ГЛАВА 4

Проектирование инфраструктуры ISA Server 2006

В ЭТОЙ ГЛАВЕ...

- Подготовка к созданию проекта ISA Server 2006
- Миграция с ISA Server 2000/2004 на ISA Server 2006
- Определение количества серверов ISA Server и их размещения
- Создание прототипа ISA Server
- Макетирование развертывания ISA Server
- Внедрение проекта ISA Server
- Проектирование ISA Server 2006 для организаций разного масштаба
- Резюме
- Полезные советы

Успех внедрения ISA Server в большой мере зависит от проекта. ISA Server 2006 — это сложная и мощная система, которой можно доверить выполнение в организации самых различных задач. Поэтому очень важно сначала понять, в чем собственно заключаются задачи обеспечения безопасности, а потом связать эти задачи с различными возможностями ISA Server.

Вследствие того, что ISA Server может решать самые разнообразные задачи, проект ISA Server не всегда будет полностью соответствовать распределенным ролям. В действительности проектирование ISA Server может затрагивать работу большого количества серверов ISA Server, распределенных в сети. Необходимость обеспечения безопасности сети была задействована для осуществления как внешнего, так и внутреннего трафика в пределах организации. Возможности ISA Server 2006 позволяют выполнить эти задачи.

Эта глава фокусируется на факторах, которые необходимо принимать во внимание в процессе такого проектирования и которые должны учитываться во время развертывания ISA Server 2006. Особенно важно выработать четкую методологию безопасности, так как это позволит избежать ошибок при развертывании. Кроме методологии создания безопасного и обновляемого проекта, также описываются шаги, необходимые для перехода с ISA 2000 Server на ISA Server 2006. Наконец, приведены примеры проектов для малых, средних и больших организаций.

Подготовка к созданию проекта ISA Server 2006

Во время проектирования внедрения ISA Server любого масштаба, лучше всего воспользоваться методологией проектирования, которая уже дала успешные результаты. Существует большое количество способов, позволяющих этого добиться, причем различные методологии характеризуются различными уровнями успеха. В целом рекомендуется следовать методологии проектирования, которая в прошлом уже доказала свою успешность. В общем случае методологию проектирования для ISA Server можно считать успешной, если она помогает определить текущие нужды обеспечения безопасности и цели и ставит им в соответствие определенные функциональные возможности ISA Server.

Определение целей, стоящих перед системой безопасности, и ее задач

Несмотря на то что эта задача довольно тривиальна, не всегда просто бывает определить, выполнение каких целей и задач должен обеспечивать ISA Server 2006. Многие организации осознают, что необходимо добиться “лучшей безопасности”, но у них нет времени на определение того, что означает “лучшей”. Без ответа на этот вопрос невозможно решить задачу, поэтому заблаговременно необходимо правильно определить цели и задачи.

Каждая организация имеет различные задачи такого рода и совершенно не представляется возможным их всех здесь перечислить, однако в числе некоторых наиболее общих можно назвать следующие:

- обеспечение безопасности служб, работающих с сетью Интернет;
- обеспечение возможности управления трафиком между сегментами сети;

- обеспечение возможности отчетности по структуре Интернет-трафика;
- снижение потребления пропускной способности канала Интернет;
- предоставление сотрудникам организации безопасного доступа к сетевым ресурсам с удаленных рабочих мест;
- проектирование инфраструктуры, соответствующей положениям таких законодательных актов, как HIPAA[1] или закон Сарбана-Оксли[2];
- снижение нагрузки и сложности инфраструктуры управления безопасностью.

Первый этап процесса проектирования заключается в предварительном выделении этих целей и задач для того, чтобы выработать план действий. Затем эта информация используется в последующих частях проекта.

Документирование и определение установок существующей инфраструктуры

Зачастую складывается очень интересная картина: во многих организациях отсутствует актуальный набор проектной документации о функционирующей сети и инфраструктуре безопасности. Когда речь заходит об этом, у ИТ-организаций, которые собственно должны разрабатывать такую документацию, часто не хватает времени. Однако очень важно хранить этот тип информации под рукой, особенно в свете таких новых законодательных положений, как закон Сарбана-Оксли, который обусловил необходимость в наличии внятной документации подобного рода.

Поэтому перед тем, как приступить к реализации ISA Server, очень важно собрать всю имеющуюся документацию для того, чтобы определить инфраструктуру, в которой будет устанавливаться ISA Server. Время, когда разворачивается ISA Server, вероятно, не самый подходящий момент для обнаружения ранее неизвестных сетей, подключенных через маршрутизаторы, установленные порой в самых неожиданных местах.

---

1 К 21 апреля 2005 года все организации здравоохранения США обязаны были выполнить предписания "Перечня правил безопасности" (HIPAA Security Rule). Исключение составляют небольшие компании — для них был срок продлен до апреля 2006 года. Цель перечня заключается в обеспечении конфиденциальности, целостности и доступности защищенных цифровых медицинских данных (Electronic Protected Health Information, ePHI). Правила безопасности касаются технических вопросов защиты данных ePHI – в отличие от "Перечня правил конфиденциальности" (Privacy Rule), принятого в апреле 2003 года и относящегося к медицинской информации любой формы представления — письменной, устной и электронной. Более конкретно, правила безопасности требуют, чтобы медицинские учреждения, хранящие или передающие данные в цифровом виде, предпринимали соответствующие защитные меры административного, технического и физического характера. — *Примеч. пер.*

2 С июля 2005 года все "неамериканские" компании, чьи акции представлены на американском фондовом рынке, должны были привести свою отчетность в соответствие с требованиями закона Sarbanes-Oxley (SOX). Положения этого закона определяют требования к документообороту и финансовой отчетности компаний. Большинство крупных компаний в США в 2002 году столкнулись с необходимостью упорядочить свою работу в соответствии с требованиями нового закона. SOX — это не просто один из новых законов, это новый способ управления бизнесом, который научит руководство предупреждать риски и эффективно преодолевать трудности, поэтому следование его положениям требует значительной коррекции деятельности предприятия и финансовых служб. В соответствии с этим законом производится автоматизация процессов работы, воздействие всевозможных рисков снижается, а также вводится необходимый контроль над работой финансовых служб и процедур деятельности. — *Примеч. пер.*

Если схема сети отсутствует, настоятельно рекомендуется ее создать, воспользовавшись для этого программой Microsoft Visio или какой-либо другой программой аналогичного плана. Это упростит визуализацию проекта и логическое проектирование размещения серверов ISA Server.

Дополнительно к схематическому отображению размещения маршрутизаторов, коммутаторов и логической сети как единого целого, неплохо было бы в проекте сети отобразить общее размещение компьютеров и компьютерных служб. Понимание логического смысла размещения в сети критических серверов и размещения рабочих станций клиентов может пригодиться для определения места расположения ISA Server. Например, если клиентская сеть состоит из рабочих станций департамента, который предрасположен к вирусным атакам или проникновению эксплойтов, очень может помочь размещение ISA Server между этой сетью и сетью, объединяющей ответственные серверы.

Таким образом, очень важно понять, как сформирована инфраструктура, перед тем как принять решение, каким образом будет использоваться ISA Server.

Установка соответствия целей, задач и возможностей ISA Server

Многие проекты развертывания ISA Server начинаются с недопонимания, что же все-таки намеревается получить организация от использования ISA Server. Во многих случаях ISA Server служит для решения специфической задачи, заключающейся, например, в защите OWA-сервера от сети Интернет, но тот факт, что сервер может служить и для решения многих других задач, в полной мере не осознается. Поэтому очень важно составить список, содержащий все типы функциональности, необходимой в заданной инфраструктуре, и отражающий, каким образом возможности ISA Server соответствуют этой функциональности. В табл. 4.1 перечислены традиционные цели и задачи, а также соответствующие им возможности ISA Server.

