IBM Systems - iSeries

Защита iSeries при работе с Internet

Версия 5, выпуск 4

IBM Systems - iSeries

Защита iSeries при работе с Internet

Версия 5, выпуск 4

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Замечания”, на стр. 37.

Седьмое издание (февраль 2006)

Это издание относится к версии 5, выпуску 4, модификации 0 IBM i5/OS (код продукта 5722-SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

Содержание

Защита системы iSeries при работе с Internet

Организация доступа к Internet из локальной сети требует серьезной модернизации вашей сети и коренного пересмотра требований к ее защите.

К счастью, в системе IBM @server iSeries предусмотрены аппаратные и программные средства защиты от попыток несанкционированного доступа к системе из Internet. Правильное применение этих средств защиты iSeries позволяет предоставлять заказчикам, сотрудникам и партнерам всю необходимую информацию в защищенной среде.

В этом разделе приведена информация о стандартных способах нарушения защиты и об их возможном влиянии на ваши планы по работе с Internet и средствами электронного бизнеса. Кроме того, вы научитесь правильно оценивать опасности, связанные с Internet, и узнаете о различных функциях iSeries, предназначенных для защиты от них. На основе этой информации вы сможете разработать собственный план организации защиты сети в соответствии с конкретными требованиями.

PDF - версия для печати

Позволяет просмотреть и распечатать документацию в формате PDF.

Для просмотра или загрузки этого документа в формате PDF выберите ссылку Защита iSeries при работе с Internet (416 Кб, 60 страниц).

Вы можете просмотреть и загрузить следующие связанные разделы:

- Обнаружение вторжений (около 160 Кб). Приведенная в документе информация поможет создать стратегию обнаружения вторжений, позволяющую получать информацию о подозрительных событиях в сети TCP/IP, например, о некорректных IP-пакетах. Также вы сможете создать приложение, проверяющее эти данные и отсылающее отчеты администратору защиты в том случае, если предположительно осуществляется атака извне.
- Технология преобразования идентификаторов в рамках предприятия (EIM) (около 700 Кб). EIM - механизм, позволяющий связывать пользователя или систему (например, службу) и пользовательские профайлы в локальной среде.
- Одиночный вход в систему (около 600 Кб). При использовании модели одиночного входа в систему пользователю необходимо реже выполнять вход в систему и помнить меньше паролей, чем при стандартных обращениях к нескольким приложениям или серверам.
- Планирование и настройка защиты системы (около 3500 Кб).

Сохранение PDF-файлов

Для того чтобы сохранить файл в формате PDF на своем персональном компьютере, выполните следующие действия:

1. В окне браузера щелкните правой кнопкой мыши на имени документа PDF (на приведенной выше ссылке).
2. Выберите опцию сохранения файла PDF на локальном диске.
3. Перейдите в каталог, в котором требуется сохранить документ PDF.
4. Нажмите кнопку **Сохранить**.

Загрузка Adobe Reader

Для просмотра и печати этих PDF-файлов требуется программа Adobe Reader. Ее можно бесплатно загрузить с Web-сайта Adobe (www.adobe.com/products/acrobat/readstep.html) .

Понятия, связанные с данным

Обнаружение вторжений

Технология преобразования идентификаторов в рамках предприятия (EIM)

Одиночный вход в систему

Планирование и настройка защиты системы

Способы защиты iSeries при работе с Internet

Приводится краткий обзор возможностей системы защиты iSeries и предлагаемых средств защиты.

Ответ на вопрос ″Что мне необходимо знать о защите в Internet?″ зависит от того, как вы хотите использовать Internet. При работе с Internet защита данных является одной из наиболее важных проблем. Необходимые меры защиты зависят от того, как вы намерены использовать Internet. Во-первых, вы можете предоставить пользователям внутренней сети доступ к Web-ресурсам и электронной почте Internet. Далее, вам может потребоваться передавать конфиденциальную информацию с одного узла на другой. Наконец, вы можете использовать Internet для электронной коммерции или для создания совмещенной сети вашей организации, ее деловых партнеров и поставщиков.

Перед тем как вы начнете работу с Internet, вам необходимо решить, что именно вы хотите делать и каким образом. Принятие решений об использовании Internet и о защите передаваемой по Internet информации может быть достаточно сложным делом. Перед началом разработки собственного плана работы с Internet рекомендуем вам ознакомиться с разделом *Пример организации электронной коммерции в компании JKL Toys*, приведенным в IBM Systems Software Information Center. (Примечание: если вы не знакомы с базовыми понятиями защиты при работе с Internet, рекомендуем вам сначала обратиться к разделу *Терминология, применяемая в средствах защиты* документации IBM Systems Software Information Center.)

Когда вы получите твердое представление о том, каким образом в вашей организации будет использоваться Internet, и какие функции и средства защиты должны быть задействованы для организации эффективной защиты от потенциальных опасностей, начните разработку стратегии защиты. Параметры стратегии защиты и ее реализация зависят от многих факторов. При подключении сети к Internet краеугольным камнем всех планов использования Internet должна быть стратегия защиты.

Параметры защиты системы iSeries

Помимо специализированных средств защиты, ориентированных на работу с Internet, в системе iSeries предусмотрена очень надежная и высокоэффективная общая схема защиты. Ниже описаны некоторые ее характеристики:

- Внутренние средства защиты гораздо более устойчивы к попыткам взлома, чем используемые в других системах внешние программные средства.
- Объектно-ориентированная архитектура, максимально затрудняющая создание и распространение вирусов. В системе iSeries файлы не могут быть приняты за программы, а программы не могут изменять друг друга. Средства обеспечения целостности системы позволяют обращаться к объектам только через интерфейсы системы. К объектам системы нельзя обращаться напрямую по их адресам в системе. Создать указатель по известному адресу объекта невозможно. Напомним, что манипулирование указателями - это широко распространенный среди взломщиков способ доступа к данным в системах с другими архитектурами.
- Гибкость системы позволяет настроить систему защиты в точном соответствии с потребностями вашей организации. Для этого можно использовать @server средство планирования защиты Эта программа поможет вам определить, какие рекомендации по организации защиты отвечают вашим потребностям.

Дополнительные средства защиты системы iSeries

В системе iSeries предусмотрен ряд дополнительных специализированных средств защиты, позволяющих повысить уровень безопасности системы при работе с Internet. В зависимости от характера вашей работы с Internet, вы можете использовать:

- Виртуальные частные сети (VPN), позволяющие организовать защищенный обмен данными через открытую сеть (например, Internet). С помощью VPN можно создавать защищенные каналы передачи данных (туннели) в открытых сетях. Средство для создания VPN входит в набор приложений i5/OS и поддерживается интерфейсом Навигатора iSeries. Дополнительная информация о сетях VPN приведена в разделе ″Виртуальные частные сети (VPN)″ справочной системы IBM Systems Software Information Center.
- Правила обработки пакетов - это встроенная функция системы i5/OS, с которой можно работать с помощью интерфейса Навигатора iSeries. Данная функция позволяет настраивать правила фильтрации IP-пакетов и преобразования сетевых адресов (NAT), с помощью которых можно управлять потоком входящих и исходящих данных TCP/IP сервера iSeries. Дополнительная информация о правилах обработки пакетов приведена в разделе ″Правила обработки пакетов″ справочной системы IBM Systems Software Information Center.
- Поддержка протокола Secure Sockets Layer (SSL) позволяет применять протокол SSL для защиты данных, передаваемых по сети между различными приложениями и их клиентами. Протокол SSL был разработан для защиты потоков данных между web-серверами и браузерами, однако сейчас он используется и другими приложениями. Текущие версии многих серверных приложений iSeries поддерживают SSL; к их числу относятся IBM HTTP Server for iSeries, iSeries Access Express, сервер FTP, Telnet и многие другие. Дополнительная информация об SSL приведена в разделе ″Защита приложений с помощью протокола SSL″ справочной системы IBM Systems Software Information Center.

Когда вы получите твердое представление о том, каким образом будет использоваться Internet и какие функции и средства защиты должны быть задействованы для организации эффективной защиты от потенциальных опасностей, вы будете способны начать разработку стратегии защиты. Параметры стратегии защиты и ее реализация зависят от многих факторов. При подключении сети к Internet краеугольным камнем всех планов использования Internet должна быть стратегия защиты.

Примечание: Подробную информацию о том, как использовать Internet в деловых целях, можно найти в следующих источниках:

- Раздел *Подключение к Internet* документации IBM Systems Software Information Center.
- Руководство *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929).

Понятия, связанные с данным

“Стратегия защиты и ее задачи” на стр. 6
Информация, приведенная в документе, поможет определить требования пользователей и опасности, исходящие от них.

Планирование защиты при работе с Internet

В этом разделе приведена информация о создании стратегии защиты, соответствующей вашим потребностям.

Определив принципы работы с Internet, необходимо тщательно продумать стратегию защиты данных. Вы должны собрать подробную информацию о предстоящей работе с Internet, а также записать и проанализировать конфигурацию внутренней сети. На основе этого вы сможете правильно определить необходимые меры по защите системы.

Например, вы должны записать и проанализировать информацию о:

- текущей конфигурации вашей сети
- конфигурации DNS и почтового сервера

- соединении с поставщиком услуг Internet (ISP)
- необходимых вам службах Internet
- службах, которые вы намерены предоставить пользователям Internet

Эта информация позволит вам определить слабые стороны системы защиты и необходимые меры противодействия.

Пусть, например, вы хотите разрешить пользователям внутренней сети подключаться по Telnet к хостам некоторой организации, которая занимается разработкой программных продуктов. В этом случае вы должны принять во внимание опасность, связанную с передачей незащищенной информации по Internet. Конкуренты могут перехватить эту информацию и воспользоваться ей, нанеся тем самым финансовый ущерб вашей фирме. Определив производственные требования (использование Telnet) и связанные с этим риски (утечка конфиденциальной информации), вы можете установить, какие дополнительные меры защиты требуются для обеспечения безопасности (применение протокола Secure Sockets Layer).

После того как вы определите стратегию работы с Internet и выберете систему защиты, рекомендуем вам еще раз изучить следующие разделы:

- В разделе *Организация многоуровневой защиты* приведена информация о наиболее важных моментах, которые следует учесть при разработке системы защиты.
- Раздел *Задачи системы защиты* содержит информацию о том, какая информация играет важную роль при выборе стратегии защиты.
- В разделе *Пример организации электронной коммерции в фирме JKL Toys* вы найдете пример схемы защиты для организации средних размеров. Вы можете создать собственную схему на основе предложенного примера.

Организация многоуровневой защиты

Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей системы.

Стратегия защиты - это основа, на базе которой проектируется защита при разработке новых приложений и расширении сетей. В стратегии защиты обычно зафиксированы области ответственности пользователей - например, от них может требоваться защита конфиденциальной информации и выбор паролей, которые сложно подобрать.

Примечание: Правильно выбранная стратегия создает оптимальный баланс между удобством работы в сети и степенью защиты внутренней сети. Правильная настройка внутренних средств защиты системы iSeries позволяет избежать многих потенциальных опасностей. Однако если система iSeries подключена к открытой сети (например, Internet), то необходимо принять дополнительные меры защиты для обеспечения безопасности внутренней сети организации.

Использование средств Internet в повседневной деятельности компании сопряжено с рядом рисков. При разработке стратегии защиты вы должны учитывать, с одной стороны, необходимость предоставления доступа к службам, а с другой - необходимость управления доступом к функциям и данным. Для компьютеров, подключенных к сети, обеспечить защиту значительно сложнее, так как сама линия связи не защищена.

Некоторые службы Internet в значительно большей степени уязвимы для определенных типов вторжений, чем другие. Поэтому вы должны понимать, с каким риском связано применение каждой службы, которую вы планируете использовать или предоставлять. Кроме того, понимание возможных угроз безопасности поможет вам четко определить круг задач защиты.

В Internet есть огромное количество пользователей, создающих угрозу для безопасной передачи данных. Некоторые типичные риски перечислены ниже:

- При **пассивной атаке** злоумышленник просто за потоком данных в вашей сети, пытаясь извлечь секретную информацию. Такие атаки могут осуществляться как через сеть (путем прослушивания канала связи), так и через систему (путем замены компонента системы на программу типа ″троянский конь″, осуществляющую перехват данных). Пассивные атаки наиболее трудно обнаружить. Вследствие этого вы должны всегда исходить из предположения, что все соединения в Internet или любой другой ненадежной сети прослушиваются.
- В случае **активной атаки** злоумышленник старается взломать вашу систему защиты. Существует несколько типов активных атак:
  - При **попытках доступа к системе** злоумышленник пытается использовать бреши в защите для получения доступа к системе клиента или сервера.
  - При атаке методом **имитации** злоумышленник пытается войти в систему под видом системы, которой вы доверяете, или пользователя, запрашивающего секретную информацию.
  - При **создании помех в работе** Атакующая сторона пытается создать помехи или заблокировать вашу систему, перенаправляя поток данных или отправляя вашей системе ненужные сообщения.
  - При **криптографической атаке** злоумышленник пытается угадать или украсть ваши пароли или расшифровать зашифрованные данные с помощью специальных средств.

Многоуровневая защита

Поскольку потенциальные опасности исходят от Internet на различных уровнях работы сети, ваша система защиты должна быть многоуровневой. В общем случае при подключении к Internet не стоит гадать, **возникнет ли** какая-либо угроза. Вместо этого следует исходить из того, что угроза **обязательно возникнет**. Поэтому ваша система защиты должна быть продуманной и активной. Если вы реализуете эффективную многоуровневую защиту, то злоумышленник, проникнувший через один уровень, будет остановлен на следующем уровне.

В следующем списке приведены основные уровни сетевого взаимодействия, защиту которых должна предусматривать ваша стратегия. Стратегия должна быть тщательно продумана от самого простого (на уровне системы) до самого сложного (на уровне передачи данных) уровня.

Защита на уровне системы

Общие средства защиты формируют главную линию обороны вашей системы от потенциальных опасностей, связанных с подключением внутренней сети к Internet. Поэтому первоочередной задачей при планировании подключения к Internet будет настройка общих средств защиты системы. Функции защиты, относящиеся к этому уровню, описаны в разделе Базовые средства защиты при подключении к Internet.

Защита на уровне сети

Средства защиты на уровне сети позволяют управлять доступом к системе iSeries и другим системам, подключенным к сети. При подключении внутренней сети к Internet вы должны обеспечить адекватные средства защиты ресурсов внутренней сети от доступа извне. Как правило, для организации защиты на уровне сети применяется брандмауэр. Важным элементом стратегии защиты будет соединение с провайдером Internet (ISP). В вашей схеме защиты должны учитываться меры, которые будет принимать ваш ISP - например, правила фильтрации IP-пакетов для соединения с маршрутизатором ISP, и меры предосторожности, предпринимаемые по отношению к DNS. В разделе Защита системы на уровне сети приведены примеры мер предосторожности, которые могут пригодиться для защиты внутренних ресурсов на уровне сети.

