ООО "Крипто-Про"
E-mail: info@CryptoPro.ru

Описание протоколов SSL/TLS

Информационный документ

2002 г.

Содержание

Аннотация

В документе описан протокол «Крипто-Про TLS», (настройка и использование протокола, состав и ключевая система), аутентификация (сервера, клиента, настройка) и Web, а также технология противодействия угрозам нарушения конфиденциальности и целостности данных.

Документ содержит определения основных терминов, используемых при работе с протоколами SSL/TLS.

1 Общее описание протокола TLS

В Средстве Криптографической Защиты Информации (СКЗИ) "КриптоПро-CSP" реализован протокол «Крипто-Про TLS», базирующийся на протоколе TLS v.1 и российских стандартах криптографической защиты конфиденциальной информации, далее по тексту – «Крипто-Про TLS».

В данном документе мы будем использовать термин «SSL/TLS» или «TLS».

В механизме защиты реализации протокола TLS (аутентификация клиента и сервера, шифрование информации, контроль целостности информации) применяются криптографические алгоритмы шифрования в соответствии с ГОСТ 28147-89, обмена ключей по алгоритму Диффи-Хеллмана, хэширования в соответствии с ГОСТ Р 34.11-94.

В случае использования клиентом эфемерной пары секретного/открытого ключей для верификации открытого ключа эфемерной пары применяются алгоритмы выработки и проверки электронной цифровой подписи в соответствии с ГОСТ Р 34.10-94 или ГОСТ Р 34.10-2001.

1.1 Основные понятия протокола TLS

Протокол предназначен для обеспечения криптографическими средствами аутентификации отправителя (клиента) – адресата (сервера), контроля целостности и шифрования данных информационного обмена.

Аутентификация опционально может быть односторонней (аутентификация сервера клиентом), взаимной (встречная аутентификация сервера и клиента) или не использоваться.

Иерархия организации информационного обмена

Иерархия информационного обмена включает в себя сессии, соединения и поток сообщений в соединении. Поток сообщений при большой длине разбивается на фрагменты с пакетной передачей фрагментов. В одной сессии может быть реализовано несколько соединений, произвольно разнесенных по времени. В каждом соединении может быть обработан необходимый поток сообщений.

Алгоритм преобразования информации при обмене

Алгоритм преобразования информации при обмене с использованием протокола TLS включает операции:

- прием от протокола верхнего уровня потока не интерпретируемых данных в блоках произвольного размера;
- фрагментация принятых с верхнего уровня данных в структурированные блоки (фрагменты) протокола TLS. Размер фрагмента – не более 2^{14} байт;
- компрессия фрагментов (опционально);
- хеширование фрагментов (используется ключевой MAC);
- конкатенация фрагмента и результата его хэширования (расширенный фрагмент);
- зашифрование расширенного фрагмента (опционально);
- передача зашифрованного расширенного фрагмента с добавленным открытым заголовком протокола транспортного уровня (например, TCP).

При приеме информации применяется обратная последовательность операций.

Атрибуты сессии

- Сессия характеризуется следующими атрибутами:
- идентификатор сессии (случайное число, 32 байта, задается сервером при открытии сессии);

- метод компрессии;
- сертификат сервера (опционально);
- сертификат клиента (опционально);
- спецификация алгоритмов и параметров защиты (алгоритмы шифрования и MAC, криптографические параметры);
- master secret (используется при генерации ключей шифрования, ключей MAC, векторов инициализации);
- флаг, разрешающий/запрещающий новые соединения в сеансе.

Сертификаты представляются в стандарте X509. v3. Спецификация алгоритмов и параметров защиты может меняться в течение сессии.

Атрибуты соединения

К атрибутам соединения относятся:

- client_random – случайные 32 байта, задаваемые клиентом;
- server_random– случайные 32 байта, задаваемые сервером;
- client write MAC secret (ключ клиента для ключевого хэширования);
- server write MAC secret (ключ сервера для ключевого хэширования);
- client write key (ключ, используемый для шифрования данных клиентом и расшифрования их сервером);
- server write key (ключ, используемый для шифрования данных сервером и расшифрования их клиентом);
- client write IV, server write IV (векторы инициализации, используемые клиентом и сервером соответственно);
- порядковый номер соединения (поддерживается независимо для передаваемых и принимаемых сообщений).

Векторы инициализации используются в блочных шифрах. Вектор инициализации задается для первого фрагмента сообщения в соединении; для последующих фрагментов вектор инициализации формируется из конечного блока зашифрованного текста предыдущего фрагмента.

Порядковые номера соединений поддерживаются независимо для передаваемых и принимаемых сообщений. При смене сессии, изменении спецификации алгоритмов и параметров защиты нумерация соединений начинается с 0. Диапазон нумерации: $0 \div 2^{64}-1$.

Соединение ассоциируется с одной сессией.

Типы сообщений

В протоколе TLS используются следующие типы сообщений:

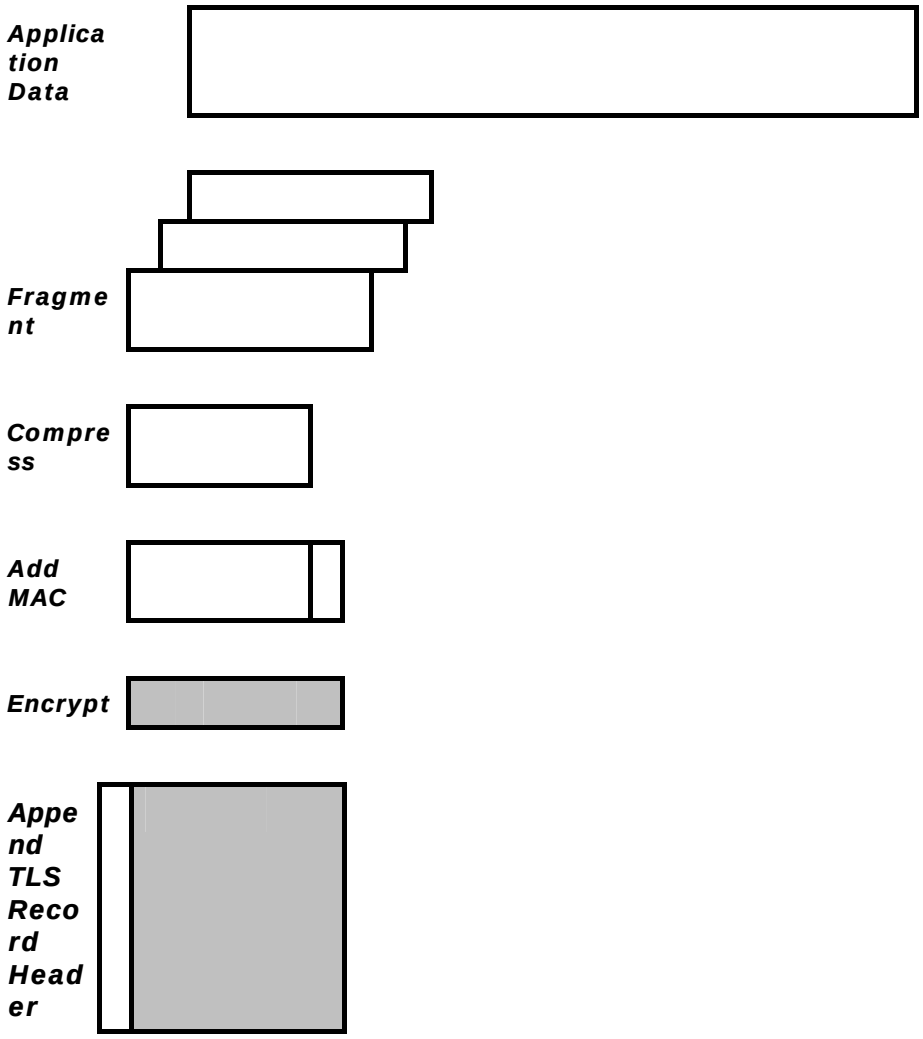
- Hello message (ClientHello, ServerHello);
- Change cipher specs message (изменение спецификации алгоритмов и параметров защиты);
- Key exchange message (передача ключа обмена ключами шифрования и MAC клиента, сервера);
- Alert message (предупреждение, оповещение о фатальной ошибке);
- Application_data message (передача данных);
- Finished message (сообщение о возможности работы в созданной сессии).

Фрагмент сообщения, передаваемый протоколу транспортного уровня

Для передачи фрагмента сообщения транспортному уровню производятся операции:

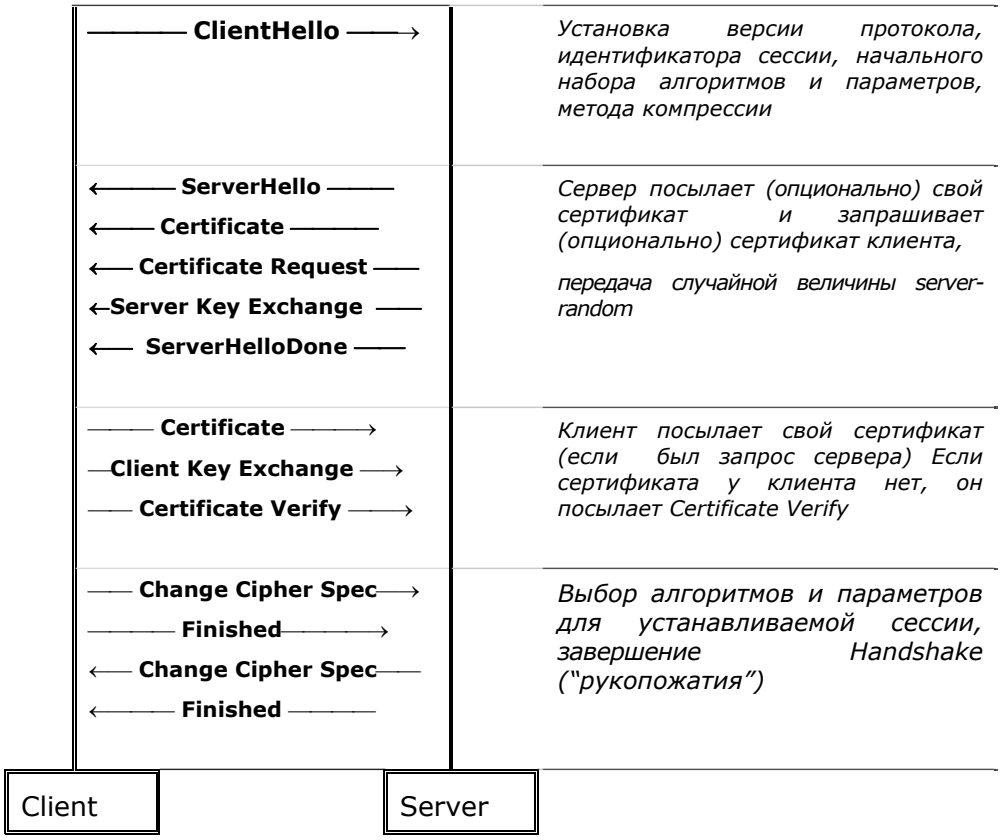
- компрессия фрагмента (опционально);
- вычисление хэша от конкатенации ключа хэширования, типа компрессии, длины компрессированного фрагмента, компрессированного фрагмента, заданной константы;
- шифрование расширенного фрагмента (конкатенация компрессированного фрагмента и его хэша);
- добавление открытого заголовка, содержащего тип сообщения (один байт), версию протокола TLS (два байта), длину компрессированного фрагмента.

Операции протокола TLS



1.2 TLS Handshake Protocol

TLS Handshake Protocol работает по следующей схеме:



TLS Handshake Protocol обеспечивает инициализацию сессии (соединения) выполнением операций:

- клиент и сервер договариваются об используемых в сессии алгоритмах и параметрах защиты, обмениваются случайными величинами client_random, server_random, договариваются, будут или нет новые соединения;
- производится обмен сертификатами для аутентификации клиента и сервера (по заданным опциям);
- клиент генерирует случайную величину pre_master secret, шифрует ее и передает серверу.
- Клиент и сервер по pre_master secret, client_random и server_random формируют master secret (набор необходимой ключевой информации) сессии.

1.3 Стек протокола TLS

Протокол TLS является двухуровневым и действует над транспортным протоколом. К первому уровню относятся TLS Handshake Protocol, TLS Change Cipher Spec, TLS Alert Protocol. Ко второму уровню относится TLS Record Protocol.

Стек протокола TLS

...			
TLS Handshake Protocol	**TLS Change Cipher Spec**	**TLS AlertProtocol**	**Протоколы обмена данными (HTTP и т.п.)**
TLS Record Protocol			
Транспортный протокол (TCP/IP и т.п.)			
...			

Таким образом, в первом разделе были даны определения основным терминам. В нем также содержится описание протокола TLS, в частности: TLS Handshake Protocol и стек протокола TLS. Далее мы переходим ко второму разделу, в котором будут рассмотрены средства защиты прикладных пакетов Microsoft Internet Explorer.

2 Средства защиты Microsoft Internet Explorer

В данном разделе мы приступаем к описанию средств защиты прикладных пакетов Microsoft Internet Explorer, Internet Information Services (IIS), Microsoft SQL Server 2000 и COM+.

COM+

В Windows 2000 Server реализованы новые технологии сервера приложений (COM+), которые помогают компаниям создавать, развертывать и администрировать размещенные на сервере приложения, сформированные с использованием модели составных объектов Microsoft Component Object Model (COM). В состав служб COM+ входит интегрированная поддержка балансировки нагрузки, транзакций, улучшенного доступа к данным и асинхронной связи. Используя мощные инструментальные средства, например Visual Basic, для проектирования масштабируемых, трехуровневых приложений, и создавая качественные приложения с помощью технологий многократно используемых объектов, COM+ идеально подходит для разработки деловых приложений и приложений электронной коммерции с Web-интерфейсом.

Internet Explorer 5

Штатный Web-обозреватель Windows 2000. Он служит для доступа к данным Web- и FTP-узлов, а также к сетевым ресурсам Windows. Большинство считает, что Internet Explorer — это процесс Iexplore.exe, но нужно принять во внимание и то, что средства Web-навигации Internet Explorer тесно интегрированы со многими аспектами графической оболочки Windows 2000 вследствие повсеместного использования общих компонентов. Вы можете, например, включить ссылки на часто посещаемые Web-узлы в интегрируемый модуль Microsoft Management Console (MMC). В стандартный набор часто используемых средств консоли MMC можно добавить ссылку на страницы узла Microsoft, посвященные безопасности (рис. 2-1).

Microsoft SQL Server 2000

Это законченное предложение в области баз данных и анализа данных для быстрого создания масштабируемых решений электронной коммерции, бизнес-приложений и хранилищ данных. Оно позволяет значительно сократить время выхода этих решений на рынок, одновременно обеспечивая масштабируемость, отвечающую самым высоким требованиям. В сервер SQL Server 2000 включена поддержка языка XML и протокола HTTP, средства повышения быстродействия и доступности, позволяющие распределить нагрузку и обеспечить бесперебойную работу, функции для улучшения управления и настройки, снижающие совокупную стоимость владения. Кроме того, SQL Server 2000 полностью использует все возможности операционной системы Windows 2000, включая поддержку до 32 процессоров и 64 ГБ ОЗУ.

Рисунок 2-1. Модуль MMC, включающий ссылку на страницу Web-сайта Microsoft, посвященную безопасности.

В этом разделе мы обсудим следующие аспекты защиты Internet Explorer:

- конфиденциальность;
- SSL/TLS протоколы (настройка, работа, сертификаты);

2.1 Конфиденциальность

Перейдем к обсуждению технологий противодействия угрозам. Как вы, наверное, заметили, существует два типа проблем:

- угрозы нарушения конфиденциальности и целостности данных, пересылаемых клиентом серверу и сервером клиенту (так называемые сквозные сценарии);
- угрозы нарушения конфиденциальности и целостности данных в постоянных хранилищах, таких как файловые системы и БД.

2.2 Защищенные протоколы

В сквозном сценарии информация должна быть защищена при передаче от клиента серверу и обратно. Снизить риск нарушения целостности данных позволяют защищенные протоколы, которые шифруют информацию при передаче через промежуточные серверы и маршрутизаторы. Риск нарушения целостности данных сокращают криптографические хэш-функции, позволяющие выявить изменение информации. Обычно данные, пересылаемые от клиента серверу, защищены, так как связь осуществляется по защищенному каналу. Иногда применяемые в таких каналах криптографические ключи регулярно изменяются, что дополнительно повышает безопасность пересылки данных.

Главная угроза, с которой сталкиваются все пользователи Web-обозревателей, — возможность несанкционированного доступа к их личной информации. Ваши тайны может раскрыть злоумышленник, перехватывающий данные, пересылаемые от обозревателя к Web-серверу. Например, по умолчанию коммуникационный канал, соединяющий Web-обозреватель и сервер, не шифруется, что позволяет хакерам «прослушивать» его и получать доступ к сведениям о кредитных картах, паролях и прочим конфиденциальным данным, пересылаемым через Интернет. Простейший способ защиты от этой угрозы — защита канала средствами протокола Secure Sockets Layer/Transport Layer Security (SSL/TLS). Ответственность за поддержку этого протокола возлагается на Web-сервер, а не на клиента, так как именно сервер определяет, шифровать ли информацию, передаваемую клиенту.

Хотя Web-узлы, как правило, применяют SSL/TLS только при работе с конфиденциальными данными, такими как пароли или номера кредитных карт, вы можете задействовать SSL/TLS для защиты всех подключений к Web-серверу, выбрав в качестве протокола не *HTTP, а HTTPS.* Однако с серверами, не поддерживающими SSL/TLS, этот подход не работает.

