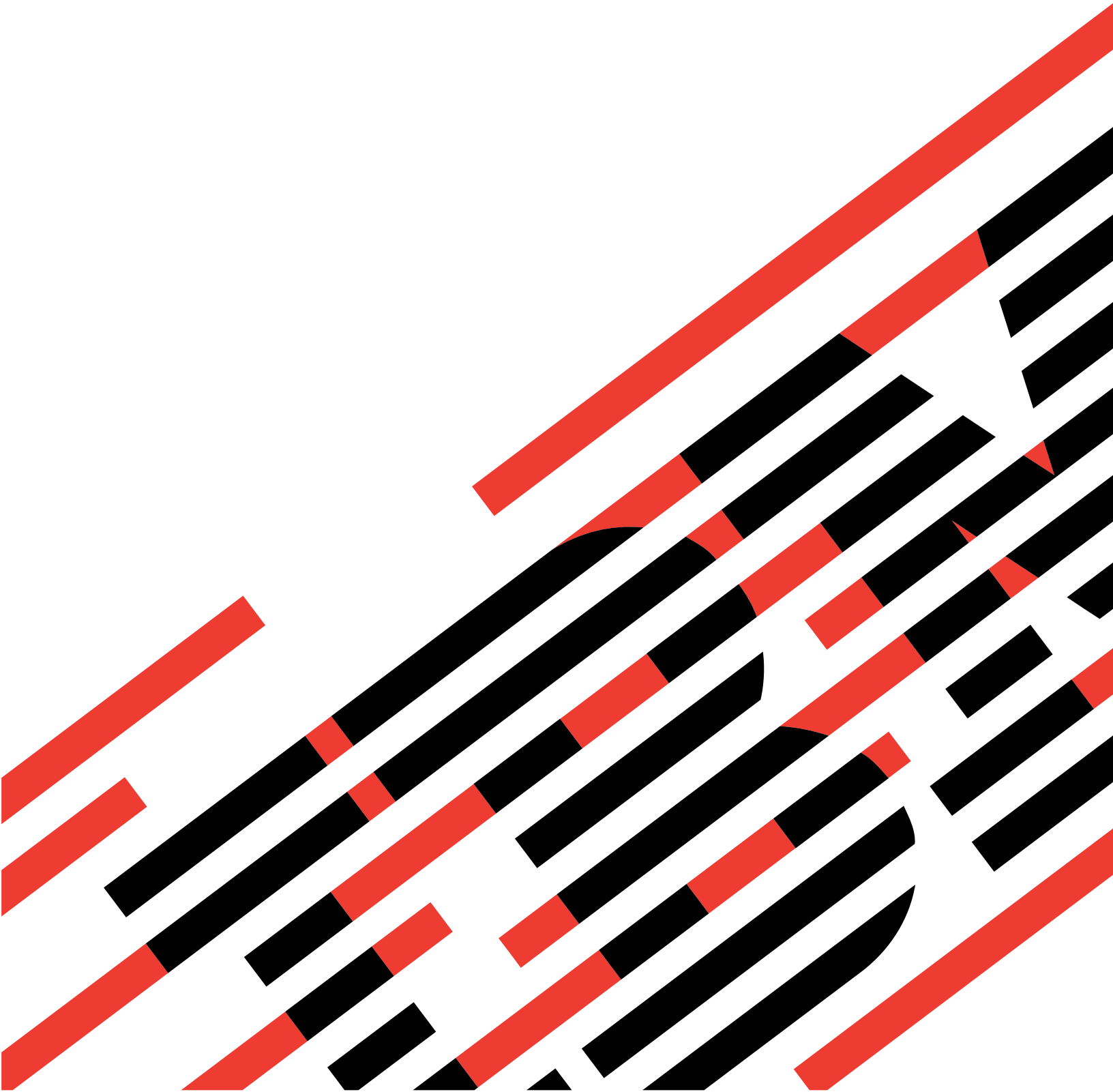
IBM

eserver

iSeries

Secure Sockets Layer (SSL)



IBM

@server

iSeries

Secure Sockets Layer (SSL)

© Copyright International Business Machines Corporation 2000, 2002. Все права защищены.

Содержание

© Copyright IBM Corp. 2000, 2002

Часть 1. Secure Sockets Layer (SSL)

Протокол Secure Sockets Layer (SSL) стал отраслевым стандартом, который применяется приложениями для установления защищенных соединений в незащищенной сети, например, в Internet. Ниже приведены ссылки на страницы с дополнительной информацией об SSL и приложениях сервера iSeries:

- **Новое в выпуске V5R2**
  содержит краткое описание новых функций и источников информации об SSL.
- **Сценарии применения SSL**
  - новый раздел с информацией об SSL, в котором описаны различные примеры применения SSL на сервере iSeries.
- **Принципы работы SSL**
  содержит дополнительную информацию с описанием основных принципов работы протоколов SSL.
- **Планирование настройки SSL**
  содержит список предварительных требований, которые должны быть выполнены на сервере iSeries для применения SSL, а также некоторые полезные советы и рекомендации.
- **Защита приложений с помощью SSL**
  содержит список приложений, для защиты которых на сервере iSeries может применяться SSL.
- **Устранение неполадок SSL**
  - краткая информация об устранении неполадок SSL на сервере iSeries.
- **Связанная информация об SSL**
  содержит ссылки на дополнительные источники информации.

