System i

Защита
System i в сети Internet

Версия 6, выпуск 1

System i

Защита
System i в сети Internet

Версия 6, выпуск 1

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Замечания”, на стр. 29.

Это издание относится к версии 6, выпуску 1, модификации 0 IBM i5/OS (код продукта 5761-SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Эта версия работает не на всех компьютерах с RISC-процессорами и не работает на компьютерах с CISC-процессорами.

Содержание

Защита System i в сети Internet

Организация доступа к Internet из локальной сети требует пересмотра требований к ее защите.

В продукте IBM System i предусмотрены аппаратные и программные средства защиты от попыток несанкционированного доступа к системе из Internet. Правильное применение этих средств защиты позволяет предоставить 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 системы, предназначенных для защиты от них. На основе этой информации вы сможете разработать собственный план организации защиты сети в соответствии с конкретными требованиями.

Защита System i в сети Internet - Файл PDF

Можно просмотреть и распечатать файл PDF с данной информацией.

Для просмотра или загрузки этого документа в формате PDF выберите Защита System i в сети Internet (около 456 КБ).

Вы можете просмотреть и загрузить следующие связанные разделы:

- Обнаружение вторжений (около 285 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.
- Преобразование идентификаторов в рамках предприятия (EIM) (около 1954 КБ). EIM - механизм, позволяющий связывать пользователя или систему (например, службу) и пользовательские профайлы в локальной среде.
- Единый вход в систему (около 1203 КБ). При использовании модели единого входа в систему пользователю необходимо реже выполнять вход в систему и помнить меньше паролей, чем при стандартных обращениях к нескольким приложениям или системам.
- Планирование и настройка защиты системы (около 3992 КБ). В этом документе рассмотрена процедура эффективного и систематического планирования и настройки защиты уровня системы.

Сохранение PDF-файлов

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

1. Щелкните правой кнопкой мыши на приведенной ссылке на документ PDF.
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 файлов PDF необходима программа Adobe Reader. Бесплатную копию этой программы можно загрузить с Web-сайта Adobe по адресу Web-сайт Adobe

(www.adobe.com/products/acrobat/readstep.html) .

Понятия, связанные с данным

Обнаружение вторжений

Технология преобразования идентификаторов в рамках предприятия (EIM)

Единый вход в систему

Планирование и установка защиты системы

Рекомендации по защите System i в сети Internet

При работе с Internet защита данных является одной из наиболее важных проблем. В этом разделе приведена общая информация о предложениях и функциях защиты i5/OS.

При подключении платформы System i к сети Internet, как правило, возникает следующий вопрос: ″Что мне необходимо знать о защите в Internet?″. Этот раздел поможет найти ответ на этот вопрос.

Объем необходимой информации зависит от того, каким образом вы хотите 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.

Примечание: Если вы не знакомы с базовыми понятиями защиты при работе с Internet, то обратитесь к разделу Терминология защиты.

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.

Характеристики защиты i5/OS

Помимо специализированных средств защиты, ориентированных на работу с Internet, операционная система i5/OS обладает следующими характеристиками защиты:

- 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 операционной системе i5/OS файлы не могут быть приняты за программы, а программы не могут изменять друг друга . Средства обеспечения целостности i5/OS 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. Планировщик конфигурации защиты поможет вам определить, какие рекомендации по организации защиты отвечают вашим потребностям.

Дополнительные средства защиты i5/OS

В операционной системе i5/OS 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. VPN - это интегрированная функция операционной системы i5/OS, к которой можно обратиться из интерфейса System i Navigator.
- Правила обработки пакетов - это интегрированная функция операционной системы i5/OS, к которой можно обратиться из интерфейса System i Navigator. Она позволяет настраивать правила фильтрации IP-пакетов и преобразования сетевых адресов (NAT), с помощью которых можно управлять потоком входящих и исходящих данных TCP/IP системы.
- 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. Поддержка протокола SSL реализована во многих приложениях, включая IBM HTTP Server for i5/OS, System i Access for Windows, протокол передачи файлов (FTP), Telnet и т.д.

  Понятия, связанные с данным

  “Стратегия защиты и ее задачи” на стр. 6
  Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей.