2.3 Протокол Secure Sockets Layer/Transport Layer Security

Протокол SSL, также известный под утвержденным Инженерной группой IETF названием TLS — защищенный протокол, обеспечивающим аутентификацию и защиту от «прослушивания» (нарушение конфиденциальности) и искажения данных (нарушения целостности). Для аутентификации служат сертификаты X.509 и проверки на основе связанных с ними закрытых ключей. Конфиденциальность обеспечивает шифрование данных, целостность — хэш-функции и *коды аутентичности сообщения* (Message Authenticity Code, MAC). SSL/TLS противостоит таким угрозам, как:

- подмена идентификатора клиента или сервера (с помощью надежной аутентификации);
- раскрытие информации (с помощью шифрования канала связи);
- искажение данных (с помощью кодов целостности сообщений).

2.4 IP и почтовые открытки

С точки зрения безопасности, Интернет-трафик, т. е. передачу IP-пакетов (блоков информации, передаваемых от отправителя получателю), можно уподобить пересылке почтовых открыток. Открытку, отправленную из одного места в другое через несколько почтовых отделений, на этом пути может прочитать кто угодно.

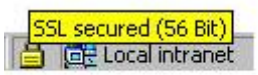


Рисунок 2-2. Просмотр длины ключа шифрования SSL/TLS в Internet Explorer.

Ярко-желтое изображение замка на панели в нижней части окна Internet Explorer показывает, что используется SSL/TLS. Подведя к нему указатель, вы узнаете длину применяемого для шифрования ключа — эта информация появится на всплывающей подсказке (рис. 2-2). Чтобы посмотреть сертификат Web-узла, достаточно дважды щелкнуть изображение замка.

Если Internet Explorer вызван из другого процесса, значка с изображением замка может не быть. Соблюдайте осторожность и пересылайте конфиденциальные данные по Интернету, только если вы абсолютно уверены, что канал защищен.

Этот значок также может не появиться и в случае использования на HTML-страницах фреймов. Одни фреймы могут применять HTTPS, а другие — просто HTTP. При этом даже если данные защищены с помощью SSL/TLS, изображение замка не появляется. Но если вы щелкнете фрейм правой кнопкой и выберете в контекстном меню пункт Properties, вы увидите, использует ли страница SSL/TLS.

2.5 Принцип работы SSL/TLS

При установке SSL/TLS-соединения выполняется несколько дополнительных операций (рис. 2-3). На иллюстрации предполагается, что Web-сервер не требует сертификатной аутентификации клиента.

Чтобы SSL/TLS действовал, Web-сервер должен иметь сертификат и личный ключ. Владелец сертификата должен подтвердить владение личным ключом, связанным с

сертификатом. Иначе говоря, для аутентификации применяется пара личный ключ — сертификат. Она позволяет клиенту проверить, что этот сервер действительно тот, за кого себя выдает. Этот этап чрезвычайно важен, так как перед началом передачи нужно полностью убедиться в подлинности сервера. Достигнув доверия, стороны выбирают ключ для симметричного шифрования данных в течение сеанса.

Рисунок 2-3. Предварительный этап установления SSL/TLS-соединения.

2.6 Различия между SSL и TLS.

Протокол SSL, разработанный компанией Netscape, стал стандартом де-факто, так как применялся в обозревателях и Web-серверах как Microsoft, так и Netscape. Из-за широкого распространения электронной коммерции в конце 90-х годов возникла потребность в защищенной передаче информации о пользователях и их кредитных карточках. Именно электронная коммерция стала катализатором популярности SSL. Существуют две основные версии SSL 2 и 3- Предпочтительнее использовать SSL версии 3, так как в ней исправлены многие слабости протокола. Обсуждение же технических деталей разных версий протокола выходит за рамки этой книги.

В 1996 г. IETF решила стандартизировать протокол SSL и при этом изменила его название на Transport Layer Security. Текущей версии TLS присвоен номер 1. Однако внутренний номер версии TLS — 3.1, так как этот протокол расширяет SSL. Так что TLS — это SSL 3.1. В данный момент TLS имеет статус стандарта IETF (спецификация RFC 2246).

2.7 Номера портов SSL/TLS

Стандартный порт для HTTP-трафика по протоколу SSL/TLS (HTTPS) — 443. Однако SSL/TLS не ограничен защитой только данных HTTP. Его можно применять и к другим Интернет-протоколам. Защищенные версии основных протоколов и соответствующие номера портов представлены ниже (табл. 2-1).

Когда вы набираете *https://www.exair.com* вместо *http://www.exair.com,* Web-обозреватель «понимает», что надо использовать порт 443, а не 80, и пытается подключиться к серверу через SSL/TLS. Если сервер не поддерживает SSL/TLS, соединение установить не удастся.

Таблица 2-1. Распространенные протоколы, поддерживающие SSL/TLS.

Протокол	Порт	Описание
HTTPS	443	HTTP по SSL/TLS
SMTPS	465	SMTP (электронная почта) по SSL/TLS
NNTPS	563	NNTP (новости) по SSL/TLS
LDAPS	636	LDAP (доступ к каталогам) по SSL/TLS
POP3S	995	POP (электронная почта) по SSLДLS
IRCS	994	IRC (чат) по SSL/TLS
IMAPS	993	ШАР (электронная почта) по SSL/TLS
FTPS	990	FTP (передача файлов) по SSL/TLS

Стоит добавить на ваши защищенные страницы изображение замка просто на тот случай, если такой значок обозревателя не виден. Кроме того, можно описать, как пользователи могут проверить наличие защиты Web-страниц. В случае Microsoft Internet Explorer им нужно щелкнуть правой кнопкой страницу и выбрать в контекстном меню пункт Properties. В Netscape Navigator нужно щелкнуть значок замка в строке состояния.

2.8 Производительность SSL/TLS

Применение криптографии в SSL/TLS заметно снижает производительность Web-приложений. Производительность различных криптографических протоколов описана ниже (табл. 2-2). Тесты проводились на компьютере с процессором Pentium III Xeon 450 МГц. Цифры в столбце «Запросов в секунду» относятся к установлению соединения.

Таблица 2-2. Относительная производительность PCT, SSL2, SSL3 и TLS

Протокол	Шифр	Хэш	Алгоритм обмена ключами/длина ключа	Запросов в секунду
PCT	40-разрядный RC4	MD5	RSA, 5 1 2 разрядов	108
SSL2	40-разрядный RC4	MD5	RSA, 512 разрядов	77
SSL3	56-разрядный RC4	SHA-1	RSA, 5 1 2 разрядов	83
TLS	56-разрядный RC4	SHA-1	RSA, 512 разрядов	90

Возможно, для вас будет интересен факт того, что SSL/TLS в Windows 2000 работает немного быстрее, если используется 128-, а не 40- или 56-разрядный ключ. Все дело в методах, которыми в SSL/TLS реализованы ключи. Все ключи — 128-разрядные, но когда требуется ключ меньшей длины, скажем, 56-разрядный, он разделяется на 56-разрядный ключ и 72-разрядную «соль». Чтобы это отследить, нужно время, поэтому работа с 128-разрядными ключами без «соли» быстрее. При увеличении длины ключа с 512 до 1024 бит количество соединений в секунду резко падает и может уменьшиться в пять раз. Производительность программных реализаций алгоритма RSA очень низка и очень быстро снижается при увеличении длины ключа. Зная все это, вы должны применять SSL/TLS только там, где это необходимо. В следующем разделе обсуждаются способы уменьшения влияния SSL/TLS на производительность Web-узла.

2.9 SSL/TLS на практике.

Основная проблема SSL/TLS — снижение производительности при соединении. Эта процедура требует больших расходов процессорного времени на выполнение сложных криптографических операций с длинными ключами. Однако после установления соединения накладные расходы на шифрование сокращаются. Чтобы повысить производительность Web-узла, следуйте этим простым правилам:

1. Сведите SSL/TLS-часть вашего Web-узла к минимуму.

Как уже говорилось, вы, возможно, не захотите применять SSL/TLS для всего Web-узла, так как большинство его страниц содержат открытую информацию вроде маркетинговых, торговых и технических документов, предназначенных для всех. Используйте SSL/TLS только для пересылки конфиденциальных данных — все остальные части Web-узла могут обойтись без защищенного соединения.

2. Делайте SSL/TLS-страницы простыми.

Помните: шифруется все содержимое страниц, передаваемых по SSL/TLS-соединению, в том числе и изображения. Поэтому число изображений на этих страницах должно быть минимальным, а сами они — простыми. Используйте небольшие картинки, сохраненные с высоким уровнем компрессии JPEG и с малой глубиной цвета — нет смысла использовать палитру в 16 миллионов цветов там, где хватит 256.

Некоторые Web-разработчики располагают изображения в каталоге, не требующем SSL/TLS, а затем помещают ссылку на них на страницы, которым SSL/TLS необходим. Иногда такая комбинация защищенных и незащищенных данных вызывает в обозревателе появление предупреждения. Рекомендуется не делать этого, так как вы можете запутать пользователей.

3. Повторно используйте кэшируемые SSL/TLS-соединения.

Установка нового SSL/TLS-соединения занимает приблизительно впятеро больше времени, чем восстановление соединения, помещенного в кэш. Стандартный тайм-аут для такого соединения в Windows NT 4 увеличен с 2 до 5 минут. Время жизни соединения в кэше можно увеличить, присвоив подразделу реестра *ServerCacheTime* значение, приведенное ниже. Это значение измеряется в миллисекундах (например, 300 000 — это 5 минут).

```
HKEY_LOCAL_MACHINE \System
\CurrentControlSet \Control
\SecurityProviders \SCHANNEL
ServerCacheTimeout: REG_DWORD : 300000
```

Выбирая значения этого параметра, будьте осторожны: при слишком большом таймауте система будет тратить память на кэширование устаревших соединений.4. Используйте аппаратные криптографические ускорители.

По сравнению с другими Web-серверами Internet Information Services (IIS) обрабатывает новые SSL/TLS-соединения очень быстро. Так, на компьютере с процессором Pentium III 500 МГц IIS 5 можно обработать 60 новых SSL/TLS-соединений в секунду. И хотя может показаться, что это немного, по сравнению с другими Web-серверами, способными на подобном оборудовании осуществить около 10 SSL/TLS-соединений, такая производительность высока. Однако IIS за секунду может обработать более 1 000 анонимных соединений, не использующих SSL/TLS. Повысить производительность Web-сервера позволяют специальные аппаратные ускорители компаний nCipher *(www.ncipher.com)* и Compaq *(www.atalla.corn).* Эти устройства освобождают сервер от сложных операций с открытыми ключами, выполняя их аппаратно.

Microsoft предлагает производителям криптографического оборудования простой способ переноса на оборудование такой требовательной к процессору операции, как дискретное логарифмирование, — функцию *OffloadModExpo.* Вы можете подготовить DLL, которая экспортирует эту функцию и перекладывает всю работу на устройство. За подробностями обращайтесь к разделу Microsoft Developer Network (MSDN), посвященному функции *OffloadModExpo.*

2.10 SSL/TLS и лицензии клиентского доступа.

В IIS 5 все параллельные, уникально аутентифицированные соединения и все уникальные SSL/TLS-соединения получают лицензию клиентского доступа (Client Access License, CAL). По умолчанию число таких лицензий равно числу Windows-серверов. Например, если на сервере Windows 2000 установлено 250 лицензий, ваш Web-узел разрешит любое число анонимных соединений, но не более 250 SSL/TLS- или аутентифицированных соединений.

Вообще-то все сложнее. Одна лицензия клиентского доступа для обработки наборов кадров разрешает каждому компьютеру 4 соединения.

Существуют неограниченные Интернет-лицензии, разрешающие Web-серверу одновременно обрабатывать любое число аутентифицированных и SSL/TLS-соединений. О лицензировании доступа клиентов к IIS 5 см. статью Q253239 Базы знаний Microsoft *(http://support.microsoft.eom/support/kb/articles/Q253/2/ 39.asp},* а о клиентских лицензиях — статью «Windows 2000 Client Access Licensing Overview» *(http://www.microsoft.com/windows2000/guide/server/pri-cing/model.asp).*

2.11 Малоизвестный факт о SSL/TLS в Windows

Приведенная ниже информация не касается конфиденциальности или целостности данных — она описывает использование SSL/TLS для аутентификации. SSL/TLS поддерживает знаки подстановки в обычных названиях серверных сертификатов. Например, при подключении к узлу *www.explorationair.com* имя в сертификате будет также *www.explorationair.com.* Существует возможность применения символов подстановки для сертификатов, используемых для нескольких Web-узлов (скажем, узлов компании Exploration Air). Допустим, сервер *development.explorationair.com* находится в домене *explorationair.com.* Обычное имя в сертификате может выглядеть как '.explorationair.com, и этот сертификат мож-

но использовать на узлах *www.explorationair.com,* development.explorationair.com и на других узлах домена explorationair.com.

Однако по умолчанию этот режим в Windows 2000 отключен; кроме того, для его работы нужно обновить системную библиотеку. Подробнее см. статью Базы знаний Q257873 «Error Message: The Name on the Security Certificate Does Not Match the Name of the Site» по адресу *http://support.microsojt.com.*

В использовании символов подстановки в сертификатах имеются ограничения:

- символы подстановки могут находиться только в левой части доменного имени; например, имя *'.explorationair.com* допустимо, а *development.'.explorationair.com* — нет;
- символы подстановки нельзя применять в доменных именах первого уровня, таких как .com или .net; например, имя *'.explorationair.com* допустимо, а *'.сот* — нет;
- подстановка заменяет только один компонент доменного имени; например, имена *www.explorationair.com* и *development.explorationair.com* соответствуют шаблону *'.explorationair.com,* а *www.development.explorationair.com* — нет.

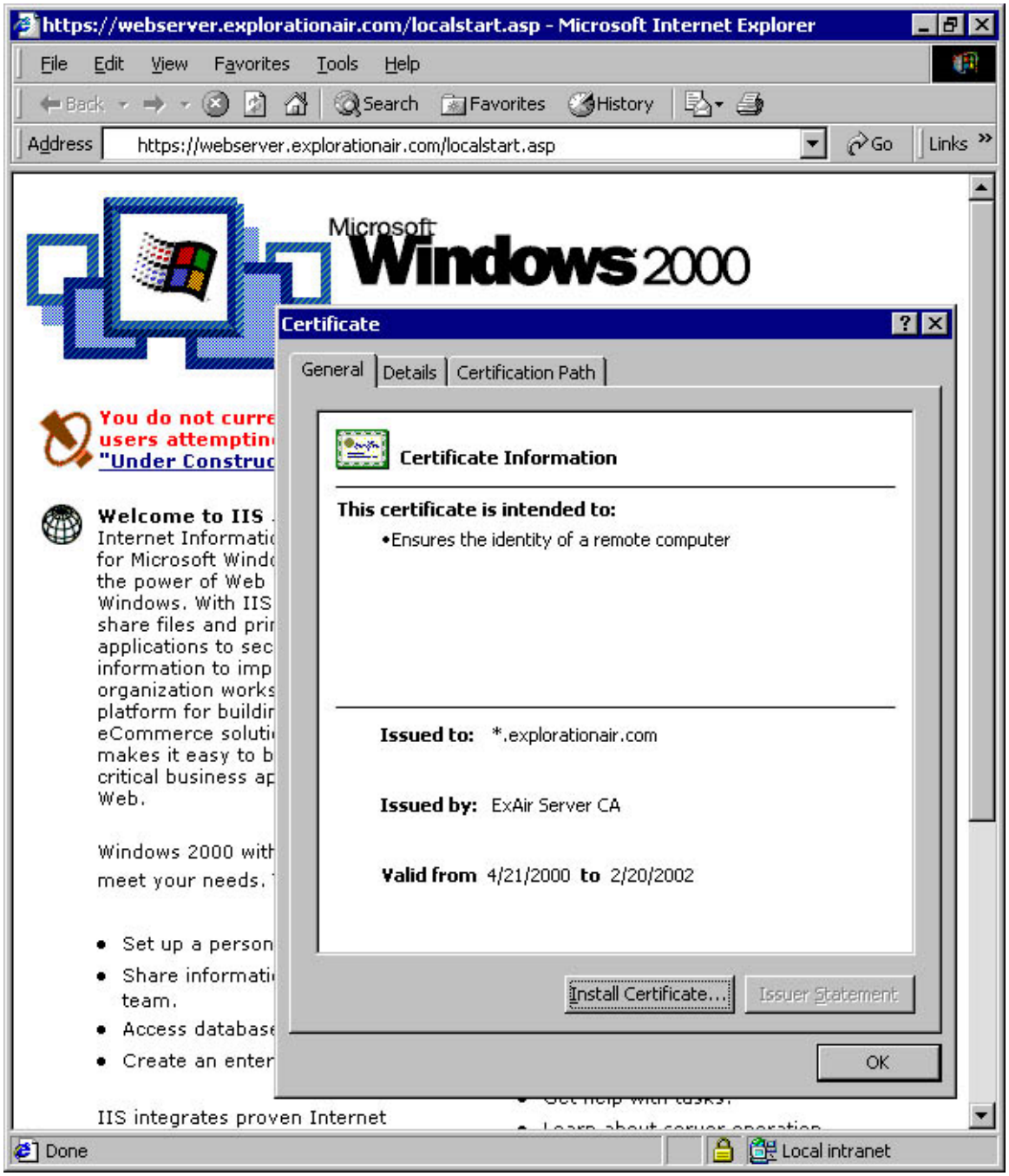


Рисунок 2-4. Символ подстановки в имени сервера в сертификате IIS 5.