© Copyright IBM Corp. 2000, 2002

Глава 1. Новое в выпуске V5R2

В выпуске V5R2M0 можно установить новый дополнительный компонент 2058 Cryptographic Accelerator for iSeries. Этот аппаратный компонент служит для шифрования данных и позволяет повысить эффективность работы SSL на сервере iSeries. Дополнительная информация об этом компоненте приведена в разделе Аппаратное обеспечение для шифрования.

Новый интерфейс прикладных программ (API) в Global Secure Kit (GSKit)

Создан новый API Global Secure Toolkit (GSKit) OS/400: `gsk_secure_soc_startInit()` . Дополнительная информация приведена в разделе API Global Secure ToolKit (GSKit).

Дополнительная информация о новых возможностях этого выпуска приведена в книге Информация для пользователей 

Информация о новых возможностях и изменениях

Информация о технических изменениях, внесенных в данный выпуск, отмечена следующим образом:

- Начало нового или измененного раздела информации помечается значком » .
- Конец нового или измененного раздела информации помечается значком « .

© Copyright IBM Corp. 2000, 2002

Глава 2. Как напечатать этот раздел

Вы можете просмотреть этот документ или загрузить его версию в формате PDF. Для этого щелкните на ссылке Защита приложений с помощью SSL (объем около 215 Кб, 34 страницы).

Прочая информация

При необходимости вы можете просмотреть или напечатать информацию, связанную с данным разделом.

Сохранение файлов PDF

Для сохранения файла в формате PDF на рабочей станции с целью последующего просмотра или печати выполните следующие действия:

1. Щелкните правой кнопкой мыши на имени файла PDF в окне браузера.
2. Выберите пункт **Сохранить как**.
3. Укажите каталог, в котором вы хотите сохранить документ.
4. Щелкните на **Сохранить**.

Загрузка программы Adobe Acrobat Reader

Для просмотра и печати этого документа можно воспользоваться программой Adobe Acrobat Reader.

Ее можно загрузить с Web-сайта фирмы Adobe (www.adobe.com/products/acrobat/readstep.html)  .

© Copyright IBM Corp. 2000, 2002

Глава 3. Сценарии применения SSL

В перечисленных ниже сценариях описаны различные способы применения SSL на сервере iSeries:

- Сценарий: Защита Централизованного управления с помощью SSL
- Сценарий: Защита FTP с помощью SSL
- Сценарий: Защита Telnet с помощью SSL
- Сценарий: Повышение эффективности работы SSL в iSeries
- Сценарий: Защита личных ключей с помощью аппаратного обеспечения для шифрования

Сценарий применения SSL: Защита Централизованного управления с помощью SSL

Проблема

Недавно была создана глобальная сеть (WAN) фирмы, содержащая несколько удаленных серверов iSeries (конечных систем), для управления которыми применяется центральный сервер iSeries. Этот сервер расположен в главном офисе фирмы. Алексей занимает должность администратора защиты. Для подключения к центральной системе iSeries, расположенной в главном офисе, Алексей применяет функцию Централизованное управление, предусмотренную в клиенте Навигатор iSeries. С помощью SSL Алексей должен обеспечить защиту данных, передаваемых по соединениям между центральной системой и конечными серверами.

Решение

Функция Централизованное управление приложения Навигатор позволяет Алексею управлять несколькими системами с помощью одной центральной системы. Использование SSL в Централизованном управлении дает возможность настроить **защищенные** соединения для управления системами. Для применения SSL Алексей должен настроить защиту приложений iSeries Access для Windows и Навигатор iSeries на том персональном компьютере, на котором запущена функция Централизованное управление.

В среде Централизованного управления предусмотрено два уровня идентификации:

Идентификация сервера
: Обеспечивает идентификацию сертификата сервера конечной системы. Центральная система выступает в соединении с конечной системой в роли клиента SSL. Конечная система выступает в роли сервера SSL и должна предъявить удостоверение личности в виде сертификата, выданного сертификатной компанией, зарегистрированной центральной системой. Для каждой конечной системы необходим сертификат, выданный уполномоченной сертификатной компанией.

Идентификация сервера и клиента
: Обеспечивает идентификацию сертификатов центральной и конечной систем. Считается, что этот уровень идентификации обеспечивает более надежную защиту, чем уровень идентификации сервера. В других приложениях это называется идентификацией клиента, так как клиент должен предоставить надежный базовый сертификат. Когда центральная система

