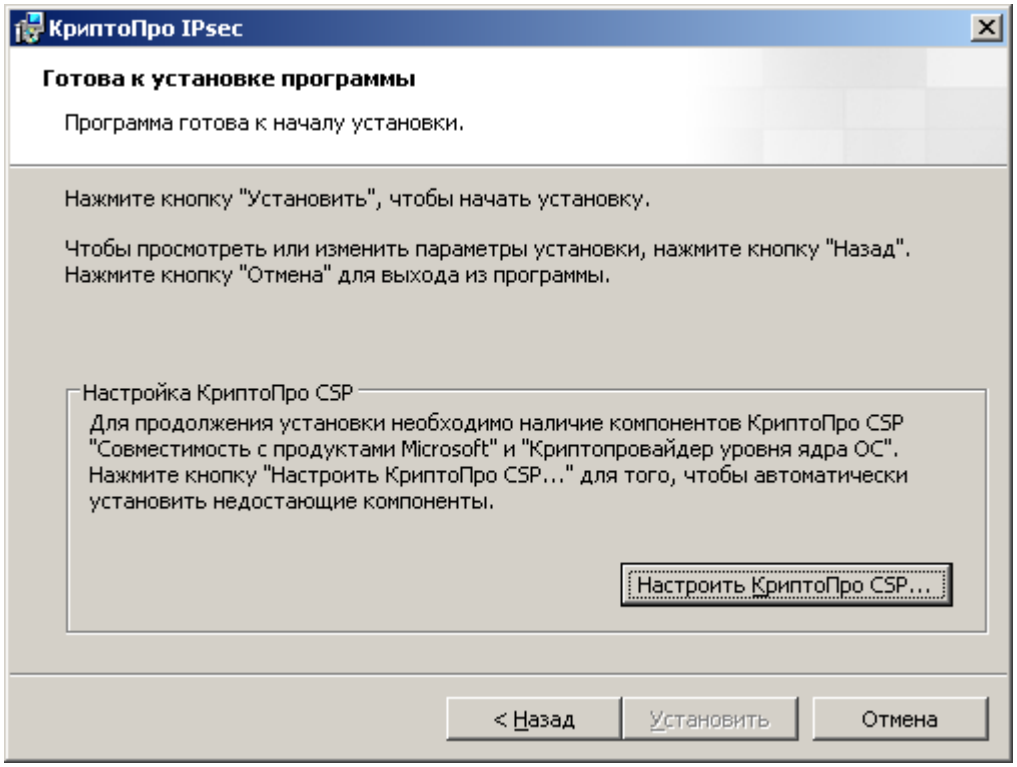
Рисунок 17. Вид установки КриптоПро IPsec



Следующее окно мастера служит для подтверждения установки. При необходимости можно вернуться назад и переопределить параметры установки.

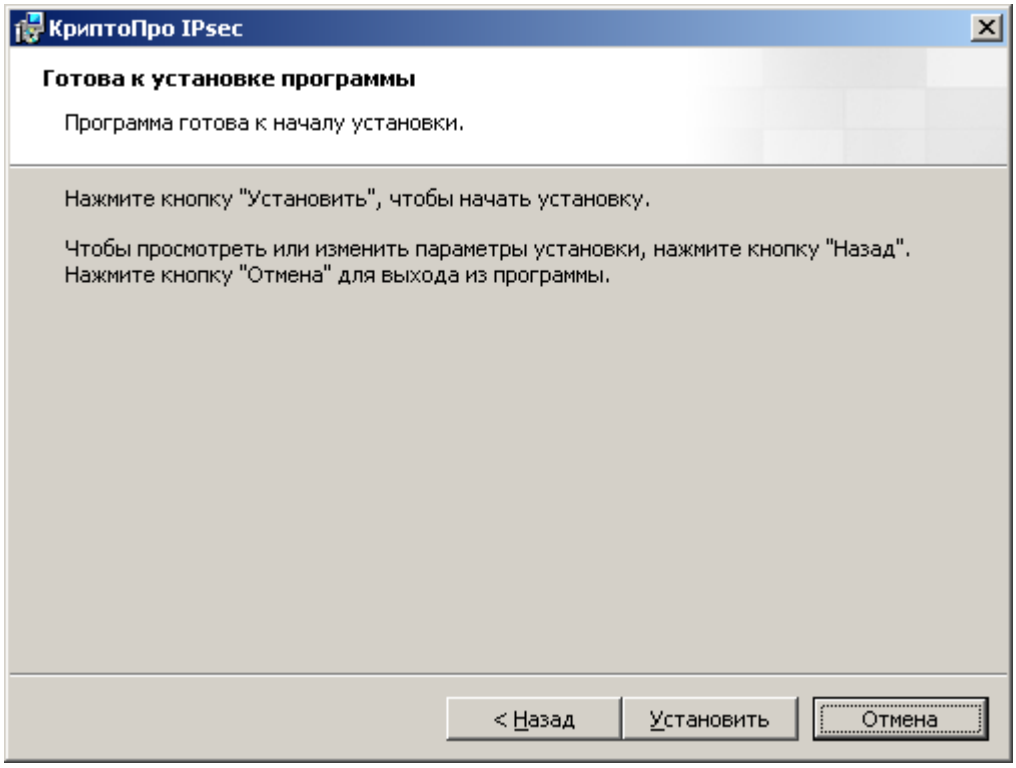
Для установки КриптоПро IPsec необходимо наличие компонентов КриптоПро CSP и «Криптопровайдер уровня ядра ОС». Если данные компоненты отсутствуют, то продолжить установку КриптоПро IPsec будет нельзя. В том случае для того, чтобы автоматически установить данные компоненты, следует нажать на кнопку **Настроить КриптоПро CSP** (см. Рисунок 18).

Рисунок 18. Установка отсутствующих компонентов КриптоПро CSP



Если все необходимые компоненты КриптоПро CSP установлены, то для подтверждения установки КриптоПро IPsec нажмите кнопку **Установить** (см. Рисунок 19).

Рисунок 19. Подтверждение установки



После выполнения всех описанных шагов мастер произведет установку КриптоПро IPsec, сопровождая свои действия комментариями. По окончании установки будет отображено окно с подтверждением успешной установки, где необходимо нажать кнопку **Готово**. Если на данном этапе появится окно с сообщением о необходимости перезагрузки компьютера, перезагрузите его.

8. Перечень сокращений

CSP	Cryptographic Service Provider (Криптопровайдер)
IPsec	IP Security (протокол Защиты IP-трафика)
OCSP	Online Certificate Status Protocol (Протокол получения статуса сертификата в реальном времени)
БД	База Данных
ПАК	Программно-Аппаратный Комплекс
СКЗИ	Средство Криптографической Защиты Информации
УЦ	Удостоверяющий центр
EAP-TLS	Extensible Authentication Protocol-Transport Level Security
PSK	Предварительно согласованные ключи
UPN	User Principal Name (Основное имя пользователя)
IPsec SA	Security Associations (Безопасное соединение)
RADIUS	Remote Authentication in Dial-In User Service (Протокол для реализации аутентификации, авторизации и учета)
PEAP	Protected Extensible Authentication Protocol (Защищённый Расширяемый Протокол Аутентификации)
ESP	Encapsulating Security Payload (Инкапсуляция зашифрованных данных)
AH	Authentication Header (Аутентифицирующий заголовок)
IKE	Internet Key Exchange (протокол Обмена ключами)
МЭ	Межсетевой Экран
ТЗ	Техническое задание
ААУ	Аутентификация Авторизация и Учет
NPS	Network Policy Server (Сервера политики сети)
IAS	Internet Authentication Service (Служба проверки подлинности в Интернете)
ISA Server	Internet Security and Acceleration Server
TMG	Threat Management Gateway
GPMC	Group Policy Management Console (Редактор управления групповыми политиками)
CMAK	Connection Manager Administration Kit (Пакет администратора диспетчера подключений)
SAN	Subject Alternative Name (Альтернативное имя субъекта)
NAT	Network Address Translation (Преобразование сетевых адресов)

9. Документация

[PUBTMG] Инструкция Microsoft «Публикация отдельного веб-сайта или системы балансировки нагрузки через HTTP» (http://technet.microsoft.com/ru-ru/library/cc441462.aspx)

[PUBISA] «Инструкции по публикации веб-узла на компьютер под управлением ISA Server 2006 или ISA Server 2004» (http://support.microsoft.com/kb/885186)

[UG] ЖТЯИ.00050-02 90 03. «Инструкции по использованию»

[UCARMU] ЖТЯИ.00067 01 90 05. «КриптоПро УЦ ЦР Руководство по эксплуатации»

[UCCA] ЖТЯИ.00067 01 90 03. «КриптоПро УЦ ЦС Руководство по эксплуатации Windows 2003»

[UCCA8] ЖТЯИ.00067 01 90 04. «КриптоПро УЦ ЦС Руководство по эксплуатации Windows 2008»

[UCARM] ЖТЯИ.00067 01 90 07. «КриптоПро УЦ АРМ администратора ЦР Практическая реализация»

[NPSOG] Руководство Microsoft «Network Policy Server (NPS) Operations Guide» (http://www.microsoft.com/downloads/en/details.aspx?FamilyID=585d2dca-c134-4568-b31c-a535ab0b0b3d&displaylang=en)

[ISADK] Документация Microsoft «ISA Server 2004 VPN Deployment Kit» (http://technet.microsoft.com/en-us/library/cc302453.aspx)

[TMGR] Инструкция Microsoft «Настройка Forefront TMG в качестве клиента RADIUS» (http://technet.microsoft.com/ru-ru/library/dd441017.aspx)

[RDS] Инструкция Microsoft «Использование проверки подлинности RADIUS» (http://technet.microsoft.com/ru-ru/library/cc778372%28WS.10%29.aspx)

[CPEAP] Страница КриптоПро EAP-TLS – Использование (http://www.cryptopro.ru/products/eap-tls/usage)

[DRA] Инструкция Microsoft «Deploying L2TP/IPSec-based Remote Access» (http://technet.microsoft.com/ru-ru/library/cc775490%28WS.10%29.aspx)

[RRASRA] Инструкция «Роль сервера удаленного доступа или VPN-сервера: настройка сервера удаленного доступа или VPN-сервера» (http://technet.microsoft.com/ru-ru/library/cc736357%28WS.10%29.aspx#rrassrvconfig)

[ONRAS] Инструкция Microsoft «Включение RRAS в качестве VPN-сервера» (http://technet.microsoft.com/ru-ru/library/dd458983.aspx)

[ONVPN] Инструкция Microsoft «Включение базового доступа удаленных клиентов» (http://technet.microsoft.com/ru-ru/library/dd897103.aspx)

[CXP] Инструкция Microsoft «Настройка подключения к виртуальной частной сети (VPN) в Windows XP» (http://support.microsoft.com/kb/314076)

[CV] Инструкция Microsoft «Create a VPN connection in Windows Vista and Windows Server 2008» (http://technet.microsoft.com/en-us/library/cc726062%28WS.10%29.aspx)

[C7] Инструкция Microsoft «Создание VPN-подключения» (http://technet.microsoft.com/ru-ru/library/cc726062%28WS.10%29.aspx)

[CMAK] Инструкция «Мастер пакета администрирования диспетчера подключений» (http://technet.microsoft.com/ru-ru/library/cc738870%28WS.10%29.aspx)

[DCMAK] Инструкция Microsoft «Установка пакета администрирования диспетчера подключений (CMAK)» (http://technet.microsoft.com/ru-ru/library/cc771679%28WS.10%29.aspx)

[S2] Инструкция Microsoft «Этап 2: разработка настраиваемых элементов» (http://technet.microsoft.com/ru-ru/library/cc738515%28WS.10%29.aspx)

[TMISA] Статья «ISA Server 2006 - IPsec Tunnel Mode Site-to-Site VPN Connections: A Couple of Things That Are Not Supported» (http://blogs.isaserver.org/shinder/2008/12/22/isa-server-2006-ipsec-tunnel-mode-site-to-site-vpn-connections-a-couple-of-things-that-are-not-supported/).