Взгляните на сертификат, используемый при обращении к Web-странице *https://webserver.explorationair.com* (рис, 2-4). Снимок сделан, когда узел был в процессе разработки и не содержал ничего, кроме стандартного сообщения, предупреждающего администратора об отсутствии на узле информационного наполнения. Обратите внимание на то шаблон в имени сертификата *'.explorationair.com.*

2.12 SSL/TLS и сертификаты

Internet Explorer поддерживает ставшие стандартами индустрии протоколы, обеспечивающие конфиденциальность и целостность данных: Secure Sockets Layer и Transport Layer Security. Кроме того, он поддерживает версию SSL, использующую технологию Fortezza.

Fortezza — это спецификация аппаратной реализации криптографических функций, используемая Министерством обороны США. Она применяется для передачи конфиденциальных, но не секретных данных. PCMCIA-платы Fortezza позволяют установить безопасное соединение с Web-узлами, поддерживающими эту технологию. IIS 5 поддерживает спецификацию Fortezza, а TLS — нет.

Определить, какие SSL/TLS-протоколы поддерживает Internet Explorer, можно следующим образом.

1. Запустите Internet Explorer.
2. В меню Tools выберите пункт Internet Options.
3. Откройте вкладку Advanced.
4. Раскройте узел Security.

Здесь вы увидите список поддерживаемых протоколов SSL/TLS. В средах с высоким уровнем безопасности нужно включить SSL 3-0 и TLS 1.0, отключив при этом SSL 2.0 и PCT 1.0 (рис. 2-5).

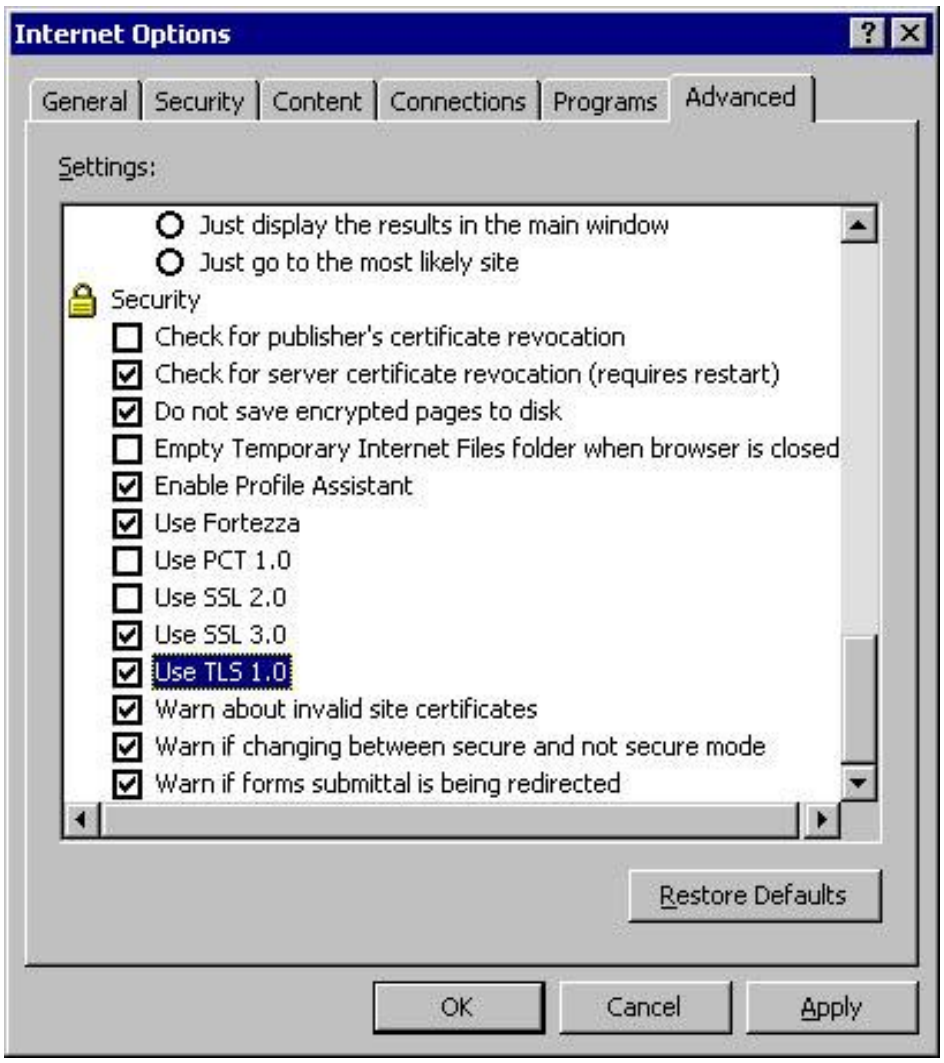


Рисунок 2-5. Настройка протоколов SSL и TLS в Internet Explorer *5.*

Internet Explorer также поддерживает клиентские сертификаты X.509, применяемые в средах с сильной аутентификацией. В настоящее время сертификаты и связанные с ними открытые ключи, как правило, хранятся в ПО или в смарт-картах.

3 Аутентификация и Web.

IIS - Internet Information Services.

Наиболее важной Интернет-технологией, интегрированной с Windows 2000 Server, является IIS 5.0, которые делают Windows 2000 Server мощным сервером Интернета и сервером интернет-приложений интрасети. Технология IIS 5.0 является полезным инструментом как для небольших рабочих групп и отделов корпоративной интрасети, так и для крупных поставщиков услуг Интернета, размещающих информацию на Web-узлах, к которым ежедневно обращаются миллионы пользователей. IIS обеспечивает простейший способ совместного использования информации, создания и развертывания приложений деловой сферы, а также размещения данных на Web-узлах и управления ими.

И IIS 4, и IIS 5 поддерживают использование клиентских сертификатов X.509 для аутентификации клиентов с применением SSL/TLS.

3.1 Аутентификация сервера

Как известно, протокол SSL/TLS всегда использует сертификат для аутентификации Web-сервера при подключении клиента.

Допустим, клиент подключается к Web-сайту www.exair.com по протоколу SSL/TLS. Обозреватель сравнивает указатель ресурса Web-сайта с именем, указанным в его сертификате. Если они одинаковы, Web-сервер считается аутентифицированным — в частности, гарантированно, что он принадлежит компании Exploration Air, а не, скажем, ее конкуренту. Для подключения по протоколу SSL нужно использовать префикс *https,* а не *http;* при этом обозреватель по умолчанию будет подключаться по протоколу SSL/TLS к порту TCP 443 вместо стандартного порта TCP 80.

На самом деле, конечно же, проверяется не только имя:

- выполняется криптографическая проверка наличия у сервера личного ключа, соответствующего открытому ключу, указанному в сертификате;
- проверяется степень доверия издателю сертификата;
- проверяется, не истек ли срок действия сертификата;
- проверяется, не отозван ли сертификат; по умолчанию Internet Explorer эту проверку не выполняет — это делает IIS.

Если любая из этих проверок приводит к отрицательному результату, пользователь получает предупреждение и может разорвать соединение (что, кстати, и рекомендуется сделать).

3.2 Аутентификация клиента

Протокол SSL/TLS позволяет аутентифицировать не только сервер, но и клиента. После проверки сертификата сервера последний может предложить клиенту предъявить свой сертификат (рис. 3-1).

Рисунок 3-1. Диалоговое окно аутентификации клиента в Internet Explorer 5.

При аутентификации клиента Web-сервер передает ему список *сертифицирующих организаций* (Certification Authority, CA), которым он доверяет. Например, если Web-сервер доверяет VeriSign и Thawte, а у клиента сертификаты компаний Thawte и Equifax, обозреватель предложит пользователю предъявить сертификат от компании Thawte, поскольку сервер не доверяет второму сертификату.

Internet Explorer «помнит», какой сертификат был предъявлен конкретному Web-сайту. В Windows 2000 Internet Explorer запоминает эти данные, даже если с их помощью не удалось зарегистрироваться на Web-сервере. Так что, если вы выбрали неверный сертификат, вам придется закрыть все открытые окна Internet Explorer и запустить его заново. Только после этого вы сможете выбрать правильный сертификат из списка.

3.3 Как IIS использует клиентские сертификаты X.509.

IIS может задействовать клиентские сертификаты X.509 четырьмя способами:

- не пользоваться ими;
- предложить (но не требовать) пользователю предъявить сертификат;
- потребовать предъявить сертификат;
- потребовать предъявить сертификат и отождествить его с учетной записью Windows 2000.

Первый вариант обсуждать нечего. Два других более-менее похожи; единственная разница в сказуемом: в первом случае пользователь может предъявить сертификат, а во втором — должен. В обоих случаях информация из сертификата (если он предъявлен) заносится в объект набора ASP *Request.ClientCertificate.* Это позволяет принимать решение об аутентификации в коде серверных страниц.

ASP - Microsoft Active Server Pages

Это выполняемые на сервере сценарии, позволяющие создавать динамические HTML-страницы, команды сценариев и COM компоненты, делающие web-сайт интерактивным.

Например, следующий код аутентифицирует пользователя на основе доменного имени его почтового адреса:

```
<%
Dim strValidDomain,  strEmail
strValidDomain = "@exair.com"
strEmail = Request.ClientCertificate("SubjectE")

If  InStr(strEmail,  strValidDomain,1) Then
'  Почтовый адрес из сертификата
'  содержит доменное имя @exair.com.

Response.Write("Доступ разрешен!")
End If
%>
```

Здесь пользователь с адресом cheryl@exair.com получит доступ, а с адресом cheryl@microsoft.com — нет.

Но одной проверки имени или любого другого поля сертификата недостаточно — надо проверить издателя сертификата. Эту криптографическую проверку выполняет IIS. Без проверки издателя нельзя гарантировать, что сертификат выпущен организацией, которой вы доверяете (скажем, «Крипто-Про», Thawte или VeriSign) а не группой экспертов по подделке документов. Любая организация с помощью сервера Microsoft Certificate Services может выпустить сертификат со значением *cheryl@exair.com* в поле «электронная почта», но если Web-сервер не доверяет издателю, соединение установлено не будет.

В нашем примере Web-сайт компании Exploration Air доверяет только сертификатам, выпущенным ее собственным центром сертификации (Exploration Air User Certification Authority). Административные средства IIS 5 позволяют указать список сертифицирующих органов (Certificate Trust List, CTL), которым доверяет ваш Web-сервер. Этот список представляет собой структуру данных интерфейса CryptoAPI 2.0. Список доверенных сертифицирующих организаций можно задавать по отдельности для каждого Web-сайта (но не виртуального каталога или файла).

3.4 Набор ClientCertificate ASP.

Мы уже отмечали, что ASP обеспечивает доступ к клиентским сертификатам через коллекцию *ClientCertificate.* В каждом элементе набора хранятся:

- исходные данные сертификата, полученные вызовом *Request.Client-Certificate("Certificate");*
- сведения об издателе клиентского сертификата, полученные вызовом *Request.ClientCertificate("IssuerX"),* где *X* — код издателя (см. ниже);
- значения полей *(Request.ClientCertificate("SubjectX"));*
- номер сертификата *Request.ClientCertificate("SerialNumber")*
- срок действия сертификата (вызовы *Request.ClientCertificate("ValidFrom")* и *Request.ClientCertificate("ValidTo")*

При работе с полями «Издатель» (Issuer) и «Тема» (Subject) можно использовать дополнительные коды, например: C – страна, O – организация и т.д. О кодах полей сертификатов X.500.

Если вы будете отождествлять несколько сертификатов с одной учетной записью, мы рекомендуем ограничить список одним доверенным сертифицирующим органом, чтобы избежать несоответствия имен. Если на Web-сервере не задан список доверенных сертифицирующих организаций, все сертификаты считаются доверенными.

Новый список доверенных сертификатов позволяют создать мастер из состава административных средств IIS и мастер глобальной политики активного каталога. Мы рассмотрим первый, так как он встроен в IIS, а для настройки глобальной политики нужна поддержка активного каталога (более того, список доверенных организаций нельзя создать с

помощью локальной политики). Мастер создания списка доверенных сертификатов глобальной политики активного каталога подробно описан в справочной системе Windows 2000.

Все манипуляции со списками доверенных организаций лучше выполнять средствами IIS, поскольку они требуют выполнения меньшего числа действий, чем аналогичные средства активного каталога.

Вот как добавить список доверенных сертификатов с помощью мастера из состава административных средств IIS (для этого нужны административные полномочия).

1. Щелкните правой кнопкой мыши значок My Computer на рабочем столе.
2. В контекстном меню выберите команду Manage.
3. Раскройте узел Services And Applications.
4. Раскройте узел Internet Information Services.
5. Щелкните правой кнопкой мыши значок нужного Web-сервера.
6. В контекстном меню выберите команду Properties.
7. Откройте вкладку Directory Security.
8. Щелкните кнопку Edit в группе Secure Communications. Если эта кнопка недоступна, значит, вы не выбрали сертификат.
9. Установите флажок Enable Certificate Trust List.
10. Щелкните кнопку New, чтобы создать новый список; эта кнопка запускает мастер. Для редактирования списка щелкните кнопку Edit.

Этот способ позволяет добавлять и удалять сертифицирующие организации из списка доверенных (рис. 3-2).

По умолчанию IIS *5* проверяет, не отозван ли клиентский сертификат. Если это случилось, будет возвращено сообщение об ошибке 403-13: *Client certificate revoked.* Если сервер, на котором хранится список отозванных сертификатов (Certificate Revocation List, CRL), недоступен, IIS следует пессимистической гипотезе, считая, что этот сервер атакован. Как следствие, если проверить, отозван сертификат или нет, невозможно, IIS возвращает сообщение об ошибке 403-13 (рис. 3-3). Этого не происходит, если IIS имеет кэшированную копию списка отозванных сертификатов.

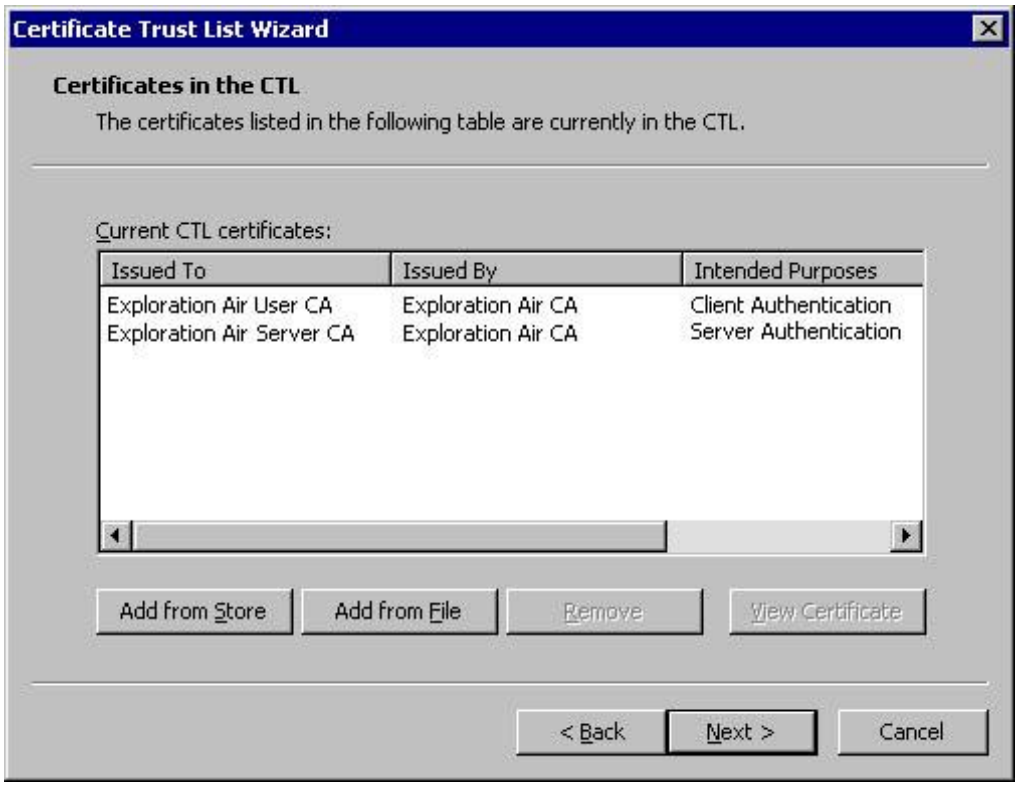


Рисунок 3-2. Редактирование списка доверенных сертифицирующих организаций с помощью мастера IIS.

Другие методы манипулирования списками сертификатов:

Функции для работы со списком доверенных сертифицирующих организаций интерфейса CryptoAPI 2.0 — *CertAddCTLContextToStore, CertDelete-CTLContextFromStore* и *CertFmdCTLJnStore* — обеспечивают возможность у программного манипулирования списком из таких языков программирования, как C++.

Утилиты MakeCTL и CertMgr из состава Microsoft Platform SDK также позволяют просматривать, создавать и изменять списки доверенных сертифицирующих организаций.

Информацию об этих средствах см. также по адресу *http://msdn.micro-soft.com.*

Проверку отзыва сертификатов можно отключить посредством интерфейса ADSI (пользовательский интерфейс не позволяет это сделать):

```
Set oWeb = GetObject("IIS://localhost/W3SVC/1")

oWeb.CertCheckMode =1   '  0 == проверка выполняется;   1 == нет.

    oWeb.SetInfo

    Set oWeb = Nothing
```

3.5 Отождествление клиентских сертификатов

IIS 5 позволяет использовать клиентские сертификаты как высоконадежные учетные данные. Соответствующая процедура аутентификации носит название *отождествления сертификатов,* так как сертификат отождествляется с учетной записью Windows 2000, после чего пользователь обращается к ресурсам в контексте отождествленной учетной записи.