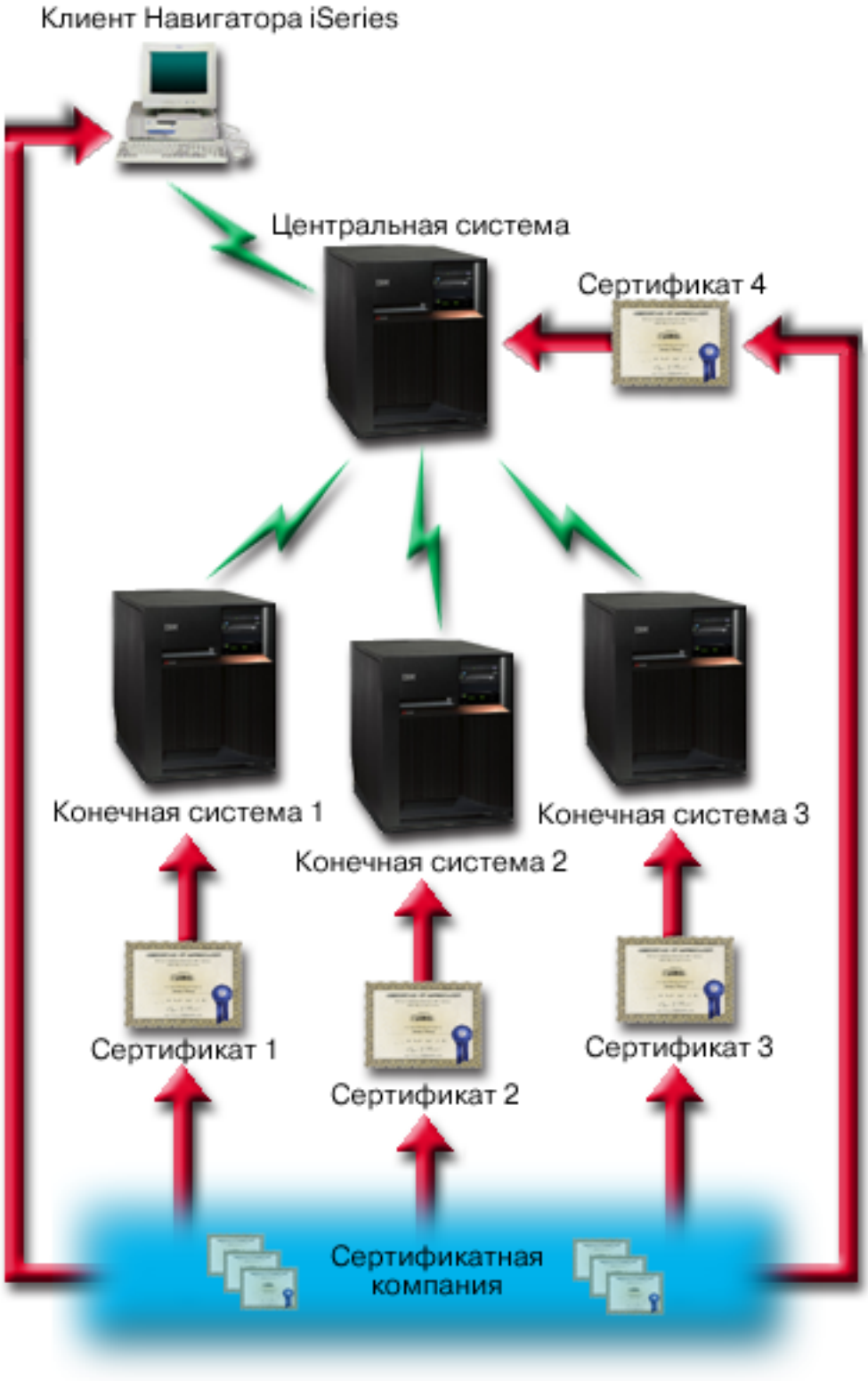
© Copyright IBM Corp. 2000, 2002

(клиент SSL) устанавливает соединение с конечной системой (сервером SSL), обе системы проверяют подлинность сертификатов друг друга.

В отличие от других приложений, Централизованное управление также поддерживает идентификацию с помощью контрольного списка, называемого контрольным списком Уполномоченной группы. Обычно в контрольном списке хранится информация, идентифицирующая пользователя, такая как ИД пользователя и информация идентификации: пароль, личный идентификационный номер или цифровой сертификат. Информация идентификации зашифрована.

В большинстве приложений нет опций для настройки идентификации клиента и сервера. Это связано с тем, что идентификация сервера почти всегда выполняется во время настройки сеанса SSL. В большинстве приложений можно дополнительно настроить идентификацию клиента. В Централизованном управлении вместо идентификации клиента применятся термин ″идентификация клиента и сервера″, так как центральная система выполняет в сети две функции. Когда персональный компьютер устанавливает с центральной системой соединение SSL, последняя играет роль сервера; однако при соединении центральной системы с другой конечной системой центральная система является клиентом. Ниже приведен пример выполнения центральной системой функций клиента и сервера в сети.

Примечание: В этом примере копия сертификата, связанного с сертификатной компанией, должна храниться в базах данных ключей центральной системы и всех конечных систем.



Предварительные требования

Для применения SSL в Централизованном управлении Алексей должен выполнить следующие задачи настройки и администрирования (см. рисунок WAN с централизованным управлением, защищенная с помощью SSL):

1. На сервере iSeries, предназначенном для работы с Централизованным управлением, должны быть выполнены все предварительные требования для применения SSL (дополнительная информация приведена в разделе Предварительные требования SSL).
2. На центральном сервере iSeries и всех конечных серверах должна быть установлена операционная система OS/400 выпуска V5R2. Если на этих серверах применяется выпуск V5R1, необходимо установить следующие исправления (PTF) для OS/400 (5722-SS1):
   a. SI01375
   b. SI01376
   c. SI01377
   d. SI01378
   e. SI01838
3. Клиент Навигатор iSeries относится к выпуску V5R2 программы iSeries Access для Windows. Если клиент относится к выпуску V5R1, установите пакет обслуживания PTF SI01907 (или выше) для iSeries Access для Windows выпуска V5R1 (5722-XE1). Дополнительная информация приведена в разделе ″Защита Централизованного управления″ справочной системы Information Center для выпуска V5R1.
4. Выберите сертификатную компанию (CA) для серверов iSeries.
5. Создайте сертификаты, подписанные CA, для всех серверов iSeries, администрирование которых выполняется с помощью Централизованного управления с поддержкой SSL.
6. Отправьте сертификаты сервера и сертификатной компании на все серверы iSeries и импортируйте их в базу данных ключей.
7. С помощью функции идентификации приложений Централизованного управления назначьте сертификаты конечным серверам, которые применяет Навигатор iSeries:
   a. Запустите Диспетчер цифровых сертификатов IBM на центральном сервере. Если Алексею требуется создать или получить сертификаты, либо выполнить другие действия с сертификатами, он должен сделать это сейчас (информация о настройке сертификатов приведена в разделе Работа с Диспетчером цифровых сертификатов).
   b. Нажмите кнопку **Выбрать хранилище сертификатов**.
   c. Выберите ***SYSTEM** и нажмите кнопку **Далее**.
   d. Введите **пароль хранилища сертификатов** *SYSTEM и нажмите кнопку **Далее**. После обновления меню разверните папку **Управление приложениями**.
   e. Нажмите **Обновить присвоение сертификата**.
   f. Выберите **Сервер** и нажмите кнопку **Далее**.
   g. Выберите **Сервер Централизованного управления** и нажмите **Обновить присвоение сертификата**. В результате серверу Централизованного управления будет назначен сертификат, который будет применяться для идентификации на клиентах iSeries Access для Windows.
   h. Нажмите **Назначить новый сертификат**. DCM снова откроет страницу **Обновить присвоение сертификата** с подтверждающим сообщением.
   i. Нажмите кнопку **Готово**.
   j. Повторите эту процедуру для всех конечных серверов, которые применяются Навигатором iSeries.
8. Настройте Навигатор iSeries:
   a. Установите компонент SSL программы Навигатор iSeries. Для этого выполните процедуру выборочной установки.
   b. Загрузите сертификат CA из системы, в которой он был создан.