  “Организация защищенного обмена данными с помощью виртуальных частных сетей (VPN)” на стр. 26
  Виртуальная частная сеть (VPN) - это расширение внутренней сети компании на основе уже существующей общей или частной сети. обеспечивающее конфиденциальный и защищенный обмен данными в пределах организации.

  “Пример организации электронной коммерции в компании JKL Toys” на стр. 8
  В процессе планирования электронного бизнеса рекомендуется обратиться к сценарию типичной компания JKL Toy, которая планирует расширить свой бизнес, воспользовавшись для этого возможностями Internet.

  Информация, связанная с данной

  Подключение к Internet

  Планировщик конфигурации защиты eServer

  Фильтрация IP-пакетов и преобразование сетевых адресов

  Secure Sockets Layer

  AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet PDF

Планирование защиты при работе с Internet

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. В зависимости от конкретных особенностей предстоящей работы с Internet вы сможете правильно оценить потребности в защите.

Например, необходимо описать следующую информацию:

- Текущая конфигурация сети.
- Конфигурации DNS и почтового сервера.
- Соединение с поставщиком услуг Internet (ISP).
- Необходимые службы Internet.
- Службы, которые планируется 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).

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 i5/OS позволяет избежать многих потенциальных опасностей. Однако если система 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:

- **Пассивные атаки**

  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.
- **Активные атаки**

  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 возникнет обязательно. 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.

Защита на уровне сети
Средства защиты на уровне сети управляют доступом к операционной системе i5/OS и другим системам в 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.

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.

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 систем. 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.

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. 10
Перед подключением к сети Internet следует выбрать уровень защиты системы.

“Средства защиты на уровне сети” на стр. 11
Для защиты внутренних ресурсов выберите подходящий уровень защиты сети.

“Средства защиты на уровне приложений” на стр. 16
Рисками защиты ряда популярных приложений и служб Internet можно управлять несколькими способами.

“Средства защиты на уровне передачи данных” на стр. 23
Для защиты данных во время их передачи по незащищенным сетям, таким как Internet, следует принять адекватные меры защиты. В частности, рекомендуется использовать протокол Secure Sockets Layer (SSL), System i Access for Windows и виртуальные частные сети (VPN).

“Стратегия защиты и ее задачи”
Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей.

“Защита электронной почты” на стр. 20
Применение электронной почты в сети Internet и в любых других незащищенных сетях всегда связано с определенным риском даже при наличии брандмауэра.

Ссылки, связанные с данной

Руководство по защите System i для IBM i5/OS версии 5, выпуска 4

Стратегия защиты и ее задачи

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

Стратегия защиты

Любая служба Internet, предоставляемая или используемая системой, 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.

Задачи стратегии защиты

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

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 System i 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 операционной системе i5/OS этот компонент защиты требует минимального внимания, так как он является фундаментальной составляющей архитектуры i5/OS. В частности, в архитектуре i5/OS практически невозможно умышленное изменение системных программ, если вы работаете с уровнем защиты 40 или 50.

Неоспоримость

Гарантирует, что транзакция произошла - например, что пользователь отправил или получил сообщение. 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) или соединения

виртуальной частной сети (VPN). 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.

Понятия, связанные с данным

“Рекомендации по защите System i в сети Internet” на стр. 2
При работе с Internet защита данных является одной из наиболее важных проблем. В этом разделе приведена общая информация о предложениях и функциях защиты i5/OS.

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

Настройка DCM

Secure Socket Layer (SSL)

“Пример организации электронной коммерции в компании JKL Toys”
В процессе планирования электронного бизнеса рекомендуется обратиться к сценарию типичной компания JKL Toy, которая планирует расширить свой бизнес, воспользовавшись для этого возможностями Internet.

Пример организации электронной коммерции в компании JKL Toys

В процессе планирования электронного бизнеса рекомендуется обратиться к сценарию типичной компания JKL Toy, которая планирует расширить свой бизнес, воспользовавшись для этого возможностями Internet.

JKL Toy - это небольшая, но быстро растущая компания по производству самых разных игрушек. Президент компании с большим энтузиазмом относится к расширению бизнеса и к возможности упростить выполнение задач, связанных с ростом компании, с помощью операционной системы i5/OS. Функции системного администратора системы возложены на Шэрон Джонс, главного бухгалтера фирмы.