IIS 4 предлагал простой метод отождествления сертификатов, который поддерживает и IIS 5. Однако в перспективе этот метод должен быть вытеснен средствами отождествления в составе активного каталога, которые отличаются большей надежностью и еще проще в использовании. Эти методы отождествления являются взаимоисключающими, и смешивать их нельзя. Поэтому подходящий метод надо выбрать до начала разработки приложения. Рассмотрим оба метода подробнее.

Метод отождествления в IIS 4 работает в одном из двух режимов: отождествление «один с одним» и «несколько с одним». В первом случае IIS связывает учетную запись с сертификатом и регистрирует пользователя по этой учетной записи. Например, администратор может связать сертификат А с учетной записью cheryl@development.exair.com, а сертификат Б — с учетной записью michael@development.exair.com. Этот метод очень гибок, поскольку, кроме того, позволяет связать сертификаты В и Г с одной учетной записью dev-team@development.exair.com. Недостаток метода — низкая производительность. IIS вынужден хранить копии всех отождествленных сертификатов, что не позволяет эффективно обрабатывать больше 2-3 тысяч сертификатов.

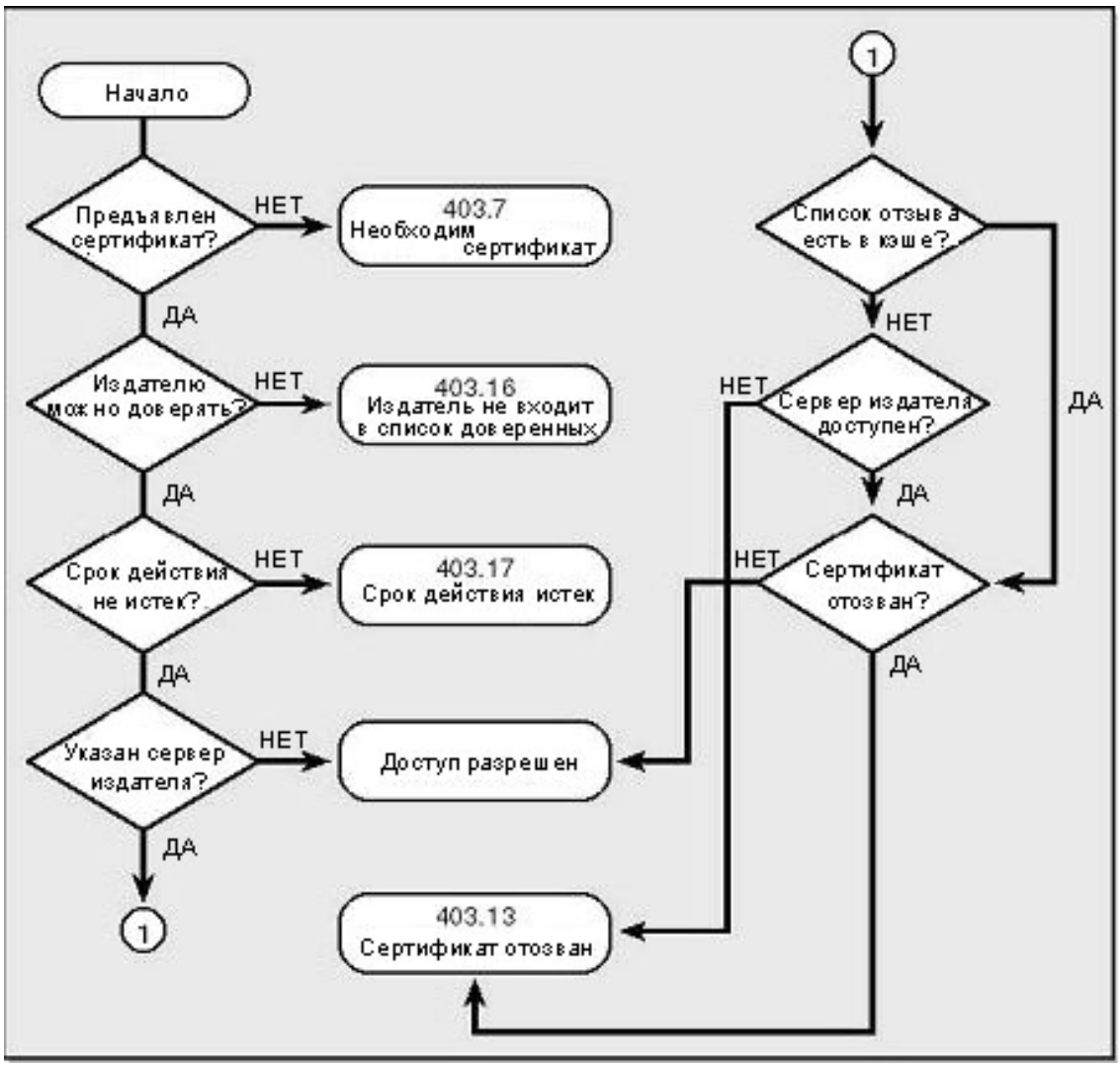


Рисунок 3-3. Проверка сертификата сервером IIS 5.

Поле «имя» не обязательно применяется для отождествления. Сертификат может указывать в качестве владельца пользователя cheryl@development.exair.com, но это не помешает связать его с учетной записью dev-team@development.exair.com.

Отождествление «несколько с одним» основано на правилах. Например, правила могут связывать все сертификаты, изданные сертифицирующим органом Exploration Air User CA (в нашем примере это единственный доверенный сертифицирующий орган), поле «организация» которых имеет значение ExAir (O = *ExAir),* а поле «отдел» — значение Development *(OU= Development), с* учетной записью dev-team@development.exair.com.

Недостатком обоих методов отождествления сертификатов IIS 4 является высокая нагрузка на администратора: он должен вручную вводить имя и пароль каждой учетной записи, участвующей в отождествлении. Кроме того, отождествление вручную неминуемо ведет к ошибкам. И все же самый гибкий метод отождествление «несколько с одним».

Встроенные методы отождествления IIS работают независимо от наличия активного каталога.

Рассмотрим пример настройки отождествления сертификатов в IIS. Мы настроим сервер IIS для отождествления всех сертификатов со следующими свойствами:

- издатель — Exploration Air User CA;
- поле «организация» имеет значение ExAir (O = *ExAir);*
- поле «отдел» — значение Development *(OU = Development).*

Нам нужно будет создать на сервере список доверенных сертифицирующих органов с единственной доверенной организацией Exploration Air User CA; это позволит нам выполнить

первое требование. Требования 2 и 3 будут удовлетворены соответствующими правилами. Сначала мы настроим список доверенных органов; этот шаг выполняется один раз для каждого Web-сайта, а соответствующие параметры являются составной частью политики Web-сайта.

1. Щелкните правой кнопкой мыши значок My Computer на рабочем столе и выберите в контекстном меню команду Manage.

2. Раскройте узел Services And Applications, а затем — узел Internet Information Services.

3. Щелкните правой кнопкой мыши Web-сервер (но не виртуальный каталог), для которого создается список доверенных органов.

4. Выберите в контекстном меню команду Properties и откройте вкладку Directory Security.

5. Щелкните кнопку Edit в группе Secure Communications. Если эта кнопка недоступна, значит, у Web-сервера нет серверного сертификата. О настройке поддержки SSL/TLS на сервере IIS см. раздел «Настройка SSL/TLS».

6. Установите флажок Enable Certificate Trust List и щелкните кнопку New.

7. Когда запустится мастер создания списка доверенных органов, щелкните кнопку Next.

8. Щелкните кнопку Add From Store и выберите из списка сертификат Exploration Air User CA. Тем самым вы выберете сертифицирующий орган, сертификатам которого вы будете доверять. (При использовании отождествления сертификатов рекомендуется ограничить список одним доверенным органом.)

9. Щелкните кнопку Next.

10. Введите имя и описание списка, например, «Доверенные издатели клиентских сертификатов» и «Корневые сертификаты доверенных издателей клиентских сертификатов для отождествления». Щелкните кнопку Next.

11. Щелкните кнопку Finish.

12. После настройки списка доверенных издателей Web-сайт будет принимать только выпущенные ими сертификаты, что отвечает первому требованию нашего примера. Взгляните на окно Secure Communications после выполнения описанной процедуры (рис. 3-4), а затем — на диалоговое окно списка доверенных издателей после добавления корневого сертификата Exploration Air (рис. 3-5).

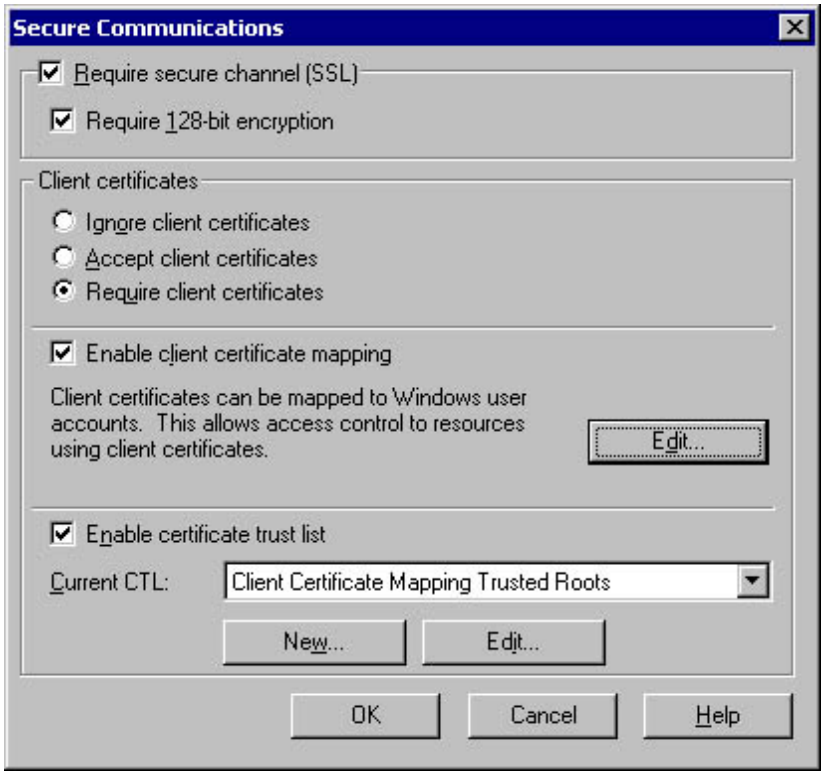


Рисунок 3-4. Отождествление клиентских сертификатов.

Чтобы удовлетворить второе и третье требования, нужно создать соответствующие правила в диалоговом окне Secure Communications.

1. Установите флажок Require Secure Channel (SSL).
2. Установите переключатель Require Client Certificates.
3. Установите флажок Enable Client Certificate Mapping.

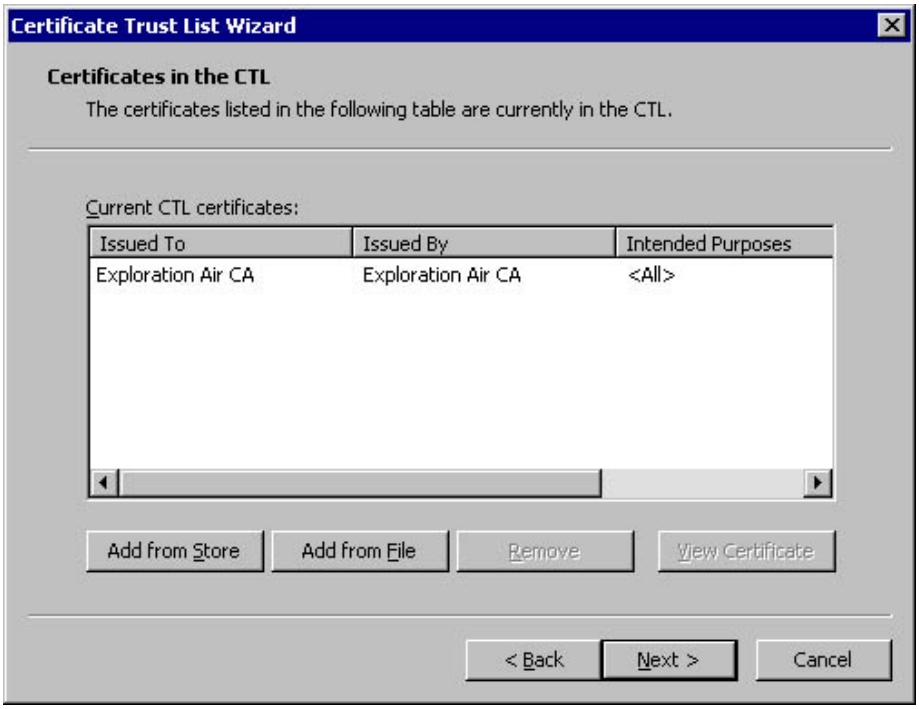


Рис. 3-5. Выбор доверенных издателей для отождествления клиентских сертификатов.

4. Щелкните кнопку Edit в группе Enable Client Certificate Mapping.
5. Откройте вкладку Many-to-1.
6. Щелкните кнопку Add.
7. В текстовом поле введите «Правила отождествления ExAir».
8. Щелкните кнопку Next.
9. Щелкните кнопку New.
10. В списке Certificate Field выберите строку «Subject», а в списке Sub Field — строку «O»; в поле Criteria наберите текст «ExAir» и щелкните кнопку OK.
11. Еще раз щелкните кнопку New, чтобы создать новое правило.
12. В списке Certificate Field выберите строку «Subject», а в списке Sub Field — строку «OU»; в поле Criteria наберите текст «Development» и щелкните кнопку OK.
13. Щелкните кнопку Next.
14. Убедитесь, что установлен переключатель Accept This Certificate For Logon Authentication.
15. Щелкните кнопку Browse и выберите учетную запись, с которой будут отождествлены сертификаты, удовлетворяющие этим правилам. В нашем примере это учетная запись dev-team.
16. Введите пароль учетной записи dev-team.
17. Щелкните кнопку Finish.
18. Подтвердите пароль и щелкните кнопку OK.

19. Щелкните кнопку OK.

Теперь сервер IIS будет регистрировать всех клиентов, предъявивших сертификат, удовлетворяющий этим правилам, по учетной записи dev-team.

3.6 Настройка SSL/TLS

Как вы помните, SSL/TLS — набор криптографических технологий, обеспечивающих аутентификацию, конфиденциальность и целостность данных. Это один из самых распространенных протоколов защиты в Интернете: он ясен и практически не требует дополнительных усилий со стороны пользователей. Единственное, что нужно для настройки SSL/TLS на сервере, — установить сертификат X.509, предварительно получив его от сертифицирующей организации.

Управление сертификатами упрощает включенный в IIS 5 мастер сертификатов. Он заметно проще утилиты KeyRing IIS 4 (там она называлась Диспетчер ключей). Кстати, мастер сертификации Web-сервера из состава IIS 5 был переработан на основе анализа мнения пользователей о KeyRing.

Конфигурирование SSL/TLS может показаться довольно сложным, но на помощь приходит мастер.

1. Получите сертификат для сервера у издателя (например, в компании VeriSign или у собственного издателя Microsoft Certificate Services, если он у вас есть).
2. Установите сертификат на Web-сервере.
3. Включите поддержку SSL/TLS для выбранного виртуального сервера, каталога или файлов.

Установка сертификата на сервере еще не означает поддержки SSL/TLS. На самом деле по умолчанию все как раз наоборот: поддержка SSL/TLS не включается по соображениям производительности.

IIS позволяет довольно гибко настроить SSL/TLS. Ниже показан Web-сайт, использующий три варианта конфигурации SSL/TLS (рис. 3-6. Сам сайт — www.exair.com — не требует подключения по SSL/TLS. Тем не менее, поскольку сертификат содержит имя Web-сайта, он установлен именно здесь; IIS не поддерживает установку нескольких сертификатов на разных разделах Web-сайта. Виртуальный каталог Marketing также не требует защиты средствами SSL/TLS. Виртуальные каталоги Secure и HighSecure, напротив, требуют SSL/TLS, причем второй использует 128-разрядное шифрование.

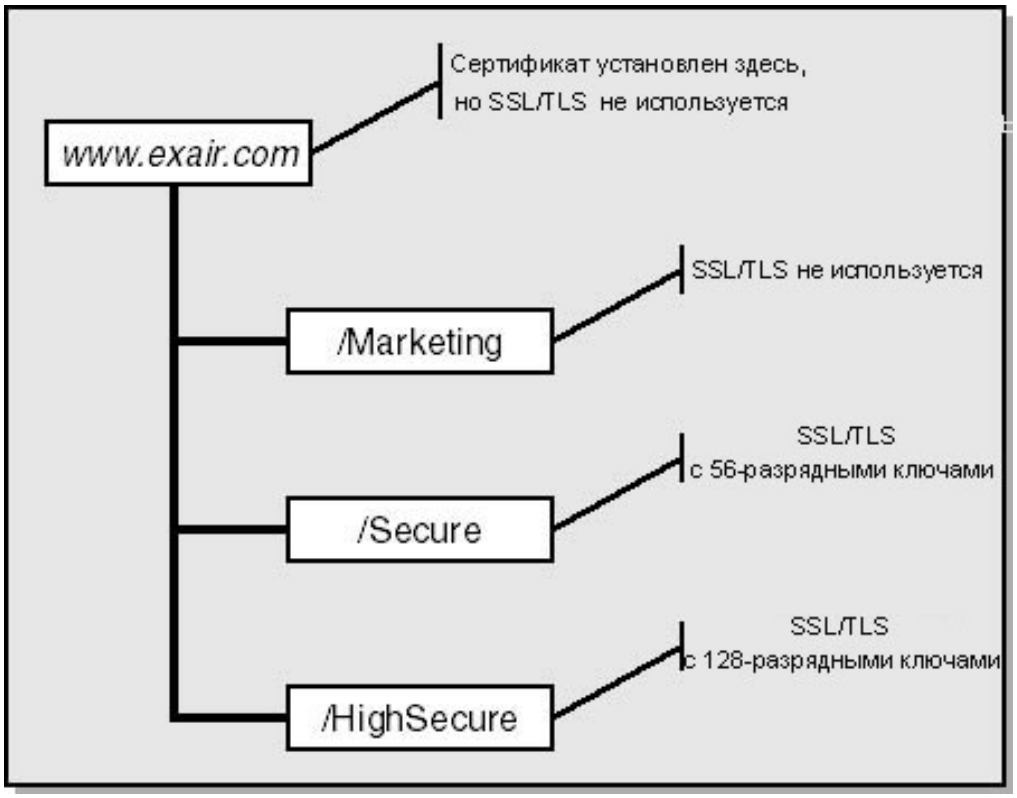


Рисунок 3-6. Web-сайт с несколькими разделами, использующими разные режимы SSL/TLS.