Защита на уровне приложений

Средства защиты на уровне приложений позволяют управлять взаимодействием пользователей с конкретными приложениями. В идеальном случае для каждого приложения должны применяться собственные параметры защиты. Вам следует с особым вниманием отнестись к настройке защиты приложений, работа которых будет так или иначе связана с Internet. Такие приложения и службы сильно уязвимы, и они будут первым объектом внимания злоумышленников. Хорошая стратегия предусматривает независимую защиту серверов и клиентов. В разделе Средства защиты приложений

вы найдете информацию о потенциальных опасностях и средствах организации защиты большинства распространенных приложений и служб Internet.

Защита на уровне передачи данных

Средства защиты на уровне передачи данных направлены на защиту данных, передаваемых по сети. Передавая информацию по открытым сетям (например, Internet), вы никогда не можете наверняка сказать, каким путем она попадет к адресату. По дороге она обязательно не минует несколько неподконтрольных вам серверов. Если вы не предпримете специальных мер по защите данных (например, можно воспользоваться протоколом SSL для шифрования передаваемой информации), они будут доступны практически всем желающим. Средства защиты на уровне передачи данных призваны обеспечить сохранность данных по пути от отправителя к адресату. В разделе Средства защиты на уровне передачи данных перечислены средства, которыми можно воспользоваться для защиты данных, передаваемых по открытым сетям (например, Internet).

При разработке глобальной стратегии защиты вам следует отдельно подумать над каждым уровнем защиты. Помимо этого, стоит проанализировать способы взаимодействия различных уровней защиты, поскольку только в этом случае вы сможете получить полноценную и эффективную систему защиты вашего бизнеса.

Понятия, связанные с данным

“Базовые уровни защиты при подключении к Internet” на стр. 11
Перечислены требования к системе защиты, которые должны быть выполнены до подключения системы к сети Internet.

“Средства защиты на уровне сети” на стр. 12
Приведены примеры мер предосторожности, которые могут пригодиться для защиты внутренних ресурсов на уровне сети.

“Средства защиты на уровне приложений” на стр. 18
Раздел посвящен защите распространенных приложений и служб Internet.

“Средства защиты на уровне передачи данных” на стр. 25
Описаны средства, которыми можно воспользоваться для защиты данных, передаваемых по открытым сетям (например, Internet). К этим средствам относится протокол Secure Sockets Layer (SSL), iSeries Access Express и виртуальные частные сети (VPN).

“Стратегия защиты и ее задачи”
Информация, приведенная в документе, поможет определить требования пользователей и опасности, исходящие от них.

“Защита электронной почты” на стр. 22
Применение электронной почты в сети Internet и в любых других общедоступных сетях представляет собой определенную опасность, от которой вас не всегда сможет защитить брандмауэр.

Виртуальная частная сеть (VPN)

“Защита FTP” на стр. 23
Протокол передачи файлов (FTP) предназначен для передачи файлов между компьютерами, подключенными к сети.

Ссылки, связанные с данной

Термины, связанные с защитой

Стратегия защиты и ее задачи

Информация, приведенная в документе, поможет определить требования пользователей и опасности, исходящие от них.

Стратегия защиты

Любая служба Internet, предоставляемая или используемая вашей системой iSeries, является дополнительным фактором риска не только для системы, но и для всей вашей сети. Стратегией защиты называется набор правил и требований, предъявляемых к работе вычислительных и коммуникационных

ресурсов организации. Эти правила и требования охватывают такие области, как физическая защита организации, защита персонала, административная защита и защита сети.

Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей системы. Стратегия защиты - это основа, на базе которой проектируется защита при разработке новых приложений и расширении сетей. В стратегии защиты обычно зафиксированы области ответственности пользователей - например, от них может требоваться защита конфиденциальной информации и выбор паролей, которые сложно подобрать. Кроме того, в стратегии защиты должен быть предусмотрен контроль за эффективностью принятых мер защиты. Такой контроль позволяет выяснить, не пытается ли какой-либо злоумышленник нарушить разработанную вами защиту.

При разработке стратегии защиты необходимо четко сформулировать задачи, поставленные перед системой защиты. После разработки стратегии необходимо предпринять все возможные меры для реализации предусмотренных в ней правил. В частности, нужно провести обучение персонала и приобрести соответствующие программные и аппаратные средства. При каждом изменении вычислительной среды следует анализировать применяемую стратегию защиты и при необходимости вносить в нее изменения, учитывающие новые опасности. Пример стратегии защиты, применяемой в компании JKL Toy Company, приведен в разделе ″Общая информация о защите системы″ продукта IBM Systems Software Information Center.

Задачи стратегии защиты

При разработке и реализации стратегии защиты необходимо четко представлять себе задачи, которые должна выполнять система защиты. Эти задачи можно разделить на несколько категорий:

ресурсы, защита
Средства защиты ресурсов позволят вам быть уверенным в том, что объекты системы будут доступны только тем, кому вы предоставите соответствующие права. Одно из достоинств системы iSeries заключается в том, что в ней предусмотрена возможность защиты всех типов системных ресурсов. Рекомендуем вам тщательно подойти к созданию категорий пользователей, которым нужен доступ к системе. Кроме того, в рамках стратегии защиты следует определить, какие права доступа должны быть предоставлены различным категориям пользователей.

Идентификация
Система защиты должна обладать возможностью проверки того, что любой ресурс (человек или компьютер) действительно является тем, за кого он себя выдает. Надежная идентификация гарантирует защиту от подлога, когда взломщик получает доступ к информации под чужим именем. Самый простой способ идентификации заключается в применении идентификаторов и паролей пользователей. В тех случаях, когда он недостаточно надежен, применяются цифровые сертификаты. При подключении системы к открытой сети проблема идентификации принимает несколько иной характер. Важное различие между Internet и внутренней сетью организации заключается в том, что у вас есть полная информация о сотрудниках вашей организации, но нет никакой информации о пользователях открытой сети. Поэтому следует рассмотреть возможность перехода на более серьезные средства идентификации, чем простые имена пользователей и пароли. По результатам идентификации пользователям могут предоставляться различные права доступа.

разграничение доступа
Система защиты должна позволять устанавливать различные права доступа пользователей к ресурсам. У вас должна быть возможность строго регламентировать доступ к ресурсам системы и права на выполнение определенных операций. Как правило, разграничение доступа тесно связано с идентификацией пользователей.

проверка подлинности
Система защиты должна гарантировать то, что полученная информация идентична отправленной. Понятие целостности включает в себя понятия целостности данных и целостности системы.

- **Целостность данных**: означает защиту данных от несанкционированного изменения или подлога. Обеспечение целостности данных позволяет устранить возможность перехвата и подмены данных посторонними лицами. Помимо защиты данных в пределах сети, вам могут потребоваться

дополнительные меры защиты в случае, если вы получаете информацию из открытой сети. Если вы получаете данные из открытой сети, то вам необходимо предпринять такие меры безопасности, которые могли бы обеспечить:

- Защиту данных от посторонних лиц. Поскольку абсолютно исключить возможность перехвата данных невозможно, рекомендуется передавать их в зашифрованном виде.
- Целостность передаваемых данных. Это необходимо для того, чтобы исключить возможность подмены.
- Гарантированную доставку данных. Вам может пригодиться электронный аналог заказной почты или уведомлений о вручении почтовых отправлений.

- **Целостность системы**: способность системы сохранять стабильность работы при заданном уровне нагрузки. В системе iSeries этот компонент защиты требует минимального внимания, так как он является фундаментальной составляющей архитектуры iSeries. В частности, в системе iSeries практически невозможно злонамеренное изменение системных программ, если вы работаете с уровнем защиты 40 или 50.

неоспоримость

Неоспоримостью называется возможность гарантированно подтвердить факт передачи или получения какой-либо информации. Для обеспечения неоспоримости важных операций (например, оплаты товаров с помощью кредитных карт по Internet) применяются цифровые подписи и шифрование данных с открытым ключом. Как отправители, так и получатели должны предоставить неоспоримые подтверждения того, что данные были отправлены или, соответственно, получены. Таким подтверждением служит цифровая подпись.

конфиденциальность

Гарантия того, что посторонним лицам будет недоступна конфиденциальная информация даже в случае, если она будет перехвачена при передаче. Это одна из самых важных составляющих системы защиты данных. Для обеспечения конфиденциальности при передаче данных по открытым сетям применяются цифровые сертификаты и протокол Secure Socket Layer (SSL). В вашей стратегии защиты должны быть предусмотрены средства обеспечения конфиденциальности при передаче информации как по внутренней сети, так и за ее пределами.

Контроль системы защиты

Возможность отслеживать все события, связанные с системой защиты, и вести протокол разрешенных и отклоненных операций доступа к данным. Для разрешенных операций в протоколе должно быть указано, кто и над какими объектами выполнял операции. Записи об отклоненных операциях в протоколе могут быть признаком того, что кто-то пытался преодолеть систему защиты, или о том, что кому-то не удается войти в систему.

Понимание задач, возлагаемых на систему защиты, поможет вам разработать максимально эффективную стратегию защиты вашей системы в сети. Перед началом разработки стратегии защиты рекомендуем вам обратиться к разделу Пример организации электронной коммерции в компании JKL Toys. В этом примере проиллюстрированы многие характерные особенности подключения внутренней сети к Internet.

Понятия, связанные с данным

“Способы защиты iSeries при работе с Internet” на стр. 2
Приводится краткий обзор возможностей системы защиты iSeries и предлагаемых средств защиты.

“Организация многоуровневой защиты” на стр. 4
Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей системы.

Цифровые сертификаты

Secure Socket Layer (SSL)

“Пример организации электронной коммерции в компании JKL Toys” на стр. 9
В этом разделе приведен пример организации электронной коммерции в компании JKL Toys, которая решила воспользоваться возможностями, предоставляемыми Internet. Хотя мы сами выдумали эту компанию, ее стратегия защиты и способ ведения дел в Internet очень близки к реальному положению дел во многих компаниях.

Пример организации электронной коммерции в компании JKL Toys

В этом разделе приведен пример организации электронной коммерции в компании JKL Toys, которая решила воспользоваться возможностями, предоставляемыми Internet. Хотя мы сами выдумали эту компанию, ее стратегия защиты и способ ведения дел в Internet очень близки к реальному положению дел во многих компаниях.

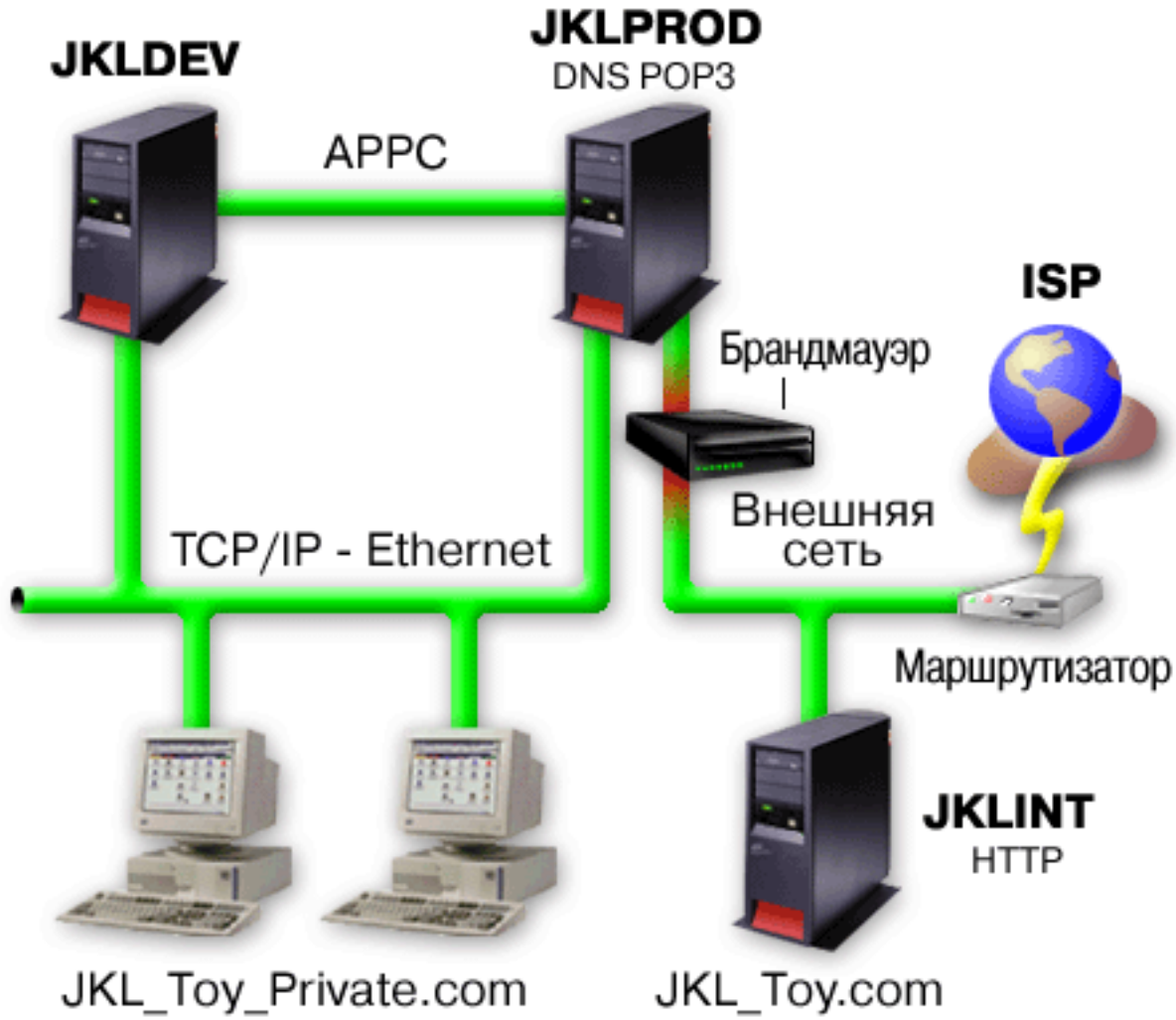
Компания JKL Toys - это не очень большой, но стремительно растущий производитель игрушек. Они начинали со скакалок и кубиков, а теперь в их ассортименте есть даже плюшевые мамонты. Президент компании с большим энтузиазмом относится к расширению бизнеса и к возможности упростить выполнение задач, связанных с ростом компании, с помощью системы iSeries. Функции системного администратора iSeries возложены на Шэрон Джонс, главного бухгалтера фирмы.