Управление проектом развертывания

Одной из наиболее сложных частей задачи развертывания технического решения является само управление проектом. Зачастую во многих организациях решения по безопасности, особенно решения по безопасности Microsoft, возводятся в ранг политической или даже почти религиозной темы. Кроме того, необходимо уделить внимание управлению и контролю над другими аспектами проекта по размещению ISA Server. Ниже перечислены области особого контроля при развертывании ISA Server 2006.

- **Определение проекта** — иногда бывает недостаточно просто определить, что будет развертываться, но часто необходимо определить почему. Что могут дать функциональные возможности ISA Server информационной инфраструктуре? Почему руководство должно выкладывать деньги, необходимые для развертывания еще одного набора серверов? Определение и документирование проекта на ранних стадиях позволит ответить на все эти вопросы.
- **Определение объема проекта** — задачи определения объема, сложности и уровня развертывания являются критическим фактором в успехе проекта ISA Server. Хорошо определенный набор границ, которыми будет ограничен этот проект, позволяет минимизировать объем производимого тестирования и помогает представить разрабатываемый проект целевой аудитории в выгодном свете.

- **Организация поддержки технологии** — если никто не поддерживает новый продукт, технология умрет еще до ее внедрения или на самой ранней стадии развития. Такие технологии, как ISA Server, требуют заинтересованности в том типе функциональности, которую она предоставляет. Например, создание сил поддержки может заключаться в вовлечении администратора Exchange, что возможно с точки зрения правил публикации почты ISA Server для Outlook Web Access. Или менеджер, оценивающий преимущество дорогих VPN-решений, может оказать существенную поддержку новой технологии, когда он или она осознают низкие цены и большую функциональность VPN-решений, предоставляемых ISA Server. Чем больше поддержки будет иметь ISA Server, тем проще довести проект до завершающей стадии.
- **Убедить скептиков** — реальности сегодняшнего дня таковы, что к любым технологиям безопасности компании Microsoft люди относятся с изрядной долей скептицизма. Этот скептицизм частично базируется на отрицательном опыте, полученном многими администраторами безопасности, которые сталки-

Таблица 4.1. Соответствие функциональных возможностей ISA Server целям и задачам организации

Цели и задачи	Функциональная возможность ISA Server
Защитить Exchange Outlook Web Access от угроз, исходящих из Интернета	Развернуть функциональность обратного прокси-сервера ISA Server 2006 с использованием правил публикации почты
Аудит всего сетевого доступа к определенной службе сервера, например, к веб-службе	Разместить ISA Server 2006 между сегментами сети и назначить соответствующие правила веб-публикации. Производить аудит трафика протоколированием в SQL СУБД
Защита серверов Exchange от RPC-атак со стороны клиентов внутренней сети	Защитить все серверы Exchange, находящиеся за ISA Server, воспользовавшись фильтрацией RPC-пакетов от всего RPC-трафика, отличного от MAPI
Развертывание дополнительных решений кэширования для клиентов с тем, чтобы разрешить пересылку HTTP-пакетов и FTP-пакетов в Интернет	Развертывание версии ISA Server 2006 Enterprise Edition, позволяющей выполнять балансировку нагрузки всей сети. Использование прокси-функциональности ISA Server для обеспечения возможности кэширования HTTP и FTP-контента
Подключение к отдельной логической сети удаленных узлов через Интернет	Развертывание VPN-сети между узлами с помощью ISA Server 2006
Наложение строгих ограничений на доступ клиентов к службам и данных для соблюдения таких положений правительства, как те, которые продиктованы законом Сарбана-Оксли	Развернуть клиентское программное обеспечение брандмауэра ISA Server на всех системах, контролировать, ограничивать и осуществлять аудит доступа к службам
Защитить веб-службы от трафика из Интернета, воспользовавшись для этого усовершенствованными методами фильтрации на прикладном уровне	Развернуть ISA Server с одной сетевой картой в демилитаризованной зоне существующего брандмауэра и настроить правила веб-публикации для фильтрации HTTP-пакетов

ваясь с прорехами в системе безопасности программных продуктов компании Microsoft в прошлом. Это затрудняет восприятие такого продукта, как ISA Server, подобной аудиторией. В таком случае ISA Server лучше реализуется в качестве какого-то дополнительного слоя к уже существующим технологиям безопасности, а не в качестве их замены. Кроме того, как и в случае с любой другой технологией, если создается впечатление, что для развертывания ISA Server 2006 потребуется фундаментальная перестройка архитектуры существующей сети или системы обеспечения безопасности, убедить заказчиков в противном будет наиболее сложным и длительным этапом внедрения.

- **Управление затратами** — несмотря на то что полное развертывание ISA Server 2006 с несколькими массивами серверов ISA Server Enterprise Edition, работающих на надежных многопроцессорных системах, повлечет за собой очень большие затраты, в большинстве своем развертывание ISA Server требует вложения незначительных средств, особенно в сравнении с другими аналогичными решениями. Однопроцессорную систему ISA Server 2006 Standard, работающую на серверном оборудовании, можно приобрести по минимальным расценкам (такая лицензия стоит порядка 1300 долларов за процессор) плюс стоимость аппаратной части. Благодаря тому, что покупать клиентские лицензии не требуется, это делает ISA Server 2006 довольно недорогим решением.
- **Отрицательное воздействие** — существенным фактором является максимально возможное смягчение влияния разворачиваемого решения. Успех внедрения IT-проекта часто определяется уровнем "болезненности", который конечные пользователи ощущают после завершения проекта миграции. Разворачивать ISA Server можно параллельно существующим развернутым инфраструктурам, снижая тем самым риск и позволяя активное тестирование технологии до момента ее полного развертывания.
- **Тренировка персонала** — ISA Server — это новая технология, и, следовательно, опыт администрирования и ведения этой инфраструктуры в IT-инфраструктуре не всегда есть. Формальный тренинг по курсу администрирования ISA Server может быть включен в гарантийные обязательства, но это совсем не обязательно, особенно если под рукой есть такое руководство, как настоящая книга. Ключом к успешной эксплуатации результатов проекта является то, насколько бесконфликтно новая инфраструктура будет взаимодействовать с существующими процессами и процедурами. Предварительный тренинг персонала, который будет задействован в работе с этим продуктом, является ключом к достижению поставленной цели.

Документирование проекта

Несмотря на то что наиболее важным шагом в процессе проектирования считается составление документации, документированию проекта ISA Server 2006 часто отводится не очень много внимания. Хорошее документирование проекта является важным моментом для IT-проектов, особенно это справедливо в случае с проектами, связанными с безопасностью и удаленным доступом.

Принимая во внимание все эти факторы, очень важно, чтобы все проектные решения, сделанные в процессе разворачивания ISA Server, были строго задокументированы и отражены схематически. Эта информация становится очень полезной, когда возникают дискуссии о том, почему система разворачивалась. Подробнее техника документирования ISA Server описывается в главе 20, "Документирование окружения ISA Server 2006".

Внимание

Доступ к документации по настройкам ISA Server должен быть ограничен кругом лиц, кого эта информация касается по долгу службы. Широкое распространение информации о том, каким образом настроена инфраструктура ISA Server, подобно выдаче сверхсекретных документов вражеской армии перед решающей битвой.