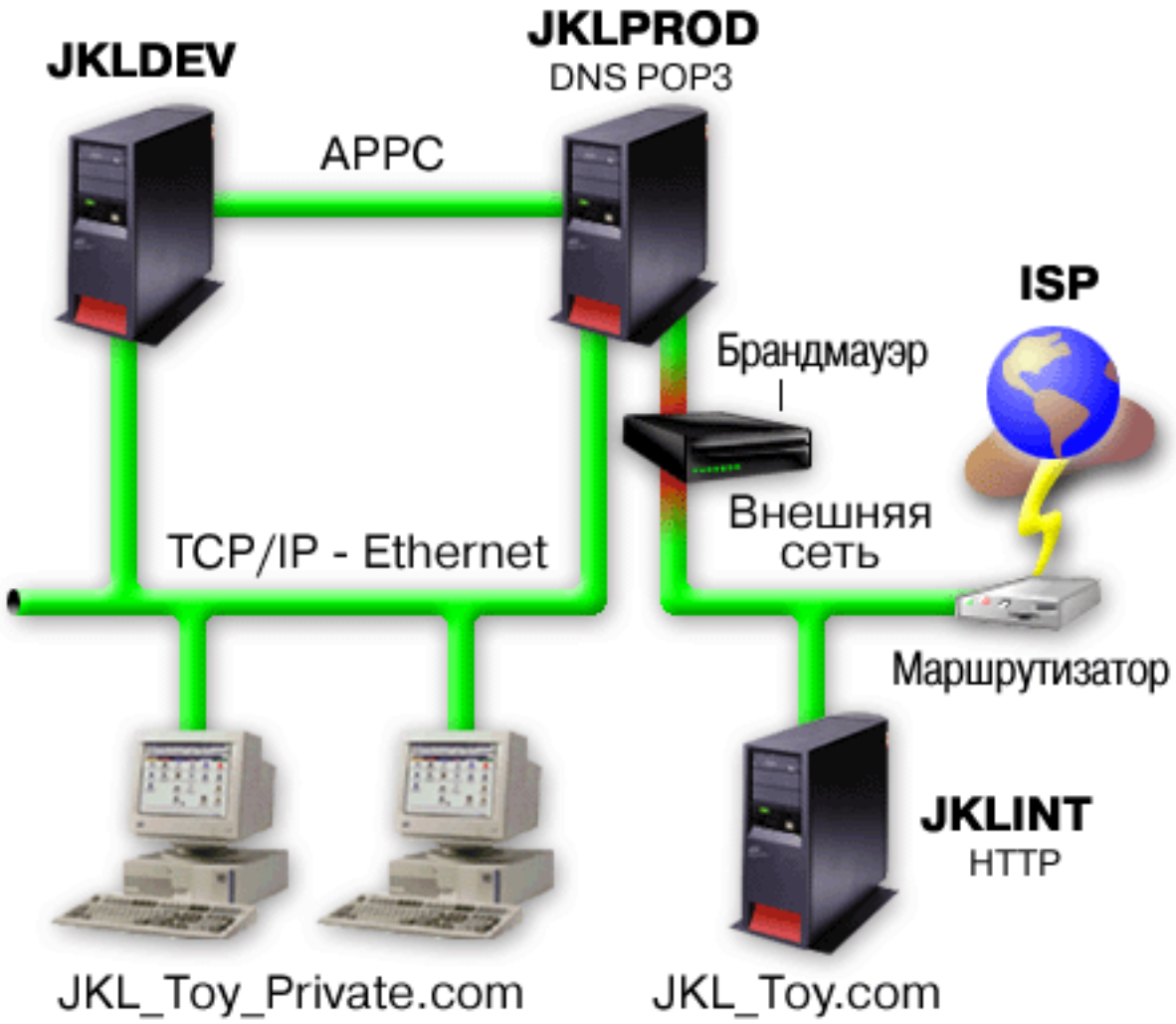
Компания JKL Toys сначала разработала стратегию защиты для внутренней сети, которая успешно применялась в течение года. Теперь возникла потребность повысить эффективность внутреннего обмена информацией, а также подключить свою сеть к Internet. В дальнейшем компания собирается создать серьезное маркетинговое 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 конце концов компания хочет предоставить заказникам возможность непосредственного заказа товаров с помощью Web-сайта. 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. Шэрон отвечает 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 в надежности защиты систем, она решила создать брандмауэр для организации защиты на уровне сети. Брандмауэр будет защищать внутреннюю сеть от многих

потенциальных опасностей, исходящих со стороны Internet. На следующем рисунке показана конфигурация сети компании.