Компания JKL Toys сначала разработала стратегию защиты для внутренней сети, которая успешно применялась в течение года. Теперь возникла потребность повысить эффективность внутреннего обмена информацией, а также подключить свою сеть к Internet. В дальнейшем компания собирается создать серьезное маркетинговое представительство в Internet, в котором будет функционировать электронный каталог товаров. Кроме того, JKL Toys планирует передавать через Internet конфиденциальную информацию из удаленных регионов в свой центральный офис. Наконец, компания решила предоставить сотрудникам доступ в Internet для поиска новых идей и более эффективного использования рабочего времени. В принципе компания рассчитывает на то, что часть клиентов начнет покупать товары через электронный магазин, который будет организован на web-странице фирмы в Internet. Шэрон работает над докладом об опасностях, которые могут повлечь за собой все эти начинания, и о том, какие меры защиты должны быть предприняты для устранения этих опасностей. В дальнейшем Шэрон будет отвечать за модернизацию корпоративной стратегии защиты и реализации тех мер, которые она предложит.

Расширение присутствия компании в Internet преследует следующие цели:

- Способствовать популяризации общего имиджа компании и расширению ее присутствия на рынке.
- Создать электронный каталог продукции для клиентов и персонала.
- Повысить качество обслуживания клиентов.
- Упростить доступ сотрудников к электронной почте и сети WWW.

После того как компания JKL Toys убедилась, что в ее системах iSeries реализована надежная система общей защиты, она решила создать брандмауэр для организации защиты на уровне сети. Брандмауэр будет защищать внутреннюю сеть от многих потенциальных опасностей, исходящих со стороны Internet. Ниже показана конфигурация подключения внутренней сети к Internet.



Как показано на рисунке, в фирме JKL Toys используются две основные системы iSeries. Одна из них (JKLDEV) применяется для разработки программ, а вторая (JKLPROD) - в производственных целях. Обе системы работают с крайне важными данными и программами. Поэтому фирма JKL решила, что на этих системах нельзя устанавливать программное обеспечение, которое будет взаимодействовать с Internet. Для этих целей было решено приобрести еще одну систему iSeries (JKLINT).

Новая система будет размещена на границе между внешней и внутренней сетью и будет обеспечивать физическое отделение Internet от внутренней сети, что снижает вероятность причинения какого-либо ущерба со стороны Internet. Благодаря тому, что новая система iSeries будет выполнять только функции сервера Internet, компания также сможет упростить управление системами защиты сети.

| В новой системе iSeries не будут выполняться важные программы. На первом этапе эта система будет играть
| роль статического общедоступного web-сервера. При этом компания стремится к тому, чтобы эта система и
| работающий на ее базе web-сервер были защищены от постороннего вмешательства и возможных атак
| злоумышленников. Как следствие, было решено защитить этот сервер с помощью службы преобразования
| сетевых адресов (NAT) и установить правила фильтрования IP-пакетов.

| В дальнейшем, когда в компании появятся специализированные приложения для web-сервера (например,
| электронный магазин), будут введены дополнительные адекватные меры защиты.

Понятия, связанные с данным

“Стратегия защиты и ее задачи” на стр. 6
Информация, приведенная в документе, поможет определить требования пользователей и опасности, исходящие от них.

“Средства защиты на уровне сети” на стр. 12
Приведены примеры мер предосторожности, которые могут пригодиться для защиты внутренних ресурсов на уровне сети.

“Средства защиты на уровне передачи данных” на стр. 25
Описаны средства, которыми можно воспользоваться для защиты данных, передаваемых по открытым сетям (например, Internet). К этим средствам относится протокол Secure Sockets Layer (SSL), iSeries Access Express и виртуальные частные сети (VPN).

Базовые уровни защиты при подключении к Internet

Перечислены требования к системе защиты, которые должны быть выполнены до подключения системы к сети Internet.

Общие средства защиты формируют главную линию обороны вашей системы от потенциальных опасностей, связанных с подключением внутренней сети к Internet. После этого первым шагом по настройке общей стратегии защиты при работе в Internet является правильная настройка основных параметров защиты i5/OS. Минимальные требования к общей защите системы включают следующее:

- Уровень защиты (системное значение QSECURITY) 50. Это обеспечивает максимальную степень защиты целостности, что настоятельно рекомендуется при работе в столь опасной с точки зрения защиты среде, как Internet. Более подробная информация о уровнях защиты iSeries приведена в разделе Планирование и настройка защиты системы.

  Примечание: Если в настоящее время в вашей системе установлен уровень защиты ниже 50, то вам может потребоваться внести определенные изменения в рабочие процедуры и программы. Перед тем как повышать уровень защиты, рекомендуется ознакомиться с книгой Руководство по защите iSeries.

- Установите системные значения, связанные с защитой, так, чтобы уровни ограничений были не ниже рекомендуемых. Установить рекомендуемые параметры защиты можно с помощью Мастера установки защиты Навигатора iSeries.
- Убедитесь, что ни для одного профайла, и в том числе для профайлов, поставляемых IBM, не используются пароли по умолчанию. Это можно сделать с помощью команды Анализировать пароли по умолчанию (ANZDFTPWD).
- Защитите важные ресурсы системы с помощью прав доступа к объектам. Придерживайтесь запретительной стратегии при распределении прав доступа. По умолчанию доступ к системным ресурсам, например, библиотекам и каталогам, должен быть запрещен всем пользователям ((PUBLIC *EXCLUDE). Доступ к важным ресурсам должен быть только у небольшого числа специально назначенных пользователей. Ограничение доступа к меню будет недостаточной мерой в случае подключения к Internet.
- **Обязательно** установите в вашей системе права доступа к отдельным объектам. .

Для упрощения процедуры начальной настройки системы защиты вы можете воспользоваться продуктом @server **Планировщик конфигурации защиты** (его можно загрузить с Web-сайта IBM Systems Software Information Center) или **Мастером настройки защиты** (поддерживается интерфейсом Навигатора the iSeries). Планировщик конфигурации защиты задаст вам несколько вопросов и на основе ваших ответов даст ряд рекомендаций, которые помогут вам правильно настроить параметры защиты системы. Мастер установки защиты устроен примерно так же, но он может задать параметры защиты системы автоматически.

Правильная настройка внутренних средств защиты системы iSeries позволяет избежать многих потенциальных опасностей. Однако если система iSeries подключена к открытой сети (например, Internet), то необходимо принять дополнительные меры защиты для обеспечения безопасности внутренней сети организации. После настройки общих параметров защиты iSeries вы можете настроить дополнительные параметры защиты системы при работе в Internet.

Понятия, связанные с данным

“Организация многоуровневой защиты” на стр. 4
Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей системы.

Информация, связанная с данной

Защита iSeries

Средства защиты на уровне сети

Приведены примеры мер предосторожности, которые могут пригодиться для защиты внутренних ресурсов на уровне сети.

Если вы планируете подключить внутреннюю сеть к открытой сети, в вашей стратегии защиты должна быть предусмотрена полноценная система защиты на уровне сети. Одним из лучших решений будет установка брандмауэра.

Кроме того, важную роль в стратегии защиты будет играть соединение с провайдером Internet (ISP). В вашей схеме защиты должны учитываться меры, которые будет принимать ваш ISP - например, правила фильтрации IP-пакетов для соединения с маршрутизатором ISP и меры предосторожности, предпринимаемые по отношению к DNS.

Хотя брандмауэр обеспечивает одну из наиболее важных ″линий обороны″, эта линия должна быть **не единственной**. Поскольку потенциальные опасности исходят от Internet на различных уровнях работы сети, ваша система защиты должна быть многоуровневой.

Хотя брандмауэр обеспечивает достаточно надежную защиту от некоторых видов атак, общая стратегия защиты должна предусматривать и другие средства. Например, брандмауэр не может защитить данные, пересылаемые через Internet посредством таких приложений, как почтовый сервер SMTP, сервер FTP и сервер TELNET. Если данные передаются незашифрованными, то они легко могут быть перехвачены на пути к месту назначения.

Необходимо уделить пристальное внимание вопросу использования брандмауэра в качестве основного средства защиты системы как при подключении iSeries к внутренней сети, так и при подключении к Internet. Несмотря на то, что продажа и поддержка брандмауэра IBM Firewall for AS/400 в настоящее время прекращена, вы можете воспользоваться рядом других продуктов. Подробные сведения и сценарии перехода от данного брандмауэра к другим продуктам приведены в документе All You Need to Know When Migrating from IBM Firewall for AS/400.

Поскольку коммерческие брандмауэры предоставляют широкий набор средств по защите сети, компания JKL Toys решила выбрать один из предусмотренных в них сценариев защиты электронного бизнеса для защиты своей сети. Однако брандмауэр не может защитить сервер Internet этой компании, работающий на базе системы iSeries. Поэтому компания решила воспользоваться правилами фильтрации iSeries, чтобы с помощью фильтров и службы NAT контролировать поток данных, поступающих на сервер Internet.

Правила фильтрации пакетов в iSeries

Фильтрация пакетов позволяет выборочно пропускать IP-пакеты на сервер согласно установленным вами критериям. Служба NAT позволяет скрыть адреса внутренней сети от внешних пользователей. Она динамически заменяет все внутренние адреса на адреса из некоторого пула внешних IP-адресов. Однако хотя фильтрация IP-пакетов и служба NAT обеспечивают очень хорошую защиту, они не заменят вам брандмауэр. Рекомендуем вам тщательно проанализировать задачи, стоящие перед вашей системой защиты, и решить, можете ли вы отказаться от брандмауэра в пользу правил фильтрации пакетов.

Правильный выбор вам поможет сделать информация из раздела Выбор средств защиты iSeries на уровне сети.

Понятия, связанные с данным

“Организация многоуровневой защиты” на стр. 4
Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей системы.

“Пример организации электронной коммерции в компании JKL Toys” на стр. 9
В этом разделе приведен пример организации электронной коммерции в компании JKL Toys, которая решила воспользоваться возможностями, предоставляемыми Internet. Хотя мы сами выдумали эту компанию, ее стратегия защиты и способ ведения дел в Internet очень близки к реальному положению дел во многих компаниях.

“Правила фильтрации пакетов в iSeries” на стр. 15
Правила обработки пакетов iSeries - это встроенная функция системы i5/OS, с которой можно работать с помощью интерфейса Навигатора iSeries.

“Выбор сетевых средств защиты системы iSeries” на стр. 16
Обсуждаются различные варианты организации защиты системы, эффективность которых зависит от характера использования Internet из вашей внутренней сети.

Информация, связанная с данной

All You Need to Know When Migrating from IBM Firewall for AS/400

Брандмауэры

Брандмауэр - это преграда между защищенной внутренней сетью и незащищенной сетью, например Internet.

Обычно брандмауэр применяется для защиты внутренней сети при ее подключении к Internet, хотя он может использоваться и для защиты одной внутренней сети от другой.

Брандмауэр позволяет организовать подключение к незащищенной сети таким образом, что весь обмен информацией между защищенной внутренней и незащищенной внешней сетями будет проходить через единственную контролируемую точку (″горловину″). Брандмауэр:

- Позволяет пользователям внутренней сети получать доступ к ресурсам внешней сети.
- Предотвращает несанкционированный доступ пользователей внешней сети к ресурсам внутренней сети.

Применение брандмауэра в качестве шлюза при подключении к Internet (или другой сети) значительно повышает защищенность внутренней сети. Кроме того, оно упрощает управление защитой сети, поскольку функции брандмауэра обеспечивают выполнение многих директив стратегии защиты.

Принципы работы брандмауэра

Рассмотрим принципы работы брандмауэра на следующем примере. Представьте, что ваша сеть - это здание, и вы хотите контролировать вход в него. В здание можно попасть только через вестибюль. В вестибюле находятся швейцары, впускающие посетителей, и охрана; кроме того, в нем установлены видеокамеры для контроля происходящего и аппаратура, идентифицирующая посетителей по их удостоверениям.

Все эти меры позволяют достаточно надежно контролировать вход в здание. В то же время, если злоумышленнику все-таки удастся проникнуть в здание, вы ничем не сможете защитить здание от его действий. Однако если вы следите за перемещениями нарушителя, у вас есть шанс обнаружить его действия, вызывающие подозрения.

Компоненты брандмауэра

Брандмауэр - это набор компонентов аппаратного и программного обеспечения, обеспечивающий защиту от несанкционированного доступа к некоторой части сети. Ниже перечислены составные компоненты брандмауэра:

- Аппаратное обеспечение. Обычно это отдельный компьютер или устройство, специально предназначенные для выполнения функций брандмауэра.
- Программное обеспечение. Состоит из нескольких приложений. Брандмауэр предоставляет следующие средства защиты:
  - IP-пакеты, фильтрация
  - Служба преобразования сетевых адресов (NAT)
  - Сервер SOCKS
  - Сервер Proxy для большинства распространенных протоколов (HTTP, Telnet, FTP и т.д.)
  - Функция передачи почты
  - Разделенные службы имен доменов (DNS)
  - Ведение протокола
  - Контроль в режиме реального времени

Примечание: Некоторые брандмауэры поддерживают организацию виртуальных частных сетей (VPN), позволяющих шифровать сеансы связи между вашим и другими брандмауэрами.

Применение средств и служб брандмауэра

Для обеспечения доступа внутренних пользователей к службам Internet на брандмауэре можно установить сервер Proxy, сервер SOCKS или службу преобразования сетевых адресов (NAT). Серверы Proxy и SOCKS играют роль барьера в соединении TCP/IP, скрывая внутренние данные от ненадежной сети. Кроме того, они предоставляют дополнительные возможности по ведению протоколов.

С помощью NAT можно обеспечить пользователям Internet удобный доступ к общему серверу, расположенному за брандмауэром. При этом сеть продолжает оставаться защищенной брандмауэром, так как NAT скрывает ваши внутренние IP-адреса.

Брандмауэр также позволяет защитить информацию внутренней сети, предоставляя свой сервер DNS. Фактически серверов DNS два: один применяется к данным, относящимся ко внутренней сети, а второй, находящийся на брандмауэре, - к данным, относящимся к внешней сети и самому брандмауэру. Это позволяет контролировать доступ извне к информации о системах внутренней сети.

При разработке стратегии брандмауэра может показаться, что достаточно запретить только то, что представляет опасность для организации, а все остальное разрешить. Но, поскольку компьютерные взломщики постоянно изобретают новые способы нападения, вы заранее должны принять меры противодействия. В примере со зданием необходимо также отслеживать признаки того, что некто смог преодолеть вашу защиту. Как правило, гораздо проще и дешевле предотвратить вторжение, чем ликвидировать его последствия.

В случае брандмауэра наилучшей стратегией будет разрешить работу только тех приложений, которые вы проверяли и в которых уверены. Если вы будете придерживаться этой стратегии, то вы должны составить исчерпывающий список служб, запускаемых на брандмауэре. Вы должны охарактеризовать каждую службу по направлению соединения (из внутренней сети во внешнюю или наоборот). Кроме того, вы должны составить список пользователей, которым будет разрешено работать с каждой из служб, и компьютеров, которым будет разрешено подключаться к службам.

Достоинства защиты с помощью брандмауэра

Брандмауэр служит промежуточным звеном между вашей внутренней сетью и точкой выхода в Internet (или другую открытую сеть). По этой причине он позволяет ограничить возможные каналы доступа извне к вашей сети. Брандмауэр позволяет организовать подключение к незащищенной сети таким образом, что весь обмен информацией между внутренней сетью и Internet будет проходить через единственную точку (″горловину″). Это значительно упрощает контроль над входящими и исходящими потоками данных.