[DGPO] Инструкция Microsoft «Creating and Editing GPOs» (http://technet.microsoft.com/ru-ru/library/cc782980%28WS.10%29.aspx)

[DIPR] Инструкция Microsoft «Создание и изменение объекта групповой политики» (http://technet.microsoft.com/ru-ru/library/cc754740%28WS.10%29.aspx)

[AIPR] Инструкция Microsoft «Добавление, изменение и удаление политик IPSec» (http://technet.microsoft.com/ru-ru/library/cc778422%28WS.10%29.aspx)

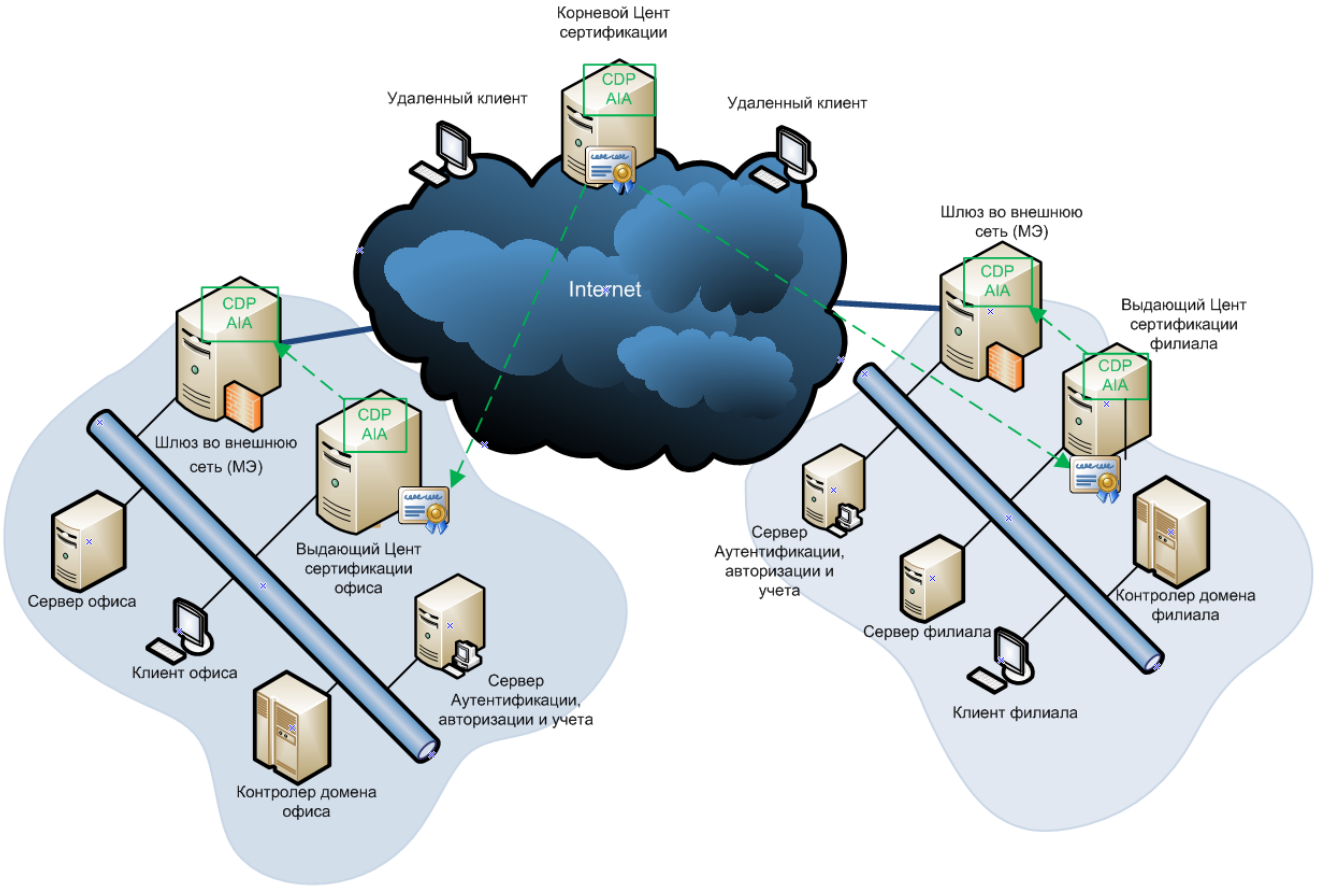
[GPOP] Статья Microsoft «Обработка и приоритеты групповых политик» (http://technet.microsoft.com/ru-ru/library/cc785665%28WS.10%29.aspx)

10. Приложение

В данном разделе рассмотрены базовые варианты использования КриптоПро IPsec в подготовленной сетевой, доменной инфраструктуре с организованной ИОК.

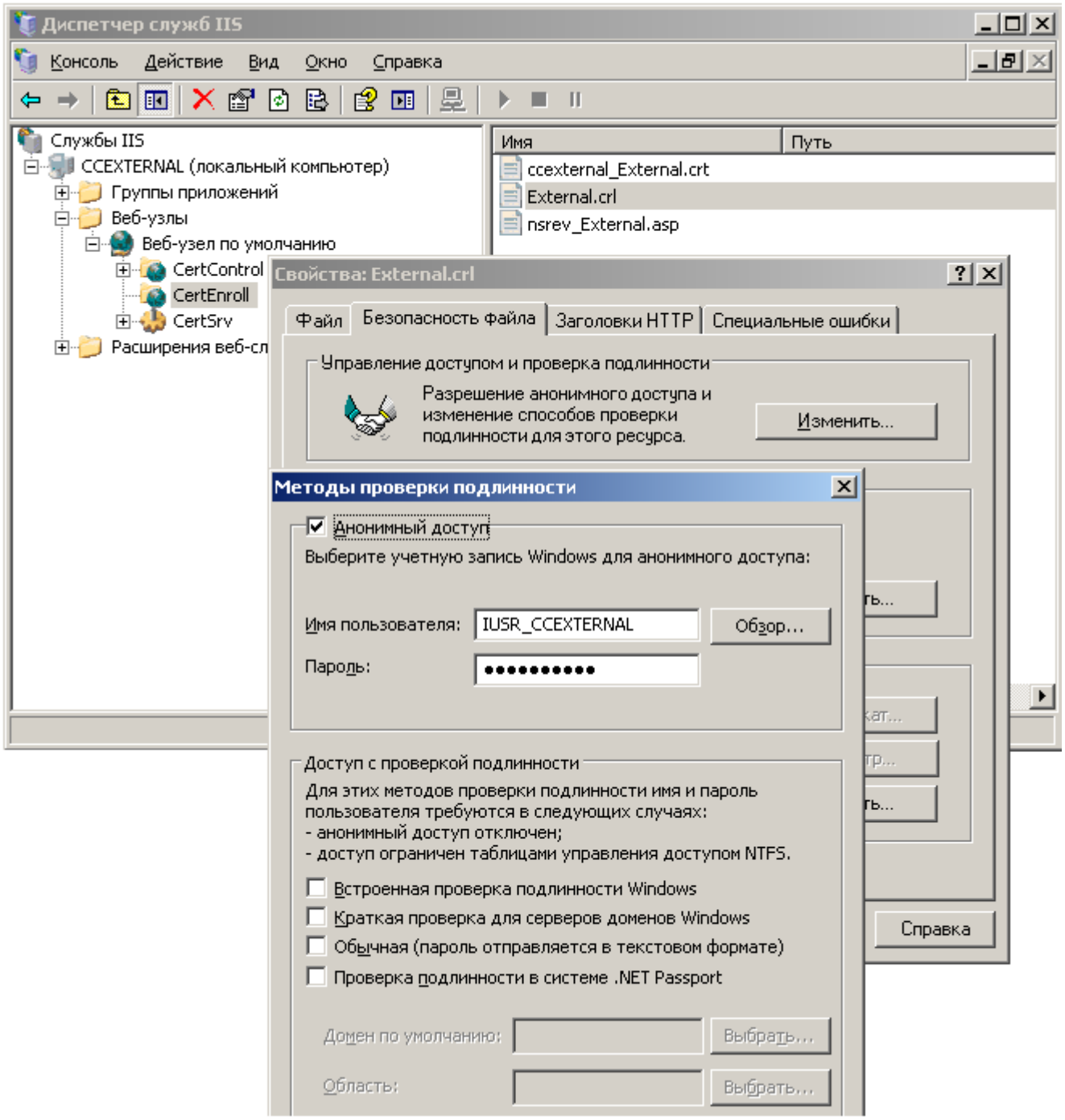
Для выпуска сертификатов развернута двухуровневая структура центров сертификации (см. Рисунок 20)

Рисунок 20 ИОК



Изолированный Корневой центр сертификации расположен во внешней сети. Проверка статуса сертификата происходит по Спискам отзыва (Certificate Revocation List, CRL). Доступ к точкам распространения списков отзыва (CRL Distribution Points, CDP) не требует аутентификации (см. Рисунок 21).