После установки сертификата сервер IIS может не требовать от пользователей подключения по SSL/TLS, однако при желании пользователь может подключиться именно так: например, ссылка https://www.exair.com/marketing позволяет подключиться к виртуальному каталогу Marketing сайта Exploration Air с использованием SSL/TLS, хотя этот виртуальный каталог и не требует применения этого протокола.

3.7 Дополнительные аспекты настройки SSL/TLS

Мастер, конечно, упрощает конфигурирование SSL/TLS, но остается несколько вопросов, на которые нужно обратить внимание. Начнем с получения сертификата для Web-сайта.

1. Щелкните правой кнопкой мыши значок My Computer на рабочем столе.
2. Выберите в контекстном меню команду Manage.
3. Раскройте узел Services And Applications, а затем — узел Internet Information Services.
4. Выберите в контекстном меню команду Properties.
5. Откройте вкладку Directory Security.
6. Щелкните кнопку Server Certificate. Если она недоступна, значит, вы выбрали не Web-сервер, а каталог или файл. В этом случае закройте диалоговое окно и выберите сервер.
7. Прочтите информацию в окне мастера создания запроса сертификата. Она не только познакомит вас с работой мастера, но и сообщит о статусе предыдущих запросов. Поскольку мастер знает статус предыдущих запросов, в процессе работы он предлагает только варианты, не влияющие на предыдущие запросы.
8. Щелкните кнопку Next.
9. Установите переключатель Create A New Certificate.
10. У вас два варианта (рис. 3-7): подготовить запрос и отправить его позже (Prepare The Request Now, But Send It Later) или сразу отправить запрос в сертифицирующую организацию (Send The Request Immediately To An Online Certification Authority). Первый доступен всегда, второй — только если у Web-сервера есть доступ хотя бы к одному серверу Microsoft Certificate Services в домене Windows 2000, сконфигурированному для выпуска сертификатов для Web-сервера. Если вы настраиваете сервер интрасети, в состав которой входит сервер сертификатов, вам, вероятнее всего, больше подойдет первый вариант. Если же вы планируете получить сертификат от внешней организации, такой как VeriSign, выберите второй. Мы будем предполагать, что вы выбрали первый вариант и щелкнули кнопку Next.
11. Введите имя Web-сайта; в сертификате оно не используется — лишь упрощает работу администратора.
12. Выберите длину открытого ключа сертификата. Обычно используют 2048-разрядные ключи, однако можно ограничиться 1024 разрядами.

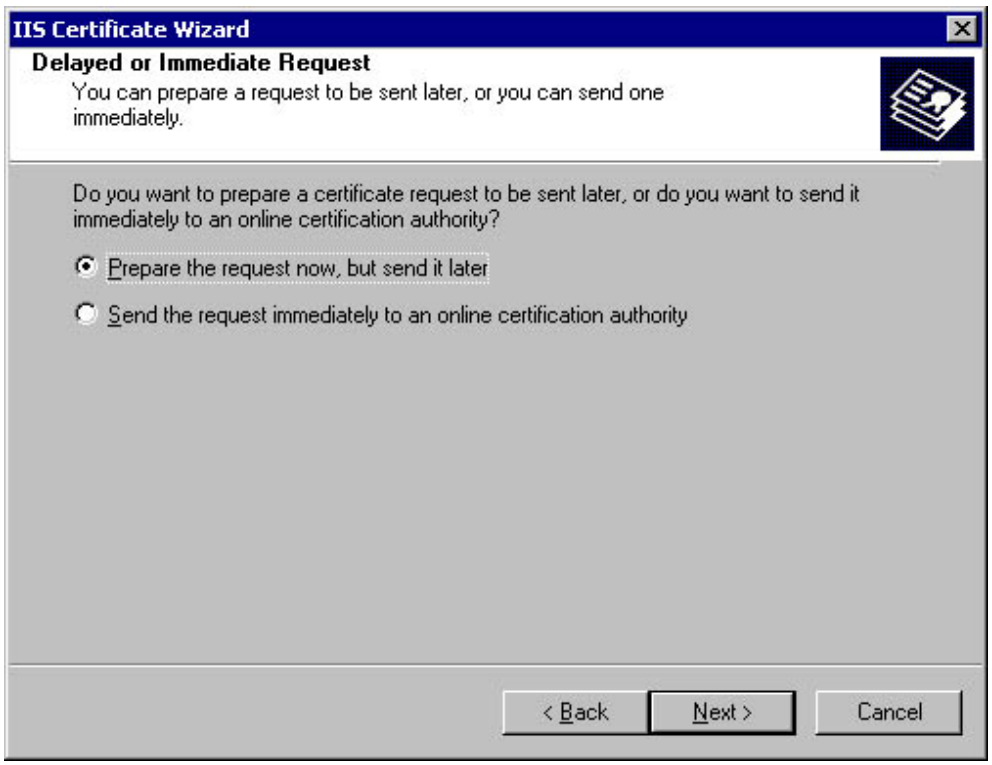


Рисунок 3-7. Мастер предлагает два варианта создания запроса сертификата.

13. Если хотите задействовать протокол Server Gated Cryptography (SGC), установите флажок SGC. SGC — это расширение SSL/TLS, позволявшее финансовым институтам в качестве исключения экспортировать 128-разрядные криптографические средства. Поскольку недавнее решение правительства США практически сняло ограничения на экспорт сильных криптографических средств, протокол SGC утратил актуальность.

14. Щелкните кнопку Next.

15. Введите название организации (например, Exploration Air) и подразделения (например, Development Department). Эта информация будет включена в сертификат, так что не делайте ошибок.

16. Щелкните кнопку Next.

17. Введите название компьютера, для которого вы хотите получить сертификат. Это название обязательно должно быть правильным, иначе у клиентов сайта будут проблемы. По умолчанию мастер предлагает выбрать NetBIOS- или DNS-имя сервера. Если он будет использоваться в интрасети, можете выбрать любое из этих имен. Если же сервер будет доступен из Интернета, надо указать его доменное имя. Например, если имя NetBIOS вашего сервера — *Web-Server,* внутреннее доменное имя — webserver.explorationair.com, а внешнее — www.exair.com, в поле Common Name надо ввести последнее из этих имен. Это имя также попадет в сертификат; на самом деле это почти самая важная информация в сертификате.

18. Щелкните кнопку Next.

19. Введите страну, область или район и город. Эти сведения также будут включены в сертификат. Все названия необходимо вводить полностью.

20. Щелкните кнопку Next.

21. Введите имя файла запроса сертификата По умолчанию мастер предлагает имя C:\Certreq.txt. Файл будет содержать закодированный методом base64 запрос сертификата в формате PKCS *10. Этот формат мы подробно обсудим в главе 15. А вот пример содержимого файла запроса:

```
-------BEGIN NEW CERTIFICATE REQUEST------

MIID+DCCAuACAQAwXjEXMBUGA1UEAxMObWlrZWhvdy1sYXBOb3AxDDAKBgNVBAsT

AORldjEOMAwGAlUEChMFRXhBaXIxCzAJBgNVBAcTAUlMQswCQYDVQQIEwJXQTEL
```

```
LNihpipWqerGWnZAmSDtKitiqnsOZsptlrTzIRMsSQSWmlmacTYExEO+6SPky02XeC
pEzrI08CBxrheiZYf14K2gm12A62AItLznxIwgV4H+qP7jqkC9KmiW9WDwhdHneA
3Dq1dsTlscfyhsFU
------END NEW CERTIFICATE REQUEST------
```

Посмотреть содержимое файла запроса сертификата в текстовом виде позволяет утилита Certutil.exe Microsoft Certificate Services. Команда *certutil -v certreq.txt* выводит на экран содержимое запроса.

22. Щелкните кнопку Next. Мастер отобразит сводку введенных вами параметров. Если все в порядке, щелкните Next, чтобы завершить работу мастера.

23. Щелкнув кнопку Click Here, можно посмотреть список издателей сертификатов для продуктов Microsoft.

24. Щелкните кнопку Finish.

Теперь можно передать запрос сертификата издателю. Список издателей см. по адресу http://backoffice.microsoft.com/securitypartners. Время обработки запроса зависит от типа сертификата и политики издателя.

Запрос сертификата содержит только открытый ключ. Парный к нему личный ключ остается на вашем компьютере.

Получив ответ издателя, можно продолжить процесс установки сертификата с помощью того же мастера. Ответ издателя соответствует формату PKCS #7.

1. Щелкните правой кнопкой мыши значок My Computer на рабочем столе.

2. Выберите в контекстном меню команду Manage.

3. Раскройте узел Services And Applications, а затем — узел Internet Information Services.

4. Выберите в контекстном меню команду Properties.

5. Откройте вкладку Directory Security.

6. Щелкните кнопку Server Certificate. Если она недоступна, значит, вы выбрали не Web-сервер, а каталог или файл. В этом случае закройте диалоговое окно и выберите сервер.

7. Прочтите сообщение мастера. Оно должно подтвердить, что вы запрашивали сертификат (рис. 3-8).

Рисунок 3-8. Окно мастера установки сертификата информирует о наличии невыполненного запроса.

8. Щелкните кнопку Next.

9. Установите переключатель Process The Pending Request And Install The Certificate и щелкните кнопку Next.

10. Введите имя файла с ответом издателя. Если нужно, найдите файл с помощью кнопки Browse.

11. Щелкните кнопку Next.

12. Изучите параметры сертификата и щелкните кнопку Next.

13. Щелкните кнопку Finish.

Теперь сертификат Web-сервера установлен на вашем компьютере.

Получив сертификат, вы можете настроить поддержку SSL/TLS для виртуальных каталогов и других разделов сайта. Для сайта в целом это обычно не нужно — вряд ли все содержимое сайта понадобится шифровать при передаче клиенту.

Чтобы проверить, что сертификат установлен, откройте в обозревателе ресурс https://имя_вашего_сервера. Изображение замка в строке состояния Internet Explorer будет свидетельствовать о корректной установке SSL/TLS. В Netscape Navigator в зависимости от версии аналогичные функции выполняет соединение двух половинок ключа или замкнутый замок.

Чтобы выяснить подробности конфигурации соединения SSL/TLS, используйте такой код ASP:

```
<H2>SSL/TLS Information</H2>
<PRE>
SSL/TLS Connection? <%= Request.ServerVariables("HTTPS") %>
Server Cert. Issuer <%= Request.ServerVariables("CERT_SERVER_ISSUER") %>
Server Cert. Subject <%= Request.SeryerVariables("CERT_SERVER_SUBJECT") %>
Symmetric Key Size  <%= Request.ServerVariables("HTTPS_KEYSIZE") %>
```

```
Public Key Size     <%= Request.ServerVariables("HTTPS_SECRETKEYSIZE") %>
</PRE>
```

3.8 Хранение личного ключа во время обработки запроса:

При создании запроса сертификата мастер создает пару ключей: открытый и личный. Открытый входит в состав запроса. Личный, наряду с другой информацией из запроса сертификата, остается на вашем компьютере в защищенном хранилище под названием REQUEST.

Его содержимое можно посмотреть следующим образом:

1. Щелкните кнопку Start.
2. Выберите в меню команду Run, наберите текст mmc /a и нажмите клавишу Return.
3. В меню Console наберите команду Choose Add/Remove Anap-In
4. Щелкните кнопку Add и выберите из списка модуль Certificates.
5. Щелкните кнопку Add, выберите свой компьютер и щелкните кнопки Next и Finish.
6. Щелкните кнопку Close, а затем – кнопку OK.
7. Раскройте узел Certificates, а затем – узел REQUEST.

В узле Certificates отображаются все текущие запросы сертификатов. Ни в коем случае не удаляйте их: при удалении запроса удаляется и соответствующий личный ключ, и восстановить его нельзя.

3.9 Протоколирование соединений SSL/TLS

Подробности соединений SSL/TLS, включая используемые алгоритмы, можно посмотреть в системном журнале Windows 2000. Для этого сначала нужно включить протоколирование соединений; это делается с помощью приведенного ниже ключа реестра:

```
HKEY_LOCAL_MACHINE \System
       \CurrentCont rolSet \Control
       \SecurityProviders \SCHANNEL
       \EventLogging:  REG_DWORD :  O
```

По умолчанию этот ключ имеет значение 0, т. е. протоколирование не ведется. Допустимые значения ключа реестра составляются из следующих (табл. 3-1) побитовой операцией *ИЛИ.*

Таблица 3-1. Типы протоколирования SSL/TLS.

Значение	Описание
1	Ошибки
2	Предупреждения
4	Все информационные сообщения

Рекомендуется присвоить ключу реестра EventLogging значение 7, обеспечивающее протоколирование всех событий, связанных с SSL/TLS.

Если включено протоколирование, после успешного установления соединения SSL в системном журнале появится запись, аналогичная этой (рис. 3-9).

SSL/TLS — простая и удобная технология, однако в некоторых сценариях ее настройка требует от администратора дополнительных усилий. Ниже мы обсудим два таких сценария: поддержку нескольких Web-сайтов и нескольких Web-серверов.

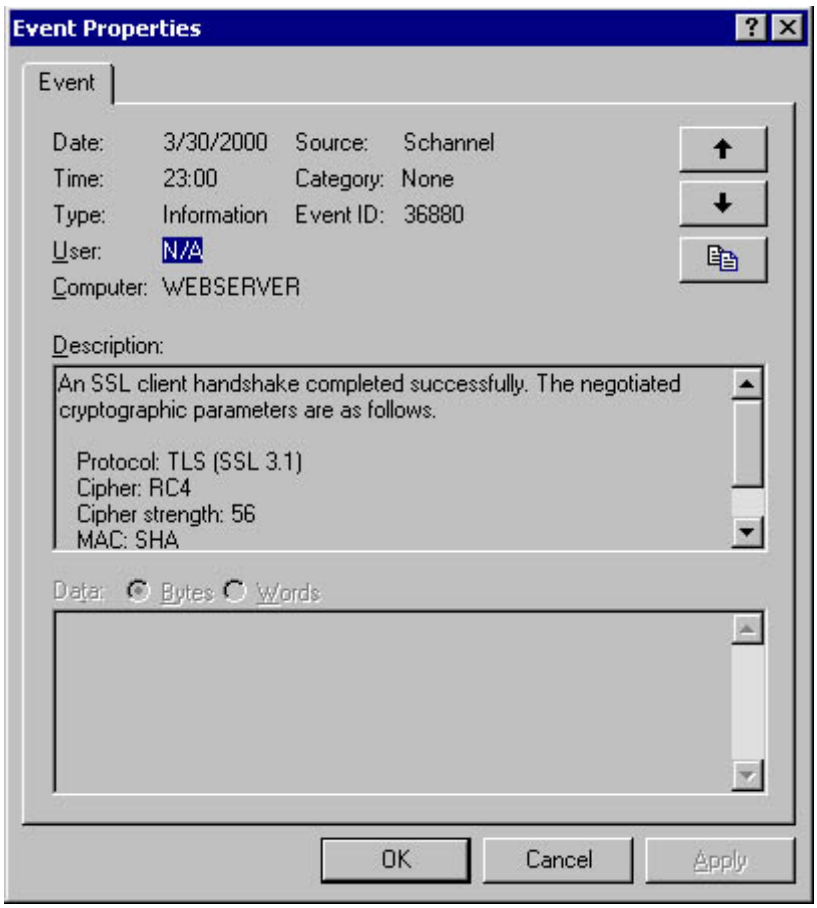


Рисунок 3-9. Запись в системном журнале об успешном установлении TLS-соединения между Web-сервером и Web-обозревателем.

3.10 SSL/TLS и виртуальные Web-сайты.

IIS может поддерживать сотни Web-сайтов на одном компьютере, однако это может привести к нетривиальным проблемам конфигурирования SSL/TLS. Прежде чем мы займемся этими проблемами, давайте разберемся в виртуальном хостинге.

IIS поддерживает виртуальные Web-сайты тремя способами:

- каждый Web-сайт использует отдельный IP-адрес, привязанный к отдельной сетевой карте;
- все Web-сайты используют один IP-адрес, но каждый прослушивает свой порт;
- все Web-сайты используют один IP-адрес и одну сетевую карту; у каждого сайта свое доменное имя, а для маршрутизации запросов служит заголовок Host протокола HTTP 1.1.

Ниже приведен пример виртуального хостинга на сервере Windows 2000 под названием \\exair (рис. 3-10). Web-сайт по умолчанию называется http://exair; кроме того, есть три виртуальных сайта отделов маркетинга (http://Marketing), разработки (http://Development) и отдела кадров (http://HumanResources).