Для пользователей внешней сети вся внутренняя сеть, защищенная брандмауэром, выглядит как узел с одним адресом. Брандмауэр скрывает адреса внутренней сети и предоставляет доступ к ней посредством серверов Proxy или SOCKS или службы Преобразования сетевых адресов (NAT). Таким образом, брандмауэр обеспечивает конфиденциальность информации внутренней сети. Это значительно снижает вероятность атаки типа ″имитация″ из Internet.

Брандмауэр позволяет контролировать входящие и исходящие потоки внутренней сети, минимизируя вероятность вторжения в нее. Фильтры брандмауэра пропускают входящие потоки данных только при условии, что они относятся к определенному типу и предназначены для конкретных узлов внутренней сети. Это минимизирует вероятность несанкционированного доступа к внутренней сети по протоколу TELNET или FTP.

Недостатки защиты с помощью брандмауэра

Хотя брандмауэр обеспечивает достаточно надежную защиту от некоторых видов атак, общая стратегия защиты должна предусматривать и другие средства. Например, брандмауэр не может защитить данные, пересылаемые через Internet посредством таких приложений, как почтовый сервер SMTP, сервер FTP и сервер TELNET. Если данные передаются незашифрованными, то они легко могут быть перехвачены на пути к месту назначения.

Правила фильтрации пакетов в iSeries

Правила обработки пакетов iSeries - это встроенная функция системы i5/OS, с которой можно работать с помощью интерфейса Навигатора iSeries.

Она включает две высокоэффективные функции управления потоком данных TCP/IP в целях защиты системы iSeries:

- преобразование сетевых адресов (NAT)
- Фильтрация IP-пакетов

Поскольку NAT и функция фильтрации IP-пакетов являются встроенными функциями i5/OS, они позволяют обеспечить надежную защиту системы без дополнительных расходов. В некоторых случаях этих средств уже достаточно для организации полноценной защиты. Однако они не могут заменить брандмауэр. Защита IP-пакетов может применяться как отдельно, так и в сочетании с брандмауэром. Это зависит от задач, стоящих перед вашей системой защиты.

Примечание: Не рекомендуем вам экономить на защите главной (рабочей) системы iSeries. Это не тот случай, когда экономия оправдывает себя. Для обеспечения достаточной защиты рабочей системы настоятельно рекомендуем вам воспользоваться брандмауэром.

Что такое NAT и фильтрация IP-пакетов и как они могут применяться совместно?

Служба преобразования сетевых адресов (NAT) изменяет IP-адреса отправителей и получателей пакетов, проходящих через систему. NAT - это упрощенная альтернатива серверам Proxy и SOCKS, применяемым на брандмауэрах. Эта служба упрощает настройку сетей, поскольку она позволяет устанавливать соединения между сетями с несовместимыми структурами адресов. За счет этого систему iSeries можно использовать в качестве шлюза между сетями, в которых применяются несовместимые или конфликтующие схемы адресации. Кроме того, с помощью NAT можно скрыть реальные IP-адреса хостов вашей внутренней сети, динамически заменяя их на фиктивные адреса. Фильтрация IP-пакетов и служба NAT дополняют друг друга и позволяют существенно повысить уровень защиты сети.

Фильтрация пакетов упрощает управление общедоступным Web-сервером, работающим под защитой брандмауэра. Общие IP-адреса преобразуются для Web-сервера во внутренние IP-адреса. Это уменьшает

число адресов, которые должны быть зарегистрированы в Internet и повышает уровень защиты внутренней сети. Кроме того, NAT позволяет пользователям внутренней сети работать с Internet, не разглашая IP-адреса своих хостов.

Фильтрация IP-пакетов позволяет выборочно блокировать и защищать поток данных протокола IP на основе содержимого заголовков пакетов. С помощью Мастера настройки Internet Навигатора iSeries можно быстро настроить основные правила фильтрации пакетов и предотвратить передачу нежелательных данных по сети.

Фильтрация IP-пакетов позволяет выполнить следующие задачи:

- Создать набор правил фильтрации, указывающих, какие пакеты следует пропускать в сеть, а какие - отбрасывать. Правила фильтрации применяются для конкретного физического интерфейса (например, Token-Ring или Ethernet). Для разных физических интерфейсов могут применяться как одинаковые, так и разные правила.
- В правилах фильтрации может применяться следующая информация из заголовков пакетов:
  - IP-адрес получателя
  - IP-адрес отправителя и протокол (например, TCP, UDP и т.д.)
  - Порт получателя (например, 80 для HTTP)
  - Порт отправителя
  - Направление дейтаграммы (входящая или исходящая)
  - Тип пакета (локальный или пересылаемый)
- Ограничить нежелательные потоки данных, вызванные попытками доступа к вашей системе. Кроме того, потоки данных могут быть перенаправлены в другие системы. Это относится и к низкоуровневым пакетам ICMP (например, к пакетам PING), для которых не требуется специальный сервер приложений.
- Указать, что информация о пропущенных и отброшенных пакетах должна заноситься в системный журнал. Записи, внесенные в журнал, нельзя изменить, поэтому журнал - идеальное средство контроля за операциями в сети.

Понятия, связанные с данным

“Средства защиты на уровне сети” на стр. 12
Приведены примеры мер предосторожности, которые могут пригодиться для защиты внутренних ресурсов на уровне сети.

преобразование сетевых адресов (NAT)

Фильтрация IP-пакетов

Выбор сетевых средств защиты системы iSeries

Обсуждаются различные варианты организации защиты системы, эффективность которых зависит от характера использования Internet из вашей внутренней сети.

В основе средств защиты сети от несанкционированного доступа лежат технологии брандмауэра. В качестве средства защиты системы iSeries можно выбрать как полнофункциональный брандмауэр, так и специальные технологии сетевой защиты, реализованные в составе протокола TCP/IP системы i5/OS. Реализация данного протокола включает функцию правил обработки пакетов (в нее входит фильтрация пакетов IP и служба NAT) и поддержку HTTP для сервера Proxy iSeries.

Выбор между правилами фильтрации пакетов и брандмауэром определяется сетевой средой, требованиями к доступу и потребностями защиты. При подключении системы iSeries или внутренней сети к Internet или другой незащищенной сети **настоятельно** рекомендуется применять брандмауэр в качестве основного средства защиты.

Брандмауэр предпочтительнее в этом случае, поскольку его аппаратное и программное обеспечение специально предназначено для обеспечения защиты и содержит ограниченное число интерфейсов, доступных извне. В том случае, если при подключении к Internet в качестве средства защиты используется реализация

TCP/IP i5/OS, система представляет из себя открытую вычислительную платформу с очень большим количеством незащищенных интерфейсов и приложений.

Разница существенна по нескольким причинам. Например, выделенный брандмауэр не предоставляет никаких иных функций и приложений кроме тех, которые обеспечивают его работу. Следовательно, если злоумышленнику все-таки удастся преодолеть защиту брандмауэра, его возможности будут крайне ограниченны. Если же злоумышленник получит возможность управления функциями TCP/IP системы iSeries, он, возможно, сможет получить доступ к различным приложениям, службам и данным. Это позволит ему нанести серьезный ущерб самой системе, а также получить доступ к другим системам внутренней сети.

Поэтому возникает вопрос - допустима ли организация защиты с помощью служб TCP/IP системы iSeries? Как и во всех остальных случаях, ваше решение должно быть приемлемым не только с точки зрения эффективности, но с точки зрения издержек. Вы должны проанализировать ваши потребности и найти компромисс между надежностью защиты и ее стоимостью. Следующая таблица содержит описание характеристик, достоинств и недостатков как средств защиты TCP/IP, так и брандмауэра. Она поможет вам определить, когда выгоднее применять средства защиты TCP/IP, когда - брандмауэр, а когда - их сочетание.

Технология защиты	**Оптимальное использование технологии TCP/IP i5/OS**	**Рекомендуется применять брандмауэр с полным набором функций**
Фильтрация IP-пакетов	• Обеспечивает **дополнительную** защиту отдельной системы iSeries, например, общедоступного Web-сервера или внутренней сети, содержащей конфиденциальные данные. • Защищает подсеть **внутренней корпоративной сети**, используя iSeries в качестве шлюза (маршрутизатора) для связи с остальной сетью. • Управляет соединением с частично защищенным компьютером с помощью **частной сети** или внешней сети, в которой сервер iSeries выполняет роль шлюза.	• Защищает всю корпоративную сеть от атак из **Internet** или другой открытой сети, с которой соединена ваша сеть. • Защищает большую загруженную подсеть от остальной сети.
Служба преобразования сетевых адресов (NAT)	• Обеспечивает соединение двух **частных сетей** с несовместимыми структурами адресов. • Скрывает адреса систем подсети от абонентов менее защищенной сети.	• Скрывает адреса клиентов, обращающихся к **Internet** или другой открытой сети. Может использоваться вместо сервера Proxy или SOCKS. • Позволяет открыть доступ к службам системы, входящей в частную сеть, для клиентов, подключенных к **Internet**.
Сервер Proxy	• Действует в качестве промежуточного сервера для **удаленных узлов** корпоративной сети при подключении к Internet через центральный брандмауэр.	• Действует в качестве промежуточного сервера для всей корпоративной сети при подключении к **Internet**.

Дополнительная информация об использовании функций защиты TCP/IP системы i5/OS приведена в следующих разделах:

- *Правила фильтрации пакетов и служба NAT*: V5R1 IBM Systems Software Information Center.
- *Документация сервера HTTP*:
  `http://www.iseries.ibm.com/domino/reports.htm`
- Руководство Примеры реализации защиты системы AS/400, подключенной к Internet (SG24-5954).

Понятия, связанные с данным

“Средства защиты на уровне сети” на стр. 12
Приведены примеры мер предосторожности, которые могут пригодиться для защиты внутренних ресурсов на уровне сети.

Средства защиты на уровне приложений

Раздел посвящен защите распространенных приложений и служб Internet.

Средства защиты на уровне приложений позволяют управлять взаимодействием пользователей с конкретными приложениями. В идеальном случае для каждого приложения должны применяться собственные параметры защиты. Вам следует с особым вниманием отнестись к настройке защиты приложений, работа которых будет так или иначе связана с Internet. Такие приложения и службы сильно уязвимы, и они будут первым объектом внимания злоумышленников. Хорошая стратегия предусматривает независимую защиту серверов и клиентов.

Хотя меры по защите каждого отдельно взятого приложения играют важную роль, они занимают незначительное место в общей стратегии защиты,

Дополнительную информацию об организации защиты для большинства распространенных приложений Internet можно найти в следующих разделах:

Понятия, связанные с данным

“Организация многоуровневой защиты” на стр. 4
Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей системы.

Защита Web-сервера

Предоставляя внешним пользователям доступ к своему Web-серверу, вы, скорее всего, не захотите раскрывать перед ними внутреннюю структуру сервера и подробности создания Web-страниц.

Ваша задача - создать простой и удобный интерфейс, в котором вся черновая работа выполняется незаметно для пользователя. Как администратору, вам следует позаботиться о том, чтобы необходимые меры безопасности не снизили привлекательность вашего Web-сервера. Если вы собираетесь применять систему iSeries в качестве Web-сервера, то учтите следующие обстоятельства:

- Перед тем, как предоставить клиентам доступ к серверу HTTP, администратор сервера должен задать необходимые директивы для защиты сервера. Существует два типа таких директив: общие директивы и директивы защиты. Поступивший запрос будет обработан Web-сервером только после того, как сервер удостоверится в соблюдении всех условий и ограничений, налагаемых этими директивами.
- Для создания и изменения этих директив служит специальная Web-страница администрирования сервера. Общие директивы определяют общие правила работы Web-сервера. Директивы защиты позволяют задавать и изменять модели защиты, согласно которым сервер предоставляет доступ к определенным URL.
- Сервер можно настраивать не только с помощью страницы администрирования, но и напрямую - с помощью директив map и pass.
  - Директивы map и pass позволяют создавать маски имен файлов для Web-сервера iSeries. Директивы pass и map позволяют задавать каталоги, используемые сервером при обработке URL. Директива EXEC задает библиотеки, в которых находятся программы CGI-BIN.

    При желании директивы защиты можно задать независимо для каждого URL, хотя в большинстве случаев это нецелесообразно. Однако если вам потребуется узнать, кто и каким способом обращается к определенным URL, то это можно сделать только с применением соответствующих директив защиты.
  - Напомним вам, что для настройки сервера можно воспользоваться не только командой WRKHTTPCFG (Работа с конфигурацией HTTP), но и специализированной страницей администрирования. Настройка сервера напрямую с помощью директив - далеко не простая задача. Если у вас недостаточно опыта, вам будет гораздо проще настроить сервер с помощью административной страницы.

Протокол HTTP позволяет только просматривать данные. Его возможностей недостаточно, если вам требуется изменить какую-либо информацию в базе данных. Однако почти наверняка некоторым из ваших приложений потребуется изменять файлы базы данных. В таких случаях применяются программы CGI-BIN. Например, можно создать формы, которые после заполнения будут обновлять базу данных iSeries. Администратор защиты должен контролировать права доступа пользователей и программ CGI, запускаемых из Web-сервера. Внимательно проанализируйте все права доступа и определите, нет ли в системе каких-либо важных объектов, для которых установлены слишком широкие права доступа.

Примечание: Интерфейс CGI (Common Gateway Interface) применяется в качестве стандартного способа обмена информацией между Web-сервером и внешними программами. Программы CGI могут быть написаны на любом языке программирования при условии, что он поддерживается системой Web-сервера.

Кроме того, Web-страницы можно создавать не только с помощью программ CGI, но и с помощью Java. Для обеспечения правильной работы web-страниц, использующих Java, следует ознакомиться с принципами защиты Java.

Сервер HTTP ведет протокол доступа, в который заносится информация о всех принятых и отклоненных попытках обращения к серверу.

Серверы Proxy принимают запросы HTTP от браузеров и пересылают их на Web-серверы. Web-серверу, принимающему запрос, известен только IP-адрес сервера Proxy, и он не может определить адреса и имена компьютеров, от которых исходят запросы. Сервер Proxy может поддерживать обращения к URL по протоколам HTTP, FTP, Gopher и WAIS.

Сервер Proxy для протокола HTTP, входящий в комплект продукта IBM HTTP Server for iSeries, можно также использовать для организации совместного доступа к Internet. Кроме того, сервер Proxy может вести протокол всех полученных запросов. Такой протокол позволяет контролировать использование сетевых ресурсов. Дополнительная информация о применении сервера Proxy для протокола HTTP приведена в справочной системе Documentation Center по продукту IBM HTTP Server for iSeries:

| `http://www.ibm.com/eserver/iseries/products/http/docs/doc.htm`

Понятия, связанные с данным

“Защита при работе с Java и Internet”
Java все чаще применяется в современных вычислительных сетях и системах.

