ЧАСТЬ VII

Унифицированные коммуникации в среде Exchange Server 2010

В ЭТОЙ ЧАСТИ...

ГЛАВА 23

Проектирование и реализация мобильных возможностей в Exchange Server 2010

В ЭТОЙ ГЛАВЕ...

- Ознакомление с улучшениями, которые появились в Exchange Server 2010 касательно мобильных возможностей
- Включение службы ActiveSync в Exchange Server 2010
- Защита доступа к ActiveSync с помощью SSL-шифрования
- Защита доступа к ActiveSync с помощью ISA Server 2006
- Работа с политиками ActiveSync
- Работа с версиями Windows Mobile Pocket PC Edition и Windows Mobile Smartphone Edition

Система Microsoft Exchange Server 2010 специально разрабатывалась таким образом, чтобы предлагать более широкие возможности по сравнению с традиционной функциональностью, обеспечиваемой предшествующими системами обмена сообщениями. Возможности пользователей больше не ограничиваются получением и отправкой ответов на сообщения во время пребывания в офисе. Современному обществу с его быстрым темпом жизни требуются более скоростные методы для доступа почтовым данным, способные позволять работающим с информацией пользователям получать доступ к их сообщениям в любое время и из любого места.

Благодаря усовершенствованию способов для получения электронных сообщений и отправки ответов на них, в Exchange Server 2010 возможность работающих с информацией пользователей оставаться на связи значительно улучшилась. В Exchange Server теперь предусмотрена практически бесшовная интеграция между портативными мобильными устройствами вроде карманных ПК, смартфонов и телефонов iPhone, и почтовым ящиком Exchange Server, посредством улучшенного приложения Exchange ActiveSync.

Настоящая глава посвящена деталям развертывания Microsoft Exchange ActiveSync с Exchange Server 2010 и устройствами Windows Mobile. Здесь приводятся пошаговые примеры процедур развертывания ActiveSync и сравниваются различные подходы.

Ознакомление с улучшениями, которые появились в Exchange Server 2010 касательно мобильных возможностей

Microsoft Exchange ActiveSync представляет собой технологию, которая позволяет работающим с информацией сотрудникам получать доступ с портативного устройства к своим электронным сообщениями, календарным данным и другой информации. Работает она за счет туннелирования данных по протоколу HTTP (Hypertext Transfer Protocol — протокол передачи гипертекста), т.е. тому же самому, который применяется для транспортировки веб-трафика в Интернете.

Использование ActiveSync в среде Exchange Server 2010 предоставляет организациям небывалые возможности для управления удаленными устройствами и безопасностью, позволяя *производить очистку* данных с устройств, которые были утеряны или украдены, и принудительно применять политики, требующие шифровать данные и использовать пароли.

Краткая история мобильных улучшений в Exchange Server

Служба ActiveSync первоначально появилась в виде дополнительного продукта для Exchange 2000 Server и называлась MIS (Mobile Information Server — сервер мобильной информации). MIS был первым шагом Microsoft в области синхронизации карманных устройств и расширил ограниченные возможности развертывания.

Exchange Server 2003 стал первым выпуском платформы обмена сообщениями Exchange Server, в котором служба ActiveSync начала поставляться в виде встроенного компонента, хотя для ее включения требовалось выполнять отдельную процедуру. Первые версии программного обеспечения в Exchange Server 2003 не поддерживали автоматическую доставку электронных сообщений на карманные устройства, за ис-

ключением разве что технологии под названием *Always Up to Date* (Уведомления об актуальных изменениях), которая позволяла отправлять соответствующее уведомление на устройство посредством короткого текстового сообщения (SMS), после чего устройство могло подключаться и выполнять синхронизацию. Это, однако, отнимало много времени, серьезно истощало ресурсы батареи и вообще обходилось очень дорого.

В пакете обновлений для Exchange Server 2003 второй версии (Service Pack 2) была представлена новая технология под названием Direct Push, похожая на технологию в стиле BlackBerry и обеспечивавшая автоматическую доставку сообщений на карманное устройство по мере их получения. Это улучшение было встречено с воодушевлением.

В это же самое время еще продолжала совершенствоваться "карманная" операционная система Windows Mobile, которая раньше называлась Windows CE and PocketPC. Средства, предлагавшиеся для Windows Mobile 5.0 в пакете Messaging Security and Feature Pack (Пакет безопасности и возможностей обмена сообщениями), уже обладали встроенными возможностями, которые позволяли производить шифрование данных для устройств на уровне файлов и интегрировать их с возможностями, предлагавшимися в пакете обновлений Exchange Server 2003 Service Pack 2 для инициализации и деинициализации устройств по радиоканалу.

В Exchange Server 2010 возможности для мобильных устройств были расширены еще больше и оставили возможности технологии Direct Push, предлагавшейся в Exchange Server 2003 SP2 далеко позади. В частности они теперь позволяют производить настройку портативных устройств автоматическим образом, шифровать соединения, сбрасывать пароли и просматривать данные файлов на сервере SharePoint.

Что собой представляет Exchange ActiveSync

Exchange ActiveSync представляет собой службу, которая в топологии Exchange 2010 запускается на сервере клиентского доступа (Client Access Server — CAS). Она использует тот же самый виртуальный сервер, что и другие HTTP-средства доступа к Exchange Server, подобные Outlook Web App и Outlook Anywhere. Однако в отличие от них в ActiveSync имеется собственный виртуальный каталог, который называется `Microsoft-Server-ActiveSync`.

Поскольку механизм доступа ActiveSync похож на механизм доступа Outlook Web App (OWA), ее развертывание может проектироваться с использованием тех же соображений, что и развертывание клиентов OWA и Outlook Anywhere. В большинстве случаев ActiveSync развертывается в виде вспомогательной службы для этих продуктов. Но в любом случае после развертывания она становится жизненно важной службой в организации.

Включение службы ActiveSync в Exchange Server 2010

В Exchange 2010 ActiveSync само приложение стало более интегрированным со всеми остальными функциональными возможностями Exchange Server. После назначения серверу роли сервера клиентского доступа он оказывается очень близким к активизации поддержки ActiveSync. То есть далее, согласно рекомендациям Microsoft, администратор может предпринять несколько шагов по настройке для улучшения и упрощения доступа к ActiveSync.

Работа с параметрами ActiveSync в консоли управления Exchange Management Console

Многие из параметров ActiveSync на сервере клиентского доступа можно изменять в окне консоли управления Exchange Management Console, раскрыв узел Client Access (Клиентский доступ), как показано на рис. 23.1. Здесь можно как отключить ActiveSync вообще, так и изменить отдельные ее параметры для определенных почтовых ящиков получателей.