Как показано на рисунке, в компании JKL Toys используются две основные системы. 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 (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 будет выполнять только функции сервера Internet, компания также сможет упростить управление системами защиты сети.

В новой системе 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
Стратегия защиты определяет, какие объекты вы защищаете и каких действий вы ожидаете от пользователей.

“Рекомендации по защите System i в сети Internet” на стр. 2
При работе с Internet защита данных является одной из наиболее важных проблем. В этом разделе приведена общая информация о предложениях и функциях защиты i5/OS.

“Средства защиты на уровне сети” на стр. 11
Для защиты внутренних ресурсов выберите подходящий уровень защиты сети.

“Средства защиты на уровне передачи данных” на стр. 23
Для защиты данных во время их передачи по незащищенным сетям, таким как Internet, следует принять адекватные меры защиты. В частности, рекомендуется использовать протокол Secure Sockets Layer (SSL), System i Access for Windows и виртуальные частные сети (VPN).

Базовые уровни защиты при подключении к Internet

Перед подключением к сети Internet следует выбрать уровень защиты системы.

Общие средства защиты формируют главную линию обороны вашей системы от потенциальных опасностей, связанных с подключением внутренней сети к Internet. Первым шагом по настройке общей стратегии защиты при работе в Internet является правильная настройка основных параметров защиты i5/OS. Для выполнения минимальных требований к защите системы следует выполнить следующие задачи:

- Уровень защиты (системное значение QSECURITY) 50. Это обеспечивает максимальную степень защиты целостности, что рекомендуется при работе в столь опасной с точки зрения защиты среде, как Internet.

  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. Обратитесь к справочнику по защите System i.
- Установите системные значения, связанные с защитой, так, чтобы уровни ограничений были не ниже рекомендуемых. Установить рекомендуемые параметры защиты можно с помощью Мастера установки защиты System i Navigator.
- 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.

Минимальные требования защиты системы можно настроить с помощью Планировщика конфигурации eServer или мастера защиты, к которому можно обратиться из интерфейса System i Navigator. Планировщик конфигурации защиты задаст вам несколько вопросов и на основе ваших ответов даст ряд рекомендаций, которые помогут вам правильно настроить параметры защиты системы. В отличие от планировщика конфигурации защиты мастер настраивает параметры защиты с учетом рекомендаций.

Правильная настройка внутренних средств защиты системы i5/OS позволяет избежать многих потенциальных опасностей. Однако если система подключена к открытой сети (например, Internet), то необходимо принять дополнительные меры защиты для обеспечения безопасности внутренней сети организации. После настройки общих параметров защиты 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.

Ссылки, связанные с данной

Системное значение Уровень защиты

Справочник по защите

Средства защиты на уровне сети

Для защиты внутренних ресурсов выберите подходящий уровень защиты 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.

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.

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.

Необходимо уделить пристальное внимание вопросу использования брандмауэра в качестве основного средства защиты системы как при подключении системы к внутренней сети, так и при подключении к Internet. Несмотря на то, что продажа и поддержка брандмауэра IBM Firewall for i5/OS в настоящее время прекращена, вы можете воспользоваться рядом других продуктов.

Поскольку коммерческие брандмауэры предоставляют полный набор технологий защиты сети, компания JKL Toys решила выбрать один из них для защиты своей сети. Поскольку выбранный брандмауэр не защищает операционную систему, была добавлена дополнительная функция защиты на основе правил обработки пакетов i5/OS. Такой подход позволил создать фильтр и правила NAT, управляющие потоком данных Web-сервера.

