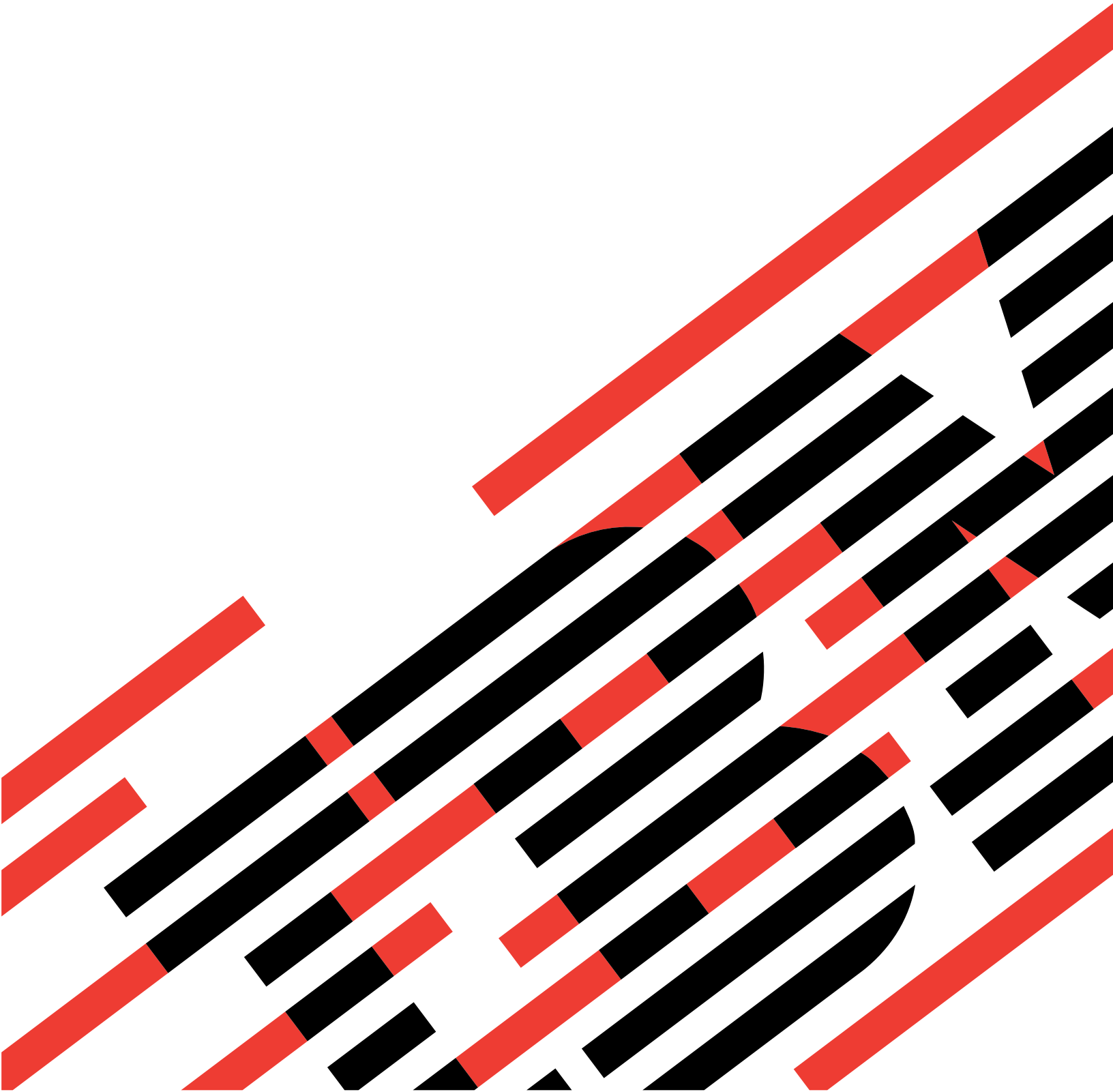
IBM

eserver

iSeries

IBM SecureWay: iSeries 400 и Internet



IBM

@server

iSeries

IBM SecureWay: iSeries 400 и Internet

Содержание

Часть 1. IBM SecureWay: iSeries и Internet

Организация доступа к Internet из локальной сети требует серьезной модернизации сети и коренного пересмотра требований к ее защите. В системе iSeries 400 предусмотрены программные и аппаратные средства защиты от попыток несанкционированного доступа к сети из Internet. Рациональное применение этих средств защиты позволит организовать удобный доступ к данным для ваших клиентов, сотрудников и деловых партнеров без какого-либо риска для конфиденциальной информации.