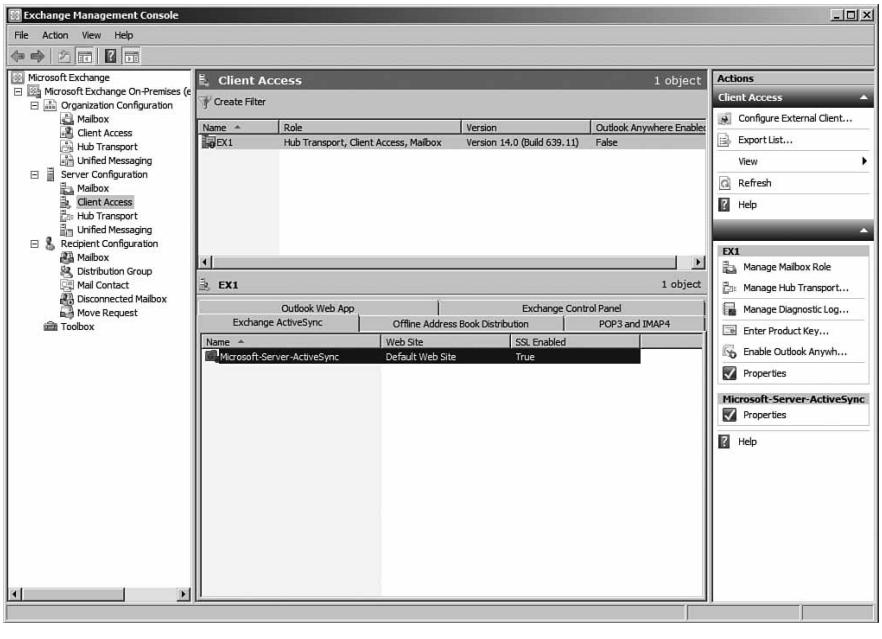

Рис. 23.1. *Администрирование параметров ActiveSync*

Щелкнув правой кнопкой мыши на элементе Microsoft-Server-ActiveSync в панели подробностей и выбрав в контекстном меню пункт Properties (Свойства), можно получить доступ к нескольким другим параметрам и изменять их. Эти параметры описаны ниже.

- External URL (Внешний URL-адрес). Этот параметр позволяет администратору вводить полностью уточненное доменное имя (Fully Qualified Domain Name — FQDN), которое будет использоваться для получения доступа к ActiveSync из Интернета, например, `https://mail.companyabc.com/Microsoft-Server-ActiveSync`.
- Authentication (Аутентификация). Здесь можно указывать методы аутентификации для виртуального каталога ActiveSync. Эта вкладка позволяет администратору конфигурировать сервер так, чтобы на нем использовалась базовая аутентификация (Basic Authentication), которая чаще всего применяется вместе с шифрованием по протоколу SSL (Secure Sockets Layer). Здесь также предлагается опция, позволяющая указывать, должна ли двухфакторная аутентификация (dual-factor authentication) с использованием сертификатов клиентов быть обязательной или же просто допустимой.

- Remote File Servers (Удаленные файловые серверы). На этой вкладке (рис. 23.2) представлены новые функциональные возможности в Exchange 2010, касающиеся доступа устройств Windows Mobile к данным файлов, которые находятся в сетевых папках (за счет указания путей в формате UNC (Universal Naming Convention — универсальное соглашение об именовании)) или на сайтах служб Windows SharePoint.

Рис. 23.2. *Конфигурирование параметров удаленных файловых серверов в ActiveSync*

НА ЗАМЕТКУ

Функциональными возможностями на вкладке Remote File Servers (Удаленные файловые серверы) можно пользоваться только в том случае, если устройство, функционирующее под управлением Windows Mobile, поддерживает их. На текущий момент их поддерживают только устройства, работающие под управлением как минимум версии Windows Mobile 6.0.

Конфигурирование параметров ActiveSync отдельно для каждого пользователя

Параметры отдельных почтовых ящиков можно конфигурировать для ActiveSync, раскрыв в панели консоли узел Mailbox (Почтовый ящик), который находится в разделе Recipient Configuration (Конфигурация получателя), как показано на рис. 23.3. Здесь можно включать и отключать ActiveSync для отдельных почтовых ящиков, а также применять к почтовому ящику политики ActiveSync, предназначенные для почтовых ящиков. Об этом более подробно рассказывается в разделе “Работа с политиками ActiveSync” далее в этой главе.

Щелкните правой кнопкой мыши на отдельном почтовом ящике и выберите в контекстном меню пункт Properties (Свойства) для открытия диалоговое окно Properties (Свойства). В этом окне перейдите на вкладку Mailbox Features (Функции почтового ящика), как показано на рис. 23.4, и включите или отключите Exchange ActiveSync для данного почтового ящика. Чтобы связать данный почтовый ящик с определенной политикой ActiveSync, щелкните на кнопке Properties.

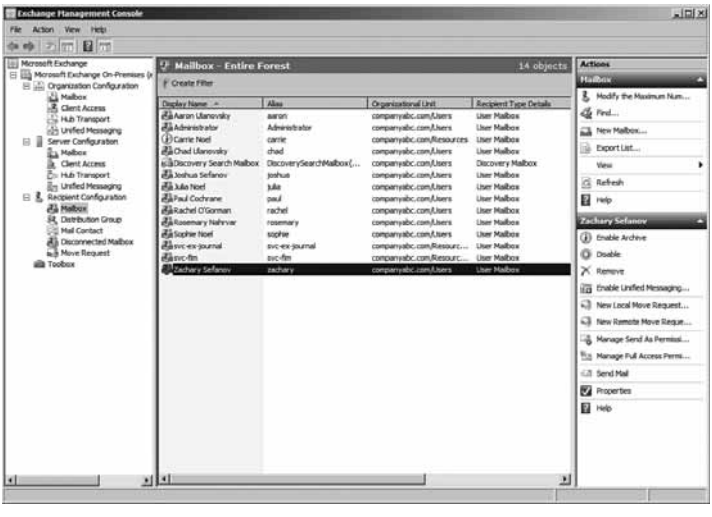

Рис. 23.3. *Просмотр почтовых ящиков в консоли управления Exchange Management Console*

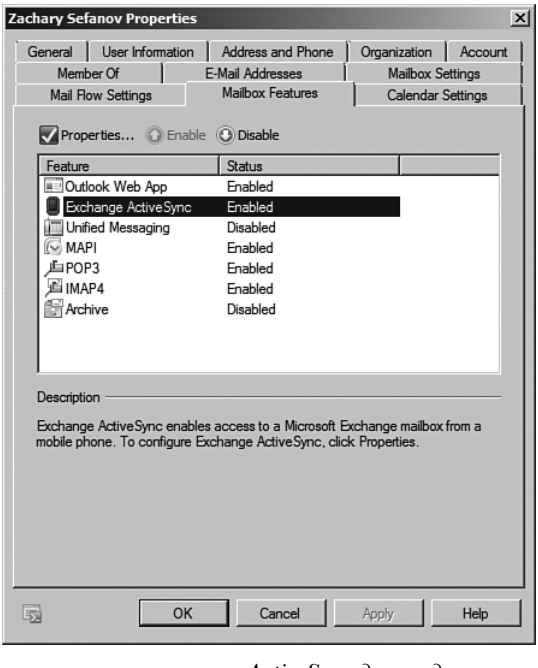

Рис. 23.4. *Включение или отключение ActiveSync для отдельного почтового ящика*

Защита доступа к ActiveSync с помощью SSL-шифрования

По умолчанию ActiveSync предусматривает использование встроенной (Integrated) аутентификации Windows. Такой метод аутентификации прекрасно подходит в случае получения доступа к серверу через надежную внутреннюю сеть, но совершенно не годится в случае получения доступа через Интернет, откуда большинство устройств его как раз и получает.