Миграция с ISA Server 2000/2004 на ISA Server 2006

Часть процесса проектирования ISA Server включает изучение существующих инсталляций ISA Server и миграции этих серверов на ISA Server 2006. К счастью, компания Microsoft обеспечивает надежным и простым инструментарием миграции существующих ISA Server 2000 на ISA Server 2006. С точки зрения проектирования, очень важно, прежде всего, понять функциональные различия между ISA Server 2000, ISA Server 2004 и ISA Server 2006, так как данные проекта должны их учитывать.

Различия между ISA Server 2000 и ISA Server 2004/2006

ISA Server 2000 был очень мощным продуктом, который обладал возможностями брандмауэра и прокси-сервера. Однако в сравнении с возможностями ISA Server 2004/2006, более старая версия программного обеспечения имеет недостатки в нескольких достаточно существенных аспектах. Эти новые возможности вместе с более мощной общей степенью безопасности дают организациям возможность обновления до новой версии.

Описанные ниже возможности составляют основу новых возможностей и доработок, имеющихся в ISA Server 2006:

- **Поддержка работы с несколькими сетями** — одним из наиболее существенных различий между ISA Server 2000 и ISA Server 2006 является возможность ISA Server 2006 работать с несколькими сетями, каждая из которых обладает своими собственными связями. Это позволяет применять к каждой сети уникальные политики, которые могут использоваться как часть правил брандмауэра.
- **Усовершенствованная фильтрация пакетов на прикладном уровне** — возможности фильтрации пакетов ISA Server 2006 на 7 уровне (прикладной уровень) были улучшены включением в ISA Server 2006 возможностей брандмауэра экспертного уровня[3] при обработке HTTP-пакетов, поддержке фильтрации RPC и возможности преобразования ссылок.
- **Усовершенствованная возможность для контроля и отчетности** — другим улучшением ISA Server 2006 является возможность ведения надежного журнала, составленного в реальном режиме времени, и его просмотра. Это суще-

[3] Брандмауэр экспертного уровня — брандмауэр, проверяющий содержание принимаемых пакетов сразу на трех уровнях модели OSI: сетевом, сеансовом и прикладном. При выполнении этой задачи используются специальные алгоритмы фильтрации пакетов, с помощью которых каждый пакет сравнивается с известным шаблоном авторизированных пакетов. — *Примеч. пер.*

ственно помогает в устранении ошибок, допущенных в правилах брандмауэра. Добавление возможностей для контроля и составления отчетности (такое как подключение верификаторов, публикация отчетов, параметры регистрации в базе данных MSDE и сеансы контроля в реальном масштабе времени) способствует серьезному расширению этой области деятельности для администраторов ISA Server 2006.

- **Существенно доработанный интерфейс управления** — GUI-инструментарий администрирования в ISA Server 2006 серьезно усовершенствован по сравнению с консолью ISA Server 2000. Дополнительно упрощает работу с консолью множество мастеров, предназначенных для выполнения рутинных заданий, сетевых шаблонов, которые довольно просты в использовании, и возможность централизованной регистрации и хранения политик брандмауэра в версии Enterprise этого программного продукта.
- **Функциональность по экспорту и импорту** — появилась возможность ISA Server 2006 экспортировать отдельные элементы или целые конфигурации ISA Server 2006 в простые текстовые файлы XML-формата, которые могут импортироваться на другие серверы, существенно усиливая возможности резервного копирования и восстановления для администраторов ISA Server 2006.
- **Усовершенствования в механизме работы с VPN-сетями** — в ISA Server 2006 были добавлены новые доработки механизма поддержки VPN-сетей, такие как поддержка VPN-карантина, поддержка клиента SecureNAT, углубленная фильтрация для клиентов VPN-сетей и поддержка режима туннельного IPSec-протокола от сторонних разработчиков для VPN-соединений типа “узел-узел”.
- **Обновление механизма кэширования контента** — возможности работы с веб-прокси и FTP-прокси были доработаны в ISA Server 2006 и включают поддержку протокола RADIUS для аутентификации, усовершенствованных правил кэширования, создания массивов кэширования с использованием протокола CARP в версии Enterprise.
- **Усовершенствованные правила брандмауэра** — в ISA Server 2006 была добавлена поддержка стандартных протоколов, включая возможность поддержки сложных протоколов при работе с клиентом брандмауэра ISA Server 2006. Кроме того, была произведена доработка публикации сервера для таких служб, как служба OWA, веб-сайты, SharePoint, FTP-сайты и другие правила брандмауэра.

Миграция с ISA Server 2000 на ISA Server 2006

Не существует прямого способа миграции ISA Server 2000 на ISA Server 2006. Единственным поддерживаемым методом обновления существующего ISA Server 2000 до сервера ISA Server 2006 является миграция настроек сервера на ISA Server 2004, с последующей миграцией с ISA Server 2004 на ISA Server 2006. Именно эта процедура описана в данном разделе.

Существует два основных варианта миграции настроек ISA Server 2000 на ISA Server 2004. Первая процедура заключается в обновлении существующего ISA Server 2000 до ISA Server 2004. Настоятельно рекомендуется по возможности избегать использования этого метода, так как он не всегда дает желательные результаты и может привести к получению системы с существенными “прорехами” в системе безопасности и неупорядоченности, которая останется после миграции из одной системы в другую.

Предпочтительным вариантом миграции на ISA Server 2004 является использование инструмента ISA Server Migration для экспортирования установок сервера ISA Server 2000 в текстовый файл XML-формата, который может затем быть импортирован во вновь инсталлированную систему ISA Server 2004, работающую под управлением Windows Server 2003. Этот вариант позволяет создать абсолютно новый ISA Server и избежать каких-либо проблем настройки ISA Server 2000 или проблем, возникающих при взаимодействии с операционной системой.

Для того чтобы выполнить такой тип миграции ISA Server 2000 на ISA Server 2004, необходимо предпринять следующие шаги:

Примечание

Для того чтобы обновить версию ISA Server 2000 Standard, необходимо воспользоваться инсталляционным CD-диском версии ISA Server 2006 Standard. аналогично, для того чтобы обновить версию ISA Server 2000 Enterprise, необходимо воспользоваться инсталляционным CD-диском версии ISA Server 2006 Enterprise. При попытке обновления между различными версиями (например, с версии ISA Server 2000 Standard на версию ISA Server 2006 Enterprise) единственным возможным путем миграции является запуск мастера миграции, копирование конфигурации одной и той же версии с последующим экспортом отдельных правил в XML-файлы и передачей их на новую версию на сервере.

1. На сервере, где установлен ISA Server 2000, вставьте инсталляционный CD-диск ISA Server 2004 в CD-привод (или дважды щелкните на файле `autorun.exe`).
2. Щелкните на ссылке Run Migration Wizard (Запустить мастер миграции).
3. В диалоговом окне приветствия щелкните на кнопке Next (Далее).
4. В следующем диалоговом окне введите имя папки, в которую будет сохранен XML-файл, а также имя файла, аналогичное показанному на рис. 4.1. При этом можно воспользоваться кнопкой Browse (Обзор).