Примечание: Если Алексей выбрал сертификат CA, которого нет в базе данных ключей клиента iSeries Access для Windows, ему потребуется добавить этот сертификат в базу данных.

Действия по настройке

Перед применением SSL в Централизованном управлении Алексей должен установить необходимые программы и настроить цифровые сертификаты на сервере iSeries (ознакомьтесь с разделом Предварительные требования из описания данного сценария). После выполнения всех предварительных требований Алексей может активировать SSL для применения в Централизованном управлении, выполнив описанные ниже действия.

Примечание: Если функция SSL включена в Навигаторе iSeries, Алексей должен выключить ее перед активацией SSL в Централизованном управлении. Если функция SSL будет включена в Навигаторе iSeries и не будет включена в Централизованном управлении, то Навигатору iSeries не удастся подключиться к центральной системе.

Для идентификации сервера (обязательно):

1. Настройте центральную систему для идентификации сервера
2. Настройте конечные системы для идентификации сервера

Для идентификации клиента (необязательно):

Примечание: Идентификацию клиента можно настроить лишь в том случае, если настроена идентификация сервера.

1. Настройте центральную систему для идентификации клиента
2. Настройте конечные системы для идентификации клиента

Настройка центральной системы для идентификации сервера

С помощью SSL Алексей может обеспечить защиту данных, передаваемых по соединению между центральной и конечной системами, а также по соединению между Навигатором iSeries и центральной системой. SSL обеспечивает передачу и идентификацию сертификатов и шифрование данных. Соединение SSL может быть установлено только между центральной и конечной системами, поддерживающими SSL. Алексей должен настроить идентификацию сервера перед тем, как он приступит к настройке идентификации клиента.

1. В окне программы Навигатор щелкните правой кнопкой мыши на папке **Централизованное управление** и выберите пункт **Свойства**.
2. Перейдите на страницу **Защита** и выберите пункт **Применять SSL**
3. Выберите уровень идентификации **Сервер**.
4. Нажмите кнопку **OK**, чтобы сохранить это значение в центральной системе.

   Примечание: **Не** перезапускайте сервер Централизованного управления до тех пор, пока идентификация сервера не будет настроена в конечных системах.
5. Настройте конечные системы для идентификации сервера.

Настройка конечных систем для идентификации сервера

Включив функцию SSL в центральной системе для идентификации сервера, Алексей должен включить SSL во всех конечных системах. Для того чтобы настроить поддержку SSL и идентификации сервера, выполните следующие действия:

1. Откройте представление **Централизованное управление**.
2. **Сравните и обновите системные значения в конечных системах:**

a. В списке **Конечные системы** щелкните правой кнопкой мыши на центральной системе и выберите пункт **Реестр—>Собрать**.

b. Для того чтобы собрать реестр системных значений в центральной системе, отметьте опцию **Системные значения** в появившемся окне диалога. Отмените выбор всех остальных опций.

c. Правой кнопкой мыши щелкните на пункте **Группы систем—>Создать группу систем**.

d. Определите новую группу систем, включающую все конечные системы, для работы с которыми будет применяться SSL.

e. Новая группа появится в списке групп систем.

f. После создания реестра щелкните правой кнопкой мыши на группе систем и выберите пункт **Системные значения—>Сравнить и обновить**.

g. Убедитесь, что в поле **Модельная система** указано имя центральной системы.

h. Выберите категорию **Централизованное управление** и убедитесь, что заданы следующие значения (отметьте переключатель рядом с ними):

- Параметру Применять SSL присвоено значение **Да**.
- Уровень идентификации SSL равен **Сервер**.

Эти значения устанавливаются в центральной системе при выполнении процедуры Настройка центральной системы для идентификации сервера.

i. Нажмите кнопку **OK**. Указанные значения будут установлены во всех конечных системах из новой группы систем.

j. Подождите, пока завершится **сравнение и обновление**. Пока не перезапускайте сервер Централизованного управления. Операция сравнения и обновления может занять несколько минут.