Рисунок 21 Анонимный доступ к CRL в IIS 6



Подчиненные, выпускающие центры сертификации развернуты во внутренних сетях в домене. Проверка статуса сертификата происходит по спискам отзыва, которые доступны без аутентификации. Для удаленных клиентов (сетей) списки отзыва и сертификаты выпускающих центров опубликованы на МЭ (шлюз) во внешнюю сеть:

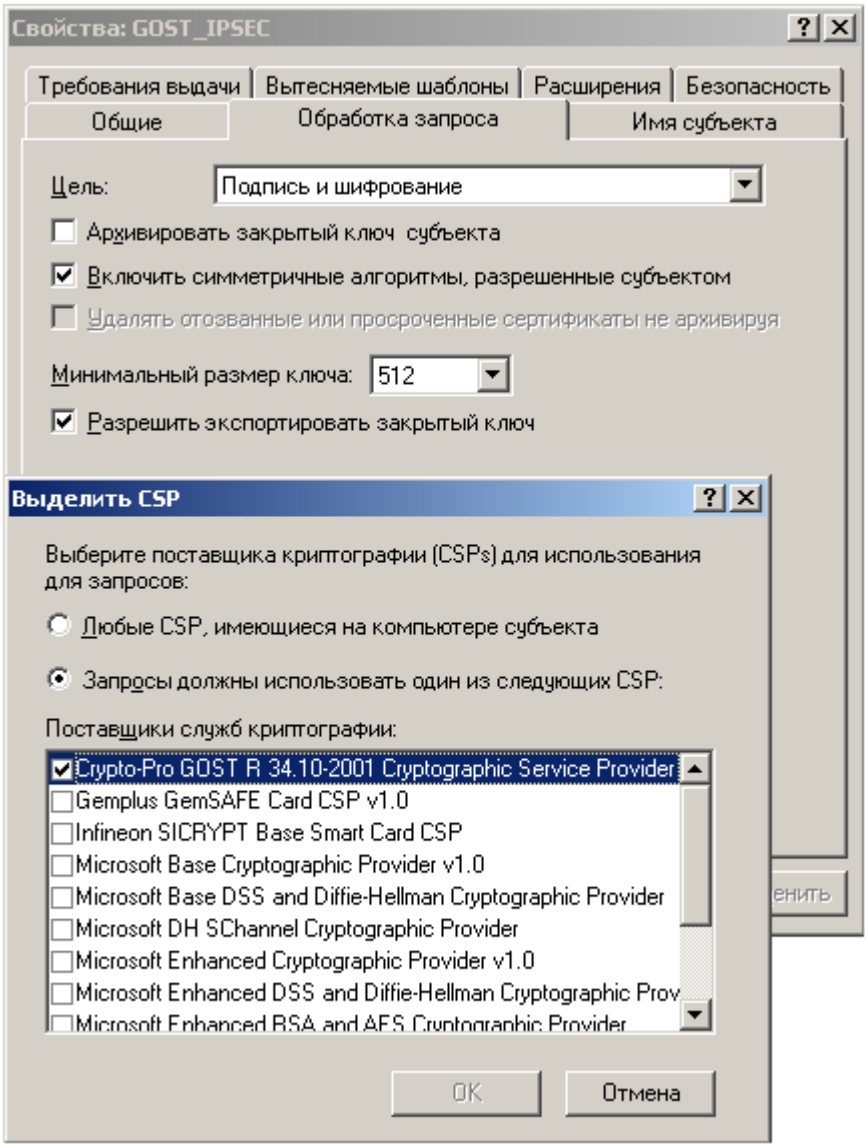
- для Microsoft Forefront TMG 2010 (TMG) настройка проводилась по инструкции Microsoft «Публикация отдельного веб-сайта или системы балансировки нагрузки через HTTP» (http://technet.microsoft.com/ru-ru/library/cc441462.aspx) ;
- для Microsoft ISA Server 2004 и ISA Server 2006 настройка проводилась по «Инструкции по публикации веб-узла на компьютер под управлением ISA Server 2006 или ISA Server 2004» (http://support.microsoft.com/kb/885186) .

В домене доверие к корневому сертификату изолированного центра настраивается с помощью групповых политик: ***Имя_объекта_политики*** **-> Конфигурация компьютера -> Конфигурация Windows -> Параметры безопасности -> Политики открытого ключа -> Доверенные корневые центры сертификации.**

Для доменных пользователей и компьютеров выпуск сертификатов производится из оснастки «Microsoft Management Console (MMC) –> Сертификаты (пользователя, компьютера)» по шаблонам доменного центра сертификации.

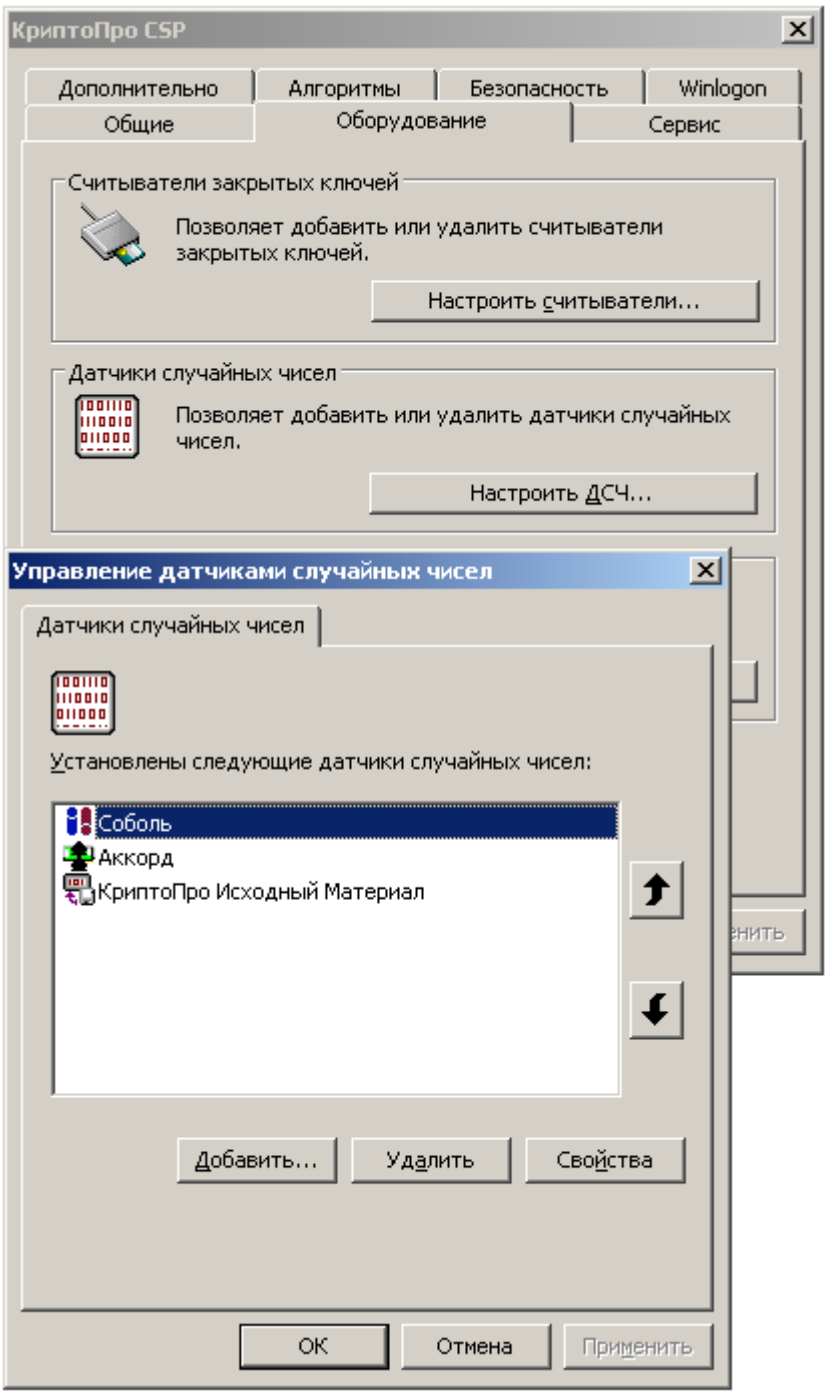
Сертификаты IPsec выпускаются по **копии** базового шаблона «IPsec» с CSP КриптоПро: «Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider» (см. Рисунок 22)

Рисунок 22 Шаблон сертификата для IPsec



В ОС Microsoft Windows XP и Microsoft Server 2003 запрос сертификата должен проходить без вывода окон CSP (в «тихом» режиме). Для этого в КриптоПро CSP необходимо указать **Считыватель по умолчанию** и не использовать **«Биологический ДСЧ»** (см Рисунок 23)

Рисунок 23 Настроить ДСЧ



В домене выпуск сертификатов клиентской аутентификации происходит по **копии** шаблона «Пользователя» с CSP КриптоПро: «Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider». При запросе клиентского сертификата настройку КриптоПро CSP «тихой» генерации производить не обязательно.

В домене выпуск сертификатов аутентификации сервера (VPN аутентификация) происходит по **копии** шаблона по умолчанию «RAS и IAS-сервер» с CSP КриптоПро: «Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider». Для запроса сертификата необходимо произвести настройку «тихого» режима КриптоПро CSP в ОС Microsoft Windows XP и Microsoft Server 2003.

На компьютерах, не являющихся членами домена, невозможно пользоваться описанным выше методом выпуска сертификатов (MMC -> Сертификаты -> шаблоны AD). Методы распространения (запрос, выпуск, установка, обновление) сертификатов определяется Администратором. В данных примерах сертификаты для удаленных клиентов создаются с помощью веб-интерфейса пользователя УЦ.

Установка личных сертификатов производится согласно «Инструкции по использованию» (ЖТЯИ.00050-02 90 03) КриптоПро CSP - глава 2.5.3. «Установка личного сертификата, хранящегося в файле» (http://cryptopro.ru/products/csp/downloads).

Выпуск сертификатов в КриптоПро УЦ.

Для выпуска сертификатов **IPsec** необходимо произвести настройку КриптоПро ЦР и КриптоПро ЦС (документация на КриптоПро УЦ доступна по ссылке: http://cryptopro.ru/products/ca/downloads) :

- создать шаблон сертификата согласно «КриптоПро УЦ ЦР Руководство по эксплуатации» (ЖТЯИ.00067 01 90 05) с OID «**IKE-посредник IP-безопасности**» (1.3.6.1.5.5.8.2.2);
- добавить в Политики ЦР разрешение на обработку запроса и отзыв сертификата, содержащего OID «**IKE-посредник IP-безопасности**» (1.3.6.1.5.5.8.2.2),.согласно «КриптоПро УЦ ЦР Руководство по эксплуатации» (ЖТЯИ.00067 01 90 05) **глава 4.2** «Политики обработки запросов»;
- добавить в Модуль политики КриптоПро ЦС Использование ключа «**IKE-посредник IP-безопасности**» (1.3.6.1.5.5.8.2.2) согласно «КриптоПро УЦ ЦС Руководство по эксплуатации Windows 2003/2008» (ЖТЯИ.00067 01 90 03/ЖТЯИ.00067 01 90 04) **глава 3.1** «Настройка областей использования ключа, политик выдачи и политик применения в сертификатах открытого ключа»;
- добавить в Модуль политики КриптоПро ЦС Расширения X.509 **«Дополнительное имя субъекта»** (2.5.29.17).