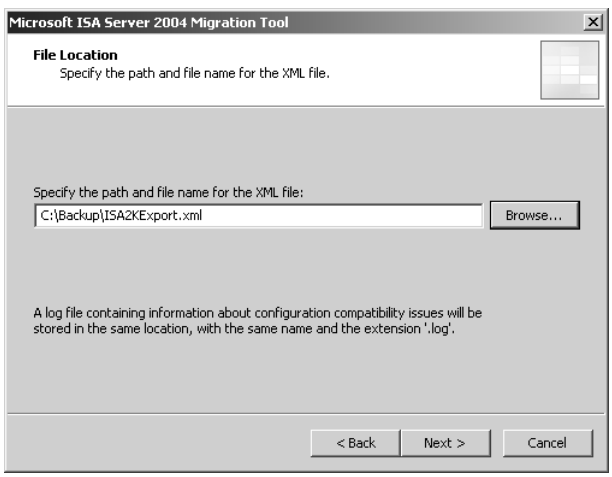

Рис. 4.1. С помощью мастера миграции ISA Server 2004 экспортируем установки ISA Server 2000

5. После ввода имени файла щелкните на кнопке Next (Далее).
6. Для того чтобы начать экспорт, щелкните на кнопке Create (Создать).
7. После завершения экспорта щелкните на кнопке Next (Далее).
8. Щелкните на кнопке Finish (Готово).

Экспортируемый XML-файл, открытый из Блокнота, выглядит аналогично файлу, показанному на рис. 4.2. С этого момента файл готов к импорту на систему ISA Server 2004.

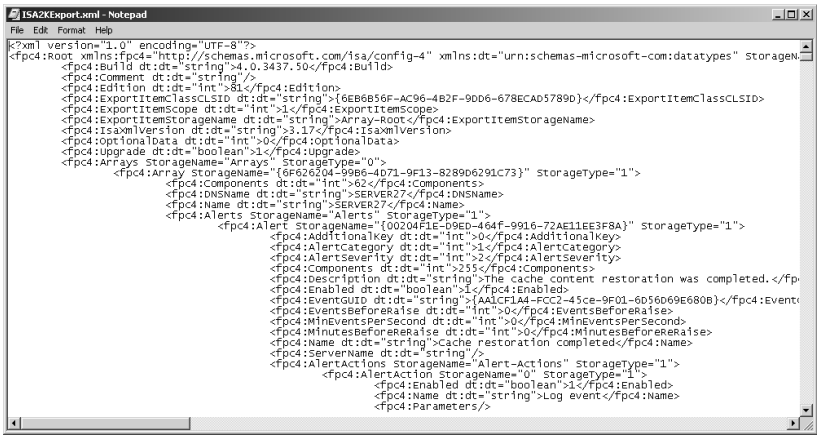

Рис. 4.2. Вид экспортируемого XML-файла для ISA Server 2004

После того как XML-файл стал физически доступным с нового сервера, он может быть импортирован с использованием следующей последовательности операций:

9. Откройте консоль ISA Server 2004.
10. Щелкните правой кнопкой мыши на имени сервера на панели Scope (Диапазон) и выберите Import (Импортировать).
11. После появления диалогового окна предупреждения (рис. 4.3) щелкните на кнопке Yes (Да).
12. Выберите XML-файл из процедуры резервного копирования ISA Server 2000 и щелкните на кнопке Import (Импортировать).
13. Щелкните на кнопке OK после завершения импорта.
14. Щелкните на кнопке Apply (Применить), размещенной вверху панели Central Details (Центральный состав).

Внимание

Как видно из диалогового окна, выполнение этого восстановления приводит к тому, что все прежние установки будут уничтожены. Перед восстановлением из экспортного файла ISA Server 2000 убедитесь в том, что на сервере отсутствуют какие-либо настройки.

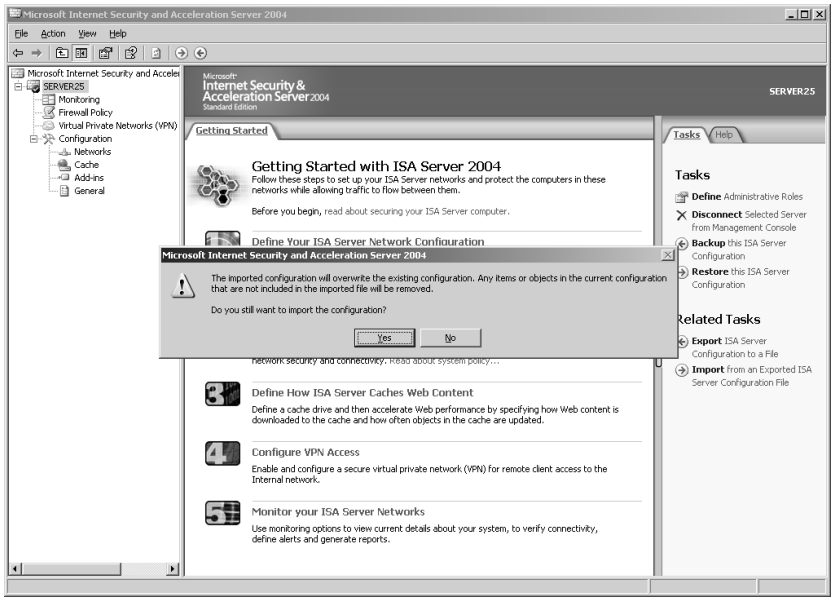

Рис. 4.3. Импортирование установок ISA Server 2000 на систему ISA Server 2004

После завершения процесса миграции и перед обновлением установок миграции до ISA Server 2006, необходимо тщательно изучить весь набор перенесенных правил ISA Server 2000. Одним из самых существенных недостатков ISA Server 2004, на который только что были перенесены правила миграции ISA Server 2000, является наличие большого количества противоречивых и взаимоисключающих правил в политике брандмауэра. Мастер миграции ISA Server экспортирует все уникальные правила, размещенные на самом сервере, которые затем импортируются на ISA Server 2004. Однако во многих случаях этим самым создается множество правил, которые будут уже продублированы правилами системной политики или другими правилами, которые имеются на сервере по умолчанию.

С учетом данного фактора этот момент может оказаться идеальным для удаления нескольких старых правил ISA Server 2000. Для уменьшения риска, связанного с этим действием, лучше всего вместо полного удаления этих правил просто отключить их на определенный период времени. И если правила доказали свою необходимость, их потом будет несложно активизировать вновь.

Миграция с ISA 2004 на ISA 2006

Процесс миграции с ISA Server 2004 на ISA Server 2006 еще проще, чем с ISA Server 2000 на ISA Server 2004, но все же существует несколько ключевых факторов, которые необходимо принимать во внимание. Так же как и с обновлением ISA Server 2000–2004, рекомендуется сначала создать новый сервер, а затем экспортировать и импортировать правила со старого сервера (а не делать обновление имеющегося сервера).

Выполнение обновления имеющегося сервера с ISA 2004 на ISA 2006

При необходимости осуществления обновления на месте, можно рассмотреть несколько следующих ключевых моментов:

- Все файлы журналов ISA Server 2004 должны быть куда-то скопированы, так как на ISA Server 2006 используется новый, совершенно другой, несовместимый с предыдущим формат, использование которого приведет к удалению всех существующих журналов.
- Общие компоненты элементов SMTP Screener и брандмауэра перед началом обновления должны быть переустановлены, так как в ISA Server 2006 они больше не поддерживаются.
- Настоятельно рекомендуется перед выполнением процедуры обновления провести резервное копирование существующей конфигурации.
- Обновление существующих инсталляций не может производиться с заменой версии. Например, версия ISA 2004 Standard Edition не может обновляться до ISA Server 2006 Enterprise Edition и наоборот. Единственным возможным способом это сделать является экспортирование отдельных правил в XML-файлы с последующим импортированием их на вновь установленную версию.
- Также необходимо обновить версию операционной системы для того, чтобы удовлетворить минимальные требования для ISA Server 2006, в соответствии с которыми это должна быть версия Windows Server 2003 SP1 или версия R2.