Из-за этого ограничения должен применяться метод аутентификации, который может работать в Интернете. Это сразу же ограничивает сервер ActiveSync применением метода базовой аутентификации, который поддерживается большинством веб-браузеров и устройств. Проблемой этого метода, однако, является то, что в случае его применения предоставляемые пользователем имя и пароль пересылаются в виде обычного текста, а это значит, что во время передачи могут перехватить. Более того, почтовые сообщения и другая конфиденциальная информация тоже передаются в виде обычного текста, что представляет серьезную угрозу безопасности.

Решением этой проблемы является применение к трафику так называемого шифрования по протоколу SSL (Secure Sockets Layer). SSL-шифрование выполняется с использованием сертификатов PKI (Public Key Infrastructure — инфраструктура открытого ключа), которые работают по принципу шифрования разделяемых ключей. Эти сертификаты сегодня очень широко применяются в Интернете, в частности, на любом веб-сайте, адрес которого начинается с префикса `https://`. Сообщество онлайновой коммерции пользуется ими для защиты своих систем.

В случае ActiveSync такой сертификат нужно устанавливать на сервере, чтобы трафик между устройством и сервером был защищен от любопытных глаз. Для этого существует два следующих способа.

- **Использование стороннего центра сертификатов.** Наиболее распространенным способом среди многих организаций является приобретение сертификата для ActiveSync (и других HTTP-средств доступа к Exchange вроде OWA) у надежного стороннего центра сертификатов (Certificate Authority — CA), например, VeriSign, Thawte и т.д. Этим центрам сертификатов уже доверяет огромное количество устройств, поэтому дополнительное конфигурирование не потребуется. Недостатком этого способа, однако, является то, что сертификат обязательно нужно приобретать, и возможности для изменения параметров этого сертификата очень ограничены.

- **Установка и использование собственного центра сертификатов.** Другим распространенным способом является установка и настройка поставляемого в Windows Server 2003/2008 компонента Certificate Services (Службы сертификатов) для создания в организации собственного центра сертификатов. Такой способ обеспечивает большую гибкость, поскольку позволяет создавать новые сертификаты, аннулировать существующие, и ничего при этом не платить. Его недостаток состоит в том, что никакие браузеры и мобильные устройства такой центр сертификатов распознавать не будут, из-за чего на них постоянно будут появляться соответствующие сообщения об ошибках.

Оба способа подробно рассматриваются в последующих разделах настоящей главы.

Использование стороннего центра сертификатов для активизации SSL-шифрования на сервере клиентского доступа

При желании использовать сторонний центр сертификатов для активизации SSL-шифрования на сервере, исполняющем роль сервера клиентского доступа (CAS), на этом сервере сначала нужно сгенерировать запрос на получение сертификата (certificate request). После генерации запрос следует отправить выбранному стороннему центру сертификатов. Далее центр проверит подлинность организации и вернет запрос с сертификатом обратно, после чего его можно будет установить на сервере.

Принимая решение о том, какой центр сертификатов использовать, следует иметь в виду, что устройства, функционирующие под управлением Windows Mobile, автоматически доверяют следующим центрам сертификатов:

- VeriSign
- Thawte
- GTE CyberTrust
- GlobalSign
- RSA
- Equifax
- Entrust.net
- Valicert (только Windows Mobile 5.0 и выше)

Если решено применять внутренний центр сертификатов, описываемые далее в этом разделе процедуры можно пропустить и перейти сразу же к разделу "Использование внутреннего центра сертификатов для сертификатов OWA".

Сгенерировать запрос на получение SSL-сертификата от стороннего CA можно либо из оболочки управления Exchange с помощью командлета `New-ExchangeCertificate`, либо прямо из IIS. Для оптимальной гибкости лучше использовать командлет PoweShell, поскольку он позволяет создавать в сертификате многочисленные записи SAN (Subject Alternative Name — альтернативное предметное имя) и тем самым предоставлять серверу Exchange возможность использовать, соответственно, многочисленные полностью уточненные доменные (FQDN) имена, подобные `mail.companyabc.com`, `autodiscover.companyabc.com`, `activesync.companyabc.com` и т.д.

После генерации запроса сертификата полученный текстовый файл, который будет выглядеть примерно так, как показано на рис. 23.5, можно отправить выбранному центру сертификатов либо по электронной почте, либо с помощью специального процесса. У каждого центра сертификатов существует своя процедура и свои шаги, которые необходимо выполнить. После проверки в центре сертификатов подлинности организации сертификат сервера будет отправлен обратно либо в виде отдельного файла, либо в виде части электронного сообщения.

Далее сертификат потребуется установить на самом сервере. Если сертификат получен в виде файла `.cer`, его можно будет просто импортировать, а если в виде вложения внутри текста сообщения, понадобится сначала вырезать и вставить его в окно текстового редактора и сохранить в файле с расширением `.cer`. После получения файла `.cer` можно переходить к его установке на сервере клиентского доступа с помощью командлета `Import-ExchangeCertificate`.

Рис. 23.5. *Пример файла с запросом на получение сертификата*

Использование внутреннего центра сертификатов для сертификатов OWA

Если использовать сторонний центр сертификатов не планируется, можно настроить внутренний центр. Для этого доступно несколько продуктов, в том числе от сторонних производителей, к тому же применение существующего внутреннего центра сертификатов может оказаться достаточно выгодным. В составе ОС Windows Server 2008 поставляется полнофункциональное решение для создания центра сертификатов, которое можно внедрить в организации.

ВНИМАНИЕ!

Надлежащее проектирование безопасной инфраструктуры открытого ключа (Public Key Infrastructure — PKI) представляет собой сложную тему, и потому организациям может потребоваться уделять больше времени изучению тех многочисленных факторов, которые способны оказывать влияние на структуру центра сертификатов. Рассматриваемый здесь пример сценария является базовым и предполагает просто установку внутреннего центра сертификатов непосредственно в домене. В большинстве организаций может оказаться выгоднее устанавливать один автономный корневой центр сертификатов (stand-alone root CA) и второй или даже третий промежуточный, который отвечает только за выдачу сертификатов, в зависимости от имеющихся в организации потребностей.