Для выпуска сертификатов **аутентификации сервера** необходимо произвести настройку КриптоПро ЦР:

- создать шаблон сертификата согласно «КриптоПро УЦ ЦР Руководство по эксплуатации» (ЖТЯИ.00067 01 90 05) с OID **«Проверка подлинности сервера»** (1.3.6.1.5.5.7.3.1);
- добавить в Политики ЦР разрешение на обработку и отзыв сертификата согласно «КриптоПро УЦ ЦР Руководство по эксплуатации» (ЖТЯИ.00067 01 90 05) **глава 4.2** «Политики обработки запросов».

Для выпуска сертификатов **аутентификации клиента** необходимо указать UPN пользователя и использовать шаблон, содержащий назначение **«Проверка подлинности клиента»** (1.3.6.1.5.5.7.3.2).

Настройку УЦ для выпуска сертификатов **аутентификации по смарт-карте** можно проводить по документаций «Настройка КриптоПро Winlogon в домене Windows с использованием КриптоПро УЦ» **глава 4.2.1** «Шаблон сертификата «Сертификат входа со смарт-картой»» (http://cryptopro.ru/products/other/winlogon#downloads) .

Организация основных методов (централизованны, распределенный) распространения сертификатов описана в руководстве «КриптоПро УЦ АРМ администратора ЦР Практическая реализация» (ЖТЯИ.00067 01 90 07).

Аутентификация, авторизация и учет.

Во время VPN-подключения после выработки IPsec SA (между компьютерами) происходит пользовательская аутентификация, авторизация, и учет информации об этом. Сервера АА и Учета могут быть развернуты как на VPN-сервере, так и на изолированном RADIUS-сервере. RADIUS обеспечивает централизованную ААУ, что может быть удобно в сложной сетевой структуре с несколькими точками удаленного доступа, в том числе, если VPN-сервер не в домене. В качестве RADIUS-серверов в следующих семействах ОС:

- Windows Server 2003 может выступать «Служба проверки подлинности в Интернете (Internet Authentication Service, **IAS**);
- Windows Server 2008 (R2) может выступать служба «Сервера политики сети» (Network Policy Server, **NPS**).

Развертывание IAS (Windows Server 2003)

Для установки и настройки IAS можно воспользоваться инструкциями Microsoft, опубликованными на странице: http://technet.microsoft.com/ru-ru/library/cc736803(WS.10).aspx .

Развертывание NPS (Windows Server 2008)

Установку и настройку NPS можно проводит согласно руководства Microsoft «Network Policy Server (NPS) Operations Guide»

(http://www.microsoft.com/downloads/en/details.aspx?FamilyID=585d2dca-c134-4568-b31c-a535ab0b0b3d&displaylang=en)

Для использования RADIUS ААУ на VPN-серверах (RRAS, ISA Server, TMG) необходимо проводить дополнительную настройку (RADIUS-клиента, RADIUS-сервера).

Настройка ISA Server 2004 и ISA Server 2006

Использование RADIUS-сервера можно настроить по документации Microsoft «ISA Server 2004 VPN Deployment Kit» (http://technet.microsoft.com/en-us/library/cc302453.aspx) **Глава 7** «Configuring Windows Server 2003 RADIUS Support for VPN Clients – Including Support for EAP/TLS Authentication» и **Глава 8** « Configuring the VPN Client and ISA Server 2004 VPN Server to Support Certificate-Based PPTP EAP-TLS Authentication»

Если RADIUS-сервер не назначен – ААУ будет проводиться средствами ISA Server.

Настройка TMG

Использование RADIUS можно настроить по документации Microsoft «Настройка Forefront TMG в качестве клиента RADIUS» (http://technet.microsoft.com/ru-ru/library/dd441017.aspx).

Если RADIUS-сервера не назначен – ААУ будет проводиться средствами TMG.

Настройка RRAS

Настройку RADIUS в RRAS можно производить согласно инструкции Microsoft «Использование проверки подлинности RADIUS» (http://technet.microsoft.com/ru-ru/library/cc778372%28WS.10%29.aspx)

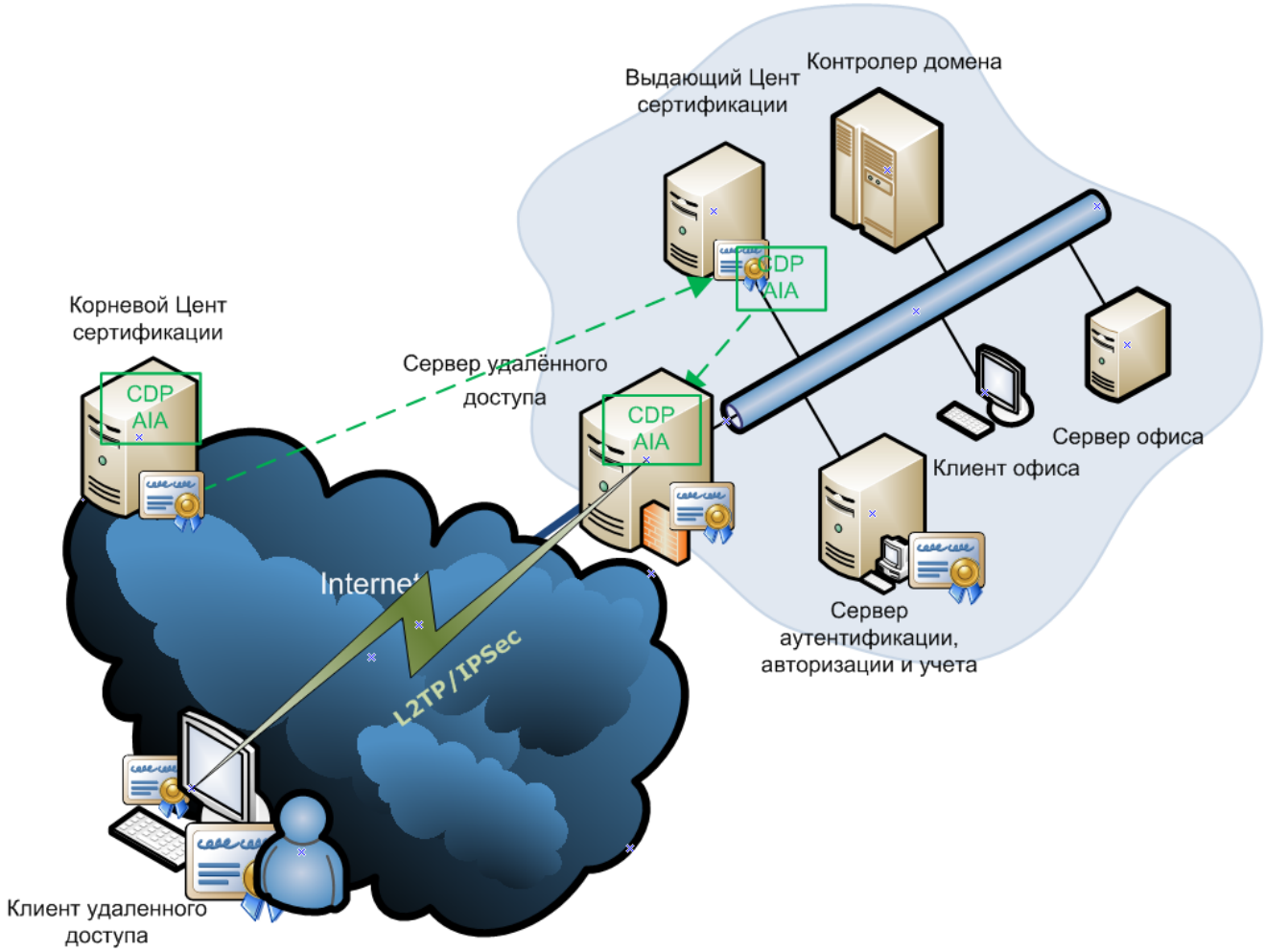
Настройку ААУ в службе RRAS можно проводить по инструкций Microsoft «Использование проверки подлинности Windows» (http://technet.microsoft.com/ru-ru/library/cc778876%28WS.10%29.aspx)

Описание реализации EAP-TLS, PEAP методов аутентификации пользователя по сертификатам опубликовано на странице: http://www.cryptopro.ru/products/eap-tls/usage

10.1. Настройка VPN для безопасного подключения клиента к сети офиса

В данном разделе будет рассмотрен сценарий создания защищенного удаленного подключения пользователя (компьютера пользователя) к сети офиса (см. Рисунок 24).

Рисунок 24 Client-to-Site



Для организации такого решения необходимо выполнить:

Настройку сервера удаленного доступа(VPN-сервер), состоящую из следующих этапов:

- выбор протокола удаленного доступа;
- определение списка IP-адресов, присваиваемых внешним клиентам(DHCP-сервер);
- настройка правил фильтрации;
- настройка методов аутентификации, авторизации и учета пользователей;
- *рекомендуется произвести настройку протокола SSTP – как резервного*;

Настройку клиента удаленного доступа:

- создание VPN-подключения (CMAK или «Мастер новых подключений»).

Допускается доступ к VPN-серверу через Back-to-Back структуру МЭ, например, доступ к внутренней сети через DMZ или «Perimeter network» с двойным NAT (Network Address Translation — Преобразование сетевых адресов).

Настройка сервера удалённого доступа (VPN-сервер)

Сервер удаленного доступа можно настроить с использованием Службы Windows Server RRAS (Routing and Remote Access Server) или развернуть на одном из поддерживаемых МЭ. Ряд инструкций по настройки VPN-сервера будут приведены ниже.

Настройка RRAS на Microsoft Windows Server 2003

Установка и настройка сервера подключения к частной сети (VPN-сервер) в службе RRAS (Routing and Remote Access Server) проводится согласно инструкции Microsoft «Deploying L2TP/IPSec-based Remote Access» (http://technet.microsoft.com/ru-ru/library/cc775490%28WS.10%29.aspx), и инструкции «Роль сервера удаленного доступа или VPN-сервера: настройка сервера удаленного доступа или VPN-сервера» (http://technet.microsoft.com/ru-ru/library/cc736357%28WS.10%29.aspx#rrassrvconfig)

Настройка RRAS на Microsoft Windows Server 2008 (R2)

Для настройки службы RRAS как сервера удаленного доступа можно использовать инструкции Microsoft «Включение RRAS в качестве VPN-сервера» (http://technet.microsoft.com/ru-ru/library/dd458983.aspx)

Настройка VPN-сервера на Microsoft ISA Server 2004

Развертывание VPN-сервера удаленного доступа можно проводит согласно руководства Microsoft «ISA Server 2004 VPN Deployment Kit» » **Глава 4** «Configuring the ISA Server 2004 Firewall as a VPN Server» (http://technet.microsoft.com/en-us/library/cc302453.aspx)

Настройка VPN-сервера на Microsoft ISA Server 2006

Развертывание VPN-сервера на ISA Server 2006 можно проводить согласно руководства Microsoft ««ISA Server 2004 VPN Deployment Kit»» **Глава 4** «Configuring the ISA Server 2004 Firewall as a VPN Server» (http://technet.microsoft.com/en-us/library/cc302453.aspx) т.к. нет существенных отличий от аналогичной настройки ISA Server 2004.