3. **Перезапустите сервер Централизованного управления в центральной системе:**

a. В окне программы Навигатор iSeries разверните список **Мои соединения**.

b. Разверните значок центральной системы.

c. Разверните **Сеть—> Серверы** и выберите **TCP/IP**.

d. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите опцию **Остановить**. Список под именем центральной системы будет свернут. Появится сообщение о том, что соединение с сервером прервано.

e. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

4. **Перезапустите сервер Централизованного управления во всех конечных системах:**

a. Разверните значок конечной системы, в которой нужно перезапустить сервер.

b. Разверните **Сеть—> Серверы** и выберите **TCP/IP**.

c. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите опцию **Остановить**.

d. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

e. Выполните эту процедуру во всех конечных системах.

5. **Активируйте SSL в Навигаторе iSeries:**

a. В окне программы Навигатор iSeries разверните список **Мои соединения**.

b. Щелкните правой кнопкой мыши на значке центральной системы и выберите пункт **Свойства**.

c. Перейдите на страницу **SSL** и выберите опцию **Применять SSL для соединения**.

d. Перезапустите программу Навигатор iSeries.

При необходимости после настройки идентификации сервера Алексей может выполнить следующие процедуры настройки идентификации клиента:

- Настройка центральной системы для идентификации клиента

- Настройка конечных систем для идентификации клиента

При идентификации клиента выполняется проверка Сертификатной компании и уполномоченной группы как центральной, так и конечных систем.

Настройка центральной системы для идентификации клиента

Когда центральная система (клиент SSL) устанавливает соединение с конечной системой (сервером SSL), обе системы проверяют подлинность сертификатов друг друга с помощью идентификации клиента (в Централизованном управлении - идентификация сертификатной компании и уполномоченной группы).

1. В окне программы Навигатор iSeries щелкните правой кнопкой мыши на папке **Централизованное управление** и выберите пункт **Свойства**.
2. Перейдите на страницу **Защита** и выберите опцию **Применять SSL**.
3. Выберите уровень идентификации **Клиент и сервер**.
4. Нажмите кнопку **OK**, чтобы сохранить это значение в центральной системе.

   Примечание: **Не** перезапускайте сервер Централизованного управления до тех пор, пока идентификация клиента и сервера с применением SSL не будет настроена в конечных системах.
5. Настройте конечные системы для идентификации клиента.

Настройка конечных систем для идентификации клиента

1. **Сравните и обновите системные значения в конечных системах:**

   Примечание: Эту задачу нельзя выполнить на серверах iSeries, в которых установлен выпуск V4R5. За дополнительной информацией обратитесь к руководству ″Management Central: A Smart Way to Manage AS/400 Systems

   ″ для выпуска V4R4.

   a. В списке **Конечные системы** щелкните правой кнопкой мыши на центральной системе и выберите пункт **Реестр—>Собрать**.
   b. Для того чтобы собрать реестр системных значений в центральной системе, отметьте опцию **Системные значения** в появившемся окне диалога. Отмените выбор всех остальных опций.
   c. Правой кнопкой мыши щелкните на пункте **Группы систем—>Создать группу систем**.
   d. Определите группу систем, включающую все конечные системы, с которыми планируется устанавливать соединения SSL.
   e. Новая группа появится в списке групп систем.
   f. После создания реестра щелкните правой кнопкой мыши на группе систем и выберите пункт **Системные значения—>Сравнить и обновить**.
   g. Убедитесь, что в поле **Модельная система** указано имя центральной системы.
   h. Выберите категорию **Централизованное управление** и убедитесь, что заданы следующие значения:
      - Параметру Применять SSL присвоено значение **Да**.
      - Параметру Уровень идентификации SSL присвоено значение **Клиент и сервер**.

      Эти значения устанавливаются в центральной системе при выполнении процедуры Настройка центральной системы для идентификации клиента. Отметьте переключатель **Обновить** напротив указанных значений.
   i. Нажмите кнопку **OK**. Указанные значения будут установлены во всех конечных системах из новой группы систем.

2. **Скопируйте контрольный список в конечные системы:**
   a. В окне программы Навигатор iSeries разверните **Централизованное управление—>Определения**.
   b. Щелкните правой кнопкой мыши на **Пакет** и выберите **Создать определение**.
   c. В окне **Создать определение** задайте следующие значения:
      - **Имя:** Введите имя определения.
      - **Исходная система:** Введите имя центральной системы.
      - **Выбранные файлы и папки:** Щелкните мышью в поле и введите `/QSYS.LIB/QUSRSYS.LIB/QYPSVLDL.VLDL`.
   d. Перейдите на страницу **Опции** и выберите пункт **Заменить существующий файл на отправленный файл**.
   e. Нажмите кнопку **Дополнительно**.
   f. В окне **Дополнительные опции** разрешите наличие различий в объектах при выполнении операции восстановления. Для этого задайте значение **Да**.
   g. Нажмите кнопку **OK**. Будет обновлен список определений и показан новый пакет.
   h. Щелкните на новом пакете правой кнопкой мыши и выберите опцию **Отправить**.
   i. В окне диалога **Отправить** добавьте уполномоченную группу и удалите все остальные группы. Затем нажмите кнопку **OK**. Уполномоченная группа - это группа систем, которая была определена на шаге 1.

      Примечание: Задача **Отправить** не будет выполнена в центральной системе, так как она является исходной системой. Во всех конечных системах задача **Отправить** должна быть успешно выполнена.