Защита при работе с Java и Internet

Java все чаще применяется в современных вычислительных сетях и системах.

Например, в вашей системе может быть установлен продукт IBM Toolbox for Java или IBM Development Kit for Java . В этом случае вы должны быть готовы принять особые меры защиты, связанные с применением Java. Хотя брандмауэр - надежное средство защиты внутренней сети при работе с Internet, он не обеспечивает защиту от многих опасностей, связанных с применением Java. В вашей схеме защиты должны быть предусмотрены особые меры предосторожности в связи с использованием таких источников повышенной опасности, как приложения, аплеты и сервлеты Java. Кроме того, вы должны изучить взаимосвязь между средствами Java и системой защиты ресурсов применительно к идентификации и разграничению доступа для программ на Java.

Приложения на Java

Язык программирования Java обладает определенными характеристиками, благодаря которым программисты Java избегают нежелательных ошибок, способных привести к нарушению целостности приложений. (Другие языки программирования для PC такие как C или C++, не обеспечивают такую надежную защиту от нежелательных ошибок, как Java.) Например, в Java применяется строгий контроль типов, что позволяет избежать некорректного использования объектов. Java не позволяет выполнять некоторые операции с указателями, благодаря чему случайный выход за пределы допустимого диапазона памяти становится невозможным. Java можно рассматривать в качестве средства разработки приложений так же, как и другие языки высокого уровня. При разработке приложений на Java следует принимать такие же меры защиты, как и при работе с другими языками программирования системы iSeries.

Аплеты Java

Аплеты Java - это небольшие программы на Java, которые можно размещать на страницах HTML. Аплеты запускаются на компьютере клиента, и поэтому их действия не относятся к системе, в которой работает Web-сервер. Тем не менее, аплет Java может получить доступ к системе iSeries. (К системе iSeries также могут обращаться программы, в которых используются интерфейсы ODBC и APPC.) В общем случае, аплеты Java могут устанавливать соединения только с тем сервером, с которого они были загружены. Поэтому аплет Java, работающий в удаленной системе PC, может получить доступ к серверу iSeries только в том случае, если он был загружен с этого сервера (например, с Web-сервера).

Аплет может попытаться подключиться к любому порту TCP/IP системы. При этом он может не обращаться к программному серверу, написанному на Java. Но если на сервере установлено серверное программное обеспечение, разработанное с использованием IBM Toolbox for Java, то аплет при подключении к серверу должен предоставить ИД пользователя и пароль. В данном контексте под сервером понимается система iSeries. (Серверное программное обеспечение, написанное на Java, может быть создано без применения IBM Toolbox for Java). Как правило, классы IBM Toolbox for Java предлагают пользователю ввести ИД и пароль при первом подключении.

Аплет сможет использовать функциональные возможности сервера iSeries только в том случае, если у пользовательского профайла есть права доступа к этим функциям. Таким образом, при реализации новых функций приложений с помощью аплетов Java необходимо разработать надежную схему защиты ресурсов. При обработке запросов, поступающих от аплетов, система не учитывает параметр ограничения возможностей пользовательского профайла.

Программа запуска аплетов позволяет проверить работу аплетов в системе сервера, но она не учитывает ограничений прав доступа, установленных для браузера. Поэтому программу запуска аплетов следует использовать только для проверки собственных аплетов. Никогда не пользуйтесь этой программой для запуска аплетов, полученных из посторонних источников. Аплеты Java часто записывают данные на диски пользовательской системы PC, что позволяет аплетам выполнять потенциально опасные действия. Тем не менее, для проверки подлинности аплетов Java можно использовать цифровые сертификаты. Аплет с цифровой подписью может выполнять даже те операции, которые запрещены браузеру по умолчанию, - например, записывать данные на локальные диски PC и даже на сетевые диски, которые теоретически могут быть дисками системы iSeries, подключенными к PC.

Примечание: Все приведенные выше замечания в общем случае справедливы как для Netscape Navigator, так и для MS Internet Explorer. Поведение конкретного аплета зависит от настройки вашего браузера.

Вы можете снабдить цифровой подписью все аплеты Java, загружаемые с сервера iSeries. Однако следует запретить пользователям принимать подписанные аплеты из непроверенных источников.

Начиная с выпуска V4R4, среду Secure Sockets Layer (SSL) можно настраивать с помощью IBM Toolbox for Java. Кроме того, продукт IBM Developer Toolkit for Java также позволяет обеспечивать защиту приложений на Java с помощью SSL. Поддержка SSL в приложениях Java обеспечивает шифрование данных, в том числе ИД пользователей и паролей, передаваемых между клиентскими и серверными системами. Настройку использования SSL в программах Java можно выполнять с помощью Администратора цифровых сертификатов.

Сервлеты Java

Сервлеты - это размещенные на сервере компоненты Java, которые динамически расширяют функциональные возможности Web-сервера, не меняя его программный код. Продукт IBM WebSphere Application Server, входящий в комплект поставки сервера IBM HTTP Server for iSeries, поддерживает применение сервлетов в системах iSeries.

При работе с сервлетами необходимо настроить защиту для объектов сервлетов, используемых сервером. Однако обычных средств защиты ресурсов в данном случае недостаточно. Когда сервлет загружен на Web-сервер, средства защиты ресурсов не исключают возможности запуска этого сервлета другими пользователями. Следовательно, помимо этих средств вы должны применять управляющие функции и директивы защиты сервера HTTP. Прежде всего, запретите запуск сервлетов под управлением профайла Web-сервера. Кроме того, строго ограничьте круг лиц, которые могут запускать сервлеты (воспользуйтесь директивами защиты с ключевыми словами mask). Для этого создайте необходимые группы и списки управления доступом (ACL) сервера HTTP. Кроме того, необходимо применять функции защиты, поддерживаемые средствами разработки сервлетов, такие, как функции продукта WebSphere Application Server for iSeries.

Для получения дополнительной информации об общих мерах безопасности для языка Java ознакомьтесь с перечисленными ниже разделами IBM Systems Software Information Center.

- Раздел Защита Java в описании продукта *IBM Developer Kit for Java*.
- Раздел Классы защиты в описании продукта *IBM Toolbox for Java*.

Средства идентификации и разграничения доступа в Java

Продукт IBM Toolbox for Java содержит классы защиты, позволяющие выполнять проверку ИД пользователей, а также присваивать эти ИД нитям сервлетов или приложений в операционной системе сервера iSeries. Дальнейшее управление доступом осуществляется средствами операционной системы. Дополнительная информация о классах защиты приведена в разделе Службы идентификации в IBM Systems Software Information Center IBM Toolbox for Java.

Продукт IBM Developer Kit for Java поддерживает Службу идентификации Java (JAAS), которая является стандартным расширением Комплекта для разработки приложений Java 2 (J2SDK) (Стандартный выпуск). В настоящее время J2SDK предоставляет средства управления доступом, основанные на определении источника и автора кода. Дополнительная информация о работе с J2SDK приведена в разделе Служба идентификации Java в IBM Systems Software Information Center - IBM Developer Kit for Java.

Организация защиты приложений Java с помощью SSL

Протокол Secure Sockets Layer (SSL) позволяет обеспечить защиту сетевых соединений приложений iSeries, разработанных с помощью IBM Developer Kit for Java. Клиентские приложения, в которых используется IBM Toolbox for Java, также поддерживают SSL. Реализация поддержки SSL в пользовательских приложениях на Java отличается от аналогичного процесса в других приложениях.

Дополнительная информация об администрировании протокола Secure Sockets Layer для приложений Java приведена в следующих разделах справочной системы IBM Systems Software Information Center:

- IBM Toolbox for Java, Среда Secure Sockets Layer (SSL).
- IBM Developer Toolkit for Java, Защита приложений на Java с помощью протокола SSL.

Понятия, связанные с данным

“Защита Web-сервера” на стр. 18
Предоставляя внешним пользователям доступ к своему Web-серверу, вы, скорее всего, не захотите раскрывать перед ними внутреннюю структуру сервера и подробности создания Web-страниц.

Администратор цифровых сертификатов

Службы идентификации

Задачи, связанные с данной

Защита приложений Java с помощью SSL

Информация, связанная с данной

Служба идентификации Java

Среда Secure Sockets Layer (SSL)

Защита электронной почты

Применение электронной почты в сети Internet и в любых других общедоступных сетях представляет собой определенную опасность, от которой вас не всегда сможет защитить брандмауэр.

Для того чтобы разработать эффективную стратегию защиты, необходимо четко представлять характер этой опасности.

Обмен сообщениями по электронной почте схож с другими способами связи. Рекомендуем вам быть крайне осмотрительными при отправке конфиденциальной информации по электронной почте. На пути от отправителя к получателю почтовое сообщение проходит через множество серверов, и на каждом из них оно теоретически может быть перехвачено и прочитано. Поэтому для обеспечения конфиденциальности переписки необходимо предпринять особые меры защиты.

Распространенные способы нарушения нормальной работы электронной почты

Применение электронной почты связано со следующими опасностями:

- **Лавинная рассылка** (создание помех в работе) - ситуация, когда злоумышленник перегружает систему, отправляя ей огромное число почтовых сообщений. Сравнительно несложно написать короткую программу, которая отправляет миллионы электронных сообщений (включая пустые) выбранному серверу с целью парализовать его работу. Без должной защиты сервер будет вынужден постоянно отказывать клиентам в обслуживании, поскольку его локальный диск будет переполнен ненужными сообщениями. Сервер может прекратить обслуживание и по другой причине - из-за того, что все его ресурсы будут тратиться на обработку поступивших сообщений.
- **Спам** (распространение рекламных и других ненужных сообщений). С увеличением числа организаций, предлагающих свои услуги в Internet, по сети стало передаваться огромное количество ненужной рекламной и иной информации. Такие сообщения, называемые спамом, обычно отправляются всем участникам больших списков рассылки и попадают в почтовые ящики очень многих пользователей.
- **Утечка конфиденциальной информации** - каждый раз, когда вы отправляете почту по Internet, вы сталкиваетесь с этой опасностью. Прежде чем ваше письмо попадет к получателю, оно пройдет через много неподконтрольных вам серверов. Если вы не зашифруете свое сообщение, злоумышленники могут перехватить и прочитать его в любой точке маршрута пересылки.

Средства защиты электронной почты

Для защиты от лавинной рассылки и спама вы должны правильно настроить сервер электронной почты. Большинство почтовых приложений предусматривают средства защиты от таких атак. Кроме того, вы можете обратиться к провайдеру Internet (ISP) с просьбой предоставить дополнительную защиту от таких атак.

Дополнительные меры защиты, которые необходимо предпринять, зависят от требуемого уровня конфиденциальности и от средств защиты, предусмотренных в приложениях электронной почты. Например, достаточно ли будет обеспечить конфиденциальность только содержимого электронного сообщения? Или вы хотите сделать конфиденциальной всю информацию, относящуюся к электронной почте, включая IP-адреса отправителя и получателя?

В некоторых почтовых клиентах предусмотрены встроенные средства защиты, которых может оказаться достаточно для ваших нужд. Например, приложение Lotus Notes Domino содержит встроенные функции защиты, которые позволяют, в частности, шифровать весь документ или его отдельные поля.

При шифровании электронных писем приложение Lotus Notes Domino создает уникальные личный и общий ключи для каждого пользователя. Своим личным ключом вы зашифровываете сообщение, и его смогут прочесть только пользователи, у которых есть ваш общий ключ. Таким образом, для того чтобы другие

пользователи могли расшифровывать ваши сообщения, вы должны отправить им свой личный ключ. Если вы получаете зашифрованное письмо, Lotus Notes Domino расшифровывает его с помощью общего ключа отправителя.

Сведения об этих функциях шифрования Notes приведены в электронной справочной системе программы.

Более подробная информация о средствах защиты Domino, реализованных в системе iSeries, приведена в следующих разделах:

- Справочная библиотека Lotus Domino по адресу:
  `http://www.ibm.com/eserver/iseries/domino/library.htm`
- Инфраструктура защиты Lotus Notes и Domino выпуска R5.0 (SG24-5341)
- Продукт Lotus Domino в системе AS/400: работа с электронной почтой и другими службами Internet (SG24-5990)

Организовать безопасную передачу конфиденциальной информации по открытым сетям с помощью электронной почты можно различными способами.

Если ваш почтовый сервер поддерживает протокол Secure Sockets Layer (SSL), то с помощью SSL вы можете создать защищенный сеанс между сервером и клиентами электронной почты. Кроме того, SSL поддерживает необязательную идентификацию клиента, если приложение клиента предусматривает такую идентификацию. Поскольку шифруется весь сеанс, SSL гарантирует также целостность данных во время их передачи.

Другой способ заключается в применении виртуальной частной сети (VPN). Начиная с выпуска V4R4, вы можете настроить в системе iSeries различные соединения VPN, в том числе соединения между удаленными клиентскими системами и системой iSeries. В случае применения VPN шифруется весь поток между конечными точками соединения, что гарантирует как конфиденциальность, так и целостность передаваемых данных.

Понятия, связанные с данным

Виртуальная частная сеть (VPN)

“Защита FTP”
Протокол передачи файлов (FTP) предназначен для передачи файлов между компьютерами, подключенными к сети.

“Организация многоуровневой защиты” на стр. 4
Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей системы.

Ссылки, связанные с данной

Термины, связанные с защитой

Защита FTP

Протокол передачи файлов (FTP) предназначен для передачи файлов между компьютерами, подключенными к сети.

В некоторых реализациях протокола FTP предусмотрена возможность выполнения команд на удаленных компьютерах. Протокол FTP очень удобен для работы с удаленными файловыми системами и для передачи файлов. Однако следует учитывать, что применение протокола FTP в сети Internet и в любых других общедоступных сетях представляет определенную опасность с точки зрения защиты. Для того чтобы разработать эффективную стратегию защиты, необходимо четко представлять характер этой опасности.

- Если к вашей системе разрешен доступ по протоколу FTP, то вам следует пересмотреть всю схему распределения прав доступа к объектам.

  Рассмотрим следующий пример. Предположим, что в вашей системе ограничен доступ пользователей к меню, и при этом для всех объектов установлены общие права доступа *USE. (Ограничением доступа к

меню называется режим, при котором пользователям недоступны некоторые пункты меню.) Поскольку на пользователей FTP не распространяются ограничения, связанные с меню, им автоматически становятся доступны все объекты системы.

Во избежание такой ситуации вам следует воспользоваться следующими возможностями:

– Активировать защиту объектов системы iSeries (другими словами, изменить модель защиты системы с ″защита меню″ на ″защита объектов.″ Этот вариант обеспечивает максимальную защиту.

– Написать для FTP программы выхода, запрещающие передачу определенных файлов. Эти программы выхода должны обеспечить по крайней мере тот же уровень защиты, что и программа меню. Однако в большинстве случаев требования к таким программам будут еще выше. В этом случае будет обеспечена только защита FTP; такие протоколы, как ODBC, DDM или DRDA, защищены не будут.