Настройка VPN-сервера на Microsoft Forefront TMG 2010

Развертывание VPN-сервера на TMG 2010 можно проводить согласно инструкции Microsoft «Включение базового доступа удаленных клиентов» (http://technet.microsoft.com/ru-ru/library/dd897103.aspx).

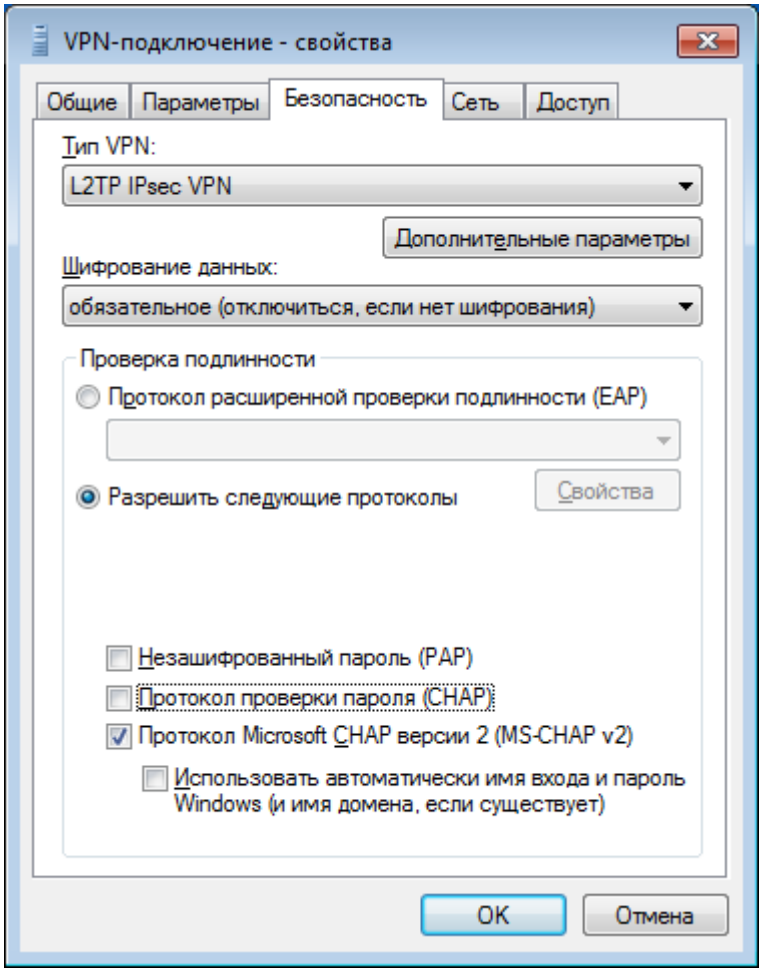
Настройка клиента удалённого доступа (VPN)

Для подключения в удаленную сеть с использованием протокола L2TP/IPsec необходимо в Свойствах Удаленного подключения указать «**Тип VPN:**» «**L2TP IPsec VPN**» (см Рисунок 25).

При настройке «**Тип VPN:**» «**Автоматически**» - запросы на подключение перебираются в следующем порядке: SSTP, L2TP/IPsec, PPTP, пока не будет согласован протокол, поддерживаемый и клиентом и сервером.

На вкладке «**Безопасность**» настроить обязательность шифрования (см Рисунок 25).

Рисунок 25 VPN-подключение -> Вкладка Безопасность



PSK используется если он указан в Свойствах, настраиваемого VPN подключения, в противном случае используется сертификат, удовлетворяющим требованиям IPsec (см. в главе 5.2 «Сертификаты открытого ключа»).

Настройка VPN подключения на Windows XP и Windows Server 2003

Создание подключения к VPN можно проводить согласно инструкции Microsoft «Настройка подключения к виртуальной частной сети (VPN) в Windows XP» (http://support.microsoft.com/kb/314076).

Настройка VPN подключения на Windows Vista и Windows Server 2008

Создание подключения к VPN можно проводить согласно инструкции Microsoft «Create a VPN connection in Windows Vista and Windows Server 2008» (http://technet.microsoft.com/en-us/library/cc726062%28WS.10%29.aspx).

Настройка VPN подключения на Windows Windows 7 и Windows Server 2008 R2

Создание подключения к VPN можно проводить согласно инструкции Microsoft «Создание VPN-подключения» (http://technet.microsoft.com/ru-ru/library/cc726062%28WS.10%29.aspx).

Настройка клиента удаленного доступа с помощью профиля соединения, созданного при помощи пакета администрирования диспетчера подключений (CMAK)

CMAK - это средство администратора, автоматизирующее создание VPN-подключения пользователя к удаленной сети.

Создание профилей соединения

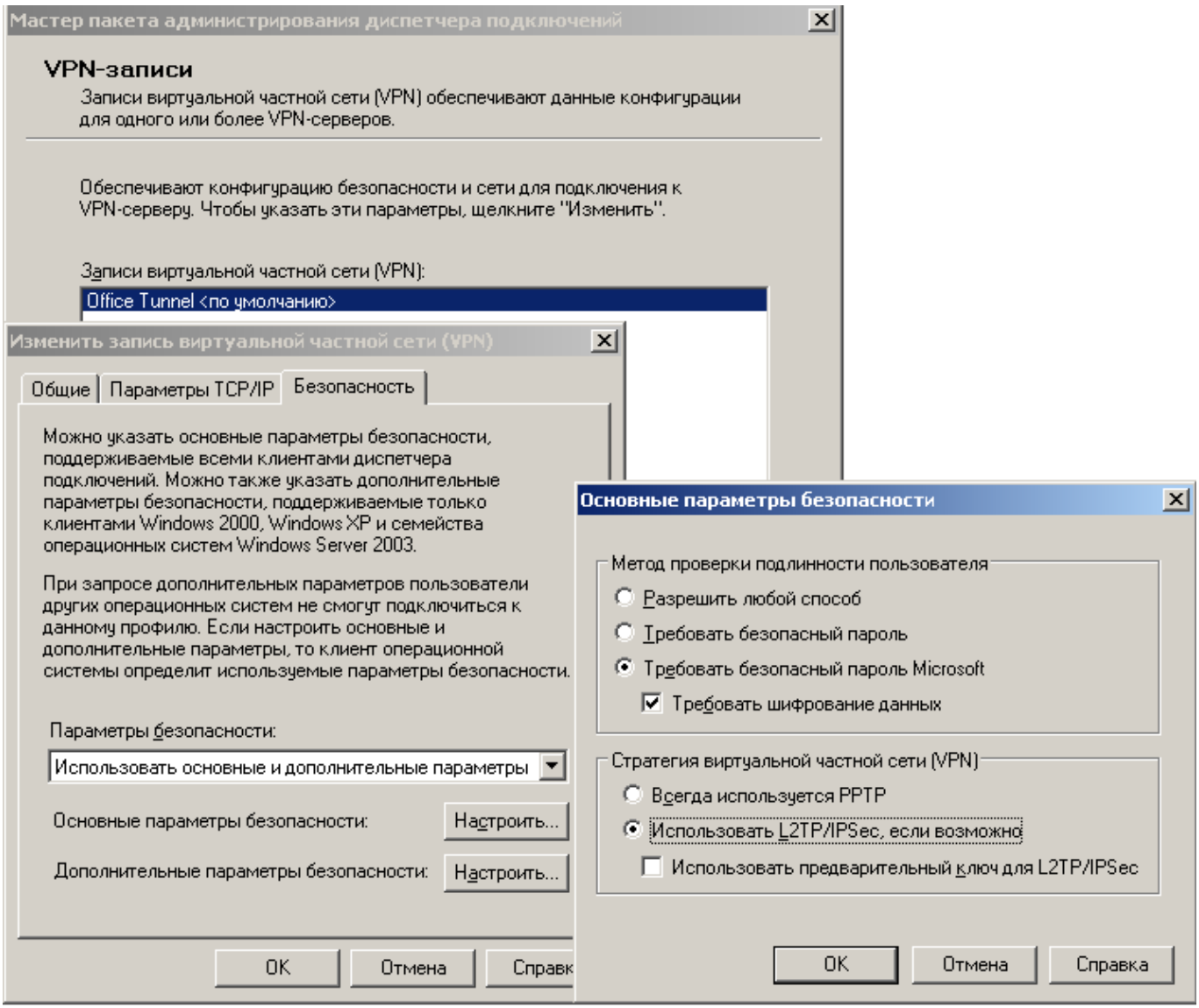
Установку CMAK можно проводить для ОС:

- Microsoft Windows Server 2003 по инструкции «Мастер пакета администрирования диспетчера подключений» (http://technet.microsoft.com/ru-ru/library/cc738870%28WS.10%29.aspx);
- Microsoft Windows Server 2008 по инструкции Microsoft «Установка пакета администрирования диспетчера подключений (CMAK)» (http://technet.microsoft.com/ru-ru/library/cc771679%28WS.10%29.aspx).

Создание профиля подключения службы с помощью мастера CMAK происходит по шагам из инструкции Microsoft «Этап 2: разработка настраиваемых элементов» (http://technet.microsoft.com/ru-ru/library/cc738515%28WS.10%29.aspx).

Во время настройки «**VPN-записи**» необходимо указать использование протокола L2TP/IPsec (см. Рисунок 26).

Рисунок 26 Параметры безопасности «VPN-записи» на Windows Server 2003



Сертификат будет использоваться если не указано «**Использовать предварительный ключ для L2TP/IPsec**».