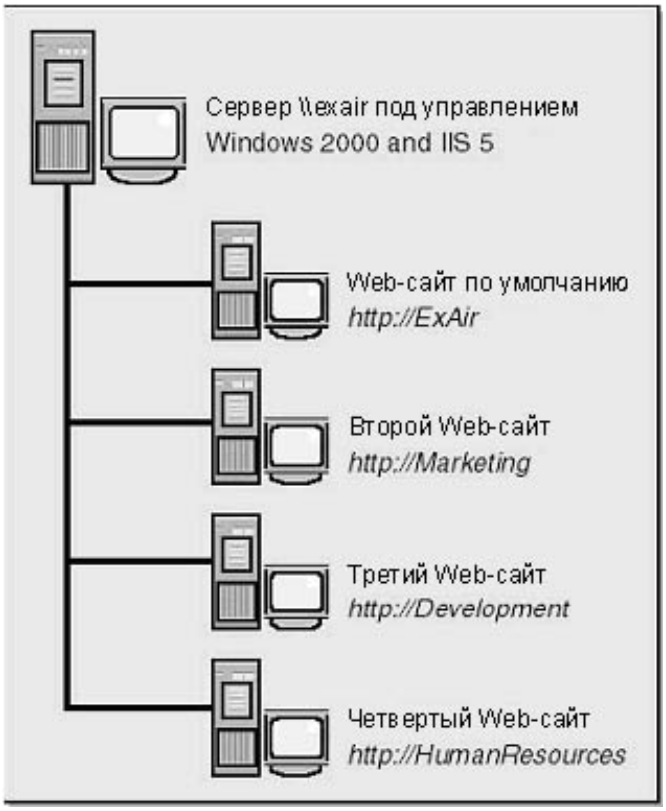


Рисунок 3-10. Сервер Windows 2000/IIS, поддерживающий Web-сайт по умолчанию и три виртуальных Web-сайта.

Три описанные выше конфигурации проиллюстрированы ниже (табл. 3-2, 3-3 и 3-4).

Таблица 3-2. Все Web-сайты используют один IP-адрес, но разные порты.

Сервер	IP-адрес	Порт HTTP	Порт SSUTLS	Заголовок Host
По умолчанию (http://exair)	157.65.122.22	80	443	Не используется
http://Marketing	157.65.122.22	81	444	Не используется
http://Development	157.65.122.22	82	445	Не используется
http://HumanResources	157.65.122.22	83	446	Не используется

Таблица 3-3. Каждый Web-сайт использует свой IP-адрес и один и тот же порт.

Сервер	IP-адрес	Порт HTTP	Порт SSUTLS	Заголовок Host
По умолчанию (http://exair)	157.65.122.22	80	443	Не используется
http://Marketing	157.65.122.23	80	443	Не используется
http://Development	157.65.122.24	80	443	Не используется
http://HumanResources	157.65.122.25	80	443	Не используется

Таблица 3-4. Все Web-сайты используют одни и те же IP-адрес и порты; для маршрутизации запросов служит заголовок Host протокола HTTP 1.1.

Сервер	P-адрес	Порт HTTP	Порт SSL/TLS	Заголовок Host
по умолчанию (http://exair)	157.65.122.22	80	443	Exair или не указан
http://Marketing	157.65.122.22	80	443	Marketing
http://Development	157.65.122.22	80	443	Development
http://HumanResources	157.65.122.22	80	443	HumanResources

3.11 Почему SSL/TLS не работает при использовании заголовка host.

Первые два сценария — с различными IP-адресами или портами — не вызывают проблем в работе SSL/TLS, так как при выполнении запроса клиента IIS выбирает сертификат и личный ключ по IP-адресу и номеру порта. При использовании заголовка «Host» IP-адреса и номер порта у всех Web-сайтов одинаковы — единственное различие заключается в доменном имени, передаваемом в заголовке «Host» запроса HTTP. Однако клиент не может передать HTTP-запрос, пока не установлено SSL-соединение, а Web-сервер в свою очередь не может найти соответствующий сертификат, пока не получит запрос — для этого нужно идентифицировать Web-сайт, что невозможно до поступления первого запроса HTTP с именем сайта в заголовке «Host».

Итак, если вы хотите использовать SSL/TLS на нескольких виртуальных Web-сайтах, вам придется ограничиться одним из двух первых сценариев: с различными IP-адресами или портами.

3.12 SSL/TLS и виртуальные Web-серверы

Web-серверы с большой нагрузкой часто представляют собой несколько серверов, объединенных в комплекс с применением различных технологий масштабирования и отказоустойчивости. При этом, однако, возникают любопытные вопросы конфигурирования SSL/TLS. Типичный пример такой конфигурации показан ниже (рис. 3-11): первая группа серверов, «откликающихся» на одно доменное имя, отвечает за распределение нагрузки и передачу запросов кластеру серверов БД.

Windows 2000 Advanced Server поддерживает кластеры из двух узлов, а Windows 2000 Datacenter Server — до четырех узлов с поддержкой избыточности и отказоустойчивости. Кроме того, средства распределения сетевой нагрузки Windows 2000 позволяют распределять нагрузку между 32 Web-серверами под управлением Windows 2000.

При использовании SSL/TLS в таких конфигурациях возникает две проблемы: сертификаты Web-сервера и преемственность запросов SSL/TLS.

3.13 Сертификаты Web-сервера

Каждый компьютер кластера должен иметь сертификат (и личный ключ) с одним и тем же именем, что и у всех Web-серверов кластера. Возможное решение — получить уникальный сертификат для каждого сервера или реплицировать один сертификат (и связанный с ним ключ) на все серверы кластера. Прежде чем заняться репликацией, изучите лицензию на сертификат.

IIS 5 позволяет реплицировать сертификат с одного компьютера на другой следующим образом.

1. Щелкните кнопку Start.
2. Выберите в меню команду Run и введите команду *mmc/a.*
3. В меню Console выберите команду Add/Remove Snap-in.
4. Щелкните кнопку Add и выберите в списке модуль Certificates.
5. Щелкните кнопку Add.
6. Установите флажок Computer Account и щелкните кнопку Next.
7. Щелкните кнопку Finish.
8. Щелкните кнопку Close.
9. Щелкните кнопку OK.

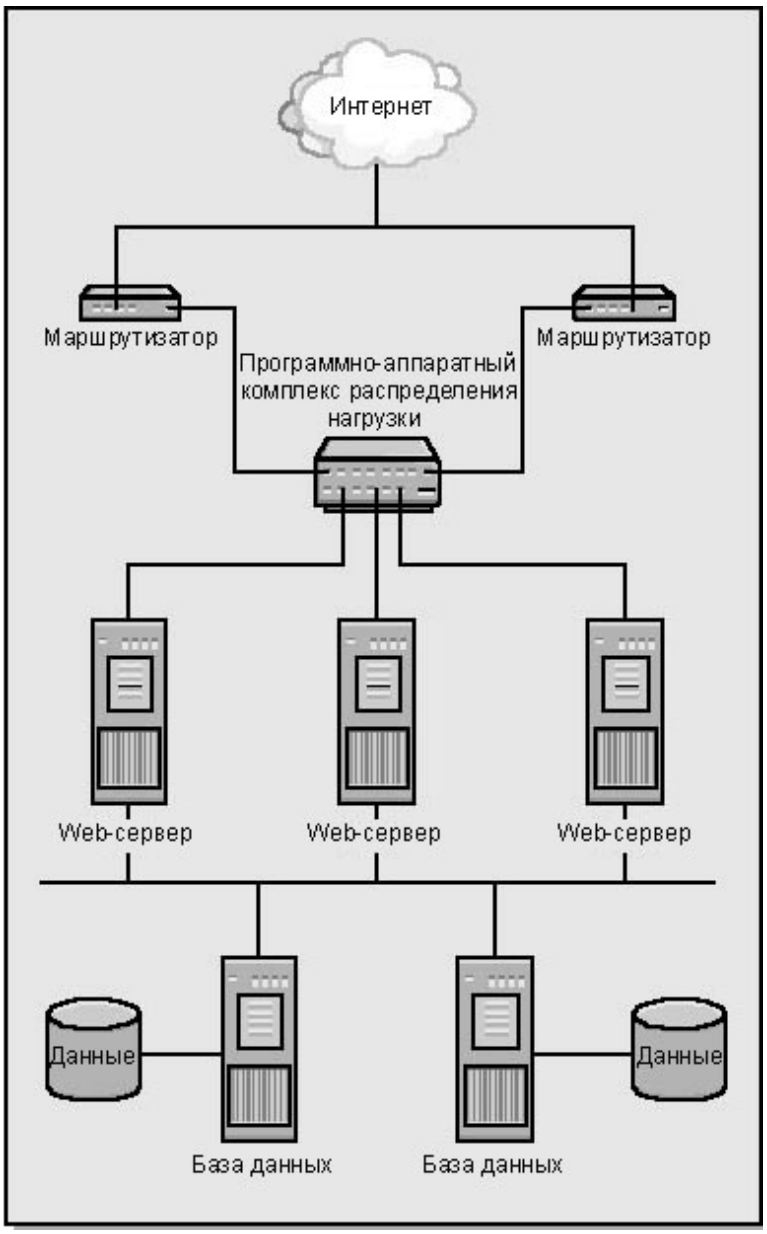


Рисунок 3-11. Пример конфигурации Web-сайта, использующего технологии распределения нагрузки и кластеризации.

10. Раскройте узел Certificates (Local Computer).
11. Раскройте узел Personal и щелкните кнопку Certificates.
12. Щелкните нужный сертификат в правой панели.
13. В контекстном меню выберите команду All Tasks.
14. Выберите команду Export.
15. Щелкните кнопку Next — будет запущен мастер экспорта сертификатов.
16. Установите флажок Yes, Export The Private Key. Для работы SSL/TLS частный ключ надо скопировать на новый компьютер. Если вы не установите флажок, упомянутый в предыдущем пункте, ключ не будет скопирован, и вся процедура завершится неудачей.
17. Установите флажок Personal Information Exchange - PKCS #12 (.PFX).
18. Установите флажок Include All Certificates In The Certification Path If Possible.
19. Щелкните кнопку Next.

20. Установите флажок Enable Strong Protection (Requires Internet Explorer 5, Windows NT 4 SP4 Or Above).

21. Введите и подтвердите пароль для защиты сертификата и частного ключа.

22. Щелкните кнопку Next.

23. Введите имя экспортируемого файла.

24. Щелкните кнопку Next, а затем — кнопку Finish.

Рекомендуется скопировать экспортированные данные на дискету и удалить файл с Web-сервера. Для импорта ключа на каждый Web-сервер кластера можно вызвать мастер сертификатов.

3.14 Преемственность соединений SSL/TLS

Соединения SSL/TLS должны быть *преемственными.* Если запрос клиента, подключившегося к вашему Web-сайту, переадресован второму серверу кластера, все последующие запросы этого клиента должны поступать на тот же сервер. В противном случае при следующем запросе придется снова устанавливать соединение SSL/TLS, что приведет к значительным накладным расходам.

Проверьте, поддерживает ли ваш комплекс распределения нагрузки такую возможность. Если вы работаете с Windows 2000 Server/Advanced Server, можно не волноваться — там эта возможность предусмотрена.

4 Использование средства сетевой аутентификации "КриптоПро TLS"

4.1 Аутентификация.

Односторонняя аутентификация

Обеспечивает минимально необходимый уровень защиты, и включает в себя:

- обязательную аутентификацию сервера, без аутентификации клиентов;
- шифрование трафика между клиентом и сервером.

При работе в данном режиме сервер на этапе "рукопожатия" не запрашивает сертификат клиента и устанавливается "анонимное" защищенное соединение. В этом случае клиент может не иметь секретного ключа и сертификата, однако при этом он лишается возможности формировать электронную цифровую подпись под документами. Режим с односторонней аутентификацией сервера может использоваться для предоставления некоторой группе пользователей конфиденциальной информации на основании парольной защиты, однако пароль в этом случае будет предъявляться пользователем только после установления защищенного SSL-соединения с Web-сервером, что повышает уровень защиты от несанкционированного доступа по сравнению с передачей пароля по открытым соединениям.

В режиме с необязательной аутентификацией сервер запрашивает сертификат клиента, но его отсутствие не считается ошибкой.

Так как двусторонняя аутентификация обеспечивает максимальный уровень защиты, именно она используется в СКЗИ «КриптоПро CSP» и «КриптоПро TLS».

Двусторонняя аутентификация

Включает в себя:

- взаимную аутентификацию клиента и Web - сервера с помощью их сертификатов;
- шифрование трафика между клиентом и сервером;
- формирование и проверку электронной цифровой подписи под электронными HTML-формами, заполняемыми пользователями.

Двусторонний метод аутентификации позволяет обеспечить доступ в закрытую часть Web - сервера только зарегистрированным владельцам сертификатов. При этом нужно иметь в виду, что разграничение доступа к информационным ресурсам сервера, основанное на проверке сертификатов клиентов, гораздо надежнее, чем просто паролевая защита.

В данном режиме работы клиенту необходимо сгенерировать открытый и секретный ключ и получить в Сертификационном Центре сертификат.

4.2 Установка «КриптоПро TLS»

Средство сетевой аутентификации «КриптоПро TLS**»** базируется на использовании криптографических преобразований и ключевой системы, реализованных в СКЗИ «КриптоПро CSP**»**.

Кроме СКЗИ «КриптоПро CSP» на компакт-диске содержится дистрибутив программного обеспечения, реализующего протокол TLS (Transport Layer Security). Протокол TLS (RFC 2246) является дальнейшим развитием протокола SSL (Secure Socket Layer) и широко используется в сети Internet для защиты соединений в клиент-серверных технологиях.

Программное обеспечение «КриптоПро TLS» является реализацией протокола TLS и использует криптографические функции «КриптоПро CSP» для обеспечения процесса аутентификации и шифрования трафика между клиентом и сервером.

Для установки программного обеспечения «КриптоПро TLS» с компакт-диска (рис.4-1) выберите значок «Установить КриптоПро TLS»

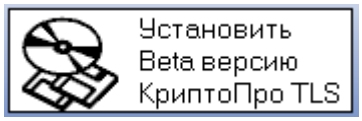


Рисунок 4-1. Установка «КриптоПро TLS».

Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. После завершения установки дистрибутива необходимо произвести перезагрузку компьютера.

4.3 Конфигурация программных средств компьютера, используемого под сервер ISA

Требования к техническим и программным средствам компьютера, на который устанавливается ISA (Internet Security and Acceleration Server) сервер, определяются в документации, поставляемой вместе с данным сервером.

Дополнительно, на компьютер должны быть установлены СКЗИ «КриптоПро CSP» и СКЗИ «КриптоПро TLS».

Для установления защищенного соединения между веб-клиентом и сервером ISA необходимо вначале выпустить сертификат открытого ключа, который будет использоваться для серверной аутентификации по протоколу TLS.

Требования к сертификату:

- имя сертификата (Common name) должно совпадать с именем публикуемого веб-сервера прикладной системы. Например: pif.nikoil.ru
- область использования ключа должна содержать «Аутентификация Сервера»

Данный сертификат должен быть установлен на сервер ISA со связкой с ключом подписи (секретным ключом). При этом, ключ подписи должен быть помещен в машинный реестр.

Выпуск и установка сертификата осуществляется через АРМ пользователя Центра регистрации. Порядок действий определяется в инструкции пользователю.

Также сертификат должен быть размещен в Local Computer certificate store на компьютере с сервером ISA. Для этого необходимо после установки сертификата через mmc консоль скопировать сертификат из хранилища учетной записи пользователя в хранилище учетной записи компьютера.

Порядок копирования:

1. Запустить консоль MMC (рис. 4-2)

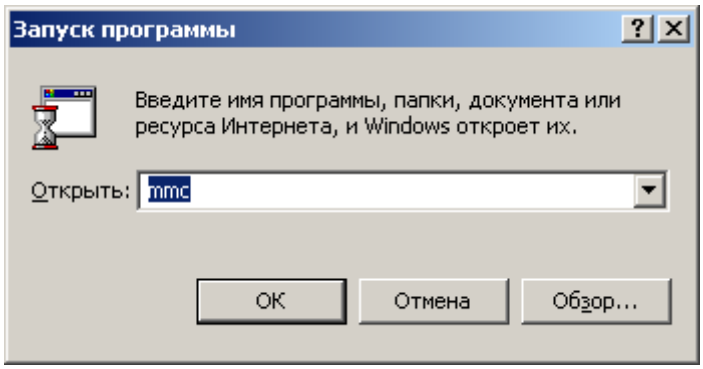


Рисунок 4-2. Запуск консоли MMC.

2. В корень консоли MMC установить две изолированные оснастки диспетчера сертификатов (рис.4-3):

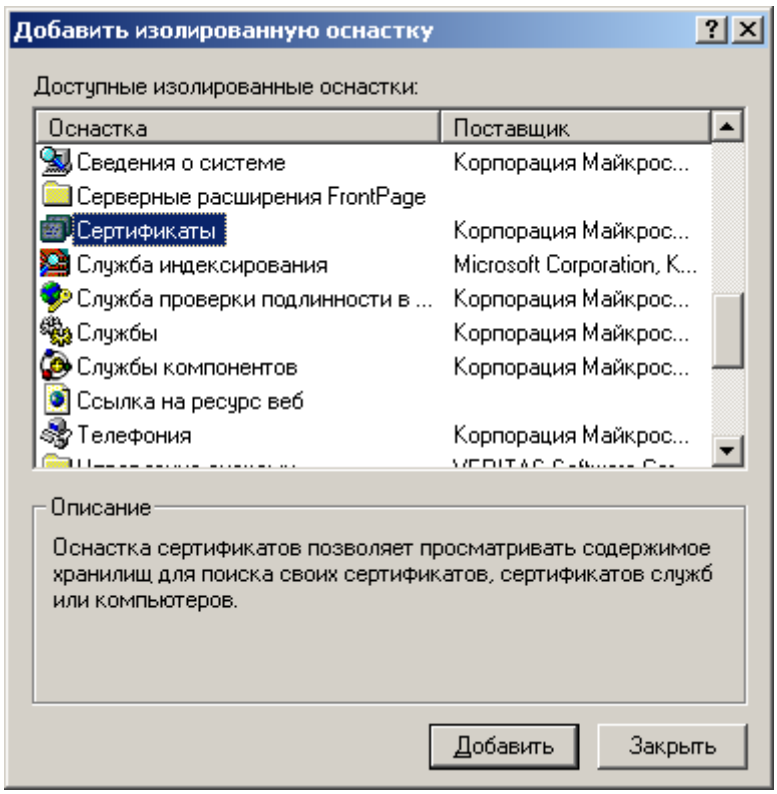


Рисунок 4-3. Добавление изолированной оснастки.