3. **Перезапустите сервер Централизованного управления в центральной системе:**
   a. В окне программы Навигатор iSeries разверните список **Мои соединения**.
   b. Разверните значок центральной системы.
   c. Разверните **Сеть—> Серверы** и выберите **TCP/IP**.
   d. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите опцию **Остановить**. Список под именем центральной системы будет свернут. Появится сообщение о том, что соединение с сервером прервано.
   e. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.
4. **Перезапустите сервер Централизованного управления во всех конечных системах:**

   Примечание: Выполните эту процедуру во всех конечных системах.
   a. Разверните значок конечной системы, в которой нужно перезапустить сервер.
   b. Разверните **Сеть—> Серверы** и выберите **TCP/IP**.
   c. Щелкните правой кнопкой мыши на пункте **Централизованное управление** и выберите опцию **Остановить**.
   d. После завершения работы сервера Централизованного управления нажмите **Запустить**, чтобы снова запустить этот сервер.

Глава 4. Принципы работы SSL

Протокол SSL позволяет устанавливать защищенные соединения между приложениями клиента и сервера, которые обеспечивают идентификацию одной или обеих конечных систем. SSL гарантирует секретность и целостность данных, которыми обмениваются клиент с сервером.

В перечисленных ниже разделах приведена информация, которая поможет вам лучше понять схему работы SSL на сервере iSeries:

- История появления SSL
- Принципы работы SSL
- Поддержка протоколов SSL и Transport Layer Security (TLS)
- Идентификация сервера
- Идентификация клиента

История появления SSL

Протокол Secure Sockets Layer (SSL) был разработан фирмой Netscape в 1994 году для защиты данных, передаваемых по сети Internet. Хотя первоначально SSL предназначался для защиты соединений между Web-браузером и Web-сервером, спецификация SSL позволяет применять этот протокол и другим приложениям, в том числе TELNET и FTP. Дополнительная информация об SSL и других связанных с ним протоколах приведена в разделе Поддержка протоколов SSL и Transport Layer Security (TLS).

Принципы работы SSL

SSL представляет собой, фактически, два протокола. Это протокол согласования и протокол передачи данных. Протокол передачи данных управляет потоком данных между двумя конечными системами соединения SSL.

Протокол согласования служит для идентификации одной или обеих конечных систем соединения SSL и создания уникального симметричного ключа, с помощью которого генерируются ключи для шифрования и расшифровки данных, передаваемых по этому соединению. Для идентификации конечных систем в протоколе SSL применяется асимметричное шифрование, цифровые сертификаты и процедуры согласования SSL. Обычно выполняется идентификация сервера, а иногда и идентификация клиента. Цифровой сертификат , выданный сертификатной компанией, может быть связан с каждой из конечной систем или с приложениями, применяющими протокол SSL в конечных системах.

Цифровой сертификат состоит из общего ключа и некоторой информации идентификации с цифровой подписью уполномоченной сертификатной компании (CA). С каждым общим ключом связан частный ключ. Частный ключ не входит в состав сертификата и хранится отдельно от него. При идентификации клиента или сервера конечная система должна предоставить доказательство наличия частного ключа, соответствующего общему ключу цифрового сертификата.

Применение общих и частных ключей в операциях шифрования обуславливает высокие требования согласований SSL к производительности системы. После установления первого соединения SSL между двумя конечными системами информация об этом соединении и приложениях может быть занесена в кэш в защищенной памяти для ускорения последующих согласований SSL. При возобновлении соединения SSL конечные системы проверяют наличие доступа к уникальной информации путем выполнения сокращенной процедуры согласования без применения общего и частного ключей. Если обе системы предоставят доказательства наличия доступа к этой информации,

© Copyright IBM Corp. 2000, 2002

будут созданы новые симметричные ключи и соединение SSL возобновится. Кэшированная информация для соединений TLS версии 1.0 и SSL версии 3.0 будет удалена из защищенной памяти по истечении 24 часов. В выпуске V5R2M0 влияние процедуры согласования SSL на центральный процессор можно минимизировать, установив аппаратное обеспечение для шифрования.

Поддержка протоколов SSL и Transport Layer Security (TLS)

Существует несколько версий протокола SSL. Последней из них является протокол Transport Layer Security (TLS). Он основан на протоколе SSL версии 3.0 и был разработан Рабочей группой Internet (IETF). Реализация OS/400 поддерживает следующие версии протоколов SSL и TLS:

- TLS версии 1.0
- TLS версии 1.0, с поддержкой SSL версии 3.0

  Примечания:

  1. TLS версии 1.0 с поддержкой SSL версии 3.0 означает, что будет выполняться согласование TLS, а если это невозможно, то согласование SSL версии 3.0. Если согласование SSL версии 3.0 выполнить нельзя, то процедура согласования SSL не будет выполнена.
  2. Кроме того поддерживается TLS версии 1.0 с SSL версии 3.0 и 2.0. Этой функции соответствует значение протокола **ALL**, при котором будет выполняться процедура согласования TLS, а если это невозможно, то процедура согласования SSL версии 3.0. Если применить процедуру согласования SSL версии 3.0 невозможно, то выполняется согласование SSL версии 2.0. Если согласование SSL версии 2.0 выполнить нельзя, то процедура согласования SSL не будет выполнена.
- SSL версии 3.0
- SSL версии 2.0
- SSL версии 3.0 с поддержкой SSL версии 2.0

Сравнение SSL версии 3.0 с SSL версии 2.0

Протоколы SSL версии 3.0 и SSL версии 2.0 имеют мало общего. Наиболее важные отличия этих двух протоколов перечислены ниже:

- Потоки процедуры согласования SSL версии 3.0 отличаются от соответствующих потоков согласования SSL версии 2.0.
- SSL версии 3.0 применяет реализацию BSAFE 3.0 компании RSA Data Security, Inc. BSAFE 3.0 содержит исправления, защищающие от атак с нарушением синхронизации, и алгоритм хеширования SHA-1. Алгоритм хэширования SHA-1 считается более надежным, чем алгоритм MD5. Применение SHA-1 позволяет SSL версии 3.0 поддерживать дополнительные сеансы шифрования с SHA-1 вместо MD5.
- Протокол SSL версии 3.0 защищает от атак типа man-in-the-middle (MITM) в процессе согласования SSL. В SSL версии 2.0 существовала небольшая вероятность успешного ослабления шифра с помощью атаки MITM. Ослабление шифра может позволить постороннему пользователю взломать ключ сеанса SSL.