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. 8
В процессе планирования электронного бизнеса рекомендуется обратиться к сценарию типичной компания JKL Toy, которая планирует расширить свой бизнес, воспользовавшись для этого возможностями Internet.

Обнаружение вторжений

Информация, связанная с данной

Redbook: 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 выполняет следующие функции:

- 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) повышает эффективность защиты 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
  - Разделенная система 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 общедоступной системе, расположенной 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). 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 обработки пакетов i5/OS

Правила обработки пакетов i5/OS обеспечивают защиту системы. Правила обработки пакетов - это функции операционной системы i5/OS, к которым можно обратиться из интерфейса System i Navigator.

Правила обработки пакетов позволяют настроить контроль потоков данных TCP/IP в базовых технологиях защиты:

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

Поскольку NAT и функция фильтрации IP-пакетов являются встроенными функциями операционной системы 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: Надежность применяемой системы защиты важнее ее стоимости. Для обеспечения достаточной защиты рабочей системы настоятельно рекомендуется использовать брандмауэр.

Преобразование сетевых адресов и фильтрация IP-пакетов

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 операционную систему i5/OS 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 System i Navigator 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 разрешенные и запрещенные IP-пакеты. 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.

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 общедоступные IP-адреса. Однако хотя фильтрация IP-пакетов и служба NAT обеспечивают очень хорошую защиту, они не заменят вам брандмауэр. Рекомендуется тщательно проанализировать задачи, стоящие перед вашей системой защиты, и решить, можете ли вы отказаться от брандмауэра в пользу правил фильтрации пакетов i5/OS.

Понятия, связанные с данным

преобразование сетевых адресов (NAT)

Фильтрация IP-пакетов

Обнаружение вторжений

Обнаружение вторжений предусматривает сбор информации об атаках и попытках несанкционированного доступа через сеть TCP/IP. В состав общей стратегии защиты входит раздел, посвященный обнаружению вторжений.

Термин *обнаружение вторжений* в документации по i5/OS имеет два значения. Первое из них относится к обнаружению рисков нарушения защиты и противодействию им. Например, хакер может попытаться проникнуть в систему с помощью недопустимого ИД пользователя или неопытный пользователь с правами администратора может изменять важные объекты в системных библиотеках.

Второе значение относится к новой функции обнаружения вторжений, которая отвечает за поиск подозрительных потоков данных с помощью стратегий. Приведенная в документе информация поможет создать стратегию обнаружения вторжений, позволяющую получать информацию о подозрительных событиях в сети TCP/IP.

Выбор средств защиты сети i5/OS

В соответствии с планами использования Internet следует выбрать средства защиты сети.

В основе средств защиты сети от несанкционированного доступа лежат технологии брандмауэра. В качестве средства защиты системы 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 i5/OS.

Выбор между правилами фильтрации пакетов и брандмауэром определяется сетевой средой, требованиями к доступу и потребностями защиты. Необходимо уделить пристальное внимание вопросу использования брандмауэра в качестве основного средства защиты системы как при подключении системы к внутренней сети, так и при подключении к Internet или другой незащищенной сети.

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.

Примечание: Можно одновременно настроить брандмауэр и интегрированные функции защиты сети i5/OS. Такой подход позволяет защитить систему от внутренних атак (в обход брандмауэра), а также атак, проникающих сквозь брандмауэр вследствие ошибок конфигурации или по другим причинам.

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, то он

может 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.

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 операционной системы i5/OS, например, общедоступного Web-сервера или внутренней сети, содержащей конфиденциальные данные. • Защищает подсеть внутренней корпоративной сети, используя операционную систему i5/OS в качестве шлюза (маршрутизатора) для связи с остальной сетью. • Управляет соединением с частично защищенным компьютером с помощью частной сети или внешней сети, в которой операционная система i5/OS 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.

Ссылки, связанные с данной

Фильтрация IP-пакетов и преобразование сетевых адресов

HTTP Server for i5/OS

Информация, связанная с данной

Сценарии защиты Интернет AS/400: Практический подход

Средства защиты на уровне приложений

Рисками защиты ряда популярных приложений и служб Internet можно управлять несколькими способами.