Как уже указывалось, обновление существующей версии ISA Server нельзя считать рекомендуемым методом перехода между версиями ISA Server. Однако если без обновления такого типа не обойтись, обновление выполняется так же просто, как запуск инсталляции ISA Server 2006 из носителя ISA Server 2006 и принятие установок по умолчанию.

Миграция с ISA Server 2004 на ISA Server 2006 с помощью мастера экспортирования

Предпочтительным способом обновления ISA Server 2004 является экспортирование правил настройки с ISA Server 2004 с последующим импортированием их на новый ISA Server 2006. Это позволит получить новую конфигурацию и также дает возможность легкого отката на старый сервер в случае возникновения проблем.

Все, что необходимо для переноса правил и настроек с ISA Server 2004 на ISA Server 2006, — это существующие правила и настройки ISA Server 2004 в формате XML-файла. Кроме того, также могут быть пересланы и инсталлированы на ISA Server 2006 любые SSL-сертификаты, которые были установлены на старом ISA Server 2004.

Для экспортирования конфигурации с ISA Server 2004 выполните следующие шаги:

1. Из консоли управления ISA Server 2004 щелкните на имени сервера на панели Scope (Диапазон).
2. Во вкладке Tasks (Задачи) панели Tasks (Задачи) щелкните на ссылке Backup This ISA Server Configuration (Сделать резервную копию этой конфигурации ISA Server).
3. Введите имя файла и путь к файлу, в котором будет сохранен XML-файл резервной копии, затем щелкните на кнопке Backup (Резервировать).

4. В диалоговом окне, изображенном на рис. 4.4, введите пароль, который будет использоваться для шифрования XML-файла, после чего щелкните на кнопке OK.
5. После завершения резервного копирования щелкните на кнопке OK.

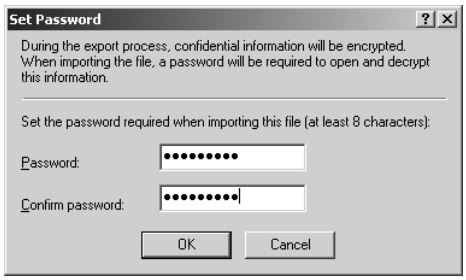

Рис. 4.4. Экспортирование конфигурации из системы ISA Server 2004

В результате экспортирования конфигурации будет получен XML-файл, который может быть скопирован на ISA Server 2006 и импортирован в соответствии со следующей процедурой:

1. Из консоли управления ISA Server 2006 щелкните на имени сервера на панели Scope (Диапазон).
2. Во вкладке Tasks (Задачи) панели Tasks (Задачи) щелкните на ссылке Import (Restore) This ISA Server Configuration (Импортировать [восстановить] эту конфигурацию ISA Server).
3. Для запуска процедуры на экране мастера щелкните на кнопке Next (Далее).
4. Для обнаружения XML-файла, полученного из ISA Server 2004, щелкните на кнопке Browse (Просмотр).
5. Перейдите к XML-файлу, щелкните на нем или на кнопке Open, затем щелкните на кнопке Next (Далее).
6. После получения подсказки в диалоговом окне, изображенном на рис. 4.5, щелкните на кнопке OK для отображения готовности к обновлению настроек в XML-файле для выбора тех, которые совместимы с ISA Server 2006.
7. Для расшифровки файла введите пароль в следующем диалоговом окне и щелкните на кнопке Next (Далее).
8. Для запуска процесса импортирования щелкните на кнопке Finish (Готово).
9. После завершения процедуры импортирования щелкните на кнопке OK, а затем последовательно на кнопках Apply (Применить) и OK на консоли для сохранения произведенных изменений.

Рис. 4.5. Импортирование XML-файла с настройками ISA Server 2004 на ISA Server 2004

С этого момента новая система ISA Server 2006 будет точной копией старой системы ISA Server 2004, причем актуализация миграции между двумя серверами включает простой обмен IP-адресами между системами. Если с новым сервером возникают какие-либо проблемы, можно будет вернуться на старый сервер ISA Server 2004, так как исходные установки на нем остались нетронутыми.

Определение количества серверов ISA Server и их размещения

Концепции масштабирования ISA Server не слишком сложны, но часто зависят от роли, которую будет играть ISA Server 2006 в структуре сети. В целом, большинство организаций редко тратятся на обновление процессорных ресурсов и наращивание оперативной памяти на сервере, на котором стоит ISA Server, полагая, что сервер загружается только таким связанным с Интернет трафиком, как веб-публикации или правила веб-публикаций. Однако когда ISA Server планируется использовать для кэширования контента, знание количества клиентов, которые будут осуществлять доступ к системе, приобретает большое значение.

Масштабирование ISA Server

К сожалению, хороших руководств по масштабированию ISA Server 2006 мало, некоторые из них предлагают минимальные конфигурации оборудования, которых следует придерживаться при развертывании ISA Server (см. табл. 4.2).

Примечание

В табл. 4.2 дается перечень только минимальных конфигураций серверов в зависимости от минимального количества пользователей. Рекомендуется немного завышать возможности серверов для того, чтобы избежать перегрузки ресурсов, особенно если он будет играть роль прокси-сервера.

Выбор между ISA Server Standard Edition и ISA Server Enterprise Edition

В цене между версией ISA Server 2006 Standard и версией ISA Server 2006 Enterprise существует достаточно большой разрыв. Поэтому важно определить, насколько оправданно использование версии Enterprise Edition. Обычно установка версии Enterprise Edition оправданна в том случае, если справедливо одно из следующих условий:

- необходимо предусмотреть восстановление сервера и обеспечение избыточности для балансировки нагрузки в сети;
- необходимо централизованное протоколирование в базу данных SQL для нескольких ISA Server;
- требуется централизованная политика брандмауэра и/или поддержка возможности работы серверного массива;
- для оптимизации кэширования контента для клиентов требуется поддержка работы трафика веб-прокси с протоколом CARP.

Таблица 4.2. Масштабирование оборудования для ISA Server

	До 50 пользователей	50–500 пользователей	Более 500 пользователей
Процессор	Один 767 МГц Pentium III или его эквивалент	Один 2 ГГц Pentium III/IV или его эквивалент	Два 2 ГГц Pentium III/IV или его эквивалент (или больше)
Память	512 Мбайт	1 Гбайт	2GB (или больше)
Дисковое пространство	Наличие 150 Мбайт (для инсталляции ПО ISA), плюс пространство для журналов и кэширования	Наличие 150 Мбайт (для инсталляции ПО ISA), плюс пространство для журналов и кэширования	Раздел 8 Гбайт для ОС; раздел 10GB+ для журналов; дополнительный раздел 18GB+ для кэширования (при необходимости)

Детальную информацию о версии ISA Server Enterprise Edition можно найти в главе 6, "Развертывание массивов ISA Server с использованием версии ISA Server 2006 Enterprise Edition".

Развертывание ISA Server 2006 в филиалах

Сценарий развертывания в филиалах часто используется в конфигурациях ISA Server. Во множестве случаев ISA Server в офисе филиала может быть первой линией защиты этого офиса. Кроме того, это позволяет создавать VPN-сеть между узлами, задействовав используемые серверы ISA Server в удаленном и родительском узлах, связав их воедино в одну непрерывную сеть.

На протяжении процесса проектирования ISA Server очень важно принять во внимание задачи каждого филиала и узнать, насколько важна установка ISA Server для этого конкретного офиса.