Сравнение TLS версии 1.0 и SSL версии 3.0

Основанный на SSL версии 3.0 протокол Transport Layer Security (TLS) версии 1.0 является последними отраслевым стандартом SSL. Его спецификация определена Рабочей группой Internet (IETF) в документе RFC 2246, ″The TLS Protocol.″ 

Цель создания TLS - повышение защиты SSL и более точное и полное определение протокола. TLS обладает следующими преимуществами по сравнению с SSL версии 3.0:

- Более надежный алгоритм MAC
- Более детальные предупреждения

- Более четкие определения спецификаций ″серой области″

Все приложения iSeries, поддерживающие SSL, автоматически поддерживают TSL, если явно не указано, что приложение должно применять SSL версии 3.0 или 2.0.

TLS предоставляет следующие усовершенствованные способы защиты:

- **Хеширование при идентификации сообщений**
  TLS применяет в коде идентификации сообщения (HMAC) хеширование, предотвращающее от изменения записи при передаче по незащищенной сети, например в Internet. SSL версии 3.0 также поддерживает идентификацию сообщений с помощью ключей, но HMAC считается более надежным, чем функция MAC, применяемая в SSL версии 3.0.
- **Улучшенная псевдослучайная функция (PRF)**
  С помощью PRF создаются данные ключа. В TLS функция PRF определена с помощью HMAC. PRF применяет два алгоритма хеширования, обеспечивающих ее защиту. Если один из алгоритмов будет взломан, данные будут защищены вторым алгоритмом.
- **Улучшенная проверка с сообщением о завершении**
  Протоколы TLS версии 1.0 и SSL версии 3.0 отправляют обеим конечным системам сообщение ″Готово″, означающее, что доставленное сообщение не было изменено. Однако в TLS эта проверка основана на значениях PRF и HMAC, что обеспечивает более высокий уровень защиты по сравнению с SSL версии 3.0.
- **Совместимость обработки сертификатов**
  В отличие от SSL версии 3.0, TLS пытается указать тип сертификата, который может применяться различными реализациями TLS.
- **Конкретные сообщения с предупреждениями**
  TLS предоставляет более точные и полные предупреждения о неполадках, обнаруженных одной из конечных систем. TLS также содержит информацию о том, когда какие сообщения с предупреждениями следует отправлять.

Идентификация сервера

При идентификации сервера клиент проверяет подлинность сертификата сервера и наличие в нем подписи сертификатной компании, уполномоченной клиентом. С помощью асимметричного шифрования и протокола согласования SSL генерирует симметричный ключ, который будет применяться только для данного соединения. С помощью этого ключа создается набор ключей для шифрования и расшифровки данных, передаваемых через соединение SSL. По окончании процедуры согласования SSL будет идентифицирована одна или обе конечные системы соединения, и будет создан уникальный ключ для шифрования и расшифровки данных. После согласования данные уровня приложения будут передаваться через соединение SSL в зашифрованном виде.

Идентификация клиента

Многие приложения поддерживают опцию идентификации клиента. При идентификации клиента сервер проверяет подлинность сертификата клиента и наличие в нем подписи сертификатной компании, уполномоченной сервером. Идентификацию клиента поддерживают следующие приложения iSeries:

- IBM HTTP Server (стандартный)
- IBM HTTP Server (на основе Apache)
- Сервер FTP
- Сервер Telnet
- Конечная система Централизованного управления
- Службы каталогов (LDAP)

Глава 5. Планирование настройки SSL

При планировании применения SSL на сервере iSeries обратите внимание на следующее:

- Предварительные требования SSL
- Требуемый тип цифровых сертификатов и планируемый источник сертификатов

Предварительные требования SSL:

- Диспетчер цифровых сертификатов IBM (DCM), компонент 34 операционной системы OS/400 (5722-SS1)
- TCP/IP Connectivity Utilities for iSeries (5722-TC1)
- IBM HTTP Server for iSeries (5722-DG1)
- Если при работе с DCM вы планируете применять сервер HTTP, необходимо установить продукт IBM Developer Kit for Java (5722–JV1). В противном случае вам не удастся запустить сервер администрирования HTTP.
- Продукт IBM Cryptographic Access Provider, 5722-AC3 (128-разрядный). Разрядность характеризует максимальный размер секретных данных в симметричных ключах, применяемых для шифрования. Максимальный размер симметричного ключа определяется законами о импорте и экспорте конкретной страны. Чем больше разрядность ключа, тем надежнее защищено соединение.
- Вы также можете установить аппаратное обеспечение для шифрования, которое позволяет ускорить процесс согласования SSL. В выпуске V5R2M0 на сервере iSeries можно установить следующие компоненты аппаратного обеспечения для шифрования:
  - Шифровальный ускоритель 2058 (код аппаратного компонента - 4805)
  - Шифровальный сопроцессор 4758 (код аппаратного компонента - 4801 или 4802)

  Если вы решите установить аппаратный компонент для шифрования, вам потребуется установить компонент 35, Cryptographic Service Provider.