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,

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. Необходимо 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 и реализовали выбранные модели защиты. Для этой цели необходимо выбрать одну из встроенных функций защиты IBM HTTP Server for i5/OS.

Раздел книги IBM HTTP Server (powered by Apache) Redbook  , посвященный развертыванию защиты, содержит инструкции по реализации функций защиты с помощью идентификации, управления доступом и шифрования.

Протокол HTTP позволяет только просматривать данные. Его возможностей недостаточно, если вам требуется изменить какую-либо информацию в базе данных. Однако в некоторых случаях может потребоваться разработать дополнительные приложения, отвечающие за обновление файла базы данных. Например, можно создать формы, которые после заполнения будут обновлять базу данных i5/OS. Для этой цели можно использовать программы Common Gateway Interface (CGI).

Дополнительную функцию защиты представляет собой сервер Proxy. Он принимает запросы, отправленные другим серверам, и затем выполняет, пересылает, перенаправляет или отклоняет их.

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

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.

Понятия, связанные с данным

“Защита Java в сети Internet”
Java все чаще применяется в современных вычислительных сетях и системах. Вы должны быть готовы принять особые меры защиты, связанные с применением Java.

Информация, связанная с данной

Типы серверов Proxy и особенности их совместного применения с сервером HTTP (на основе Apache)

Рекомендации по защите сервера HTTP

Common Gateway Interface

Защита Java в сети Internet

Java все чаще применяется в современных вычислительных сетях и системах. 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.

Java, приложения

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 применяются строгие правила контроля типов без исключений, 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 Java следует принимать такие же меры защиты, как и при работе с другими языками программирования системы.

Аплеты Java

Аплеты Java - это небольшие программы Java, которые можно добавлять на страницы HTML. Они выполняются на клиенте и могут обладать доступом к операционной системе i5/OS. Кроме того, к операционной системе также могут обращаться программы, в которых используются интерфейсы ODBC и APPC. Например, если система обслуживает приложения или применяется в качестве Web-сервера. В общем случае, аплеты Java могут устанавливать соединения только с той операционной системой i5/OS, из которой они были загружены. Таким образом, аплет Java, работающий в удаленном компьютере, обладает доступом к операционной системе i5/OS только в том случае, если он был загружен из этой операционной системы i5/OS.

Аплет может попытаться подключиться к любому порту TCP/IP системы. При этом он может не обращаться к программному серверу, написанному на Java. Системы, разработанные с помощью IBM Toolbox for Java, дополнительно запрашивают у аплета идентификационные данные. В этом документе рассматриваются только операционные системы i5/OS. (Сервер приложений Java не требует 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 операционной системы i5/OS 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 операционной системе i5/OS, 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 компьютера пользователя, 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, подключенными к PC.

Вы можете снабдить цифровой подписью все аплеты Java, загружаемые из системы. 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 (DCM).

Сервлеты Java

Сервлеты - это размещенные на сервере компоненты Java, которые динамически расширяют функциональные возможности Web-сервера, не изменяя его программный код. Продукт IBM WebSphere Application Server, входящий в состав IBM Web Enablement for i5/OS, обеспечивает поддержку сервлетов в операционных системах i5/OS.

При работе с сервлетами необходимо настроить защиту для объектов сервлетов, используемых системой. 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, необходимо применять функции защиты, поддерживаемые средствами разработки сервлетов, такие, как функции продукта WebSphere Application Server for i5/OS.

Для получения дополнительной информации об общих мерах безопасности для языка Java ознакомьтесь с перечисленными ниже ресурсами:

- IBM Developer Kit for Java: Защита Java.
- IBM Toolbox for Java: Классы защиты.
- Защита браузеров при работе с Internet.

Идентификация Java для ресурсов

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 i5/OS. Дальнейшее управление доступом осуществляется средствами операционной системы.

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.

Защита приложений Java с помощью протокола SSL

Протокол Secure Sockets Layer (SSL) позволяет обеспечить защиту сетевых соединений приложений i5/OS, 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.