В этом разделе приведена информация о стандартных способах нарушения защиты и об их возможном влиянии на работе с Internet и средствами электронной коммерции. Кроме того, здесь описаны достоинства и недостатки различных приемов и средств защиты системы iSeries. На основе этой информации вы сможете разработать собственный план организации защиты сети в соответствии с конкретными требованиями. Чрезвычайно важно выбрать правильную стратегию защиты.

Дополнительная информация о возможных нарушениях защиты при работе с Internet и предусмотренных в системе iSeries средствах защиты приведена в следующих разделах:

- **Новое в выпуске V5R1**
  Изменения и дополнения к предусмотренным в системе iSeries средствам защиты при работе с Internet, появившиеся в выпуске V5R1.
- **Как напечатать этот раздел**
  Инструкции по печати PDF-версии этого раздела (с помощью Adobe Acrobat).
- **Защита системы iSeries при подключении к Internet**
  Общее представление об организации защиты электронного бизнеса в системе iSeries и доступных средствах защиты.
- **Планирование защиты при работе с Internet**
  Рекомендации по созданию стратегии защиты при работе с Internet и средствами электронного бизнеса
- **Базовые уровни защиты системы iSeries при подключении к Internet**
  Информация об обязательных средствах защиты при подключении к Internet.
- **Средства защиты на уровне сети**
  Информация о приемах организации защиты на уровне сети, применяемых для защиты внутренних ресурсов.
- **Средства защиты на уровне приложений**
  Сведения о потенциальных опасностях для большинства распространенных приложений и служб Internet и средствах организации защиты этих приложений и служб.
- **Средства защиты на уровне передачи данных**
  Информация о том, какие меры можно принять для защиты данных во время их передачи по открытым сетям - таким, как Internet. Здесь вы найдете подробную информацию о протоколе Secure Sockets Layer (SSL), продукте Client Access Express и организации виртуальных частных сетей (VPN).
- **iSeriesСредства защиты на уровне Internet**
  Сведения о средствах защиты iSeries, которые помогут вам организовать защиту систем и ресурсов в соответствии с вашими планами по работе с Internet и средствами электронного бизнеса.

Примечание: Если вам нужна базовая информация о защите и сети Internet, рекомендуем вам обратиться к разделу Терминология, применяемая в средствах защиты информации Internet.

Глава 1. Новое в выпуске V5R1

В выпуске V5R1 в предлагаемые средства защиты для системы iSeries 400 внесены несколько улучшений и дополнений. Ниже рассмотрены наиболее важные из них:

- **Усовершенствования продукта Диспетчер цифровых сертификатов (DCM)**
  Теперь с помощью DCM вы можете создавать и контролировать сертификаты, применяемые для цифрового подписывания объектов с целью обеспечения их целостности и подтверждения их подлинности. Вы также можете создавать и контролировать соответствующие сертификаты проверки подписи, с помощью которых вы или другие пользователи могут идентифицировать подпись объекта и удостовериться в его целостности и подлинности. Кроме того, с помощью DCM или соответствующих API вы можете подписать объект или проверить его подпись.
- **Операционная система с цифровой подписью**
  Начиная с выпуска V5R1 операционная система OS/400 и лицензионные программные продукты (LPP) фирмы IBM поставляются с цифровой подписью. Пользователи могут удостовериться в том, что программы фирмы IBM не подвергались изменениям с момента их подписания. Проверку цифровой подписи можно выполнить во время восстановления, либо введя команду CHKOBJITG. Кроме того, теперь поставляются специальные API, с помощью которых заказчики и деловые партнеры смогут подписывать и проверять свои собственные приложения.
- **Новые правила создания паролей пользовательских профайлов (QPWDLVL 2 и 3)**
  Максимальная длина пароля пользовательского профайла увеличена до 128 символов. В паролях учитывается регистр букв и допускаются внутренние пробелы. Пример допустимого пароля: ″This is my New Password.″ Конечные пробелы отсекаются; пароли не могут состоять целиком из пробелов.
- **Усовершенствования в системе управления паролями пользовательских профайлов**
  Для управления уровнем паролей в системе предусмотрено новое системное значение QPWDLVL, которое может принимать любое из следующих четырех значений:
  - PWDLVL 0 — Допустимы пароли длиной до 10 байт; пароли Netserver поддерживаются. Это значение по умолчанию.
  - PWDLVL 1 — Допустимы пароли длиной до 10 байт; пароли Netserver не поддерживаются.
  - PWDLVL 2 — Допустимы пароли длиной до 128 символов; пароли, соответствующие старому или новому формату, поддерживаются.
  - PWDLVL 3 — Допустимы пароли длиной до 128 символов; пароли, соответствующие старому формату, не поддерживаются.
- **Повышение надежности хранения ключей с помощью IBM 4758–023 PCI Cryptographic Coprocessor**
  Если в системе установлен IBM 4758–023 PCI Cryptographic Coprocessor, то с его помощью вы можете повысить надежность хранения цифровых сертификатов. При создании или обновлении сертификатов с помощью DCM вы можете задать опцию хранения ключа непосредственно в сопроцессоре, либо с помощью главного ключа сопроцессора зашифровать личный ключ и сохранить его в специально предназначенном для этого файле. Кроме того, при хранении ключей на сопроцессоре вы можете повысить производительность приложений, применяющих протокол Secure Sockets Layer (SSL), поскольку сопроцессор берет на себя задачу дешифровки личного ключа для процедуры согласования SSL. Вы также можете распределить выполнение согласования SSL по 4758 картам.

- **Поддержка сертификатов в Виртуальной частной сети (VPN)**
  В выпусках до V5R1 серверы Обмена ключами Internet (IKE) VPN могли идентифицировать друг друга только посредством подготовленного ключа. Однако применение такого ключа небезопасно, поскольку его необходимо вручную передавать администратору целевой конечной системы VPN. Следовательно, существует вероятность перехвата этого ключа во время его передачи. В выпуске V5R1 этот недостаток устранен - теперь конечные точки могут идентифицировать друг друга посредством цифровых сертификатов. С помощью Диспетчера цифровых сертификатов (DCM) вы можете управлять сертификатами, применяемыми сервером IKE для установления динамического соединения VPN.
- **Усовершенствования поддержки Secure Sockets Layer (SSL) в приложениях**
  В выпуске V5R1 появилось несколько усовершенствований, относящихся к SSL. Теперь вы можете настраивать защищенные SSL-сеансы по протоколу FTP iSeries. Вы также можете настроить на сервере FTP применение цифровых сертификатов для идентификации клиента. Кроме того, начиная с выпуска V5R1 OS/400 поддерживает 128-разрядное шифрование AES. AES - это новый, более эффективный алгоритм шифрования, который пришел на смену DES.
- **Усовершенствования Простого протокола передачи почты (SMTP)**
  Теперь SMTP поддерживает черные списки на основе полей Субъект, Отправитель и IP-адрес.
- **Мастер настройки Internet**
  Широко распространенный Мастер настройки Internet, который ранее предоставлялся в виде загружаемого файла, теперь доступен непосредственно в Навигаторе AS/400. С помощью этого Мастера вы можете настроить соединение системы iSeries с Internet и защитить его автоматически создаваемыми правилами фильтрации.
- **Усовершенствования в схеме повторного создания программ**
  Программы, разработанные для систем iSeries выпуска V5R1 или выше, содержат информацию, позволяющую при необходимости создавать программу заново во время восстановления. Такая информация остается в программе даже в случае удаления информации наблюдаемости. Если при проверке программы во время восстановления в ней обнаружится ошибка, то программа будет создана заново, что позволит исправить ошибку. Операцию повторного создания программы во время восстановления нельзя назвать нововведением выпуска V5R1 iSeries. В предыдущих выпусках любая ошибка при проверке программы во время восстановления приводила к повторному созданию программы при условии, что это было возможно (если в восстанавливаемой программе существовала информация наблюдаемости). Отличие системы iSeries выпуска V5R1 или выше состоит в том, что информация, необходимая для создания программы заново, доступна в любом случае, даже если информация наблюдаемости удалена. Таким образом, начиная с выпуска V5R1 любая программа, при проверке которой обнаруживается ошибка, создается заново во время восстановления, а ее прежняя версия, послужившая причиной ошибки, удаляется.