Ниже перечислены типы центров сертификатов, доступные для установки.

- Enterprise Root CA (Корневой центр сертификатов предприятия). Корневой центр сертификатов предприятия является для организации CA самого высокого уровня. По умолчанию все члены леса, в котором он устанавливается, доверяют ему, что может делать корневой CA удобным механизмом для защиты OWA и других служб в среде домена. Если корневой центр сертификатов предприятия существует, чаще всего именно он выбирается для создания в организации собственного внутреннего CA.
- Enterprise Subordinate CA (Подчиненный центр сертификатов предприятия). Подчиненный центр сертификатов предприятия подчиняется существующему корневому центру сертификатов и для нормальной работы требует, чтобы сертификаты поступали именно из корневого CA. В определенных крупных орга-

низациях может быть удобно создавать иерархию центров сертификатов или выделять для обслуживания OWA отдельную структуру подчиненных центров сертификатов.

- Stand-Alone Root CA (Автономный корневой центр сертификатов). Автономный корневой центр сертификатов похож на корневой CA предприятия тем, что также предусматривает использование собственных подтверждающих подлинность данных и может конфигурироваться уникальным образом. Отличается он тем, что никакие клиенты леса в организации ему автоматически не доверяют.
- Stand-Alone Subordinate CA (Автономный подчиненный центр сертификатов). Автономный подчиненный центр сертификатов похож на подчиненный CA и отличается от него только тем, что не имеет ни связи, ни отношений доверия ни с какой структурой леса и может получать свои сертификаты только от автономного корневого CA.

После установки внутреннего центра сертификатов в среде сервер клиентского доступа может автоматически начинать использовать его для генерирования сертификатов. На этом сервере также автоматически становится доступным SSL-шифрование. В случае установки центра сертификатов в домене Active Directory он будет автоматически добавляться на всех членах этого домена в список надежных корневых служб и подключаться к OWA через SSL без ошибок. Однако на внешних по отношению к этому домену клиентах центр сертификатов нужно будет специально добавлять в такой список. Это касается и устройств, функционирующих под управлением Windows Mobile. Процедура установки стороннего сертификата на устройстве, функционирующем под управлением Windows Mobile, более подробно описывается в следующем разделе этой главы.

Установка корневого сертификата на устройстве Windows Mobile

В случае использования для ActiveSync стороннего или сгенерированного самостоятельно центра сертификатов, устройства Windows Mobile должны конфигурироваться на доверие этому центру, иначе при попытке установить соединение через ActiveSync они будут выдавать сообщение об ошибке наподобие показанного на рис. 23.6.

В случае настольных систем и ноутбуков, функционирующих под управлением Windows, эта задача решается довольно легко и подразумевает установку корневого центра сертификатов предприятия для данного стороннего сертификата, в группу Trusted Root Certificate Authority (Надежный корневой центр сертификатов) на компьютере.

Рис. 23.6. *Ошибка, получаемая, когда устройство Windows Mobile не доверяет корневому центру сертификатов*

НА ЗАМЕТКУ

Выбирать необходимо корневой сертификат, а не фактический, который используется для виртуального сервера.

Для устройств Windows Mobile, однако, сначала нужно экспортировать выданный корневой службой сертификат в файл `.cer`, а затем физически скопировать этот файл на устройство Windows Mobile либо с помощью кнопки Explore (Найти) в Microsofr ActiveSync (пока устройство находится в подключенном состоянии), либо с помощью съемной карты памяти.

После копирования щелкните на файле `.cer` в проводнике файлов Windows Mobile (выберите в меню Start (Пуск) пункт Programs⇨File Explorer (Программы⇨Проводник файлов). Это приводит к отображению диалогового окна с предупреждением об установке сертификата. Щелкните на кнопке Yes (Да), чтобы автоматически установить сертификат и работать с ActiveSync через SSL.

Защита доступа к ActiveSync с помощью ISA Server 2006

Предоставление работающим с информацией сотрудникам доступа к технологиям, подобным ActiveSync, может значительно увеличить продуктивность, но в то же время подвергнуть организацию потенциальным угрозам извне. Подобно Outlook Web App или Outlook Anywhere, служба ActiveSync требует наличия доступного веб-соединения с сервером клиентского доступа. Она предназначена для использования при нахождении за пределами офиса, а это значит, что веб-трафик должен проходить через Интернет и быть доступен без использования специального клиента виртуальной частной сети (VPN).

Это приводит к появлению в некотором роде дилеммы: ведь используемый ActiveSync протокол HTTP может подвергаться атакам, а значит и потенциально подвергать данные организации ненужному риску. К счастью, Microsoft Exchange Server 2010 можно легко защитить от подобного рода атак за счет применения продукта для инспектирования уровня приложений вроде Internet Security and Acceleration (ISA) Server 2006, предлагаемого Microsoft.

Обратите внимание, что версия Exchange Server 2010 в ISA Server 2006 не распознается, но в нем все равно можно создавать правила для Exchange Server 2007 ActiveSync, которые подходят и для Exchange Server 2010. После выхода новой версии сервера ISA, в настоящее время называемой Forefront Edge Threat Management Gateway (TMG), рекомендуется ею заменить ISA Server 2006.

Как ISA Server 2006 может защитить ActiveSync

Продукт ISA Server 2006, по сути, представляет собой брандмауэр прикладного уровня, способный фильтровать HTTP-трафик на предмет наличия средств атаки и вредоносных программ. Он может быть как размещен на пути трафика ActiveSync (вместе с традиционным брандмауэром), так и выделен в отдельный обратный прокси-сервер, размещенный в демилитаризованной зоне (Demilitarized Zone — DMZ) брандмауэра, который отвечает за фильтрацию пакетов.

В последнем сценарии клиент будет считать, что получает доступ к серверу клиентского доступа напрямую, а на самом деле проходить секретную аутентификацию и сканирование на сервере ISA. Использование такого сценария, равно как и сценария с размещением ISA Server 2006 и обычного брандмауэра на пути трафика, является очень удобным способом для защиты трафика ActiveSync.

Создание правила защиты ActiveSync в ISA Server 2006

В этом разделе главы кратко объясняется, как с помощью ISA Server 2006 создать для ActiveSync правило веб-публикации. Более подробные сведения об использовании ISA Server с Exchange 2010 приведены в главе 13.

Ниже перечислены шаги, необходимые для создания правила в консоли ISA Server.