Понятия, связанные с данным

“Защита Web-сервера” на стр. 17
Предоставляя внешним пользователям доступ к своему Web-серверу, вы, скорее всего, не захотите раскрывать перед ними внутреннюю структуру сервера и подробности создания Web-страниц. Необходимо создать простой и удобный интерфейс, в котором вся черновая работа выполняется незаметно для пользователя.

Настройка DCM

Службы идентификации

Информация, связанная с данной

Служба идентификации Java
Secure Sockets Layer (SSL)

Защита электронной почты

Применение электронной почты в сети Internet и в любых других незащищенных сетях всегда связано с определенным риском даже при наличии брандмауэра.

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

Обмен сообщениями по электронной почте схож с другими способами связи. Важно быть крайне осмотрительными при отправке конфиденциальной информации по электронной почте. На пути от отправителя к получателю почтовое сообщение проходит через множество систем, в каждой из которых 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. Система может прекратить обслуживание и по другой причине - из-за того, что все ее 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 систем. 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.

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). В системе можно настроить различные соединения VPN, в том числе соединения с удаленными клиентами. В случае применения VPN шифруется весь поток между конечными точками соединения, что гарантирует как конфиденциальность, так и целостность передаваемых данных.

Понятия, связанные с данным

"Защита FTP"
Протокол передачи файлов (FTP) предназначен для передачи файлов между компьютерами, подключенными к сети. Эффективная стратегия защиты должна учитывать все риски защиты, связанные с применением FTP.

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

Виртуальная частная сеть (VPN)

Ссылки, связанные с данной

Термины, связанные с защитой

Информация, связанная с данной

Библиотека справочной информации по Lotus Domino

Документация по Lotus

Redbook: Lotus Notes and Domino R5.0 Security Infrastructure Revealed

Redbook: Lotus Domino for AS/400 Internet Mail and More

Защита FTP

Протокол передачи файлов (FTP) предназначен для передачи файлов между компьютерами, подключенными к сети. Эффективная стратегия защиты должна учитывать все риски защиты, связанные с применением FTP.

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. Учитывая эти риски, вы обеспечиваете более эффективную защиту системы.

- 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 i5/OS (другими словами, вместо защиты меню применить защиту объектов. Это оптимальный и наиболее безопасный вариант).
– 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. Данный вариант обеспечивает только защиту FTP; остальные интерфейсы, такие как ODBC, DDM или DRDA, не защищаются.

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 путем 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.
  – Воспользуйтесь системой обнаружения вторжений для обнаружения 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.

Понятия, связанные с данным

“Защита электронной почты” на стр. 20
Применение электронной почты в сети Internet и в любых других незащищенных сетях всегда связано с определенным риском даже при наличии брандмауэра.

Задачи, связанные с данной

Настройка анонимной работы с протоколом передачи файлов

Управление доступом с помощью программ выхода FTP

Информация, связанная с данной

Защита FTP

Защита сервера FTP с помощью SSL

Средства защиты на уровне передачи данных

Для защиты данных во время их передачи по незащищенным сетям, таким как Internet, следует принять адекватные меры защиты. В частности, рекомендуется использовать протокол Secure Sockets Layer (SSL), System i Access for Windows и виртуальные частные сети (VPN).

Напомним, что в сценарии компании JKL рассматриваются две основные системы. 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 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 будет выполнять только функции сервера Internet, компания также сможет упростить управление системами защиты 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.

Риски, связанные с передачей данных между незащищенными системами, можно минимизировать с помощью двух специальных продуктов защиты данных операционной системы i5/OS: протокол SSL и VPN.

Протокол SSL - это отраслевой стандарт защиты данных, передаваемых между клиентами и серверами. Первоначально протокол SSL разрабатывался для браузеров, но теперь он поддерживается и многими другими приложениями. В частности, следующими приложениями операционной системы i5/OS:

- IBM HTTP Server for i5/OS (стандартный и на основе Apache)
- Сервер FTP
- Сервер Telnet
- Сервер архитектуры распределенных реляционных баз данных (DRDA) и управления распределенными данными (DDM)
- Функция Централизованное управление в System i Navigator
- Сервер служб каталогов (LDAP)
- Приложения System i Access for Windows, включая System i Navigator, и приложения, разработанные с помощью API System i Access for Windows
- 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.