3. Установить одну оснастку для управления сертификатами учетной записи пользователя (рис 4-4).

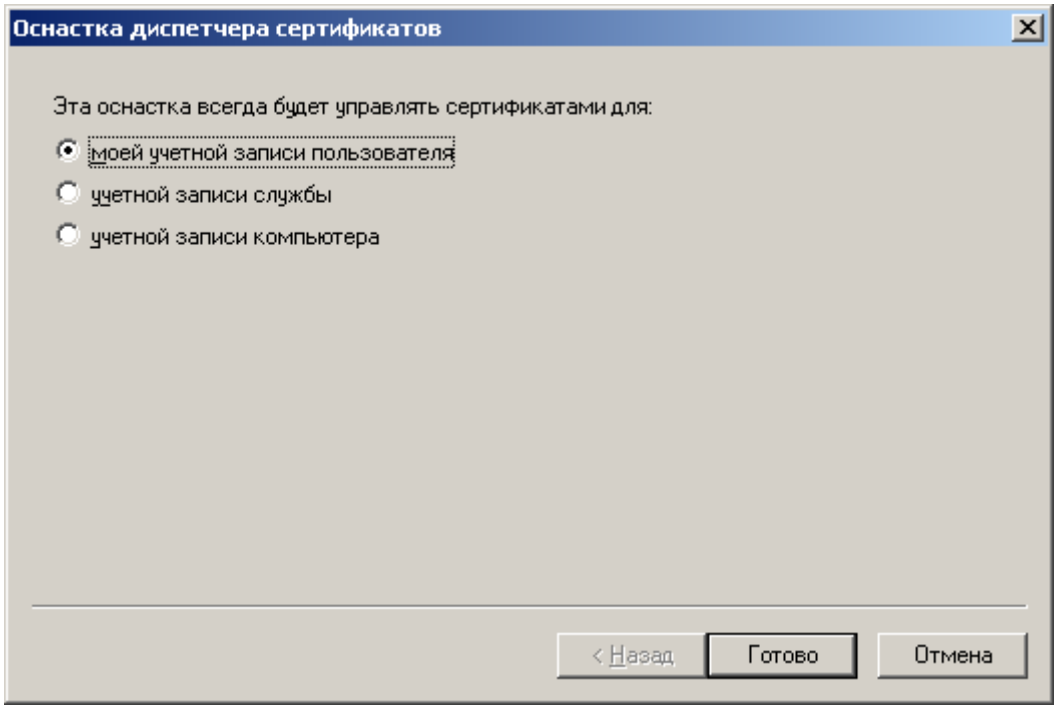


Рисунок 4-4. Оснастка диспетчера сертификатов (1).

4. Установить вторую оснастку для управления учетной записи компьютера (рис. 4-5)

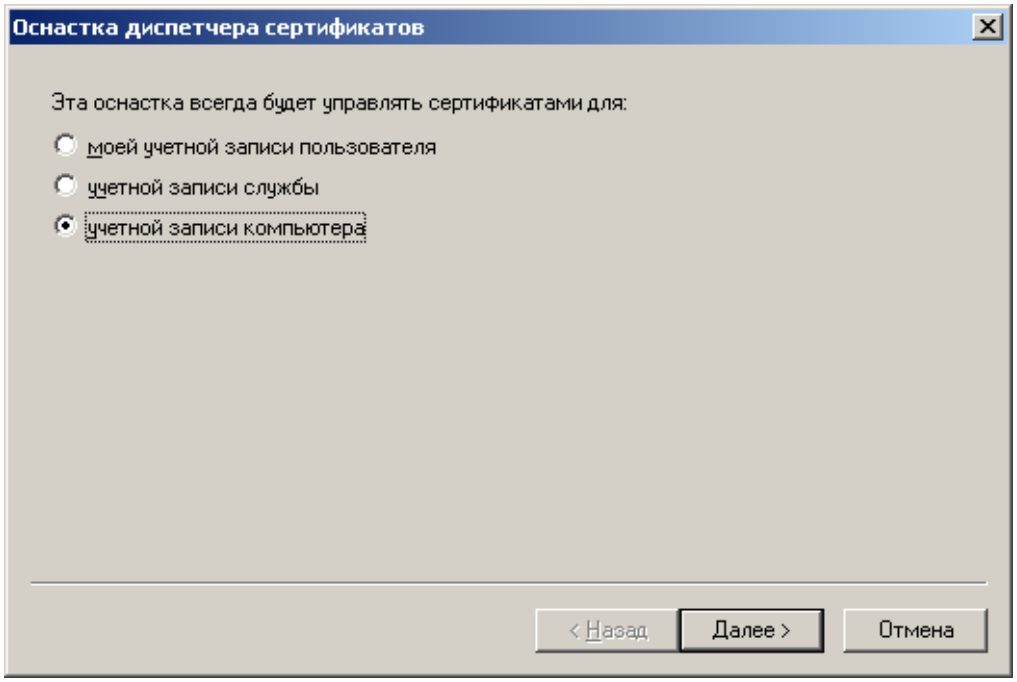


Рисунок 4-5. Оснастка диспетчера сертификатов (2).

После выбора этих оснасток корень консоли должен выглядеть приблизительно так (рис.4-6):

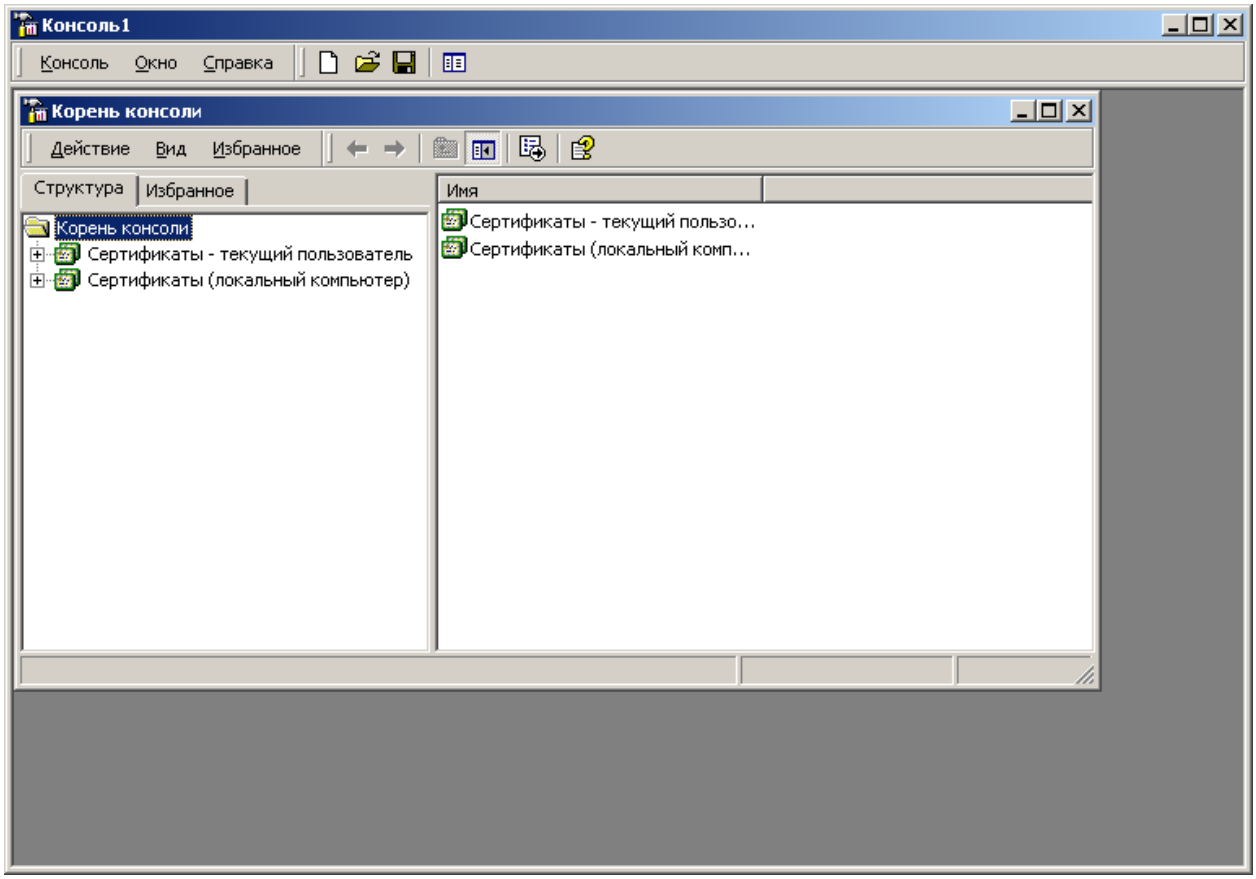


Рисунок 4-6. Консоль MMC.

5. Установите курсор на сертификат сервера ISA (рис. 4-7):

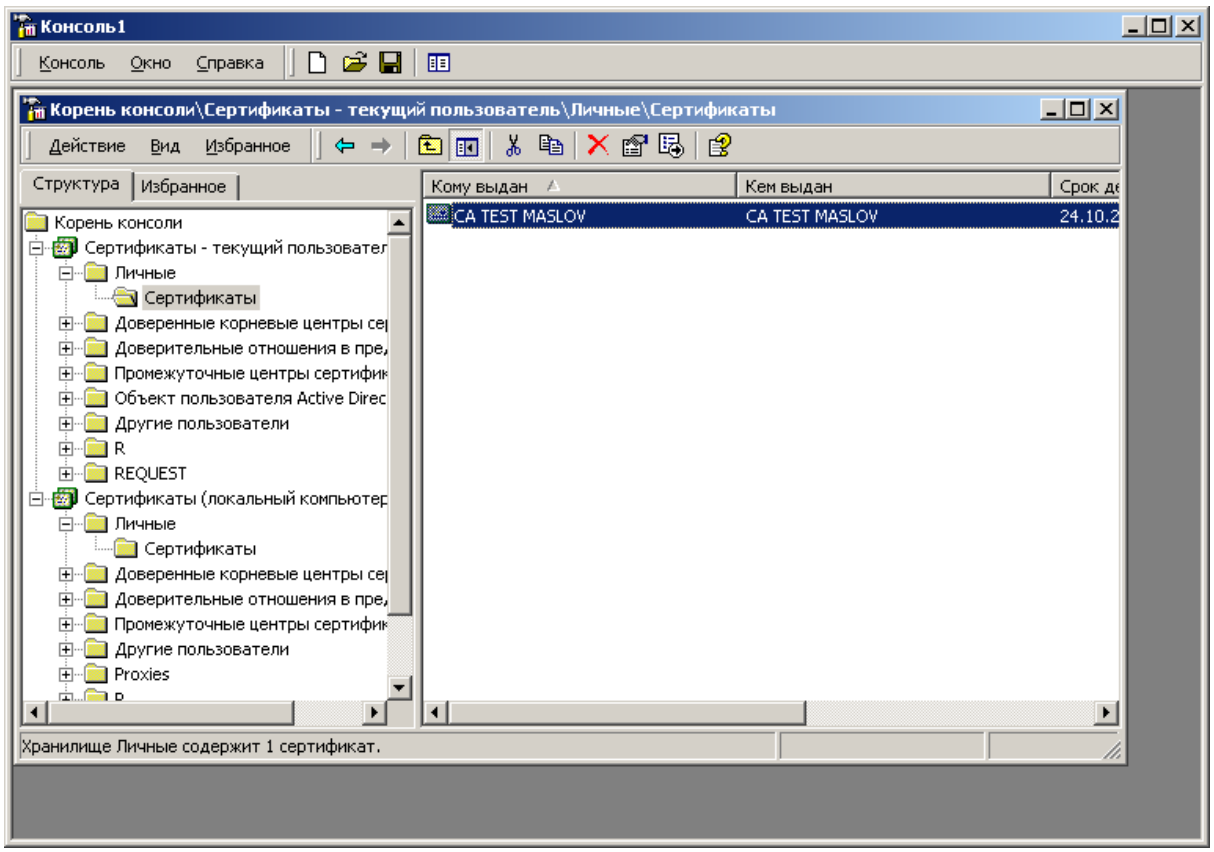


Рисунок 4-7. Корень консоли MMC.

6. С использованием функции Copy, занесите сертификат в буфер Clipboard

7. После этого установите курсор на разделе «личные» сертификатов локального компьютера и выполните функцию Paste

После установки сертификата серверной аутентификации ISA, таким же образом установите сертификат центра сертификации в раздел «Доверенные корневые центры сертификации» хранилища локального компьютера.

4.4 Настройка соединения с веб-клиентом.

После установки сертификатов открытых ключей, необходимо установить и настроить Слушателя для внешнего IP адреса сервера (IP адрес сетевого интерфейса, доступного из внешней сети).

Установка и настройка Слушателей осуществляется на вкладке Incoming Web Requests окна свойств ISA сервера (рис.4-8):

1. В окне ISA Management установить курсор на имя сервера и нажать правую кнопку мыши.

2. В появившемся меню выбрать пункт Properties.

3. В окне свойств сервера выбрать закладку Incoming Web Requests.

4. Выберите режим индивидуального Слушателя для каждого IP адреса в поле Identification.

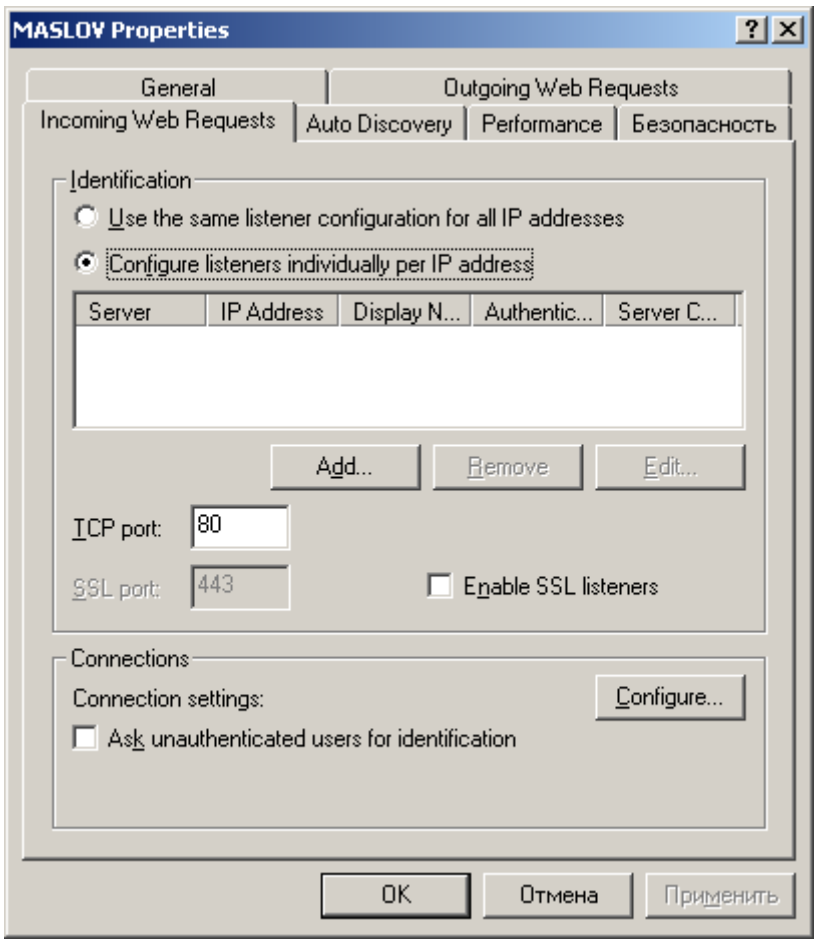


Рисунок 4-8. Установка и настройка Слушателей.

5. Добавьте нового Слушателя в список слушателей ISA сервера.
6. Установите имя сервера.
7. Установите внешний IP-адрес, на который будет настроен Слушатель.
8. Введите имя, с которым будет отображаться данный Слушатель в дальнейшем (опционально).