Создание профилей подключений пользователей с L2TP/IPsec на PSK, требует дополнительных действий. Профиль созданный с помощью мастера считается родительским. На его базе создаются профили для конечных пользователей. Для этого необходимо:

- в файле родительского профиля (%ProgramFiles%\Cmak\Profiles\Имя_профиля\Имя_профиля.sed) указать актуальный путь к файлу «установщика профилей» **cmstp.exe** (файл cmstp.exe находится в пакете %ProgramFiles%\Cmak\Support**cmbins.exe**);
- скопировать файлы "%ProgramFiles%\Crypto Pro\IPsec**cpcmak_builder.exe**", "%ProgramFiles%\Crypto Pro\IPsec**cpcmak_cpacker.exe**", "%ProgramFiles%\Crypto Pro\IPsec**genpsk.exe**" в директорию родительского профиля (%ProgramFiles%\Cmak\Profiles\Имя_профиля);
- создать текстовый файл с конечными пользователями. Первая строка в этом файле должна соответствовать следующим 4 сущностям разделенным пробелами: ИмяОфисаИлиДомена ИмяСети ИмяКонтейнера ПинКонтейнера (эти параметры будут использоваться для генерации PSK см раздел «*5.1 Pre-Shared Key*»). В остальных строках задаются имена пользователей

Пример:

TestNet ForClient MainCont 12345678
mDima
Sergei
Ivan
bDima

- запустить **cpcmak_builder.exe** , используя в качестве одного параметра файл(полный путь в кавычках) с пользователями (созданный на предыдущем шаге);

Процесс заканчивается созданием исполняемых и текстовых файлов с паролями для каждого пользователя.

Создание VPN-подключения с помощью профиля соединения

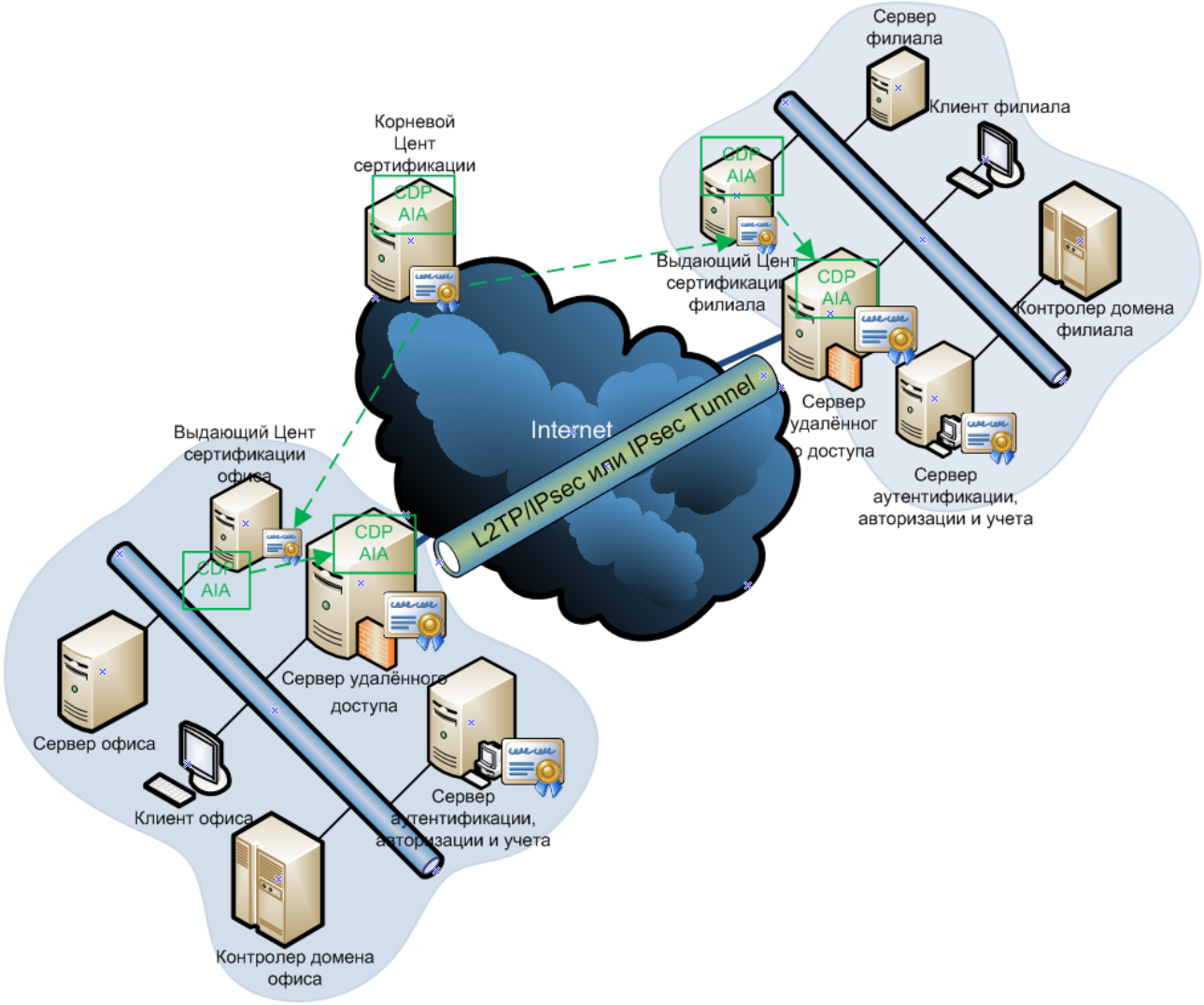
Способы распространение, передачи исполняемого файла профиля определяются администратором.

Создание VPN-подключения происходит после запуска файла профиля. Если использовались PSK, то будет запрошен пароль соответствующего пользователя (созданный во время запуска **cpcmak_builder.exe**).

10.2. Настройка Site-to-Site

В данном разделе будет рассмотрен сценарий создания защищенного соединения сетей, подключенных к сетям общего пользования (см. Рисунок 27).

Рисунок 27 Site-to-Site



Для организации такого решения необходимо выполнить настройку VPN-шлюзов сетей партнеров по следующей схеме:

- выбор протокола удаленного доступа;
- настройка правил маршрутизации;
- настройка правил IP-фильтрации;
- настройка методов аутентификации, авторизации и учет site-to-site подключений.

Допускается VPN-соединений сетей по схеме site-to-site с применением двух типов протоколов: IPsec-tunnel и L2TP\IPsec. IPSec в туннельном режиме целесообразно применять, только если необходимо создать канал связи site-to-site с VPN-шлюзами сторонних производителей. Существует несколько причин для отказа от использования IPSec в туннельном режиме:

- IPSec в туннельном режиме менее защищен;

- IPSec в туннельном режиме обладает ограничениями по маршрутизации на компьютерах с системой Windows Server 2003;
- IPSec в туннельном режиме может уменьшить эффективную пропускную способность VPN-туннеля.

Допускается развертывание VPN-туннеля между сетями с Back-to-Back структурой МЭ, например, между DMZ или «Perimeter network» сетями филиала и офиса.

Настройка шлюза VPN на Microsoft ISA Server 2004

Для развертывания VPN-шлюза на **ISA Server 2004** по **L2TP\IPsec** можно воспользоваться руководством Microsoft «ISA Server 2004 VPN Deployment Kit» **Глава 10** «Creating PPTP and L2TP/IPSec Site-to-Site VPNs with ISA Server 2004 Firewalls» (http://technet.microsoft.com/en-us/library/cc302453.aspx).

Для развертывания VPN-шлюза на **ISA Server 2004** по **IPsec Tunnel mode** можно воспользоваться руководством Microsoft «ISA Server 2004 VPN Deployment Kit» **Глава 11** «Creating a Site-to-Site VPN with ISA Server 2004 at Local and Remote Sites using IPSec Tunnel Mode» (http://technet.microsoft.com/en-us/library/cc302453.aspx).

Настройка шлюза VPN на Microsoft ISA Server 2006

В ISA Server 2006 для настройки подключения VPN site-to-site используются Wizards (мастера):

- Branch Office Connectivity Wizard (BOCW) (Мастер настройки соединения с филиалом сервера) (http://www.isaserver.org/tutorials/Creating-Branch-Office-VPN-Connection-Remote-Site-Network-Wizard.html) ;
- VPN Site-to-Site Connection Wizard (Мастер создания VPN-соединения по схеме Site-to-Site) (http://www.isaserver.org/tutorials/Creating-VPN-ISA-Server-2006-Firewalls-Main-Branch-Office-Part1html.html). В этом мастере последовательно выполняются шаги, описанные в руководстве Microsoft «ISA Server 2004 VPN Deployment Kit» (http://technet.microsoft.com/en-us/library/cc302453.aspx) в **Главе 10** «Creating PPTP and L2TP/IPSec Site-to-Site VPNs with ISA Server 2004 Firewalls» **для L2TP**. И в **Главе 11** «Creating a Site-to-Site VPN with ISA Server 2004 at Local and Remote Sites using IPSec Tunnel Mode» **для IPSec Tunnel Mode**.

Стоит учитывать ряд ограничений IPsec Tunnel опасных в статье «ISA Server 2006 - IPsec Tunnel Mode Site-to-Site VPN Connections: A Couple of Things That Are Not Supported»: (http://blogs.isaserver.org/shinder/2008/12/22/isa-server-2006-ipsec-tunnel-mode-site-to-site-vpn-connections-a-couple-of-things-that-are-not-supported/).

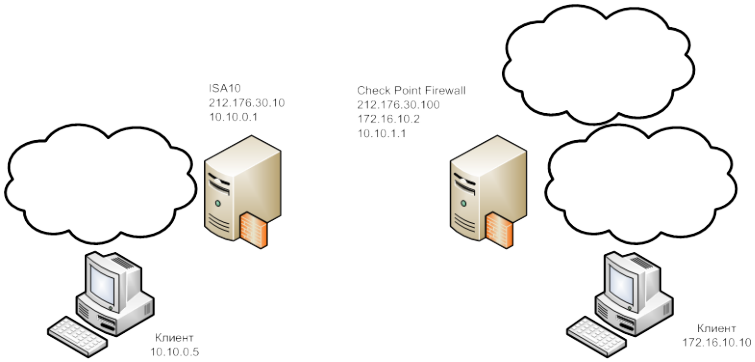
Настройка шлюза VPN на Microsoft Forefront TMG 2010

Последовательность шагов по развертыванию VPN-шлюза на Forefront TMG описаны в инструкции Microsoft “Настройка VPN-доступа типа сеть-сеть” (http://technet.microsoft.com/ru-ru/library/bb838949.aspx)