Виртуальная частная сеть

Соединение VPN позволяет защитить данные, передаваемые между между двумя конечными точками. 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.

Выбор метода

SSL и VPN обеспечивают конфиденциальность, подлинность и целостность при передаче данных. Выбор зависит от нескольких факторов. Следует 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 System i Access for Windows, 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. 8
В процессе планирования электронного бизнеса рекомендуется обратиться к сценарию типичной компания JKL Toy, которая планирует расширить свой бизнес, воспользовавшись для этого возможностями Internet.

Ссылки, связанные с данной

API SSL

Информация, связанная с данной

Secure Sockets Layer (SSL)

Виртуальная частная сеть (VPN)

Применение цифровых сертификатов для SSL

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

Операционная система i5/OS 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 i5/OS, 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 (CA) . Основанием для доверия к цифровому сертификату как удостоверению личности служит доверие к CA.

У каждой CA есть стратегия, определяющая идентификационную информацию, которую необходимо предоставить для получения сертификата. В некоторых компаниях для получения сертификата достаточно предоставить отличительное имя - имя лица или системы, на которое будет выдан 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.

Несмотря на то, что многие приложения по-прежнему не поддерживают SSL, многие другие, такие как Telnet и System i Access for Windows, позволяют применять протокол SSL.

Понятия, связанные с данным

Настройка DCM

Secure Sockets Layer (SSL)

Ссылки, связанные с данной

Термины, связанные с защитой

Защита Telnet с помощью протокола Secure Sockets Layer

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 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. Применением SSL в сеансах Telnet можно управлять с помощью параметра Разрешить SSL (ALWSSL) команды Изменить атрибуты Telnet (CHGTELNA). Для дополнительного ограничения доступа приложений к портам SSL и незащищенными портам воспользуйтесь командой Добавить ограничение порта TCP/IP (ADDTCPPORT).

Более подробная информация о Telnet в операционной системе i5/OS и рекомендации по защите данных в случае применения Telnet без SSL приведены в разделе IBM Systems Software Information Center, посвященном Telnet.

Понятия, связанные с данным

Сценарий Telnet: Защита Telnet с помощью SSL

Планирование работы с DCM

Информация, связанная с данной

Telnet

Защита System i Access for Windows с помощью Secure Sockets Layer

Соединения System i Access for Windows можно защитить с помощью протокола Secure Sockets Layer (SSL).

Применение SSL позволяет обеспечить надежное шифрование всех сеансов System i Access for Windows, что гарантирует конфиденциальность связи.

Информация, связанная с данной

Администрирование Secure Sockets Layer

Защита Java

Классы защиты

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

Виртуальная частная сеть (VPN) - это расширение внутренней сети компании на основе уже существующей общей или частной сети. обеспечивающее конфиденциальный и защищенный обмен данными в пределах организации.

С появлением и развитием 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 операционные системы i5/OS и соединения VPN обеспечивают защищенную передачу данных между сетями. Затраты на обслуживание обычных некоммутируемых линий существенно выше, чем затраты на организацию VPN.

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. 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 операционной системой i5/OS 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.

Понятия, связанные с данным

“Рекомендации по защите System i в сети Internet” на стр. 2
При работе с Internet защита данных является одной из наиболее важных проблем. В этом разделе приведена общая информация о предложениях и функциях защиты i5/OS.

Виртуальные частные сети (VPN)

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 этом документе 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, Соглашения о лицензии на машинный код 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.

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. Работа примеров не была проверена во всех возможных условиях. 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.

Информация об интерфейсе программирования

В публикации Защита System i в сети Internet приведена информация об интерфейсах программирования панели управления, позволяющих заказчикам создавать программы, использующие службы IBM i5/OS.

Товарные знаки

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

Domino
Distributed Relational Database Architecture (DRDA)
i5/OS
IBM
IBM (эмблема)
Lotus Notes
Notes
System i
WebSphere

Adobe, эмблема Adobe, PostScript и эмблема PostScript являются товарными знаками или зарегистрированными товарными знаками Adobe Systems Incorporated в США 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.

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

Условия и соглашения

Разрешение на использование этих публикаций предоставляется в соответствии с следующими условиями и соглашениями.

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 эти 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