Примечание: Права доступа *USE допускают загрузку файлов из системы. Права доступа *CHANGE позволят пользователю FTP изменять файлы из удаленной системы.

- Злоумышленник может попытаться нарушить работу FTP посредством отключения пользовательских профайлов системы. Для этого ему достаточно несколько раз попытаться войти в систему с неверным паролем, и соответствующий пользовательский профайл будет отключен. Обычно профайл отключается после трех неудачных попыток входа в систему.

  Действия, которые вы можете предпринять во избежание такой ситуации, определяются компромиссом между надежностью защиты и простотой доступа пользователей к системе. В протоколе FTP обычно применяется системное значение QMAXSIGN, так как в противном случае злоумышленник может постепенно подобрать пароль. Ниже приведены некоторые рекомендации:

  – Воспользуйтесь программой выхода для процедуры подключения к серверу по протоколу FTP. Эта программа выхода должна отклонять попытки входа в систему с посторонних систем и под управлением пользовательских профайлов, которым при обычной работе не нужен доступ по протоколу FTP. (Такие отклоненные попытки **не** будут учитываться при проверке ограничения QMAXSIGN.)

  – Воспользуйтесь программой выхода для сервера FTP, которая будет разрешать клиентам входить в систему только с определенных удаленных систем. Например, если вы разрешаете сотруднику бухгалтерии подключаться к системе по протоколу FTP, сервер FTP должен принимать соединения только с тех IP-адресов, которые относятся к компьютерам, установленным в бухгалтерии.

  – Воспользуйтесь программой выхода для сервера FTP, которая будет записывать в журнал ИД пользователя и IP-адрес при каждой попытке входа в систему по протоколу FTP. Если вы будете регулярно просматривать протоколы, у вас будут высокие шансы обнаружить злоумышленников и предпринять соответствующие меры.

  – Приведена информация о обнаружении атак типа ″отказ в обслуживании″.

Однако при необходимости можно разрешить даже анонимный доступ с ограниченными правами к серверу FTP. Для организации защищенного анонимного сервера FTP необходимо подключить программы выхода к точкам выхода сервера, соответствующим входу в систему **и** запросу на идентификацию.

Для защиты сеансов FTP можно применять протокол Secure Sockets Layer (SSL). Применение SSL гарантирует, что вся информация, передаваемая по протоколу FTP, будет шифроваться. Это обеспечивает конфиденциальность всех данных, включая имена пользователей и пароли. Сервер FTP также поддерживает идентификацию клиентов с помощью цифровых сертификатов.

В дополнение к этим возможностям защиты FTP, можно предоставить пользователям доступ к неконфиденциальной информации с помощью анонимной пользовательской учетной записи. Анонимный FTP позволяет предоставлять открытый доступ (без пароля) к части информации, размещенной в удаленной системе. Информация, к которой предоставляется общий доступ, определяется настройками удаленной системы. Эта информация считается общедоступной и к ней могут обращаться любые пользователи. Перед настройкой анонимной учетной записи для FTP необходимо оценить потенциальные опасности и рассмотреть возможность защиты сервера FTP с помощью программ выхода.

- Настройка анонимного FTP.

- Управление доступом к службе FTP с помощью программ выхода.

Дополнительная информация о протоколе FTP, возможных опасностях при его применении и соответствующих мерах защиты приведена в следующих разделах:

- Раздел Реализация защиты FTP в системе справки IBM Systems Software Information Center.
- Раздел Анонимный FTP в системе справки IBM Systems Software Information Center.
- Раздел Защита FTP с помощью протокола SSL в системе справки IBM Systems Software Information Center.

Понятия, связанные с данным

"Защита электронной почты" на стр. 22
Применение электронной почты в сети Internet и в любых других общедоступных сетях представляет собой определенную опасность, от которой вас не всегда сможет защитить брандмауэр.

Виртуальная частная сеть (VPN)

"Организация многоуровневой защиты" на стр. 4
Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей системы.

Обнаружение вторжений

Ссылки, связанные с данной

Термины, связанные с защитой

Средства защиты на уровне передачи данных

Описаны средства, которыми можно воспользоваться для защиты данных, передаваемых по открытым сетям (например, Internet). К этим средствам относится протокол Secure Sockets Layer (SSL), iSeries Access Express и виртуальные частные сети (VPN).

Напомним, что в нашем примере компании JKL Toys принадлежат две системы iSeries. Одна из них применяется для разработки продуктов, а вторая используется в производственных целях. Обе системы работают с крайне важными данными и программами. Руководство компании принимает решение установить третью систему iSeries и подключить ее к внешней сети для обработки сетевых приложений и приложений Internet.

За счет этого компании удастся организовать физическое отделение внутренней сети от Internet, что снижает вероятность причинения какого-либо ущерба со стороны Internet. Благодаря тому, что новая система iSeries выполняет только функции сервера Internet, компании удалось упростить схему управления защитой сети.

Поскольку обеспечение безопасности в среде Internet является первостепенной задачей, компания IBM продолжает разработку решений по защите сети, позволяющих обеспечить безопасное выполнение операций электронного бизнеса при работе в Internet. При работе в среде Internet обязательно должна быть обеспечена защита как на уровне системы, так и на уровне приложений. Перемещение конфиденциальной информации по внутренней сети и тем более по Internet требует серьезных мер по организации защиты. В частности, необходимо принять меры по защите данных при их передаче по Internet.

Опасности, связанные с передачей данных между незащищенными системами, можно минимизировать с помощью двух специальных продуктов защиты данных для системы iSeries: протокола Secure Sockets Layer (SSL) и виртуальных частных сетей (VPN).

Защита приложений с помощью SSL

Протокол Secure Sockets Layer (SSL) на сегодня является фактическим стандартом защиты сеансов связи между клиентами и серверами. Первоначально протокол SSL разрабатывался для браузеров, но теперь он поддерживается и многими другими приложениями. Поддержка SSL в системе iSeries включает:

- Сервер IBM HTTP Server for iSeries (стандартный и на основе Apache)
- Сервер FTP

- Сервер Telnet
- Архитектура распределенных реляционных баз данных (DRDA) и управление распределенными данными
- (DDM)
- Функция Централизованное управление Навигатора iSeries
- Сервер служб каталогов (LDAP)
- Приложения iSeries Access Express, включая Навигатор iSeries, и приложения, разработанные с помощью набора прикладных программных интерфейсов (API) iSeries Access Express
- Программы, разработанные с помощью продукта Developer Kit for Java и клиентские приложения, в которых используется IBM Toolkit for Java
- Программы, разработанные с помощью API Secure Sockets Layer (SSL), которые позволяют применять SSL в приложениях. Информация о написании программ, применяющих SSL, приведена в разделе API Secure Sockets Layer.

Некоторые из вышеперечисленных приложений также поддерживают идентификацию клиентов с помощью цифровых сертификатов. В основе протокола SSL лежат цифровые сертификаты, позволяющие идентифицировать клиентов и серверов и создавать защищенное соединение.

Виртуальные частные сети (VPN) системы iSeries

Система iSeries позволяет создавать защищенные соединения между конечными точками с помощью VPN. Так же, как и в протоколе SSL, предусмотрена возможность шифрования данных и идентификации отправителей. Однако соединения VPN позволяют управлять параметрами защиты для каждого отдельно взятого соединения. Поэтому соединения VPN частично обеспечивают и защиту на уровне сети.

Что выбрать?

Оба способа защиты связаны с поставленной задачей: обеспечить конфиденциальность, подлинность и целостность при передаче данных. Выбор зависит от нескольких факторов. Вы должны учесть, с кем вы устанавливаете соединение, какие приложения применяются для связи, насколько защищенным должно быть соединение и какие издержки в стоимости и производительности вы готовы понести в связи с защитой этого соединения.

Учтите также следующее обстоятельство: протокол SSL может применяться только теми приложениями, которые специально рассчитаны на его применение. Несмотря на то, что многие приложения по-прежнему не поддерживают SSL, многие другие, такие как Telnet и iSeries Access Express, позволяют применять протокол SSL. В отличие от SSL, соединения VPN позволяют защитить весь поток данных между двумя конечными точками соединения.

Например, в вашей среде может применяться протокол SSL для HTTP для обмена данными с деловым партнером в пределах внутренней сети. Если Web-сервер является единственным приложением, поток данных которого должен быть защищен, то вам совершенно не обязательно переходить на VPN. Однако если вам нужно защищать много разнообразных потоков данных, будет целесообразно перейти на VPN. Кроме того, VPN может оказаться оптимальным вариантом в ситуациях, когда вам нужна полная защита данных на каком-либо участке сети, но при этом вы не хотите отдельно настраивать каждый клиент и сервер для применения SSL. В этом случае можно создать соединение VPN между шлюзами, лежащими на этом участке сети. При этом весь поток данных будет защищен, но это никак не отразится на работе серверов и клиентов, лежащих за шлюзами.

Понятия, связанные с данным

“Организация многоуровневой защиты” на стр. 4
Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей системы.

“Пример организации электронной коммерции в компании JKL Toys” на стр. 9
В этом разделе приведен пример организации электронной коммерции в компании JKL Toys, которая

решила воспользоваться возможностями, предоставляемыми Internet. Хотя мы сами выдумали эту компанию, ее стратегия защиты и способ ведения дел в Internet очень близки к реальному положению дел во многих компаниях.

“Применение цифровых сертификатов для SSL”
Цифровые сертификаты - это основной инструмент для надежной идентификации и защищенного обмена данными с помощью протокола SSL.

“Организация защищенного обмена данными с помощью виртуальных частных сетей (VPN)” на стр. 28
С помощью виртуальных частных сетей (VPN) можно обеспечить защищенную передачу данных между системами, принадлежащими одной организации.

Ссылки, связанные с данной

API Secure Sockets Layer

Применение цифровых сертификатов для SSL

Цифровые сертификаты - это основной инструмент для надежной идентификации и защищенного обмена данными с помощью протокола SSL.

Сервер iSeries позволяет управлять цифровыми сертификатами, а также быстро создавать цифровые сертификаты для систем и пользователей с помощью Диспетчера цифровых сертификатов (DCM), входящего в состав i5/OS.

Кроме того, цифровые сертификаты могут применяться в различных приложениях, таких как IBM HTTP Server for iSeries, в качестве более надежного средства идентификации, чем традиционные имя пользователя и пароль.

Что такое цифровой сертификат?

Цифровой сертификат - это электронный документ, удостоверяющий личность его владельца, подобно паспорту. Цифровые сертификаты выдаются пользователям и серверам специальными **сертификатными компаниями** . Основанием для доверия к цифровому сертификату как удостоверению личности служит доверие к CA.

Для того чтобы получить сертификат, вам нужно предоставить в сертификатную компанию определенную информацию о себе. Состав этой информации зависит от конкретной компании. В некоторых компаниях для получения сертификата достаточно предоставить отличительное имя - имя лица или сервера, на которое будет выписан цифровой сертификат. Для каждого цифрового сертификата создается пара ключей, состоящая из общего и личного ключа. Общий ключ входит в состав сертификата, а личный хранится в браузере или в защищенном файле. Пара ключей, связанная с сертификатом, используется для ″подписания″ и шифрования данных - например, отправляемых сообщений или документов. Цифровые подписи гарантируют подлинность и целостность документов.

Дополнительная информация о работе с Диспетчером цифровых сертификатов приведена в IBM Systems Software Information Center.

Несмотря на то, что многие приложения по-прежнему не поддерживают SSL, многие другие, такие как Telnet и iSeries Access Express, позволяют применять протокол SSL. Дополнительная информация о применении SSL при работе с приложениями iSeries приведена в разделе **Защита приложений с помощью SSL** IBM Systems Software Information Center.

Понятия, связанные с данным

“Средства защиты на уровне передачи данных” на стр. 25
Описаны средства, которыми можно воспользоваться для защиты данных, передаваемых по открытым сетям (например, Internet). К этим средствам относится протокол Secure Sockets Layer (SSL), iSeries Access Express и виртуальные частные сети (VPN).

Администратор цифровых сертификатов

защита приложений с помощью протокола SSL

Ссылки, связанные с данной

Термины, связанные с защитой

Применение SSL для защиты Telnet

На сервере Telnet можно настроить применение протокола Secure Sockets Layer (SSL) для защиты сеансов Telnet.

Для этого настройте сертификат, который будет применять сервер Telnet, с помощью Диспетчера цифровых сертификатов (DCM). По умолчанию сервер Telnet принимает как защищенные, так и незащищенные соединения, но при необходимости его можно настроить таким образом, чтобы он применял только защищенные соединения. Кроме того, вы можете настроить на сервере Telnet применение цифровых сертификатов для расширенной идентификации клиента.

Применение протокола SSL с Telnet обеспечит серьезную дополнительную защиту. Помимо идентификации пользователей, сервер Telnet будет шифровать все передаваемые данные. После установки сеанса SSL все данные, передаваемые по протоколу Telnet, включая ИД и пароли пользователей, будут передаваться в зашифрованном виде.

Основной фактор, который должен влиять на выбор сервера Telnet (защищенного или незащищенного), - это степень важности информации, передаваемой между сервером и клиентом. Если информация является важной или конфиденциальной, то возможно, предпочтительнее будет настроить сервер iSeries Telnet с поддержкой SSL. Если приложению Telnet системы iSeries будет выдан цифровой сертификат, то сервер Telnet сможет работать как с незащищенными клиентами, так и с клиентами SSL. Если ваша стратегия защиты предполагает обязательное шифрование сеансов Telnet, вы можете запретить применение незащищенных сеансов Telnet. Когда необходимость применения SSL с Telnet отпадет, порт SSL можно отключить. (Для отключения портов применяется команда ADDTCPPORT.) В этом случае сервер Telnet будет поддерживать только незащищенные соединения Telnet.

Более подробная информация о Telnet и рекомендации по защите данных в случае применения Telnet без SSL приведены в разделе IBM Systems Software Information Center документа Telnet. Прежде чем использовать Telnet в системе iSeries, следует ознакомиться с этой информацией.

Понятия, связанные с данным

Безопасный Telnet

Цифровой сертификат

Применение SSL для защиты iSeries Access Express

Серверы iSeries Access Express позволяют настроить применение протокола Secure Sockets Layer (SSL) для защиты соединений iSeries Access Express.

Применение SSL позволяет обеспечить надежное шифрование всех сеансов iSeries Access Express, что гарантирует конфиденциальность связи.

Дополнительная информация о применении SSL для защиты сеансов iSeries Access Express приведена в разделе IBM Systems Software Information Center:

- Администрирование Secure Sockets Layer
- IBM Developer Kit for Java SSL
- IBM Java Toolbox SSL

Организация защищенного обмена данными с помощью виртуальных частных сетей (VPN)

С помощью виртуальных частных сетей (VPN) можно обеспечить защищенную передачу данных между системами, принадлежащими одной организации.