1. Откройте консоль управления ISA Management Console и перейдите в ее панели в раздел Firewall Policy (Политика брандмауэра).
2. На вкладке Tasks (Задачи) в панели задач щелкните на ссылке Publish Exchange Web Client Access (Публикация доступа к веб-клиентам Exchange).
3. На начальном экране мастера введите желаемое описательное имя, например, ActiveSync Rule (Правило ActiveSync), и щелкните на кнопке Next (Далее).
4. На экране Select Services (Выбор служб), который показан на рис. 23.7, выберите в списке Exchange version (Версия Exchange) вариант Exchange Server 2007 (он подходит и для Exchange Server 2010) и отметьте флажок Exchange ActiveSync (Служба Exchange ActiveSync). Для продолжения щелкните на кнопке Next.

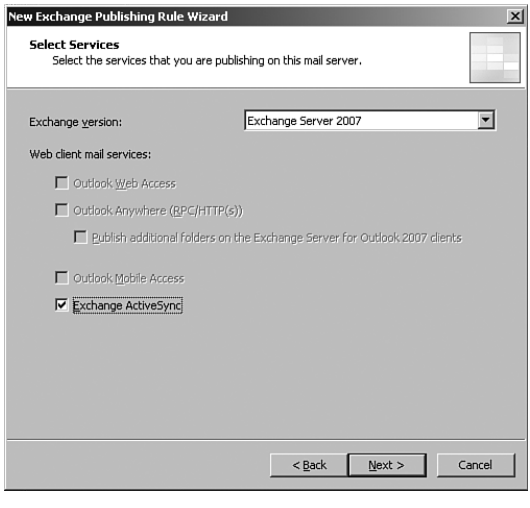

Рис. 23.7. *Создание правила ActiveSync с помощью ISA Server 2006*

5. На экране Publishing Type (Тип публикации) выберите переключатель Publish a Single Web Site or Load Balancer (Публикация балансировки одного веб-узла или внешней нагрузки) и щелкните на кнопке Next.
6. На экране Server Connection Security (Безопасность подключений сервера), который показан на рис. 23.8, выберите переключатель Use SSL to Connect to the Published Web Server or Server Farm (Использовать SSL для подключения к опубликованному веб-серверу или группе серверов). Это приведет к созданию сквозного SSL-подключения. Для продолжения щелкните на кнопке Next.
7. В поле Internal Site Name (Имя внутреннего узла) введите полное доменное имя (FQDN), которое клиенты используют для подключения к серверу клиентского доступа (CAS), как показано на рис. 23.9. Это имя обязательно должно совпадать с тем, которое применяют внешние клиенты, потому что в случае несовпадения

этих имен при установке SSL-подключения могут возникнуть проблемы. Если внутренняя служба DNS не перешлет данное FQDN-имя серверу клиентского доступа, может потребоваться "обмануть" сервер ISA и вынудить его преобразовать это имя в имя сервера клиентского доступа с помощью файла HOSTS. Для продолжения щелкните на кнопке Next.

8. На экране Public Name Details (Подробности общего имени) введите "This domain name" (Имя этого домена), а затем само общедоступное имя в формате FQDN, например, mail.companyabc.com. Щелкните на кнопке Next.

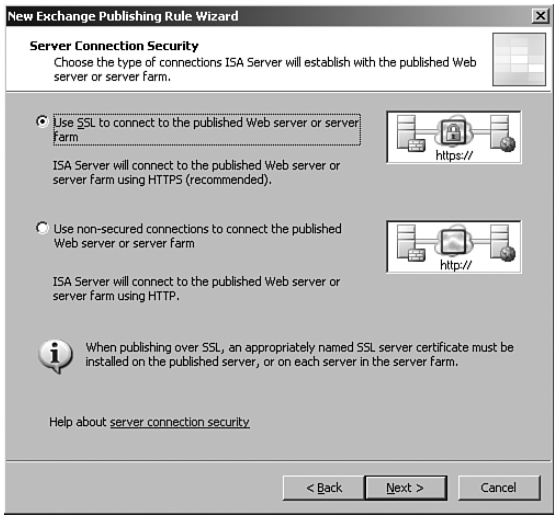

Рис. 23.8. *Защита правила ISA с помощью SSL*

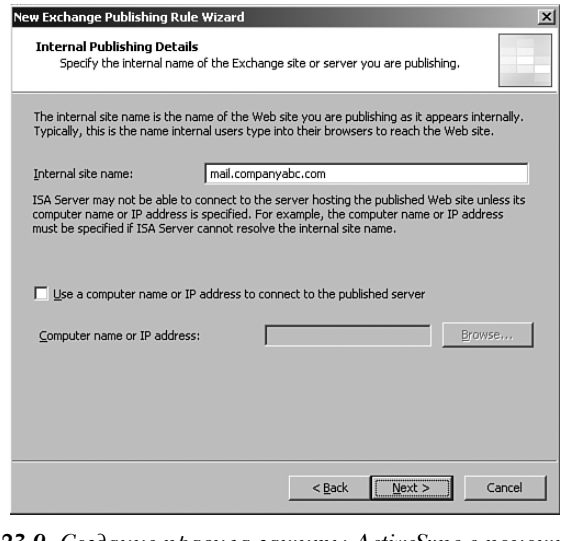

Рис. 23.9. *Создание правила защиты ActiveSync с помощью ISA*

9. На экране Web Listener (Веб-слушатель) можно либо выбрать существующего слушателя, который допускается использовать для OWA или Outlook Anywhere, либо щелкнуть на кнопке New (Создать) и создать нового. В данном примере щелкните на кнопке New.
10. На начальном экране мастера создания веб-слушателей (Web Listener Wizard) введите желаемое описательное имя для слушателя, например, Exchange HTTP/HTTPS Listener (Exchange-слушатель портов HTTP/HTTPS), и для продолжения щелкните на кнопке Next.
11. Откроется окно с приглашением указать, должно ли использоваться SSL-шифрование. Это приглашение касается трафика между клиентом и ISA, к которому SSL-шифрование должно применяться всегда, когда это возможно. Поэтому оставьте выбранным предлагаемый по умолчанию вариант и щелкните на кнопке Next.
12. На экране Web Listener IP Addresses (IP-адреса веб-слушателя) установите переключатель External Network (Внешняя сеть) и оставьте для него выбранным значение All IP Addresses (Все IP-адреса), после чего щелкните на кнопке Next.
13. На экране Listener SSL Certificates (SSL-сертификаты слушателя) щелкните на кнопке Select Certificate (Выбрать сертификат).
14. Выберите сертификат `mail.companyabc.com`. Если сертификат находится не на сервере ISA, его следует установить на этом сервере в хранилище Certificates (Сертификаты), выполнив шаги, описанные в главе 3.
15. Для продолжения щелкните на кнопке Next.
16. На экране Authentication Settings (Параметры аутентификации) выберите в раскрывающемся списке значение HTTP Authentication (HTTP-аутентификация) и отметьте флажок Basic (Базовая), как показано на рис. 23.10. Оставьте выбранным переключатель Windows (Active Directory) и щелкните на кнопке Next.