Для применения SSL в компонентах iSeries Access для Windows и IBM Toolbox for Java необходимо установить продукт iSeries Client Encryption, 5722-CE3 (128-разрядный). Этот продукт применяется приложением iSeries Access для Windows для установления защищенных соединений.

Примечание: Продукт Client Encryption не требуется для работы эмулятора PC5250, поставляемого с продуктом Personal Communications. Программы Personal Communications содержат собственный код шифрования.

Цифровые сертификаты

В разделе Применение глобальных сертификатов и выдача локальных сертификатов описаны различия между глобальными и локальными сертификатами и даны рекомендации, в каких случаях лучше применять те или иные сертификаты.

Для управления цифровыми сертификатами на сервере iSeries применяется Диспетчер цифровых сертификатов (DCM) фирмы IBM. Дополнительная информация о DCM приведена в разделе Работа с Диспетчером цифровых сертификатов справочной системы Information Center.

© Copyright IBM Corp. 2000, 2002

Глава 6. Защита приложений с помощью SSL

SSL может применяться для защиты следующих приложений сервера iSeries:

- IBM HTTP Server for iSeries (стандартный)
- IBM HTTP Server for iSeries (на основе Apache)
- Сервер FTP
- Сервер Telnet
- Сервер архитектуры распределенных реляционных баз данных (DRDA) и управления распределенными данными (DDM)
- Централизованное управление
- Сервер Служб каталогов (LDAP)
- Enterprise Identity Mapping (EIM)
- Приложения iSeries Access для Windows, в том числе Навигатор iSeries
- Приложения, написанные с использованием интерфейсов прикладных программ (API) iSeries Access для Windows
- Программы, созданные с помощью Developer Kit for Java, и приложения клиента, использующие IBM Toolbox for Java
- Приложения, созданные с применением API защищенных сокетов, поддерживаемых на сервере iSeries. Поддерживаются API из Global Secure Toolkit (GSKit) и встроенные API SSL_ системы iSeries. Информация о GSKit и SSL_API приведена в разделе API защищенных сокетов.

© Copyright IBM Corp. 2000, 2002

Глава 7. Устранение неполадок SSL

В этом разделе приведены общие рекомендации по устранению неполадок, которые могут возникнуть на сервере iSeries при работе с SSL. Данный раздел не является полным руководством по устранению неполадок.

Убедитесь, что выполнены следующие условия:

- На сервере iSeries выполнены предварительные требования SSL (дополнительная информация приведена в разделе Предварительные требования SSL).
- Если вы планируете применять функцию Централизованное управление программы Навигатор iSeries в системе выпуска V5R1, убедитесь, что в этой системе установлены следующие PTF:
  - si01375
  - si01376
  - si01377
  - si01378
  - si01838
- Убедитесь, что срок действия сертификатной компании и сертификатов не истек, и сертификатная компания является уполномоченной CA.

Если несмотря на соблюдение всех перечисленных выше условий на сервере iSeries возникла неполадка SSL, попробуйте выполнить следующие действия:

- Найдите код ошибки SSL в протоколе задания сервера, а затем найдите дополнительную информацию об ошибке в таблице ошибок по ее коду. Информация о сообщениях с кодами ошибок SSL приведена на странице Сообщения с кодами ошибок API SSL. Например, если в протоколе задания сервера указан код ошибки -93, то по таблице можно определить, что он соответствует константе SSL_ERROR_SSL_NOT_AVAILABLE.
  - Отрицательный код возврата (есть дефис перед значением кода) означает, что применялся SSL_ API.
  - Положительный код возврата означает, что применялся API GSKit. Для получения краткого описания кода возврата, свидетельствующего об ошибке, в программах могут применяться API gsk_strerror() и SSL_Strerror(). С помощью этих API приложение может занести в протокол задания сообщение с описанием ошибки.

  Для получения более подробной информации просмотрите сообщение с идентификатором, указанным в таблице, на сервере iSeries. В этом сообщении описана возможная причина ошибки и перечислены действия по ее исправлению. Дополнительную информацию с описанием кодов ошибок можно найти в документации по тому API защищенных сокетов, который вернул код ошибки.
- Имена констант, соответствующие системным кодам возврата SSL, перечислены и в указанных ниже файлах заголовков (без ссылки на ИД сообщения):
  - QSYSINC/H.GSKSSL
  - QSYSINC/H.SSL

  Хотя все имена констант, перечисленные в этих файлах, уникальны, один код возврата может соответствовать разным ошибкам.

Дополнительная информация об устранении неполадок на сервере iSeries приведена на странице Устранение неполадок и обслуживание. 

© Copyright IBM Corp. 2000, 2002

Глава 8. Связанная информация

Ниже перечислены источники дополнительной информации об SSL:

Источники IBM

- На странице SSL и Java Secure Socket Extension (JSSE) приведено краткое описание JSSE и информация о его применении.
- На странице Java Secure Socket Layer (JSSL) приведено краткое описание функции JSSL и информация о ее использовании.
- На странице IBM Toolbox for Java приведено краткое описание классов Java и рекомендации по их использованию.

Документы RFC

- RFC 2246: ″The TLS Protocol Version 1.0 ″ содержит подробное описание протокола TSL.
- RFC2818: ″HTTP Over TLS″ содержит информацию о защите соединений HTTP в Internet с помощью TSL.

Другие источники

- Документ The SSL Protocol Version 3.0 содержит подробное описание протокола SSL версии 3.0.

© Copyright IBM Corp. 2000, 2002

Напечатано в Дании