Глава 2. Как напечатать этот раздел

Вы можете просмотреть и загрузить этот документ в формате PDF. Для просмотра и печати файлов в формате PDF нужна программа Adobe Acrobat Reader. Эту программу можно загрузить с домашней страницы Adobe. 

Для просмотра или загрузки этого документа в формате PDF щелкните на ссылке IBM SecureWay: iSeries и Internet (416 Кб, 60 страниц).

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

1. Откройте файл в формате PDF в браузере (щелкните на ссылке выше).
2. Откройте меню **Файл** браузера.
3. Выберите пункт **Сохранить как...**
4. Выберите каталог, в котором нужно сохранить файл.
5. Нажмите кнопку **Сохранить**.

Глава 3. Защита системы iSeries 400 при подключении к Internet

Оценивая необходимость подключения внутренней сети к Internet, вы обычно задаете себе следующий вопрос: ″Как использовать возможности Internet в деловых целях?″ Второй вопрос: ″Что следует знать о защите данных в Internet?″ Данный раздел поможет вам ответить на второй вопрос.

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

Перед тем как вы начнете работу с Internet, вам необходимо решить, что именно вы хотите делать и каким образом. Принятие решений об использовании Internet и о защите передаваемой по Internet информации может быть достаточно сложным делом. Перед началом разработки собственного плана работы с Internet рекомендуем вам ознакомиться с разделом Пример организации электронной коммерции в компании JKL Toys. Если вам нужна базовая информация о защите и сети Internet, обратитесь к разделу Терминология, применяемая в средствах 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.

Параметры средств защиты системы iSeries

Помимо специализированных средств защиты, ориентированных на работу с Internet, в системе iSeries 400 предусмотрена очень надежная и высокоэффективная общая схема защиты. Ниже описаны некоторые ее характеристики:

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

Security Advisor - эта программа поможет вам определить, какие рекомендации по организации защиты отвечают вашим потребностям.

Дополнительные средства защиты системы iSeries

В системе iSeries предусмотрен комплекс функций защиты, повышающих безопасность системы при работе в 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. Поддержка VPN встроена в операционную систему OS/400; для работы с ней применяется интерфейс Навигатора AS/400.
- Правила фильтрации пакетов - это интегрированная функция операционной системы OS/400. Она предусмотрена в Навигаторе AS/400. С ее помощью вы можете задать правила фильтрации IP-пакетов и задействовать службу преобразования сетевых адресов (NAT) для управления исходящим и входящим потоками данных TCP/IP.
- 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. В настоящее время многие серверы системы iSeries поддерживают протокол SSL, в том числе IBM HTTP Server для iSeries, Client Access Express и Telnet.

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, связанных с этим, 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.

Примечание: Подробную информацию о том, как использовать Internet в деловых целях, можно найти в следующих разделах Information Center и публикациях:

- *Подключение к Internet*
- Руководство *AS/400 Internet Security: Protecting Your AS/400 from HARM on the Internet* (SG24-4929).

Глава 4. 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. На основе этого вы сможете правильно определить необходимые меры по защите системы.

Например, вы должны записать и проанализировать информацию о:
- текущей конфигурации вашей сети
- конфигурации DNS и почтового сервера
- соединении с поставщиком услуг Internet (ISP)
- необходимых вам службах Internet
- службах, которые вы намерены предоставить пользователям Internet

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

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

После того как вы определите стратегию работы с Internet и выберете систему защиты, рекомендуем вам еще раз изучить следующие разделы:
- В разделе **Организация многоуровневой защиты** приведена информация о наиболее важных моментах, которые следует учесть при разработке системы защиты.
- Раздел **Задачи системы защиты** содержит полезные сведения о том, каким условиям должна удовлетворять эффективная схема защиты.
- В разделе **Пример организации электронной коммерции в фирме JKL Toys** вы найдете пример схемы защиты для организации средних размеров. Вы можете создать собственную схему на основе предложенного примера.