Создание прототипа ISA Server

Перед запуском проекта ISA Server в эксплуатацию рекомендуется протестировать прототип ISA Server на изолированной лабораторной инфраструктуре. Установка инфраструктуры такого типа помогает обратить внимание на конкретные проблемы задолго до запуска ISA Server в промышленную эксплуатацию. Это позволяет снизить риски, сопровождающие любой проект, и может оказаться достаточно полезным с точки зрения дополнительного тренинга и в качестве своеобразной пробной площадки для проверки новых правил и установок.

Создание лабораторной инфраструктуры для прототипа ISA Server 2006

Для установки прототипа ISA Server 2006 очень важно максимально правдоподобно промоделировать реальную инсталляцию ISA Server и установить все серверы или компоненты, которые также будут подвергнуты тестированию. Например, если ISA Server будет установлен для того, чтобы защитить MAPI-доступ к серверам Exchange, необходимо восстановить эти серверы на запасном оборудовании в изолированной инфраструктуре, а затем протестировать новый ISA Server в такой инфраструктуре.

Ключ к созданию успешной инфраструктуры макета тесно связан с тем, каким образом он отражает настоящие промышленные настройки. В идеальном случае все серверы и установки лабораторного прототипа должны полностью соответствовать. Однако в реальности расходы, связанные с воссозданием такой всеобъемлющей инфраструктуры прототипа, могут привести к не реализуемости самого проекта. Это означает, что в большинстве случаев прототипная инфраструктура отражает только часть наиболее критических служб, функциональность которых должна тестироваться.

Эмуляция и тестирование настроек ISA Server

Процесс проектирования должен производиться в полном соответствии с уже созданной проектной документацией, со всей точностью описывающей все настройки инфраструктуры ISA Server. В идеальном случае он будет включать информацию по отдельным элементам ISA Server, таким как правила публикации и сети, которые должны быть созданы. Эта информация может использоваться для создания различных правил и настроек, которые потребуются для тестирования компонентов в прототипной лаборатории.

После того как все компоненты будут установлены, а правила — настроены, начинается тестирование ISA Server. В идеальном случае тестирование будет включать эмулирование шагов, предпринимаемых пользователем для получения доступа к определенным службам или системам, защищать которые и будет призван ISA Server. Например, это может включать тестирование OWA-доступа извне с помощью правила публикации ISA Server. После тестирования всех типов доступа, которые могут быть протестированы, информация, полученная с помощью тестирования, может использоваться для внесения изменений в существующий проект.

Экспортирование настроек прототипной лаборатории

Одной из наиболее полезных возможностей ISA Server, которая существенно благоприятствует в тестировании прототипа, является возможность экспортирования отдельных элементов ISA Server в XML-файлы на другие системы. Эта концепция, полезная при резервном копировании систем, может также использоваться для экспорта "хорошо зарекомендовавших себя" настроек лабораторного прототипа и импортирования их на реально работающие промышленные серверы.

В идеальном случае лабораторный прототип может постоянно использоваться для тестирования новых правил в работе или настройки в инфраструктуре ISA Server. Любое необходимое изменение может быть сделано на прототипе ISA Server, протестировано, экспортировано в XML-файл, а затем импортировано на промышленный сервер.

Макетирование развертывания ISA Server

Следующим шагом, который по логике следует за этапом создания прототипа ISA Server, является макетирование, когда функциональность, протестированная в лабораторных условиях, проверяется уже в промышленной инфраструктуре, но только на ограниченное количество пользователей. В некоторых условиях это может представлять проблему, в то время как в других — представлять собой достаточно тривиальную задачу.

Организация группы макетирования

Первым шагом при создании макета ISA Server является поиск ограниченного круга пользователей, которые согласны принять участие в апробировании новых функциональных возможностей ISA Server. В идеальном случае общее количество пользователей макета будет составлять от 5 до 10% общего числа пользователей организации. Эти пользователи также должны иметь желание заполнять проверочные листы и отчеты о ходе тестирования макета. Данная информация затем может использоваться для окончательной доработки конфигурации ISA Server перед запуском его в промышленную эксплуатацию.

Сценарии макетирования ISA Server

От цели развертывания ISA Server 2006 зависит сложность задачи организации группы макетирования. Ниже приведены следующие сценарии и соответствующие им обоснования макетирования.

- **ISA Server разворачивается в качестве переднего прокси-сервера** — этот сценарий наиболее простой для макетирования. Рабочие станции пользователей, участвующих в работе макета, могут актуализировать использование ими прокси-сервера ISA для веб-кэширования с помощью групповой политики Active Directory.
- **ISA Server разворачивается как обратный прокси-сервер** — установка ISA Server в качестве обратного прокси-сервера для осуществления OWA-публикаций и публикаций веб-сервера может быть макетирована с помощью создания временного веб-сервера для новой конфигурации ISA Server. Если взять в качестве иллюстрации пример OWA, если прежний OWA-доступ осуществлялся через узел `mail.companyabc.com`, а ISA Server был установлен для защиты трафика, может быть временно создан второй узел `mail2.companyabc.com` для того, чтобы дать возможность пользователям макета проверить OWA-доступ через обратный прокси-сервер. После проверки макета запись `mail2` может быть отключена, а запись `mail.companyabc.com` — использована только для реализации ISA Server.
- **ISA разворачивается как полностью пограничный брандмауэр** — если ISA Server разворачивается в качестве полного граничного брандмауэра (на границе Интернет), тогда развертывание макета сложнее администрировать, учитывая тот факт, что трафик, поступающий из Интернет, по умолчанию должен идти одним путем. Таким образом, если и старая, и новая конфигурации ISA Server, выполняющего роль граничного брандмауэра, будут развернуты одновременно, можно будет протестировать доступ ISA Server, имея два набора шлюзов до тех пор, пока макет не будет протестирован полностью, а старая инфраструктура — отключена.
- **ISA Server разворачивается между сегментами сети** — этот сценарий аналогичен сценарию развертывания граничного брандмауэра. Единственное отличие состоит в том, что ISA Server будет размещен между сегментами внутренней сети для контроля трафика между этими сегментами. Вследствие того что сетевой трафик попробует пройти через стандартный маршрут, а не через новые серверы ISA, это представляется нетривиальной задачей. Лучшее решение этой про-

блемы предполагает создание альтернативного пути для пользователей макета посредством жесткого программирования маршрутов на их рабочих станциях, с тем чтобы они смогли протестировать доступ через тестируемый ISA Server.

Выполнение тестов по проникновению и атакам макетируемой инфраструктуры

Макетируемая инфраструктура должна быть полностью протестирована на наличие уязвимостей и общую производительность. Лучший и наиболее эффективный способ это сделать — это, воспользовавшись средствами взлома и создания эксплойтов от сторонних производителей, провести тестирование вторжения с инфраструктуру ISA Server. Вследствие того что вероятность подобных атак для любой системы, работающей с Интернет (и даже систем, работающих с доверенными сетями), достаточно высока, очень важно провести такое тестирование ISA Server.

Внедрение проекта ISA Server

После успешного проведения фазы создания прототипа и фазы макетирования и внедрения всех изменений в проект, проект ISA Server можно полностью вводить в эксплуатацию для всех пользователей. Во многих случаях это заключается в простой перемаршрутизации трафика на новый ISA Server. Воспользуемся для этих целей предыдущим примером обратного прокси-сервера, в котором после завершения фазы создания прототипа изменяется запись `mail.companyabc.com`, указывая уже на ISA Server. Аналогичная концепция также применима и к другим сценариям развертывания ISA Server.