С появлением и развитием виртуальных частных сетей (VPN) компания JKL Toys решила начать обмен данными через Internet. Она недавно приобрела другую небольшую фирму по производству игрушек, которая будет выполнять функции филиала. Фирме JKL потребуется передавать информацию из филиала в головное отделение и обратно. В обеих организациях используются серверы iSeries, и соединения VPN обеспечивают защищенную передачу данных между системами. Затраты на обслуживание обычных некоммутируемых линий существенно выше, чем затраты на организацию VPN.

Сети VPN позволяют создавать защищенные соединения с филиалами, сотрудниками, работающими вне офиса, поставщиками, деловыми партнерами и другими заинтересованными лицами.

Преимущества VPN особенно актуальны для следующих пользователей:

- Пользователи, работающие вне офиса и находящиеся в командировках.
- Филиал, соединенный с головным предприятием и другими отделениями фирмы.
- Деловые партнеры.

Если вы не ограничиваете доступ пользователей к областям, где хранится конфиденциальная информация, то вы сильно рискуете. В такой ситуации высока вероятность утечки важной для вас информации. Вам необходимо разработать схему предоставления доступа к информации о системе. С помощью VPN вы сможете передавать защищенные данные через открытые сети, не рискуя тем, что кто-либо сможет перехватить их. Создав несколько соединений VPN, вы сможете установить независимые режимы доступа для каждого из них. Например, можно настроить специализированное соединение VPN между бухгалтерией и отделом кадров.

Наибольшей опасности ваши конфиденциальные данные подвергаются при пересылке через открытые сети, где они не защищены от перехвата. Решение проблемы заключается в применении шифрования и идентификации для обеспечения конфиденциальности и защиты от атак извне. Сети VPN позволяют решить конкретную проблему - проблему защиты соединений между системами. Сеть VPN защищает данные, которыми обмениваются две конечные точки соединения. Кроме того, вместе с правилами фильтрации пакетов она может применяться для фильтрации IP-пакетов.

Сети VPN позволяют создавать защищенные соединения для обмена данными между контролируемыми и защищенными конечными системами. Тем не менее, вы должны соблюдать осторожность, предоставляя права доступа партнерам по VPN. Сети VPN зашифровывают данные при их передаче по общим сетям. Однако, если сеть настроена неправильно, поток данных может быть направлен через Internet, минуя сеть VPN. В таком случае (данные передаются по внутренним сетям, между которыми установлено соединение) VPN не выполняет шифрование. Следовательно, вам необходимо тщательно планировать настройку каждого конкретного соединения VPN. Убедитесь в том, что вы предоставили партнеру по VPN права доступа именно к тем хостам и ресурсам в вашей внутренней сети, к которым вы хотели их предоставить.

Например, у вас может быть поставщик, которому нужно получать информацию о том, какими компонентами вы располагаете. Эта информация хранится в базе данных, используемой для обновления Web-страниц в вашей внутренней сети. Вы можете разрешить поставщику прямой доступ к этим страницам через соединение VPN. Однако при этом поставщику должен быть запрещен доступ к другим ресурсам вашей системы, например, к самой базе данных. К счастью, сеть VPN можно настроить таким образом, чтобы поток данных между двумя конечными системами проходил только через порт 80. Порт 80 используется по умолчанию при обмене данными по протоколу HTTP. Следовательно, поставщик сможет отправлять и получать запросы HTTP и отвечать на них только по этому соединению.

Поскольку вы можете явно указать, какие данные можно передавать через VPN, соединение VPN позволяет управлять защитой на уровне сети. Однако в VPN регулирование потока, проходящего в систему и выходящего из нее, происходит не так, как в брандмауэре. Кроме того, VPN - это не единственное средство для защищенной передачи данных между системами iSeries и другими системами. Возможно, в вашей ситуации целесообразнее применять протокол SSL.

Ответ на вопрос о том, способна ли VPN предоставить защиту в нужном объеме, зависит от того, что именно вы хотите защитить и на какие компромиссы вы готовы пойти, чтобы обеспечить такую защиту. В любом случае, какое бы решение о защите вы ни приняли, вам необходимо определить, каким образом VPN может поддержать вашу стратегию защиты.

Дополнительная информация о соединениях VPN приведена в разделе *Виртуальные частные сети* справочной системы IBM Systems Software Information Center.

Понятия, связанные с данным

“Средства защиты на уровне передачи данных” на стр. 25
Описаны средства, которыми можно воспользоваться для защиты данных, передаваемых по открытым сетям (например, Internet). К этим средствам относится протокол Secure Sockets Layer (SSL), iSeries Access Express и виртуальные частные сети (VPN).

Виртуальные частные сети (VPN)

Термины, связанные с защитой

Приводятся термины, связанные с защитой информации, и их определения.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

authentication
Идентификация. Идентификацией называется проверка подлинности клиентов и серверов. После идентификации вы можете быть уверены, что ваш партнер по обмену данными - именно тот, за кого он себя выдает.

B

C

certificate authority (CA)
Сертификатная компания (CA). Компания, выдающая цифровые сертификаты и осуществляющая управление ими.

cipher Шифр. То же самое, что алгоритм шифрования.

ciphertext
Зашифрованная информация (текст или данные).

cracker
Взломщик. Лицо, пытающееся получить несанкционированный доступ к информации или обойти системы защиты.

cryptography
Криптография. Раздел математики, в котором изучаются способы шифрования данных. Программы и устройства, в которых применяются криптографические методы защиты информации от посторонних лиц, называются средствами шифрования. Шифрованием называется процесс преобразования данных, в результате которого становится невозможной правильная интерпретация данных. Обратное преобразование называется дешифрованием. Оба процесса представляют собой применение некоторого математического алгоритма к шифруемым или дешифруемым данным и к некому секретному блоку данных (ключу).

Методы шифрования можно разделить на два класса:

- **Симметричные**: взаимодействующие стороны имеют одинаковый секретный ключ, используемый как для шифрования, так и для дешифровки. Такая система также называется шифрованием с совместным ключом.
- **Несимметричные**: у каждой стороны есть два ключа, общий и частный. Они математически связаны между собой, но получить один из другого практически невозможно. Сообщение,

зашифрованное с помощью общего ключа, можно расшифровать только с помощью соответствующего личного ключа. Частный ключ можно использовать для создания электронной подписи к документу, а общий - для проверки этой подписи. Если хэш подписи, расшифрованной с помощью открытого ключа, соответствует хэшу документа, то подпись и документ считаются подлинными. Такая система также называется шифрованием с открытым ключом.

D

data confidentiality
Защита данных. Скрытие содержимого сообщения (обычно с помощью алгоритмов шифрования).

data integrity
Целостность данных. При проверке целостности устанавливается, не была ли дейтаграмма изменена при передаче (это может произойти как вследствие злого умысла, так и из-за технических неполадок).

data origin authentication
Проверка отправителя. Устанавливается, была ли дейтаграмма действительно отправлена указанной в ней системой.

denial of service attack
Отказ в обслуживании (DoS). Превышение пропускной способности сети в результате создания большого потока данных. Вследствие этого службы, такие как Web-серверы, становятся недоступными.

digital certificate
Цифровой сертификат. Электронный документ, удостоверяющий личность его владельца подобно паспорту. Цифровые сертификаты выдаются пользователям и организациям специальными сертификатными компаниями (CA). Основанием для доверия к цифровому сертификату как удостоверению личности служит доверие к CA. Цифровые сертификаты применяются для выполнения следующих задач:

- Определение ИД пользователей.
- Идентификация пользователей.
- Проверка подлинности документов, полученных по сети, по цифровой подписи отправителей.
- Подтверждение того, что пользователь действительно отправил какую-либо информацию. Например, у покупателя, оплатившего товары по сети Internet с помощью кредитной карты, не должно быть возможности оспорить факт оплаты.

digital signature
Цифровая подпись. Электронный аналог личной подписи на бумажном документе. Цифровая подпись гарантирует подлинность происхождения документа. Отправитель подписывает документы с помощью личного ключа, связанного с его сертификатом. Получатели документов дешифруют его подпись с помощью соответствующего общего ключа и убеждаются в подлинности отправителя.

Digital Certificate Manager (DCM)
Диспетчер цифровых сертификатов. Благодаря DCM iSeries может выполнять функции локальной сертификатной компании (CA). С помощью DCM можно создавать цифровые сертификаты для серверов и пользователей. Помимо этого, можно импортировать сертификаты, выданные другими CA. Цифровой сертификат можно также связать с пользовательским профайлом i5/OS. DCM позволяет программам применять протокол SSL для организации защищенного обмена данными по сети.

distinguished name
Отличительное имя. Имя лица или сервера, на которое выписан цифровой сертификат. Это - официальное имя владельца сертификата, указанное в сертификате. Помимо отличительного имени, в сертификате может быть указана и другая информация о его владельце. Это зависит от конкретной сертификатной компании.

Domain Name System (DNS)
Система имен доменов. Набор данных, позволяющих устанавливать, кто является владельцем

цифрового сертификата. В случае цифровых сертификатов класса 1 сюда входят имя и адрес электронной почты владельца, а также название компании, выдавшей сертификат (VeriSign, Inc.).

При подключении к какому-либо хосту в сети Internet ваша программа-клиент узнает его IP-адрес у сервера DNS.

E

encryption
Шифрование. Преобразование данных, в результате которого их правильная интерпретация становится невозможной для посторонних лиц (т. е. лиц, не знающих метод шифрования и ключ). Шифрование не защищает данные от перехвата, однако для использования перехваченных данных их требуется дешифровать, что невозможно без знания алгоритма и ключа шифрования.

Enterprise Identity Mapping (EIM)
Технология преобразования идентификаторов в рамках предприятия (EIM). EIM - механизм, позволяющий связывать пользователя или систему и пользовательские профайлы в локальной среде. EIM содержит API, предоставляющий функции создания и управления профайлами, а также получения информации из профайлов.

extranet
Этим термином обозначают сегмент частной сети, расположенный снаружи корпоративного брандмауэра. В extranet используется существующая инфраструктура Internet, в том числе стандартные серверы, клиенты электронной почты и Web-браузеры. За счет этого применение сетей Extranet экономически более оправданно, чем создание и обслуживание собственной сети. Сети Extranet позволяют торговым партнерам, поставщикам и клиентам обмениваться данными через сеть Internet.

F

брандмауэр
Логический барьер, отделяющий внутреннюю сеть организации от внешней сети - например, Internet. Брандмауэр может состоять из одной или нескольких аппаратных и программных систем либо логических разделов. Он управляет доступом к внутренней сети и передачей информации между внутренними (надежными) и внешними (ненадежными) системами.

G

H

хакер Любое лицо, пытающееся получить несанкционированный доступ к системе.

hypertext links
Гипертекстовые ссылки. Способ представления информации в интерактивных системах, при котором различные информационные объекты (узлы гипертекста) связаны между собой с помощью гипертекстовых ссылок.

Hypertext Markup Language (HTML)
Язык описания гипертекстовых документов (HTML). Язык, применяемый для создания гипертекстовых документов. В языке HTML предусмотрены широкие возможности по форматированию документов и описанию связей с другими документами и объектами.

Hypertext Transfer Protocol (HTTP)
Протокол передачи гипертекстовой информации (HTTP). Стандартный протокол передачи гипертекстовых документов по сети.

I

Internet
Глобальная сеть TCP/IP, к которой подключены миллионы компьютеров, и система взаимодействующих программ, позволяющих компьютерам обмениваться информацией. В Internet хранится огромное количество информации и действуют различные службы передачи данных, электронной почты, новостей и т.д. Internet часто называют просто ″Сетью″.

клиент Internet
Программа или пользователь, отправляющие запросы к серверам по сети Internet и получающие их ответы. Для работы с различными службами Internet применяются разные программы. Примерами таких программ могут служить web-браузеры и клиенты FTP (протокола передачи файлов).

хост Internet
Любой компьютер, подключенный к Internet или к intranet. На хосте могут быть установлены различные серверы Internet - например, сервер FTP, обслуживающий запросы клиентов FTP, или сервер HTTP, обслуживающий запросы браузеров. Обычно серверы работают в фоновом (пакетном) режиме.

Internet Key Exchange (IKE) protocol
Обмен ключами Internet (IKE). Протокол IKE позволяет заинтересованным сторонам автоматически согласовывать параметры защиты, а также автоматически генерировать и обновлять ключи шифрования, используемые в виртуальной частной сети (VPN).

имя доменное
Псевдоним, используемый вместо IP-адреса хоста. Поскольку IP-адреса представляют собой длинные последовательности цифр (например: 10.5.100.75), их трудно запоминать. Поэтому IP-адресам присваивают доменные имена, например, system1.vnet.ibm.com. Эти имена называют доменными, потому что в них последовательно указаны имена всех вложенных доменов, в которых находится хост. В большинстве случаев на объявлениях вида ″посетите нашу страницу в Internet″ указаны именно доменные имена, а не IP-адреса хостов. Полное доменное имя состоит из нескольких частей. Например, имя system1.vnet.ibm.com состоит из следующих частей:

com: Указывает, что домен находится в коммерческой сети. Имена в этом домене распределяются Комитетом по присвоению имен Internet (независимой организацией). Эта часть имени различна для различных типов сетей (например, общеобразовательным организациям США обычно выделяются адреса в корневом домене *edu*, а российским организациям - в домене *ru*).

ibm: Идентификатор организации. Эта часть имени домена также присваивается Комитетом по присвоению имен Internet. Только одной организации в мире может быть предоставлен идентификатор ibm.com.

vnet: Группа систем в пределах домена ibm.com. Этот идентификатор определяется внутри организации. Администратор домена ibm.com может создать несколько таких групп по своему усмотрению.

system1:
Имя хоста в домене vnet.ibm.com.

сервер Internet
Программа или набор программ, принимающих запросы от клиентов по сети Internet и отвечающих на эти запросы. Сервер Internet можно рассматривать как независимую территорию, которую могут посещать клиенты Internet. Серверы могут обслуживать различные протоколы и службы, например:

- Просмотр гипертекстовых документов (″домашней страницы″ и связанных с ней документов и объектов).
- Передачу файлов. Клиент может запросить какие-либо файлы у сервера: например, документы, программы, перечни продукции предприятий и прочую информацию.
- Средства электронной коммерции. Клиентам может быть предоставлена возможность запрашивать информацию или заказывать какую-либо продукцию.