Несмотря на то, что продукт IBM Firewall for AS/400 более не поддерживается, при выборе стратегии рекомендуем вам воспользоваться его формами планирования. В этих формах вы можете подробно записать важную информацию о конфигурации внутренней сети, требованиях к системе защиты и предполагаемому характеру работы с Internet. Формы приведены в разделе Начало работы с брандмауэром продукта iSeries Information Center V4R5. Большая часть этих сведений потребуется вам независимо от того, планируете ли вы использовать брандмауэр при работе с Internet.

Организация многоуровневой защиты

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

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

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

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

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

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

Многоуровневая защита

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

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

Защита на уровне системы
Общие средства защиты формируют главную линию обороны вашей системы от потенциальных опасностей, связанных с подключением внутренней сети к Internet. Поэтому первоочередной задачей при планировании подключения к Internet будет настройка общих средств защиты системы.

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

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 серверов. Если вы не предпримете специальных мер по защите данных (например, можно воспользоваться протоколом SSL для шифрования передаваемой информации), они будут доступны практически всем желающим. Средства защиты на уровне передачи данных призваны обеспечить сохранность данных по пути от отправителя к адресату.

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.

Стратегия защиты и ее задачи

Стратегия защиты

Любая служба Internet, предоставляемая или используемая вашей системой iSeries, является дополнительным фактором риска не только для системы iSeries, 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 при 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 риски. Пример стратегии защиты, применяемой в компании JKL Toys, приведен в разделе ″Общая информация о защите системы″ продукта iSeries Information Center.

Задачи стратегии защиты

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

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

Идентификация
Система защиты должна обладать возможностью проверки того, что

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

Разграничение доступа

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

Проверка подлинности

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

- **Целостность данных**: означает защиту данных от несанкционированного изменения или подлога. Обеспечение целостности данных позволяет устранить возможность перехвата и подмены данных посторонними лицами. Помимо защиты данных в пределах сети, вам могут потребоваться дополнительные меры защиты в случае, если вы получаете информацию из открытой сети. Если вы получаете данные из открытой сети, то вам необходимо предпринять такие меры безопасности, которые могли бы обеспечить:
  - Защиту данных от посторонних лиц. Поскольку абсолютно исключить возможность перехвата данных невозможно, рекомендуется передавать их в зашифрованном виде.
  - Целостность передаваемых данных. Это необходимо для того, чтобы исключить возможность подмены.
  - Гарантированную доставку данных. Вам может пригодиться электронный аналог заказной почты или уведомлений о вручении почтовых отправлений.
- **Целостность системы**: способность системы сохранять стабильность работы при заданном уровне нагрузки. В системе iSeries этот компонент защиты требует минимального внимания, так как он является фундаментальной составляющей архитектуры iSeries. В частности, в системе iSeries практически невозможно злонамеренное изменение системных программ, если вы работаете с уровнем защиты 40 или 50.

Неоспоримость

Неоспоримостью называется возможность гарантированно подтвердить факт передачи или получения какой-либо информации. Для обеспечения неоспоримости важных операций (например,

оплаты товаров с помощью кредитных карт по Internet) применяются цифровые подписи и шифрование данных с открытым ключом. Как отправители, так и получатели должны предоставить неоспоримые подтверждения того, что данные были отправлены или, соответственно, получены. Таким подтверждением служит цифровая подпись.

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

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

Понимание задач, возлагаемых на систему защиты, поможет вам разработать максимально эффективную стратегию защиты вашей системы в сети. Перед началом разработки стратегии защиты рекомендуем вам проанализировать пример стратегии, применяемой компанией JKL Toys. В этом примере проиллюстрированы многие характерные особенности подключения внутренней сети к Internet.