Настройка шлюза на Check Point Firewall-1/VPN-1 версии R65 HFA50 GOST

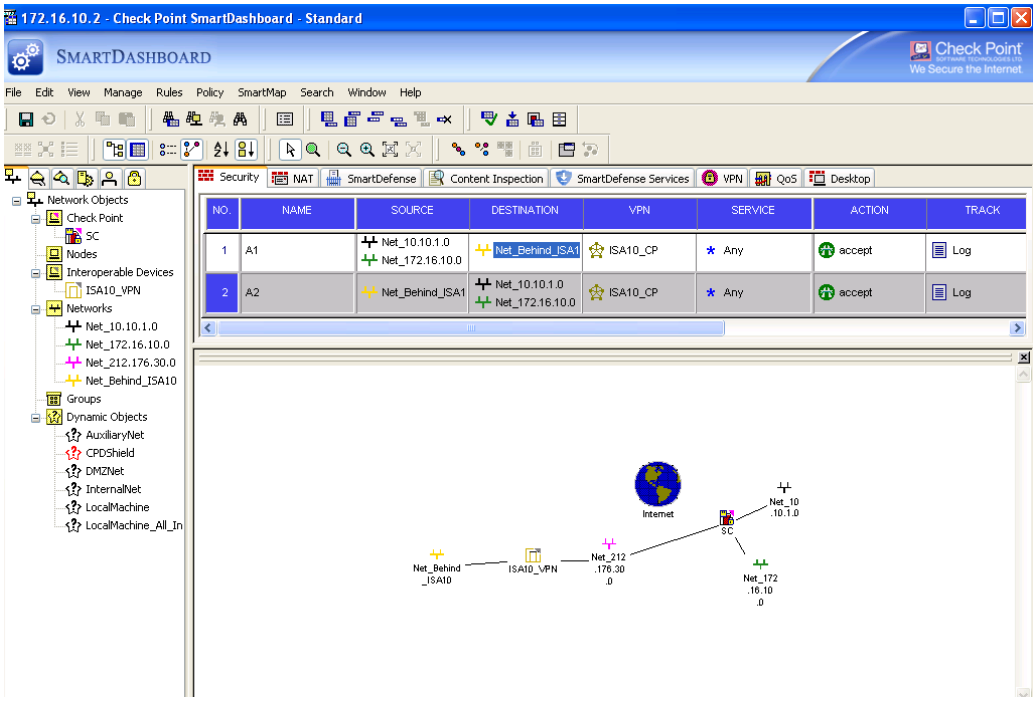
Рассмотрим настройку на примере подключения двух подсетей: 10.10.0.0/24 (ISA Server) и 172.16.10.0/24 (Check Point Firewall) (см. Рисунок 28).

Рисунок 28 Check Point Firewall



Все настройки производятся из панели Check Point Smart Dash Board (см. Рисунок 29).

Рисунок 29 Smart Dash Board



VPN соединение на Check Point Firewall-1/VPN-1 версии R65 HFA50 GOST создается используя Simplified Mode – Policy \ Global Properties.

Создадим сетевой объект (**New Network)** Net_10.10.1.0 для сети 10.10.1.0, используя закладку NAT добавим трансляцию адресов.

Аналогично создадим сетевой объект (**New Network)** Net_172.16.10.0 для сети 172.16.10.0.

Рисунок 30 Net_10.10.1.0

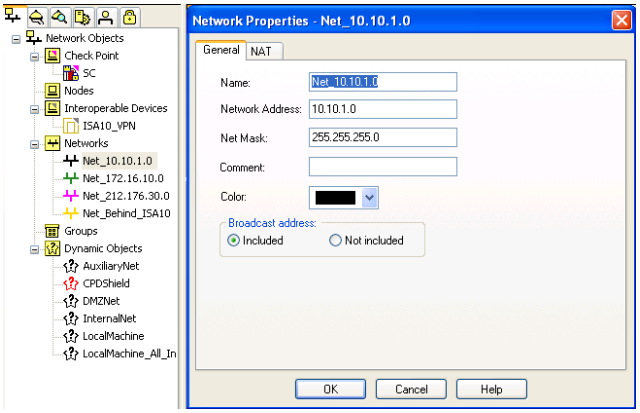
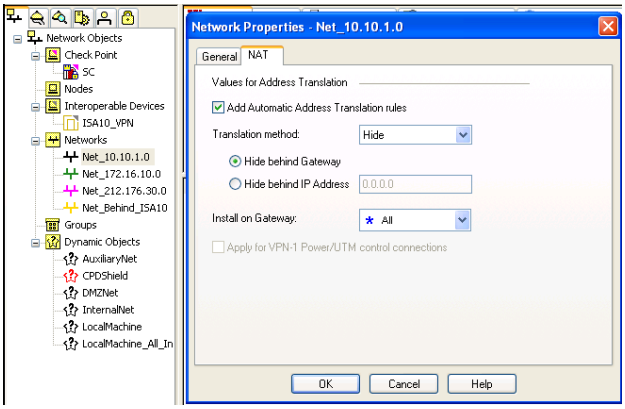


Рисунок 31 Net_172.16.10.0



Выбираем панель **NAT**, должно добавится четыре правила два из них поддерживают трансляцию адресов, два разрешают доступ из соответствующей сети к интерфейсам.

Создадим сетевой (**Network**) объект (**New Network)** для сети 212.176.30.0 (внешнего интерфейса), без добавления трансляции адресов(Net_212.176.30.0).

Создадим сетевой (**Network**) объект (**New Network)** для сети 10.10.0.0, которая расположена за ISA сервером(Net_behind_ISA10) .

Из SmartDashboard интерфейса нажмем **Manage** меню, и выберем **Network Object.** В окне **Network Object** выберем объект Net_behind_ISA10, нажмем кнопку **New** и выбираем «**Interoperable Device...»**.

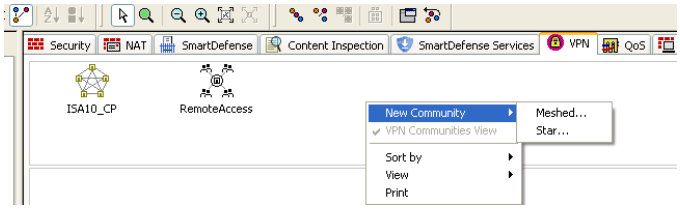
Interoperable Device описывает наш ISA VPN шлюз. В **General Properties** этого **Interoperable Device** вводим его имя (**Name**) - ISA10_VPN и IP адрес шлюза ISA - 212.176.30.10.

В **Topology** - в таблице вручную описываем интерфейсы ISA: 212.176.30.10(ext_212.176.30.10) объявляем как external, 10.10.0.1(int_10.10.0.1) объявляем как internal – specific и привязываем к Net_behind_ISA10. В **VPN Domain** выберем опцию **All IP address behind Gateway…** .

Нажимаем OK для того чтобы добавить новый **Interoperable Device** и закрываем **Network Object**.

Используя **SmartDashboard** - выбираем **VPN manager** панель и на пустом поле правым щелчком выбираем **New Community** –> **Meshed** (см. Рисунок 32).

Рисунок 32 New Community



В **General** вводим удобное нам имя, цвет, если помечаем **Accept all encrypted traffic** то правило безопасности создаются автоматически, поскольку мы будем создавать вручную мы его не активизируем.

В **Participating Gateways** добавляем(Add) Interoperable Device ISA10_VPN и Check Point gateway SC.

В **VPN Properties** помечаем **This community uses GOST standard for both IPSEC and IKE**.

В **Advanced Settings** –> **Shared Secret** помечаем «галочкой» **Use only Shared Secret for all External** members и используя кнопку **Edit** вводим PSK.

В **Advanced Settings** –> **Advansed VPN Properties** помечаем **Disable NAT inside the VPN community**. **Use Perfect Forward Secrecy** на время тестирования можно отключить, а в дальнейшем включить. Нажимаем кнопку **OK**.

Перейдем к редактированию **Check Point gateway network object.**

В **General Properties: Name** – наименование(SC), **IP Address** внешний IP адрес интерфейса(212.176.30.100);

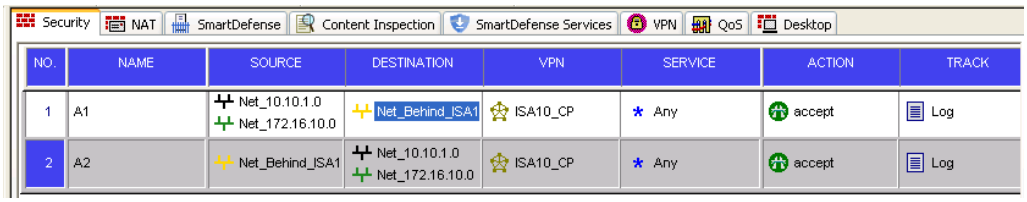
В **Topology**:нажмем кнопку **Get** –> **Interfaces with Topology**, должны в таблице появится интерфейсы устройства, **VPN Domain** выберем опцию **All IP address behind Gateway…**;

В VPN нажимаем кнопку Traditional mode configuration, в появившемся окне **Traditional mode configuration** убеждаемся что помечен Pre-Shared Secret .

В **VPN** –> **VPN Advansed** помечаем **Support NUT traversal…** и с помощью кнопки **Pre-Shared Secret** вводим PSK.

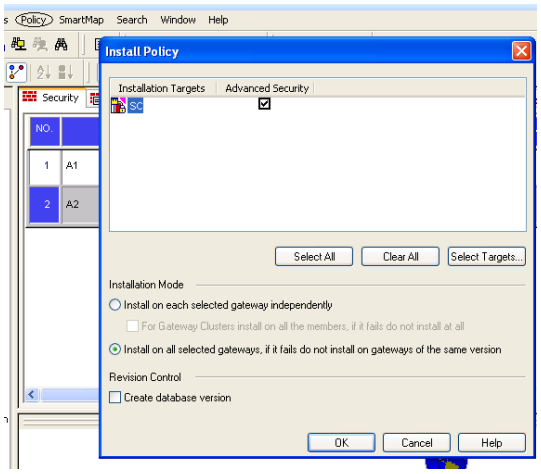
Создаем два правила безопасности одно исходящее и входящее (см. Рисунок 33).