Проверка работоспособности

Для того чтобы проект ISA Server был признан успешным, он должен быть проверен в работе под полной нагрузкой. В идеальном случае такое тестирование должно охватывать всех сотрудников всех подразделений организации для проверки работоспособности стандартных приложений и процессов, которые они использовали прежде. Это необходимо делать сразу же после внедрения ISA Server, например, в субботу, если внедрение осуществлялось в ночь на субботу.

После проведения такой проверки инфраструктуры во всех подразделениях организации и получения их подтверждения, что все их требования были удовлетворены, успешное завершение проекта можно считать решенным делом.

Долговременная поддержка инфраструктуры ISA Server

После внедрения решения ISA Server 2006 наступает очередь решения задач администрирования, сопровождения и общих вопросов инфраструктуры. Долговременная поддержка продукта требует учета самых разнообразных факторов. Дополнительную информацию по этому вопросу можно найти в главах 16, “Администрирование окружения ISA Server 2006” и 17, “Обслуживание ISA Server 2006”.

Проектирование ISA Server 2006 для организаций разного масштаба

Все организации решают самые разнообразные задачи и тот факт, что ISA Server может решать большое количество задач, означает, что существует большое количество сценариев развертывания ISA Server. Определенные варианты рекомендуемого развертывания ISA Server обычно можно подобрать для организаций самого разного типа. Эти варианты развертывания применяются также к организациям определенных размеров. Для более яркой иллюстрации данной концепции рассмотрим в этом разделе три примера организаций различных масштабов для того, чтобы получить наглядную иллюстрацию, каким образом чаще всего используется ISA Server.

Пример развертывания ISA Server 2006 в организации малого размера

Компания CompanyABC является юридической фирмой, в которой занято 30 сотрудников, ее офис расположен в городе Миннеаполис. Все локальные рабочие станции подключены к единой офисной коммутируемой сети. Удаленным пользователям требуется доступ к офисным ресурсам из дому и на период командировок. Часто клиентам, посещающим офис, требуется беспроводной доступ к Интернету, да и сотрудникам тоже необходима такая возможность.

Схема проекта ISA Server, развернутого в компании CompanyABC, показана на рис. 4.6. В проекте задействован один сервер ISA Server 2006 Standard как граничный брандмауэр организации.

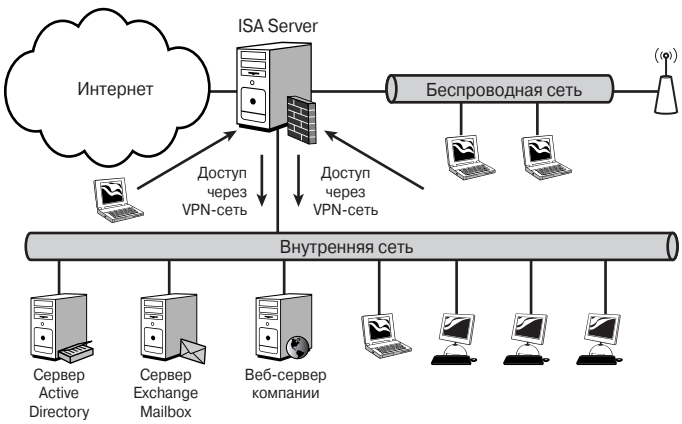

Рис. 4.6. Пример развертывания ISA Server 2006 в организации малого размера

Этот ISA Server оснащен тремя сетевыми картами, что позволяет серверу подключиться к трем физическим сетям: к Интернету, внутренней сети и защищенной беспроводной сети. Все сотрудники, работающие с внутренними ресурсами компании через Интернет и беспроводную сеть, должны устанавливать соединения через VPN-сеть с обращением к ISA Server. Веб-сервер компании защищен с помощью обратного

прокси-сервера и правил публикации веб-сервера. Кроме того, ISA Server обеспечивает кэширование контента для всех внутренних клиентов и клиентов беспроводной сети, что позволяет еще более ускорить безопасный просмотр данных в Интернете.

С помощью этого простого, но надежного проекта компания CompanyABC сможет удовлетворить требования по обеспечению безопасности через развертывание одного ISA Server, который извлекает максимум преимуществ из возможностей ISA Server.

Пример развертывания ISA Server 2006 в организации среднего размера

Организация OrganizationY является одним из городских муниципалитетов в штате Гавайи. При наличии 2000 сотрудников, IT-отдел муниципалитета должен отражать не только внешние угрозы, но и внутренние вирусные атаки и атаки эксплойтов, которые часто проникают на настольные системы и ноутбуки внутренней сети. Городскому муниципалитету требуется защитить свои серверные фермы, сохраняя при этом их работоспособными и доступными для обслуживания клиентов сети.

Как видно на рис. 4.7, организация OrganizationY развернула один сервер ISA Server 2006 Standard Edition, оснащенный шестью сетевыми картами. Каждая сетевая карта подключена к отдельной физической сети организации:

- Интернет;
- сеть периметра;
- беспроводная сеть;
- клиентская сеть, установленная на первом этаже;
- клиентская сеть, установленная на втором этаже;
- серверная сеть.

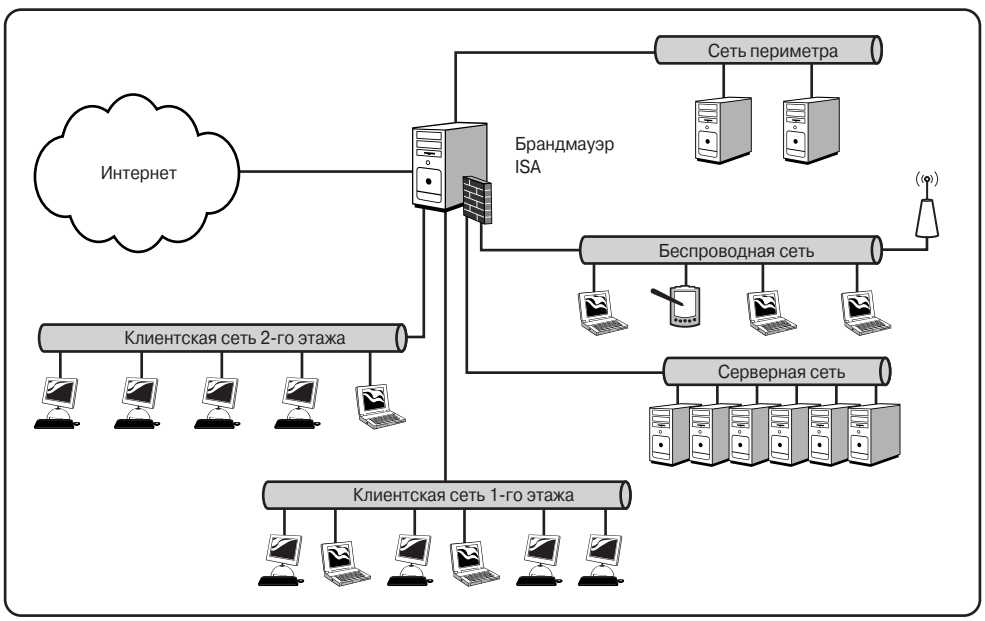

Рис. 4.7. Пример развертывания ISA Server 2006 в организации среднего размера

ISA Server настроен таким образом, чтобы разрешить специальный тип доступа от клиентской сети, беспроводной сети и сети периметра. В частности, сервер настроен на фильтрацию пакетов RPC для того, чтобы разрешить доступ к серверу Exchange только с использованием протокола MAPI, печать на определенный принт-сервер и установить соответствующие правила.