Пример организации электронной коммерции в компании JKL Toys

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

Компания JKL Toys - это не очень большой, но стремительно растущий производитель игрушек. Они начинали со скакалок и кубиков, а теперь в их ассортименте есть даже плюшевые мамонты. Президент компании доволен темпами роста, как и возможностями системы iSeries, удовлетворяющей растущие потребности компании. Функции системного администратора iSeries возложены на Шэрон Джонс, главного бухгалтера фирмы.

Компания JKL Toys сначала разработала стратегию защиты для внутренней сети, которая успешно применялась в течение года. Теперь возникла потребность повысить эффективность внутреннего обмена информацией, а также подключить свою сеть к Internet. В дальнейшем компания собирается создать серьезное маркетинговое представительство в Internet, в котором будет функционировать электронный каталог товаров. Кроме того, JKL Toys планирует передавать через Internet конфиденциальную информацию из удаленных регионов в свой центральный офис. Наконец, компания решила предоставить сотрудникам доступ в Internet для поиска новых идей и более эффективного использования рабочего времени. В принципе

компания рассчитывает на то, что часть клиентов начнет покупать товары через электронный магазин, который будет организован на web-странице фирмы в Internet. Шэрон работает над докладом об опасностях, которые могут повлечь за собой все эти начинания, и о том, какие меры защиты должны быть предприняты для устранения этих опасностей. В дальнейшем Шэрон будет отвечать за модернизацию корпоративной стратегии защиты и реализации тех мер, которые она предложит.

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

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

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

Новая система будет размещена на границе между внешней и внутренней сетью и будет обеспечивать физическое отделение Internet от внутренней сети, что снижает вероятность причинения какого-либо ущерба со стороны Internet. Кроме того, применение специальной системы iSeries в качестве сервера Internet упрощает управление защитой сети.

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

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

Глава 5. Базовые уровни защиты при подключении к Internet

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. Минимальные требования к общей защите системы включают следующее:

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

  Примечание: Работа на уровне защиты 50 с приложением, интенсивно выполняющим транзакции или использующим Интегрированную файловую систему, может привести к снижению производительности. Более подробная информация об уровнях защиты iSeries приведена в руководстве Рекомендации по организации защиты в системе iSeries. 

  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. Прежде чем изменять уровень защиты системы, ознакомьтесь с книгой iSeries Security Reference  .
- Установите системные значения, связанные с защитой, так, чтобы уровни ограничений были не ниже рекомендуемых. Для сравнения ваших значений с рекомендуемыми можно воспользоваться Мастером установки защиты или Technical Studio Security Advisor.
- 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. Дополнительную информацию о работе с правами доступа к объектам можно найти в разделе, посвященном Навигатору, книги Рекомендации по организации защиты в системе iSeries  .

Для упрощения процедуры минимальной настройки системы защиты вы можете воспользоваться продуктом **Security Advisor** (его можно загрузить с Web-страницы Technical Studio) или **Мастером настройки защиты** (входит в комплект поставки Навигатора). Продукт Technical Studio Security Advisor  задаст вам несколько вопросов и на основе ваших ответов даст ряд рекомендаций, которые помогут вам

правильно настроить параметры защиты системы. Мастер установки защиты устроен примерно так же, но он может задать параметры защиты системы автоматически.

Правильная настройка внутренних средств защиты системы iSeries позволяет избежать многих потенциальных опасностей. Однако если система iSeries подключена к открытой сети (например, Internet), то необходимо принять дополнительные меры защиты для обеспечения безопасности внутренней сети организации. Когда вы будете уверены, что в системе iSeries настроена надежная общая система защиты, перейдите к настройке функций защиты, относящихся непосредственно к подключению системы к Internet.

Глава 6. Средства защиты на уровне сети

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

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

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

Несмотря на то, что брандмауэр обеспечивает надежную защиту от некоторых видов атак, система защиты должна включать и другие средства. Например, защита с помощью брандмауэра не распространяется на данные, пересылаемые через Internet через приложения почты SMTP, FTP и TELNET. Если данные пересылаются в незашифрованном виде, то любой злоумышленник может перехватить и прочесть их.

При подключении системы iSeries или внутренней сети к Internet настоятельно рекомендуется применять брандмауэр в качестве основного средства защиты. Несмотря на то, что продукт IBM Firewall for AS/400 и поддержка к нему более не предоставляются, существуют другие продукты, которыми вы можете воспользоваться.