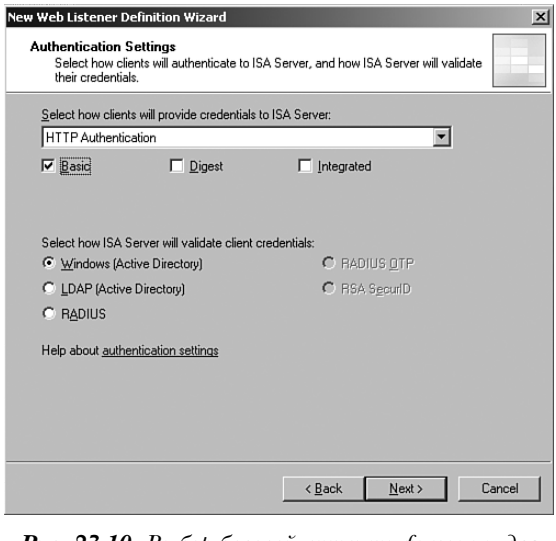

Рис. 23.10. *Выбор базовой аутентификации для правила ActiveSync на сервере ISA*

17. На экране Single Sign On Settings (Настройка единого входа) щелкните на кнопке Next. При базовой аутентификации возможность настройки единого входа (SSO) не доступна.
18. Щелкните на кнопке Finish (Готово), чтобы завершить работу мастера.
19. После того, как новый слушатель появится в диалоговом окне Web Listener (Веб-слушатель), щелкните на кнопке Next.
20. На экране Authentication Delegation (Делегирование аутентификации) выберите в раскрывающемся списке значение Basic. Это значение нужно использовать потому, что был выбран защищенный механизм транспортировки. Для продолжения щелкните на кнопке Next.
21. На экране User Sets (Наборы пользователей) оставьте выбранным переключатель All Authenticated Users (Все аутентифицированные пользователи). В более строгих сценариях права на доступ к OWA могут предоставляться только определенным группам Active Directory. В данном случае значение по умолчанию вполне подходит. Для продолжения щелкните на кнопке Next.
22. Щелкните на кнопке Finish, чтобы завершить работу мастера.
23. Щелкните на кнопке Apply (Применить) в панели подробностей, а затем, когда изменения будут применены, щелкните на кнопке OK.

После этого созданная политика ActiveSync появится в панели подробностей, как показано на рис. 23.11. При необходимости ее можно будет настроить даже еще более точно.

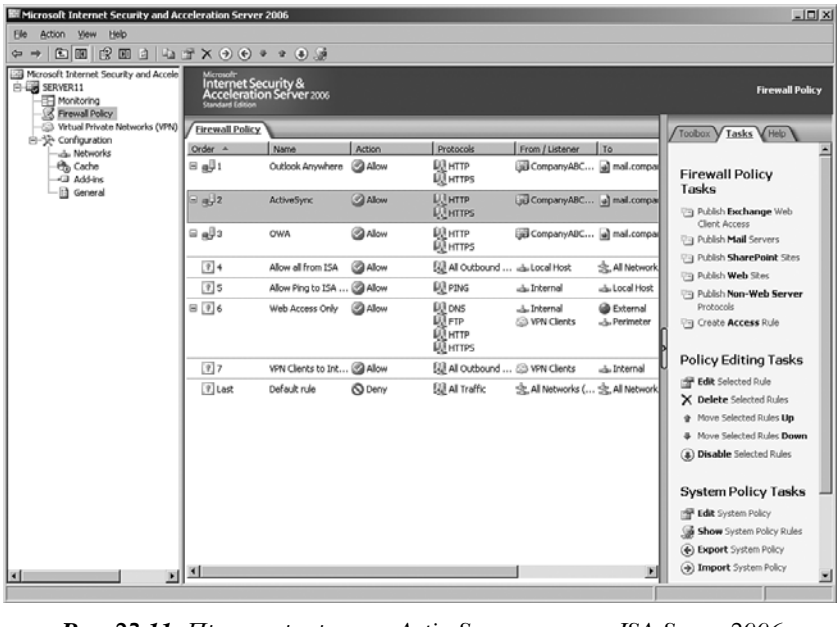

Рис. 23.11. *Просмотр правила ActiveSync в консоли ISA Server 2006*

Работа с политиками ActiveSync

Служба ActiveSync в Exchange 2010 предоставляет беспрецедентные возможности для защиты и управления устройствами. В частности, она позволяет администратору создавать предназначенные для почтовых ящиков политики ActiveSync, способные принуждать устройства соблюдать конкретные ограничения, например, требовать применения сложных паролей или шифрования файлов.

Помимо этого, ActiveSync в Exchange 2010 позволяет администратору создавать много политик в организации и тем самым применять, скажем, в отношении пользователей с карманными устройствами более строгие политики, не ограничивая при этом столь же строго всех остальных пользователей. Например, в лечебном учреждении может потребоваться, чтобы все устройства, на которых хранятся конфиденциальные данные пациентов, принудительно шифровались и защищались паролем, а на остальных пользователей эти ограничения не распространялись.

Создание политик ActiveSync для почтовых ящиков

Создание новой политики для почтового ящика в Exchange Server 2010 не является сложной задачей. Ниже перечислены необходимые шаги.

1. Откройте консоль управления Exchange Management Console, разверните узел Organization Configuration (Конфигурация организации) и щелкните на папке Client Access (Клиентский доступ).
2. В панели задачи щелкните на ссылке New Exchange ActiveSync Mailbox Policy (Создать политику ActiveSync для почтового ящика Exchange).
3. Введите описательное имя для политики, например, Manager's ActiveSync Mailbox Policy (Политика ActiveSync для почтового ящика менеджера). Настройте параметры, касающиеся пароля, например, так, как показано на рис. 23.12, и щелкните на кнопке New (Создать).
4. Щелкните на кнопке Finish (Готово).

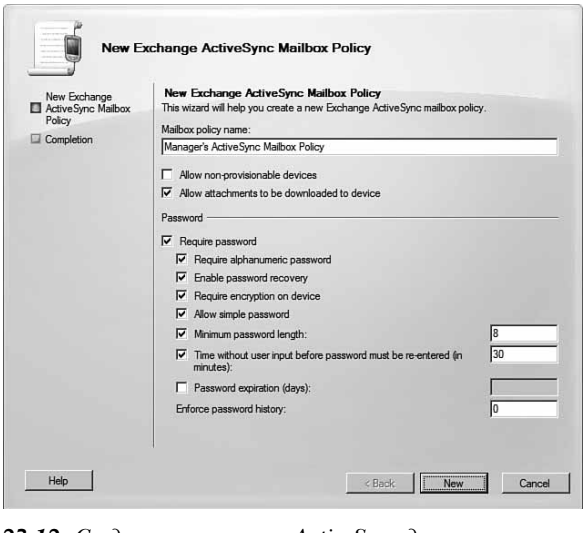

Рис. 23.12. *Создание политики ActiveSync для почтовых ящиков*

Применение политик к почтовым ящикам пользователей

После создания политику можно применять к почтовым ящикам. Это делается либо во время процесса подготовки, либо после создания почтовых ящиков. Шаги, необходимые для применения политики к существующим почтовым ящиками, перечислены ниже.