Разворачивая ISA Server таким образом, организация OrganizationY может смягчить угрозу, исходящую от вирусов или эксплойтов, которые могут инфицировать рабочие станции сети организации.

Пример развертывания ISA Server 2006 в большой организации

Компания CompanyA представляет собой крупную финансовую организацию, в которой занято 20 000 сотрудников, работающих в трех офисах, расположенных в Нью-Йорке, Токио и Париже. Компания CompanyA в прошлом испытывала трудности, связанные с обеспечением безопасности и контролем за доступом к своим почтовым службам. Тогда было принято решение перейти с существующей среды Exchange 5.5 на Exchange Server 2003. Параллельно с этим переходом пошел процесс по дальнейшему обеспечению безопасности в пределах существующей сети и инфраструктуры безопасности. Результаты этого проекта отражены на рис. 4.8.

Компания CompanyA защитила доступ к своему почтовому ресурсу, разместив все компоненты, связанные с почтой, после ISA Server. В Нью-Йорке вся поступающая почта отправляется на узел SMTP Smarthost, который сканирует ее на наличие вирусов и спама, а затем пересылает почтовые сообщения на Exchange Server Нью-Йорка, расположенный за массивом ISA Server предприятия. Этот массив настроен таким образом, чтобы разрешить входящий SMTP-трафик, поступающий с узла Smarthost. Весь остальной трафик ограничен входящим MAPI-трафиком, поступающим от клиентов, который контролируется и отслеживается.

ISA Server, установленный в сети периметра существующего брандмауэра, фильтрующего пакеты, выполняет функцию обратного прокси-сервера для Exchange Outlook Web Access. Вследствие необходимости соответствия существующей модели безопасности, ISA Server разворачивается на сервере с одной сетевой картой и размещается в демилитаризованной зоне. Затем брандмауэр фильтрации пакетов настраивается таким образом, чтобы разрешить поступление пакетов только по порту 443 через ISA Server на внутренний сервер.

На удаленных точках службы Exchange защищены такими же серверами ISA Server. Весь трафик, отправленный между этими изолированными сетями, сканируется ISA Server на прикладном уровне.

Резюме

Просто открыть упаковку с дистрибутивом ISA Server 2006 и быстренько установить ПО — не самая лучшая стратегия. Прежде всего потому, что мощность и функциональные возможности инфраструктуры требует хорошо продуманного процесса проектирования, причем во внимание берется функциональность ISA Server, которая должна соответствовать конкретным задачам, стоящим перед организацией. Благодаря использованию основных методов проектирования и управления проектом, ISA Server 2006 может быть инсталлирован таким образом, чтобы извлечь все преимущества из функциональных возможностей, которыми он обладает.

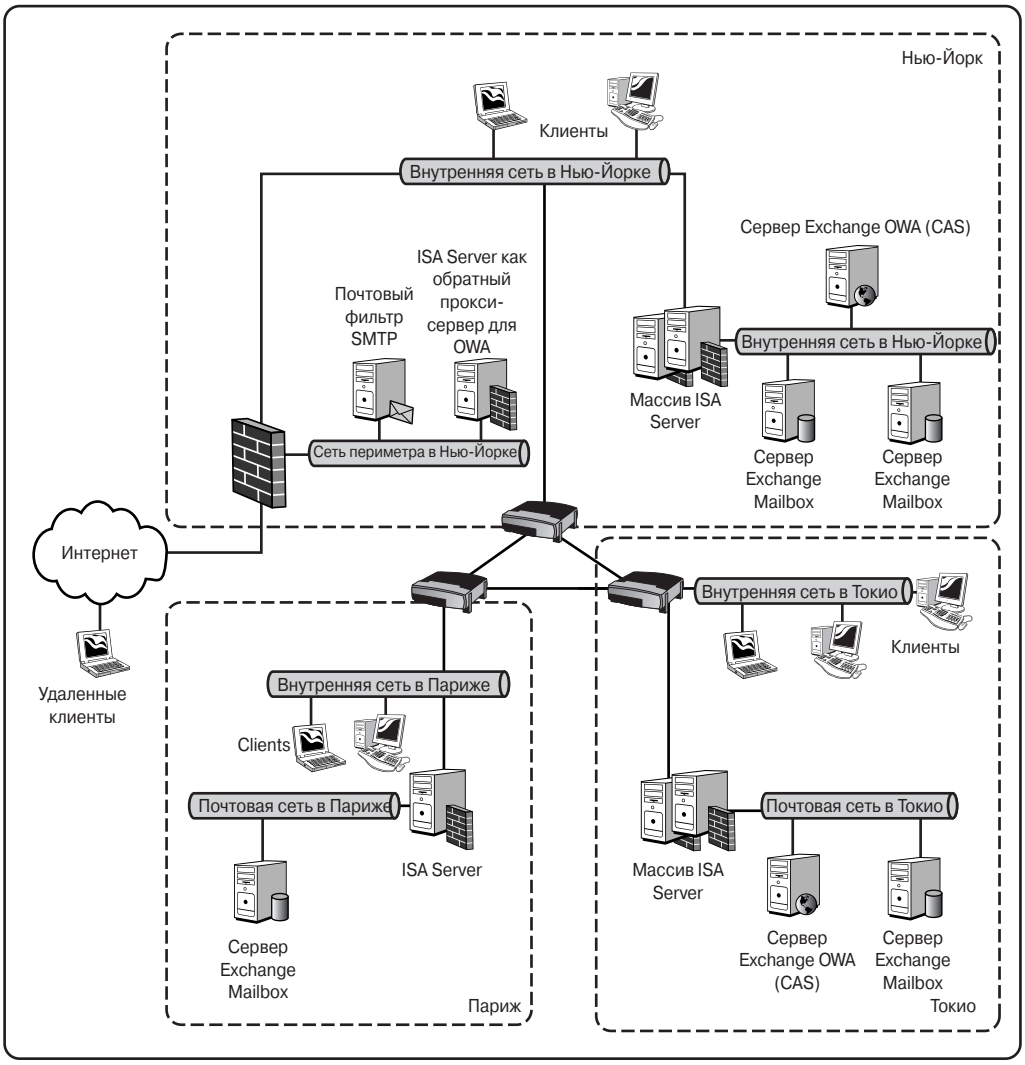

Рис. 4.8. Пример развертывания ISA Server 2006 в большой организации

До промышленного внедрения ISA Server проектные решения, принятые во время процесса проектирования, могут быть протестированы и оценены в прототипной лаборатории и при проведении макетирования. Следование такой методологии и правильное проектирование помогут обеспечить успех проекта внедрения ISA Server.

Полезные советы

- Задокументируйте проект инфраструктуры ISA Server и сохраните документы в безопасном месте.
- Перед тем как внедрять проект ISA Server в промышленную эксплуатацию, протестируйте его в изолированной лабораторной среде на специальном прототипе.
- Создайте список задач и целей, стоящих перед проектом ISA Server, которые затем необходимо соотнести с имеющимися функциональными возможностями ISA Server.
- Поищите опытных специалистов по ISA Server, кто мог бы помочь вам в продвижении проекта ISA Server.
- Рассмотрите возможность увеличения мощности процессора и объема памяти на тот случай, когда ISA Server используется для кэширования контента при постоянно увеличивающемся количестве пользователей.
- Проведите тестирование на вторжение на макете ISA Server, чтобы таким образом проверить безопасность инфраструктуры.