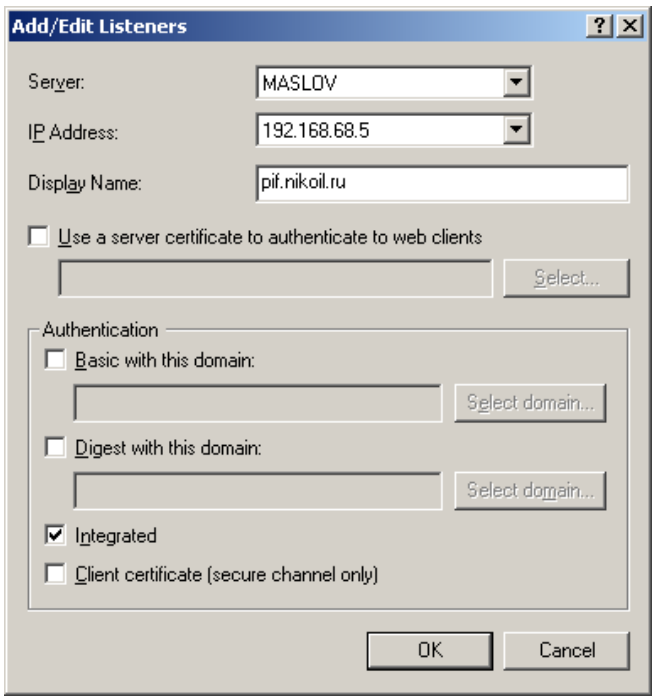


Рисунок 4-9. Добавление Слушателя/редактирование свойств Слушателя(1).

Для настройки защищенного соединения по протоколу TLS с двухсторонней аутентификации сервера ISA необходимо:

1. В окне добавления Слушателя или в окне редактировании свойств Слушателя, указать на использование сертификата сервера при аутентификации с веб-клиентом.

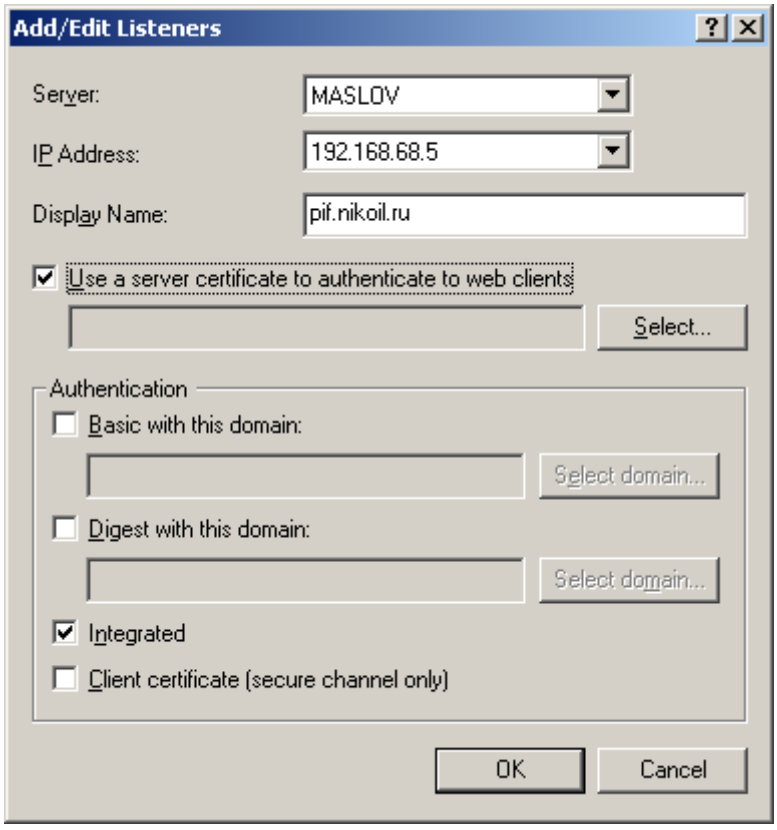


Рисунок 4-10. Добавление Слушателя/редактирование свойств Слушателя(2).

2. Выбрать сертификат сервера, который будет использоваться для аутентификации.
3. Нажать кнопку Select.

4. В появившемся окне выбрать из списка сертификат открытого ключа сервера (рис.4-11).

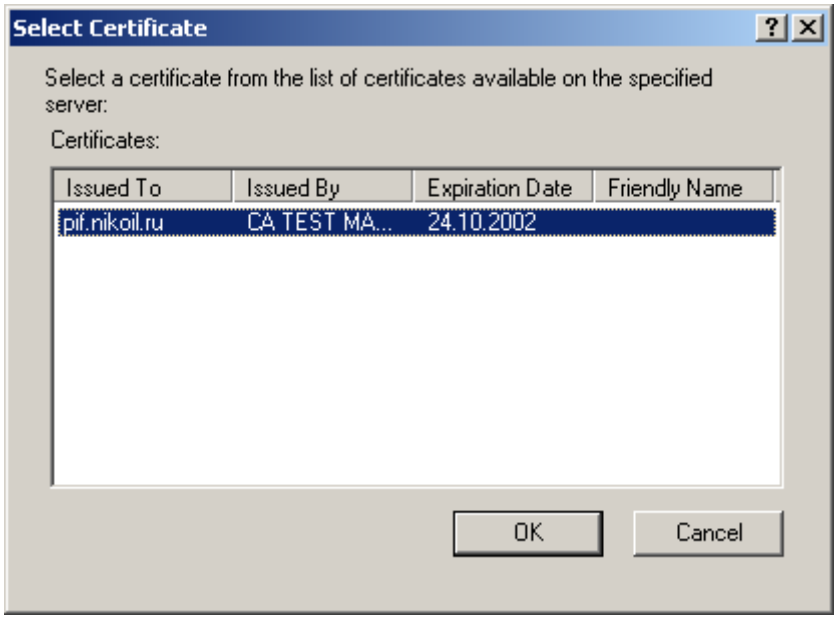


Рисунок 4-11. Выбор сертификата открытого ключа сервера.

5. Указать на использование сертификата клиента (опция Client certificate (secure channel only)).

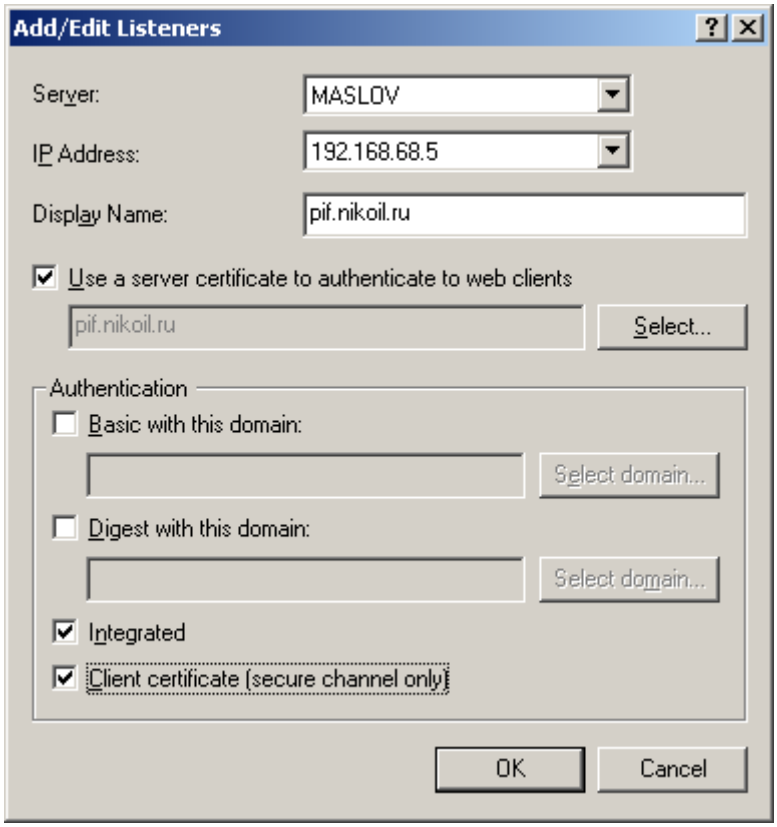


Рисунок 4-12. Добавление Слушателя/редактирование свойств Слушателя(3).

4.5 Публикация веб-сервера автоматизированной информационной системы в сети Интернет.

В этом разделе будет рассмотрен порядок действий при опубликовании веб-сервера, расположенного во внутренней сети. При этом соединение сервера ISA и веб-сервера будет установлено по протоколу SSL.

Для публикации веб-сервера во внешнюю сеть необходимо:

1. Получить и установить на публикуемый веб-сервер сертификат открытого ключа, который будет использоваться для серверной аутентификации.

Требования к сертификату:

- Имя сертификата (Common name) должно совпадать с доменным именем веб-сервера, указываемого для редиректа поступающих запросов (закладка **Action** окна свойств правила веб публикации). Например: epif.big.nikoil.ru
- область использования ключа должна содержать «Аутентификация Сервера»

2. Установить сертификат веб-сервера на сервере ISA, в хранилище локального компьютера (**Local Computer certificate stor**), раздел «Доверенные корневые центры сертификации»

3. Настроить веб-сервер для поддержки SSL соединения

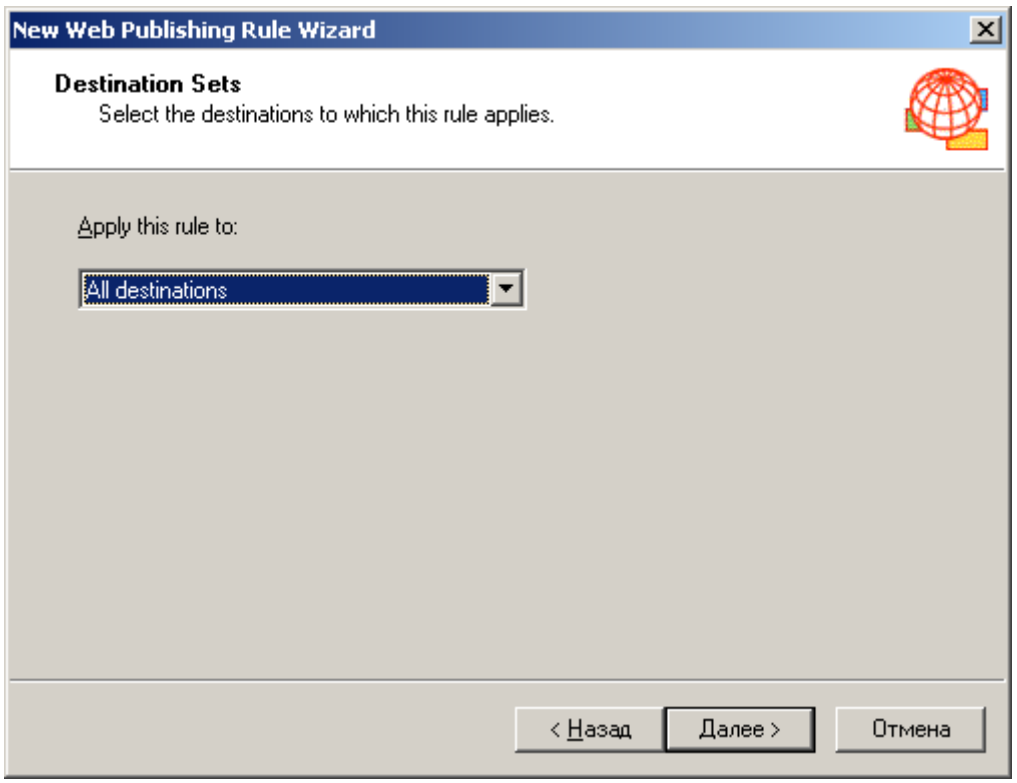
Настройка веб-сервера производится в соответствии с документацией соответствующего веб-сервера.

4. Создать и настроить правила публикации на сервере ISA.

- В окне **ISA Management** установить курсор на **Web Publishing Rules,** находящийся в группе **Publishing**
- Нажать правую кнопку мыши и в появившемся меню выбрать последовательно **New** и **Rule**
- В открывшемся окне, с помощью Мастера создания Правила веб публикации, создать правило.

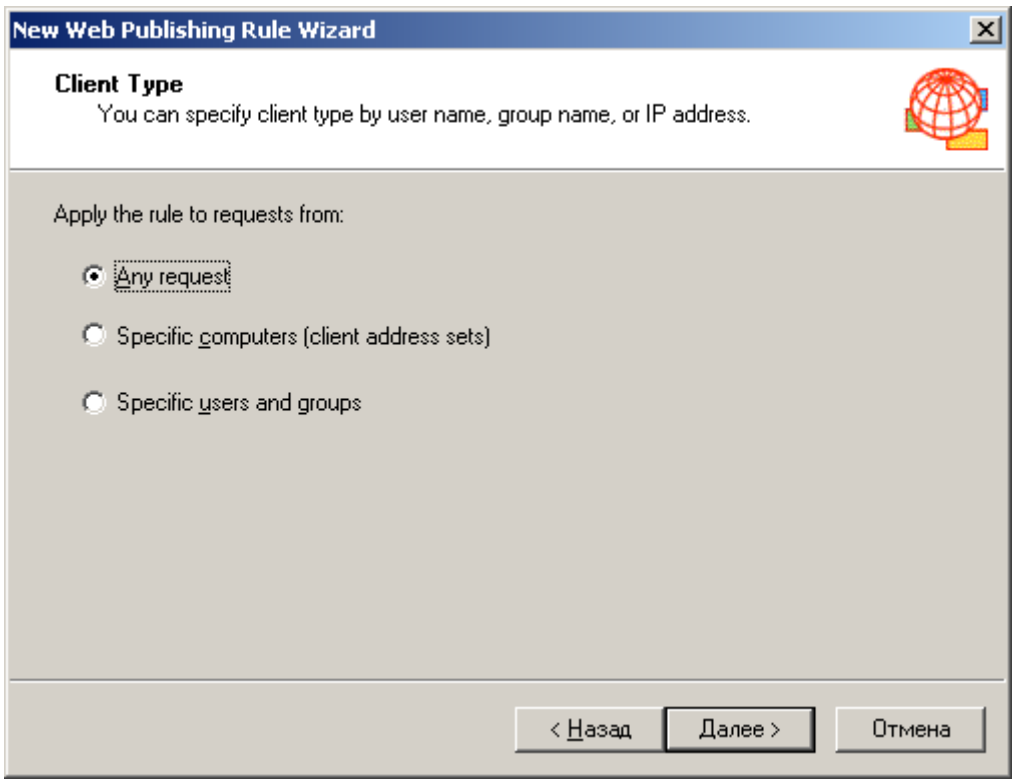
5. Ввести имя публикации (произвольное имя) и нажать «Далее»

6. В окне **Destination Sets** оставить значение, предлагаемое по умолчанию (любые назначения) и нажать «Далее».



Этой установкой определяется, что данное правило публикации (фактически редирект) будет применяться ко всем веб-запросам, прошедшим через Слушателей, вне зависимости от того, какой ресурс из внутренней сети они запросили. В случае публикации нескольких веб-серверов, необходимо создать и применять в правилах публикации назначения.

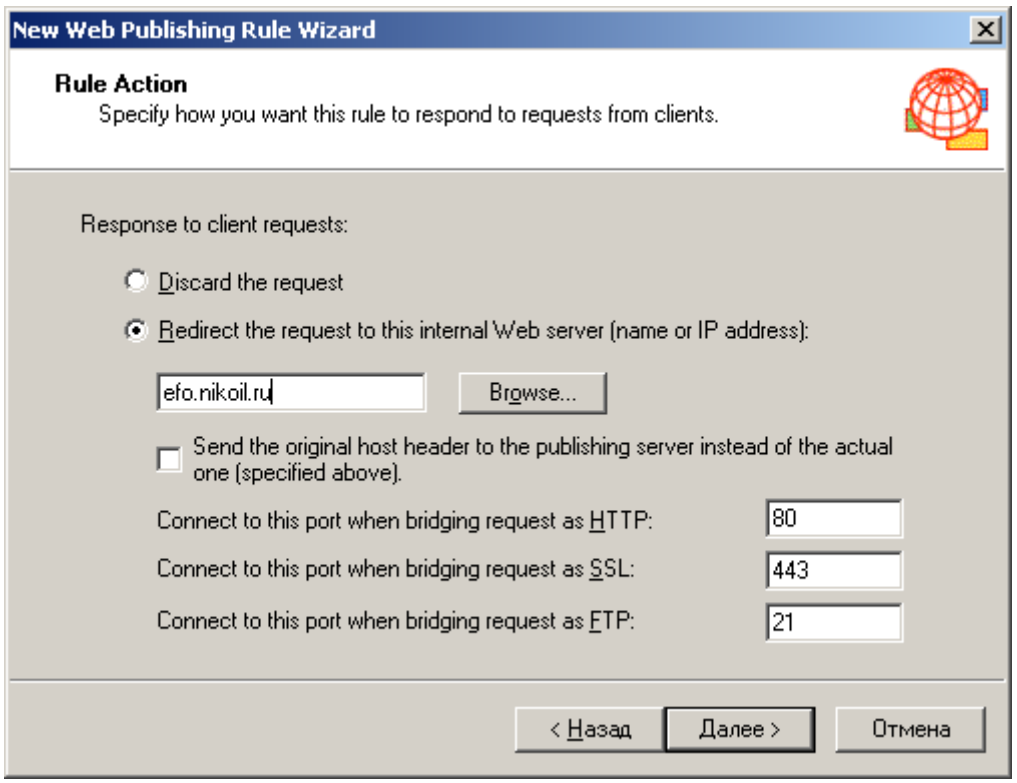
7. В окне Client Type оставить значение, предлагаемое по умолчанию (любые запросы) и нажать «Далее»



В этом окне мы указываем, что правило применяется ко всем веб-запросам, вне зависимости от того клиента, кто сформировал запрос.

8. В окне **Rule Action** выбрать редирект запросов во внутренний веб-сервер (**Redirect the request to this …**)

9. Ввести доменное имя публикуемого веб-сервера и нажать «Далее»



Установив правило редиректа таким образом, все запросы, пришедшие к Слушателю на 80 порт, будут редиректиться на 80 порт веб-сервера. Тоже самое будет происходить с запросами, поступившими на 443 порт (по протоколу TLS).

10. Завершить работу Мастера, нажав «Готово»

В списке правил веб-публикации появиться новая строка, соответствующая созданному нами правилу.