1. Откройте консоль управления Exchange Management Console, разверните узел Recipient Configuration (Конфигурация получателя) и щелкните на папке Mailbox (Почтовый ящик).
2. Щелкните правой кнопкой мыши на почтовом ящике, к которому требуется применить политику, и выберите в контекстном меню пункт Properties (Свойства).
3. Перейдите на вкладку Mailbox Features (Функции почтового ящика), выберите переключатель ActiveSync (Служба ActiveSync) и щелкните на кнопке Properties (Свойства).
4. Отметьте флажок Apply an Exchange ActiveSync Mailbox Policy (Применить политику ActiveSync для почтовых ящиков Exchange).
5. Выберите в списке нужную политику, например, как показано на рис. 23.13, и щелкните на кнопке OK.
6. Щелкните на кнопке OK два раза, чтобы сохранить изменения.

Применять определенную политику сразу к нескольким почтовым ящиками лучше всего с помощью консоли PowerShell.

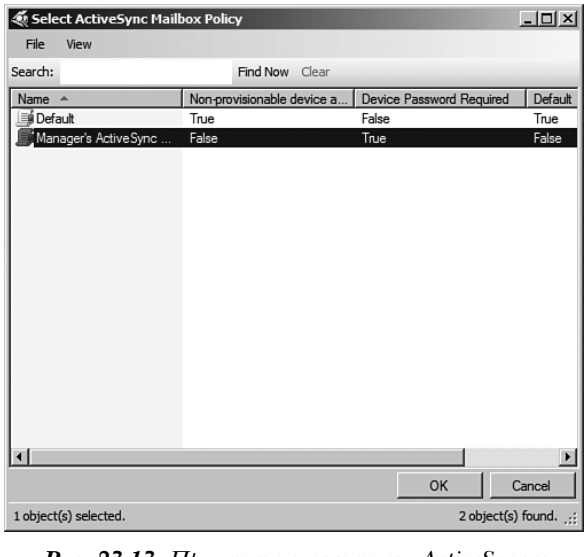

Рис. 23.13. *Применение политики ActiveSync к конкретному почтовому ящику*

Очистка и сброс устройств ActiveSync

Одним из преимуществ службы ActiveSync в Exchange Server 2010 является наличие у нее оптимизированных возможностей для управления. ActiveSync позволяет произ-

водить удаленный сброс паролей и полную очистку данных на устройствах Windows Mobile в случае их утери или кражи. В сочетании с возможностями шифрования, доступными в пакете средств защиты системы обмена сообщениями (Messaging Security Feature Pack), эта концепция позволяет организациям развертывать ActiveSync и не бояться того, что важные данные могут оказаться в чужих руках.

Чтобы получить доступ к этим функциональным возможностям ActiveSync, необходимо щелкнуть правой кнопкой мыши на интересующем почтовом ящике в подразделе Mailbox (Почтовый ящик) внутри раздела Recipient Configuration (Конфигурация получателя) и выбрать в контекстном меню пункт Manage Mobile Device (Управление мобильным устройством). Вдобавок пользователям разрешено удаленно производить очистку устройств через Outlook Web App.

Работа с версиями Windows Mobile Pocket PC Edition и Windows Mobile Smartphone Edition

Служба Exchange Server 2010 ActiveSync поддерживает синхронизацию с клиентами многих типов, в том числе и с некоторыми устройствами, функционирующими под управлением операционных систем, которые не являются продуктами Microsoft. Однако в принципе лучше всего поддерживаются, конечно же, устройства, работающие под управлением ОС Windows Mobile 5.0 или 6.0. Устройства Windows Mobile 5.0 могут интегрироваться с пакетом Messaging Security Feature Pack для шифрования данных и обеспечения возможностей удаленной смены пароля и удаленной очистки. В Windows Mobile 6.0 имеются дополнительные возможности, такие как получение доступа к файлам через UNC-пути и управление документами с помощью библиотек Microsoft Office SharePoint Server 2007 Document.

Доступно две *разновидности* Windows Mobile, которые могут синхронизироваться с Exchange Server. Первая называется Windows Mobile Pocket PC Edition и предназначена для устройств типа Pocket PC, многие из которых оборудованы пером и/или клавиатурой. Вторая называется Windows Mobile Smartphone Edition и предназначена для более простых мобильных устройств типа телефонов с раскрывающейся клавиатурой и экраном и карманных устройств, не имеющих клавиатуры. В этом разделе приводятся инструкции по конфигурированию обеих версий Windows Mobile.

Настройка версии Windows Mobile Pocket PC Edition для синхронизации с ActiveSync

Версия Windows Mobile Pocket PC Edition широко используется во многих ультрасовременных устройствах и предполагает наличие у них экрана, большего, чем у большинства сотовых телефонов. У многих из таких устройств также имеется и клавиатура. Ниже перечислены шаги, необходимые для настройки телефона, функционирующего под управлением Windows Mobile Pocket PC Edition, на поддержку синхронизации с сервером Exchange через ActiveSync.

1. На экране Windows Mobile выберите в меню Start (Пуск) пункт Programs (Программы).
2. Щелкните на ActiveSync.
3. Когда появится окно с вариантами синхронизации, выберите в нем ссылку Set Up Your Device to Sync with It (Настроить устройство для синхронизации).

4. В диалоговом окне, которое появится после этого, введите полное доменное имя (FQDN) сервера ActiveSync, как показано на рис. 23.14, и удостоверьтесь, что флажок This Server Requires an Encrypted (SSL) Connection (Этот сервер требует использовать шифрованное (SSL) соединение) отмечен. Полное доменное имя должно соответствовать тому, что указано в сертификате. Для продолжения щелкните на кнопке Next (Далее).