Internet service provider (ISP)
Провайдер Internet. Организация, предоставляющая доступ к сети Internet подобно тому, как телефонная компания предоставляет вам соединение с мировой телефонной сетью.

intranet
Внутренняя сеть организации, в которой используются средства Internet, например, браузеры или клиенты FTP.

intrusion detection

Обнаружение вторжений. Этот термин может означать обнаружение многих нежелательных действий. Целью вторжения может быть получение информации, доступ к которой не разрешен (кража информации). Возможные последствия - нанесение ущерба бизнесу путем нарушения работы сети, системы или приложения (атака вида ″отказ в обслуживании″) или получение доступа к локальной системе (за этим могут последовать дальнейшие вторжения). Большая часть вторжений выполняется по следующей схеме: сбор информации о сети, попытка доступа, и затем - деструктивные действия. Целевая система способна обнаружить и эффективно нейтрализовать лишь некоторые виды атак. Обычно при проведении атаки в IP-пакетах подменяется адрес отправителя, что делает задачу выявления этого адреса очень сложной. В настоящее время для проведения атак используются компьютеры или сети, к которым злоумышленник имеет нелегальный доступ. При этом обнаружить его становится еще труднее. Поэтому в комплекс действий по обнаружению вторжений входит сбор информации о работе сети, попытках доступа и возможных попытках вторжения.

IP address

IP-адрес. Уникальный идентификатор системы в сети TCP/IP (Internet - очень большая сеть TCP/IP). Большинству серверов Internet присвоены уникальные фиксированные IP-адреса. Клиенты Internet могут использовать временные адреса, выделенные провайдером, но эти адреса также должны быть уникальными.

IP datagram

Дейтаграмма IP. Минимальный блок информации, передаваемой по сети TCP/IP. Дейтаграмма IP (также называемая пакетом) состоит из заголовка, в котором указаны IP-адреса отправителя и получателя, и полезных данных.

IP filters

Фильтры IP. Управляют потоком данных в IP-сети, осуществляя фильтрацию пакетов в соответствии с заданными правилами. Благодаря этому внутреннюю сеть можно защитить от несанкционированного доступа извне с применением как простых, так и очень сложных методов. Фильтрацию IP-пакетов можно рассматривать как основу, на которой базируются все остальные средства защиты. Она предоставляет инфраструктуру для работы средств защиты и служит препятствием для всех взломщиков, кроме самых искушенных.

IP security (IPSec) protocol

Протокол IPSec. Набор протоколов, применяемых для защищенного обмена пакетами на уровне сети. Протоколы IPSec применяются в системе i5/OS и во многих других системах для организации виртуальных частных сетей (VPN).

IP-адреса, подмена

Попытка проникновения в систему путем имитации системы (IP-адреса), которой разрешен доступ к вашей сети. Лицо, предпринимающее попытку вторжения, присваивает своей системе IP-адрес одной из ваших доверенных систем. Фирмы-производители маршрутизаторов встраивают в свои изделия защитные механизмы, позволяющие обнаружить и отвергнуть попытки подмены адреса.

J

K

L

M

N

network address translation (NAT)

Служба преобразования сетевых адресов (NAT). NAT - это хорошая альтернатива серверам Proxy и SOCKS. Эта служба упрощает настройку сетей, поскольку она позволяет устанавливать соединения между сетями с несовместимыми структурами адресов. NAT реализует две важнейшие функции. Для этого фактический адрес сервера скрывается и заменяется на внешний адрес, к которому открыт общий доступ. NAT обеспечивает защиту внешнего Web-сервера, управление которым

осуществляется из внутренней сети организации. Кроме того, NAT позволяет пользователям внутренней сети работать с Internet, не разглашая IP-адреса своих хостов. Благодаря этому NAT обеспечивает доступ к Internet из внутренней сети, не разглашая IP-адреса ваших компьютеров.

non-repudiation
Неоспоримость. Возможность гарантированно подтвердить факт передачи или получения какой-либо информации. Для обеспечения неоспоримости важных операций (например, оплаты товаров с помощью кредитных карт по Internet) применяются цифровые подписи и шифрование данных с открытым ключом.

O

P

пакет Минимальный блок информации, передаваемой по сети TCP/IP. Пакет (также называемый дейтаграммой) состоит из заголовка, в котором указаны IP-адреса отправителя и получателя, полезных данных, а также сведений о протоколе линии связи - например, Ethernet, Token-Ring или Frame Relay.

proxy server
Сервер Proxy. Приложение TCP/IP, отвечающее за пересылку информации между клиентами, расположенными в защищенной внутренней сети, и внешними незащищенными серверами. Серверы Proxy выполняют функции барьеров, скрывающих информацию о внутренней сети (например, IP-адреса клиентов) от внешней сети. Во внешнюю сеть все запросы поступают от сервера Proxy.

public key infrastructure (PKI)
Инфраструктура общих ключей. Система цифровых сертификатов, сертификатных компаний и других регистрационных служб, обеспечивающих идентификацию участников транзакций в сети Internet.

Q

R

replay protection
Защита путем задержки. Дейтаграмма отправляется только в том случае, когда она не может быть перехвачена злоумышленником.

S

Secure Sockets Layer (SSL)
Протокол SSL был разработан компанией Netscape для шифрования сеансов связи между клиентами и серверами, и на сегодня стал стандартным протоколом, применяемым для создания защищенных сеансов связи. В SSL применяется шифрование данных с симметричным ключом. Клиент и сервер обмениваются цифровыми сертификатами, а затем выбирают симметричный ключ. Для каждого соединения между клиентом и сервером создается новый ключ. Даже в случае, если постороннему лицу удастся перехватить и расшифровать ключ сеанса (что само по себе крайне маловероятно), он будет пригоден только для расшифровки информации, передаваемой в текущем сеансе.

single sign-on (SSO):
Одиночный вход в систему. При использовании этой схемы идентификации пользователь, будучи опознан системой, получает доступ к ресурсам нескольких систем или приложений. См. Enterprise Identity Mapping.

перехват информации
Перехватом называется несанкционированное прослушивание сеансов обмена данными по сети. На пути от отправителя к получателю информация может пройти через множество маршрутизаторов. Изготовители маршрутизаторов, провайдеры Internet и разработчики операционных систем предпринимают максимальные усилия по предотвращению перехвата данных в магистральных сетях Internet. Случаи успешного перехвата данных встречаются все реже. Большинство таких случаев приходится не на магистральные линии, а на частные локальные сети, подключенные к

Internet. Тем не менее, поскольку в подавляющем большинстве случаев информация передается в незашифрованном виде, следует все же учитывать возможность ее перехвата.

SOCKS

Протокол SOCKS применяется для передачи потоков данных TCP/IP через защищенные шлюзы. Он реализован по принципу клиент-сервер. Серверы SOCKS функционально схожи с серверами Proxy.

подмена адресов

Подмена адресов - это один из способов проникновения во внутреннюю сеть, основанный на том, что взломщик присваивает своей системе IP-адрес какой-либо системы, которой разрешено подключение к вашей сети.

T

TCP/IP

Основной протокол передачи данных, используемый в Internet. Аббревиатура TCP/IP означает Transmission Control Protocol/Internet Protocol (Протокол передачи данных/протокол Internet). Протокол TCP/IP получил широкое распространение и в локальных сетях.

Trojan horse

″Троянский конь″. Компьютерная программа (либо сценарий), на первый взгляд предназначенная для выполнения полезных и не вызывающих подозрений функций. При этом такая программа содержит скрытые функции, в которых используются права доступа запустивших ее пользователей. Например, она может скопировать с компьютера конфиденциальную информацию и переслать ее своему разработчику.

U

V

virtual private network (VPN)

Виртуальная частная сеть (VPN). Один из способов объединения нескольких внутренних сетей через внешнюю сеть. С помощью VPN можно создавать защищенные каналы передачи данных (туннели) в открытых сетях. Основное назначение VPN заключается в пересылке конфиденциальной информации по открытым сетям (например, Internet). С помощью VPN можно организовать доступ к внутренней сети предприятия для:

- Удаленных пользователей
- Филиалов компании
- Деловых партнеров и поставщиков

W

браузер

Программа-клиент протокола HTTP. Браузеры позволяют просматривать гипертекстовые документы, написанные на языке HTML, в удобном для восприятия формате. Гиперссылки в тексте документа специально выделены для того, чтобы пользователь мог перейти по ним, щелкнув на них мышью. Гиперссылки часто называют **активными областями**. В настоящее время наибольшее распространение получили браузеры Internet Connection Web Explorer и Netscape Navigator.

World Wide Web (WWW)

Всемирная система связанных серверов, в которой используется единый формат документов (HTML) и единый протокол доступа к ним (HTTP). Такое название (дословный перевод WWW - **всемирная паутина**) отражает структуру этой сети с ее множеством ссылок между различными серверами и документами.

X

Y

Z

Приложение. Замечания

Настоящая документация была разработана для продуктов и услуг, предлагаемых на территории США.

IBM не распространяет продукты, службы и компоненты, описанные в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Никакие упоминания продуктов, программ и служб IBM не означают, что допустимо использовать только этот продукт, программу или службу IBM. Допускается использовать любой функционально эквивалентный продукт, программу или службу, при условии, что права интеллектуальной собственности IBM не нарушаются. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

IBM могут принадлежать патенты или заявки на патенты, относящиеся к материалам этого документа. Предоставление настоящего документа не означает предоставления каких-либо лицензий на эти патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Запросы на лицензии, связанные с информацией DBCS, следует направлять в отдел интеллектуальной собственности в местном представительстве IBM или в письменном виде по следующему адресу:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

Следующий абзац не относится к Великобритании, а также к другим странам, в которых это заявление противоречит местному законодательству: ФИРМА INTERNATIONAL BUSINESS MACHINES CORPORATION ПРЕДОСТАВЛЯЕТ НАСТОЯЩУЮ ПУБЛИКАЦИЮ НА УСЛОВИЯХ “КАК ЕСТЬ”, БЕЗ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, НЕЯВНЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КАКОЙ-ЛИБО ЦЕЛИ. В некоторых странах запрещается отказ от каких-либо явных и подразумеваемых гарантий при заключении определенных договоров, поэтому данное заявление может не действовать в вашем случае.

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право вносить изменения в продукты и/или программы, описанные в этом документе, без каких-либо уведомлений.

Все встречающиеся в данной документации ссылки на Web-сайты других компаний предоставлены исключительно для удобства пользователей и не являются рекламой этих Web-сайтов. Материалы, размещенные на этих Web-сайтах, не являются частью информации по данному продукту IBM, и ответственность за применение этих материалов лежит на пользователе.

IBM может использовать и распространять любую предоставленную вами информацию на свое усмотрение без каких-либо обязательств перед вами.

Для получения информации об этой программе для обеспечения: (i) обмена информацией между независимо созданными программами и другими программами (включая данную) и (ii) взаимного использования информации, полученной в ходе обмена, пользователи данной программы могут обращаться по адресу:

| IBM Corporation
| Software Interoperability Coordinator, Department YBWA
| 3605 Highway 52 N
| Rochester, MN 55901
| U.S.A.

Такая информация может предоставляться на определенных условиях, включая, в некоторых случаях, уплату вознаграждения.

| Описанная в этой информации лицензионная программа и все связанные с ней лицензионные материалы
| предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного
| соглашения о лицензии на программу IBM, Лицензионного соглашения о машинном коде IBM или любого
| другого эквивалентного соглашения.

Все приведенные показатели производительности были получены в контролируемой среде. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Реальные результаты могут отличаться от указанных. Пользователи, работающие с этим документом, должны удостовериться, что используемые ими данные применимы в имеющейся среде.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. IBM не выполняла тестирование этих продуктов других фирм и не может подтвердить точность заявленной информации об их производительности, совместимости и других свойствах. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

Все заявления, касающиеся намерений и планов IBM, могут изменяться и отзываться без предварительного уведомления, и отражают только текущие цели и задачи.

Все указанные цены IBM являются розничными и действующими на данный момент. Они могут быть изменены без предварительного уведомления. Цены поставщиков могут от них отличаться.

Вся информация предоставлена только для целей планирования. Информация, приведенная в данном документе, может быть изменена до выпуска описанных продуктов.

Данная информация содержит примеры данных и отчетов, применяемых в повседневных деловых операциях. Для большей наглядности примеры содержат имена, названия компаний, торговых марок и продуктов. Все имена и названия являются вымышленными; совпадения с именами, названиями и адресами реальных предприятий абсолютно случайны.

ЛИЦЕНЗИЯ НА АВТОРСКИЕ ПРАВА:

В этой публикации приведены примеры программ, иллюстрирующие технологии программирования на различных платформах. Разрешается бесплатно копировать, изменять и распространять эти примеры кода в любом виде с целью разработки, использования, рекламирования или распространения приложений, отвечающих требованиям интерфейса операционной платформы, для которой предназначены эти примеры кода. Эти примеры кода не были тщательно и всесторонне протестированы. По этой причине IBM не может гарантировать, ни прямо, ни косвенно, их правильной работы, надежности и удобства в использовании.

| Каждый экземпляр или часть этих примеров кода, как и производные от них, должны содержать следующее
| заявление об авторских правах:

| © (название вашей компании) (год). Этот код разработан на основе примеров кода фирмы IBM Corp. ©
| Copyright IBM Corp. _год или годы_. Все права защищены.

При просмотре данного документа в электронном виде фотографии и цветные иллюстрации могут не отображаться.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:

| AIX
| AIX 5L
| e(логотип)server
| eServer
| i5/OS
| IBM
| iSeries
| pSeries
| xSeries
| zSeries

| Intel, Intel Inside (эмблемы), MMX и Pentium являются товарными знаками Intel Corporation в Соединенных
| Штатах и/или других странах.

Microsoft, Windows, Windows NT и логотип Windows являются товарными знаками корпорации Microsoft в Соединенных Штатах и/или других странах.

Java и все товарные знаки на основе Java являются товарными знаками Sun Microsystems, Inc. в Соединенных Штатах и/или других странах.

| Linux является товарным знаком Линуса Торвальдса (Linus Torvalds) в США и/или других странах.

UNIX является зарегистрированным товарным знаком The Open Group в Соединенных Штатах и/или других странах.

Названия других компаний продуктов и услуг могут быть товарными или служебными знаками других компаний.

Условия

Разрешение на использование публикаций предоставляется в соответствии с следующими условиями.

Личное использование: Вы можете воспроизводить эти публикации для личного, некоммерческого использования при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается распространять, демонстрировать или использовать для создания других продуктов без явного согласия IBM.

Коммерческое использование: Вы можете воспроизводить, распространять и демонстрировать данные публикации в рамках своей организации при условии сохранения информации об авторских правах. Данные публикации, а также любую их часть запрещается воспроизводить, распространять, использовать для создания других продуктов и демонстрировать вне вашей организации, без явного согласия IBM.

На данные публикации, а также на содержащиеся в них сведения, данные, программное обеспечение и другую интеллектуальную собственность, не распространяются никакие другие разрешения, лицензии и права, как явные, так и подразумеваемые, кроме оговоренных в настоящем документе.

IBM сохраняет за собой право аннулировать предоставленные настоящим документом разрешения в том случае, если по мнению IBM использование этих публикаций может принести ущерб интересам IBM или если IBM будет установлено, что приведенные выше инструкции не соблюдаются.

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта.

IBM не несет ответственности за содержание этих публикаций. Публикации предоставляются на условиях ″как есть″, без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности, отсутствия нарушений или применения для каких-либо конкретных целей.

Напечатано в Дании