Более подробная информация о переходе от продукта IBM Firewall for AS/400 к другим продуктам или к стандартным средствам сетевой защиты системы iSeries приведена в книге All You Need to Know When Migrating from IBM Firewall for AS/400

 (SG24-6152).

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

О правилах фильтрации пакетов iSeries

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

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

Брандмауэры

Брандмауэр - это преграда между защищенной внутренней сетью и незащищенной сетью, например Internet. Обычно брандмауэр применяется для защиты внутренней сети при ее подключении к Internet, хотя он может использоваться и для защиты одной внутренней сети от другой.

Брандмауэр позволяет организовать подключение к незащищенной сети таким образом, что весь обмен информацией между защищенной внутренней и незащищенной внешней сетями будет проходить через единственную контролируемую точку (″горловину″). Брандмауэр:
- Позволяет пользователям внутренней сети получать доступ к ресурсам внешней сети.
- Предотвращает несанкционированный доступ пользователей внешней сети к ресурсам внутренней сети.

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

Принципы работы брандмауэра

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

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

Компоненты брандмауэра

Брандмауэр - это набор компонентов аппаратного и программного обеспечения, обеспечивающий защиту от несанкционированного доступа к некоторой части сети. Ниже перечислены составные компоненты брандмауэра:
- Аппаратное обеспечение. Обычно это отдельный компьютер или устройство, специально предназначенные для выполнения функций брандмауэра.
- Программное обеспечение. Состоит из нескольких приложений. Брандмауэр предоставляет следующие средства защиты:
  - Фильтрация IP-пакетов
  - Служба преобразования сетевых адресов (NAT)
  - Сервер SOCKS
  - Сервер Proxy для большинства распространенных протоколов (HTTP, Telnet, FTP и т.д.)
  - Функция передачи почты
  - Разделенные службы имен доменов (DNS)
  - Ведение протокола
  - Контроль в режиме реального времени

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

Применение средств и служб брандмауэра

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

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

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

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

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

Достоинства защиты с помощью брандмауэра

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

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

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

Недостатки защиты с помощью брандмауэра

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

Правила фильтрации пакетов iSeries

Правила фильтрации пакетов iSeries 400 - это интегрированная функция операционной системы OS/400. Она предусмотрена в Навигаторе AS/400. Она включает две высокоэффективные функции управления потоком данных TCP/IP в целях защиты системы iSeries:

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

Поскольку поддержка NAT и фильтрация IP-пакетов включены в систему OS/400, их применение не требует дополнительных затрат. В некоторых случаях этих средств уже достаточно для организации полноценной защиты. Однако они не могут заменить брандмауэр. Защита IP-пакетов может применяться как отдельно, так и в сочетании с брандмауэром. Это зависит от задач, стоящих перед вашей системой защиты.

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

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

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

Фильтрация пакетов упрощает управление общедоступным Web-сервером, работающим под защитой брандмауэра. Общие IP-адреса преобразуются для Web-сервера во внутренние IP-адреса. Это уменьшает число адресов, которые должны быть зарегистрированы в Internet и повышает уровень защиты внутренней сети. Кроме того, NAT позволяет пользователям внутренней сети работать с Internet, не разглашая IP-адреса своих хостов.

Фильтрация IP-пакетов позволяет выборочно блокировать и защищать поток данных протокола IP на основе содержимого заголовков пакетов. Из Навигатора AS/400 вы можете запустить Мастер настройки Internet - удобное средство, позволяющее быстро задать основные правила фильтрации для блокирования нежелательного сетевого потока.

Фильтрация IP-пакетов позволяет выполнить следующие задачи:

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

Выбор сетевых средств защиты системы iSeries

В основе средств защиты сети от несанкционированного доступа лежат технологии брандмауэра. Для защиты системы iSeries 400 вы можете воспользоваться брандмауэром, предоставляющим полный набор функций, или некоторыми функциями брандмауэра, реализованными в протоколе TCP/IP для OS/400. В их число входят правила фильтрации пакетов (включая фильтрацию IP-пакетов и службу NAT), а также сервер Proxy для протокола HTTP.