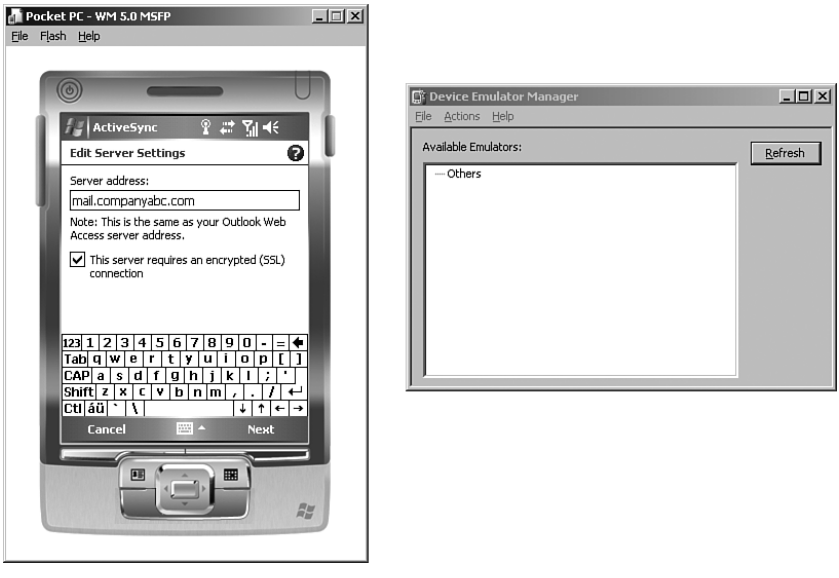

Рис. 23.14. *Настройка параметров сервера, касающихся ActiveSync*

5. Введите действительное имя пользователя, пароль и имя домена, и укажите, что пароль должен быть сохранен, после чего щелкните на кнопке Next.

6. В диалоговом окне, которое появится далее и показано на рис. 23.15, выберите типы данных, подлежащие синхронизации. После выбора элемента Calendar (Календарь) или E-mail (Электронная почта) и щелчка на кнопке Settings (Настройка) появится возможность указать, какой объем таких данных подлежит синхронизации. По завершении щелкните на кнопке Finish (Готово).

7. Щелкните на кнопке Sync (Синхронизировать), чтобы подключиться к серверу Exchange.

После этого на мобильном устройстве автоматически запустится процесс синхронизации. Он может инициироваться и вручную, но если устройство, функционирующее под управлением Windows Mobile, поддерживает технологию Direct Push, то электронные сообщения будут доставляться на телефон автоматически.

Настройка версии Windows Mobile Smartphone Edition для синхронизации с ActiveSync

Во многих традиционных мобильных телефонах (у которых не имеется ни клавиатуры, ни пера, ни большого, как у карманных ПК, дисплея) используется операцион-

ная система версии Windows Mobile 5.0 или 6.0 Smartphone Edition, которая позволяет оператору синхронизировать телефон с Exchange Server 2010 и ActiveSync. Процедура по настройке синхронизации для этой версии очень похожа на ту, что применяется для версии Windows Mobile 5.0 Pocket PC Edition, и отличается от нее лишь несколькими действиями. Ниже описаны шаги, из которых она состоит.

НА ЗАМЕТКУ

Оборудование на многих смартфонах отличается, поэтому некоторые из приводимых в описываемой далее пошаговой процедуре кнопок могут называться по-другому. Однако в целом процесс должен выглядеть примерно одинаково для любой системы Windows Mobile 5.0 Smartphone Edition.

1. Нажмите на смартфоне кнопку, которая соответствует команде Start (Пуск).
2. Перейдите к ActiveSync и нажмите на смартфоне кнопку, которая соответствует команде Select (Выбрать) или Enter (Ввод).
3. Когда появится диалоговое окно, показанное на рис. 23.16, выберите в нем ссылку Set Up Your Device to Sync with It (Настроить устройство для синхронизации).
4. Ввести полное доменное имя (FQDN) сервера ActiveSync, такое как `mail.companyabc.com`. Отметьте флажок, указывающий на использование SSL-шифрования, и нажмите на смартфоне кнопку, которая соответствует команде Next (Далее).

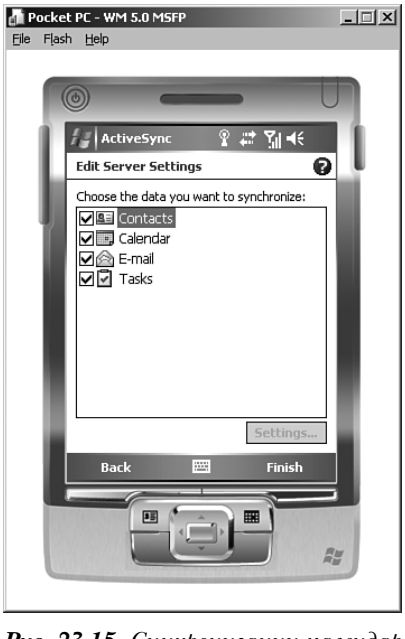

Рис. 23.15. *Синхронизации календаря, электронной почты и контактной информации с помощью ActiveSync*

Рис. 23.16. *Настройка версии Windows Smartphone Edition для синхронизации с ActiveSync*

5. Введите действительное имя пользователя, пароль и имя домена, и удостоверьтесь, что флажок Save Password (Сохранить пароль) отмечен, как показано на рис. 23.17, после чего нажмите кнопку, соответствующую команде Next.
6. В следующем диалоговом окне выберите данные, которые требуется синхронизировать, например, контакты, календарь, электронную почту или задачи, и нажмите кнопку, которая соответствует команде Finish (Готово).

После этого на телефоне начнется процесс синхронизации выбранных данных с сервером ActiveSync. Аналогичные шаги можно использовать для телефонов Apple iPhones и других поддерживающих ActiveSync устройств: достаточно ввести полное доменное имя сервера ActiveSync в Интернете, а потом предоставить имя пользователя и пароль.

Рис. 23.17. *Ввод учетных данных, необходимых для получения доступа к ActiveSync*

Резюме

Концепция "офис без стен" быстро становится реальностью, поскольку в распоряжении работающих с информацией сотрудников теперь имеется масса вариантов, которые позволяют им связываться со своими коллегами с помощью таких технологий Exchange Server 2010, как ActiveSync. Служба ActiveSync в Exchange Server 2010 предлагает небывалые возможности для управления и защиты устройств, благодаря которым организации могут пользоваться предоставляемыми такими устройствами преимуществами и повышать свою продуктивность, не рискуя безопасностью.

Полезные советы

Ниже представлен набор полезных советов, основанный на материале этой главы.

- Всегда применяйте вместе с технологиями ActiveSync SSL-шифрование.
- Для получения возможности более точной настройки связанных с паролями и шифрованием параметров для мобильных устройств стоит рассмотреть вариант использования политик ActiveSync, предназначенных для почтовых ящиков.
- В случае использования для синхронизации почтового ящика с ActiveSync смартфона или телефонного устройства типа PDA (Personal Digital Assistant — персональный цифровой помощник), рассмотрите вариант приобретения у поставщика этого мобильного телефона безлимитного пакета, поскольку объем подлежащих передаче данных может оказаться очень большим.
- Чтобы избежать необходимости устанавливать сертификат на каждом мобильном устройстве, рассмотрите возможность использования надежного стороннего корневого центра сертификатов для обеспечения SSL-соединения с ActiveSync.
- Защищайте HTTP-трафик ActiveSync на серверах клиентского доступа за счет реализации ISA Server 2006, чтобы иметь возможность следить за трафиком с помощью возможностей инспектирования прикладного уровня.