Рисунок 33 Правила безопасности



Теперь необходимо сохранить и инсталлировать все введенные правила. Из SmartDashboard интерфейса нажмем Policy меню и выберем Install (см. Рисунок 34):

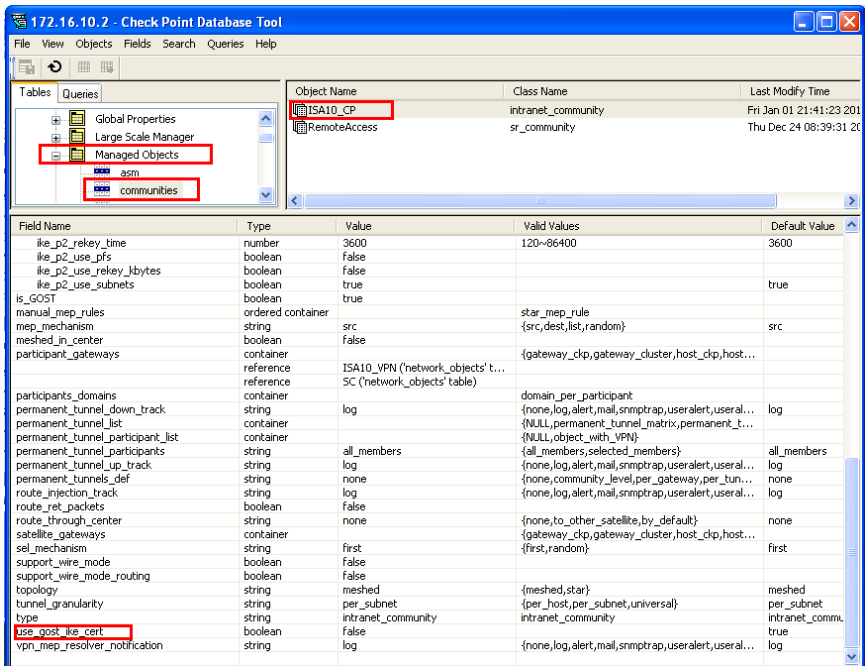
Рисунок 34 Install Policy



Закрываем окно **SmartDashboard**.

Подготовим **Check Point Firewall-1/VPN-1 версии R65 HFA50 GOST** для работы с PSK, для этого необходимо открыть утилиту из директории …\CheckPoint\SmartConsole\R65\PROGRAM\GuiDBedit.exe.

Рисунок 35 Check Point Database Tool

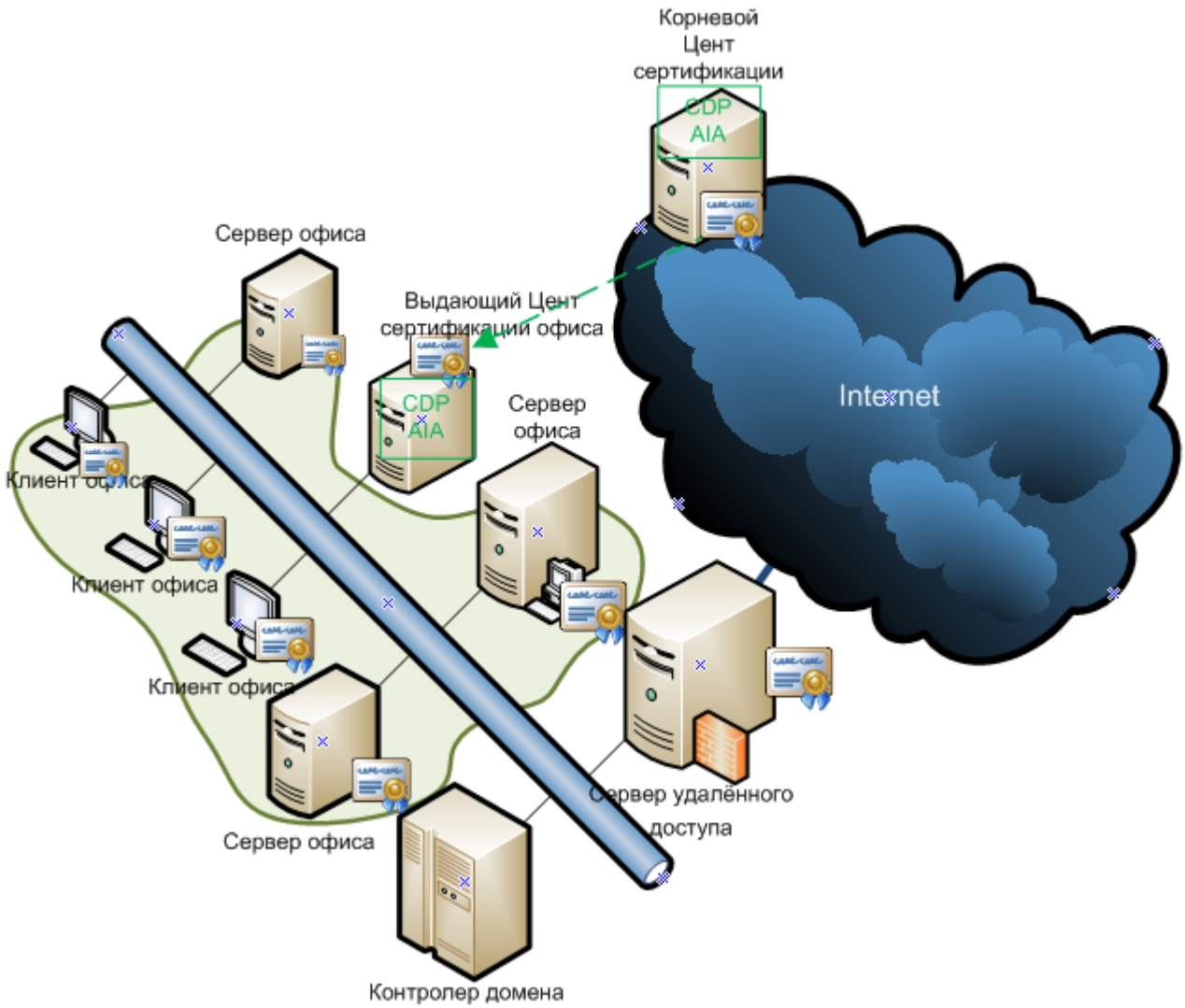


- в нашем тестовом VPN соединении ISA10_CP - переменную use_gost_ike_cert выставить в false.

10.3. Изоляция домена

В данном разделе будет описан сценарий настройки IPsec с помощью «**Политик IP-безопасности**». Применение IPsec в сетевых политиках позволяет криптографически, изолировать (на 3ем уровне модели OSI) как весь домен, так и: подразделения, сайты, группы компьютеров и серверов. Рассмотрим частный случай изоляции нескольких компьютеров в домене (см. Рисунок 36).

Рисунок 36 Изоляция группы компьютеров в домене



Установка политик безопасности IPsec может выглядеть следующим образом:

- Планирование и проектирование. Формирование логических групп безопасности: определение IP-фильтров, соответствующих компьютерам, подсетям, условиям окружения и необходимые для них действия безопасности;
- Создание Политик IPsec, Правил IPsec (фильтры, действия);
- Распространение Групповых политик (GPO) IPsec.

При проектировании сложных схем рекомендуется составлять таблицы и диаграммы сетевых подключений. В этом примере будут использованы всего 2 политики, перейдем к их определению без предварительного планирования.

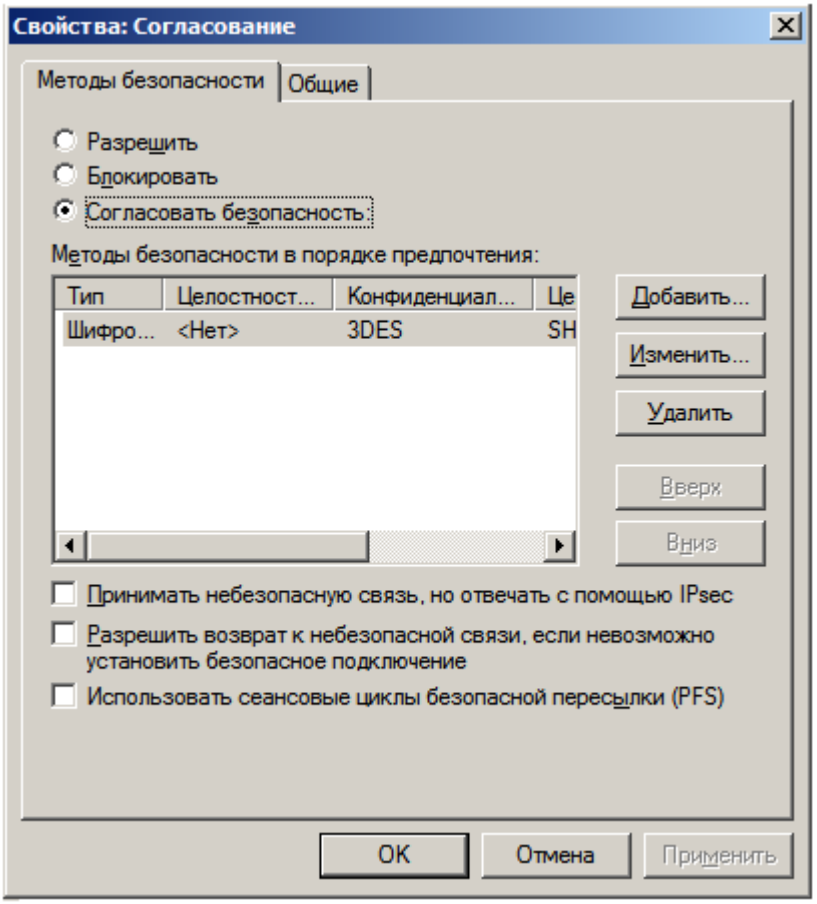
Для управления GPO в домене используется «**Редактор управления групповыми политиками**» (Group Policy Management Console,GPMC). Создаются два объекта групповой политики по инструкции:

- для Windows Server 2003 - «Creating and Editing GPOs» (http://technet.microsoft.com/ru-ru/library/cc782980%28WS.10%29.aspx);
- для Windows Server 2008 «Создание и изменение объекта групповой политики» (http://technet.microsoft.com/ru-ru/library/cc754740%28WS.10%29.aspx).

Один GPO назначается компьютерам в группе (в **подразделении**) **исключений**: контроллер домена, цент сертификации, DHCP, DNS-сервер. Для них трафик шифроваться не будет. В GPO для исключений создается Политика безопасности по инструкции Microsoft «Добавление, изменение и удаление политик IPSec» (http://technet.microsoft.com/ru-ru/library/cc778422%28WS.10%29.aspx), но без Правил безопасности.

Другой GPO привязан ко **всему домену**. В нем два правила безопасности. Первое Разрешает (действие фильтра) прохождение трафика к группе исключений (фильтр). Второе, строго требует шифрование (см. Рисунок 37) всего трафика (фильтр по умолчанию «**All IP Traffic**»)

Рисунок 37 Действие фильтра



Применение (замещение) GPO происходит в порядке, перечисленном в статье Microsoft «Обработка и приоритеты групповых политик» (http://technet.microsoft.com/ru-

ru/library/cc785665%28WS.10%29.aspx). Обновляется политика через заданные промежутки времени и при загрузке ОС.

При использование политик для изоляции всего домена (предприятия) без исключений важно помнить:

- о сложности конфигурации и управлении IPSec для защиты соединения между членами домена и: их контроллерами, DHCP, DNS-серверами, службами распространения ключей;
- IPSec не может согласовывать безопасность для многоадресного и широковещательного трафика;
- о проблемах, которые могут возникать с трафиком связи реального времени, и в одноранговых сетях.