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

Брандмауэр предпочтительнее в этом случае, поскольку его аппаратное и программное обеспечение специально предназначено для обеспечения защиты и содержит ограниченное число интерфейсов, доступных извне. Если же вы делаете выбор в пользу технологий TCP/IP OS/400 для защиты от доступа из Internet, то вы применяете платформу общего назначения с практически неограниченным числом интерфейсов и приложений, открытых для внешнего доступа.

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 взломает защиту, созданную с помощью средств TCP/IP в системе iSeries, то он может получить доступ к самым различным (в том числе

важным!) приложениям, службам и данным. Это позволит ему нанести серьезный ущерб самой системе, а также получить доступ к другим системам внутренней сети.

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

Технология защиты	**Рекомендуется применять средства защиты TCP/IP OS/400**	**Рекомендуется применять брандмауэр с полным набором функций**
Фильтрация IP-пакетов	• Обеспечивает **дополнительную** защиту отдельной системы iSeries, например Web-сервера, или системы intranet, содержащей важные данные. • Защищает подсеть корпоративной сети **intranet**, используя iSeries в качестве шлюза (маршрутизатора) к остальной сети. • Управляет соединением с частично защищенным компьютером посредством **частной сети** или сети extranet, в которой iSeries играет роль шлюза.	• Защищает всю корпоративную сеть от атак из **Internet** или другой открытой сети, с которой соединена ваша сеть. • Защищает большую загруженную подсеть от остальной сети.
Служба преобразования сетевых адресов (NAT)	• Обеспечивает соединение двух **частных сетей** с несовместимыми структурами адресов. • Скрывает адреса систем подсети от абонентов менее защищенной сети.	• Скрывает адреса клиентов, обращающихся к **Internet** или другой открытой сети. Может использоваться вместо сервера Proxy или SOCKS. • Позволяет открыть доступ к службам системы, входящей в частную сеть, для клиентов, подключенных к **Internet**.
Сервер Proxy	• Действует в качестве промежуточного сервера для **удаленных узлов** корпоративной сети при подключении к Internet через центральный брандмауэр.	• Действует в качестве промежуточного сервера для всей корпоративной сети при подключении к **Internet**.

Дополнительная информация о применении средств защиты TCP/IP OS/400 приведена в следующих разделах:

- Правила фильтрации пакетов (IP-фильтрация и служба NAT).
- HTTP Server Documentation Center.
- Руководство AS/400 Internet Security Scenarios: A Practical Approach (SG24-5954).

Глава 7. Средства защиты 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.

Хотя меры по защите каждого отдельно взятого приложения играют важную роль, они занимают незначительное место в общей стратегии защиты, которую вы реализуете в своей системе.

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

Защита Web-сервера

Предоставляя внешним пользователям доступ к своему Web-серверу, вы, скорее всего, не захотите раскрывать перед ними внутреннюю структуру сервера и подробности создания Web-страниц. Ваша задача - создать простой и удобный интерфейс, в котором вся черновая работа выполняется незаметно для пользователя. Как администратору, вам следует позаботиться о том, чтобы необходимые меры безопасности не снизили привлекательность вашего Web-сервера. Если вы собираетесь применять систему iSeries в качестве Web-сервера, то учтите следующие обстоятельства:

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

    При желании директивы защиты можно задать независимо для каждого URL, хотя в большинстве случаев это нецелесообразно. Однако если вам потребуется узнать, кто и каким способом обращается к определенным URL, то это можно сделать только с применением соответствующих директив защиты.
  - Напомним вам, что для настройки сервера можно воспользоваться не только командой WRKHTTPCFG (Работа с конфигурацией HTTP), но и

специализированной страницей администрирования. Настройка сервера напрямую с помощью директив - далеко не простая задача. Если у вас недостаточно опыта, вам будет гораздо проще настроить сервер с помощью административной страницы.

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

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

Кроме программ CGI, ваши Web-страницы могут запускать программы на Java. Прежде чем применять Java на Web-сервере, обязательно ознакомьтесь с рекомендациями по защите при работе с Java.

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

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

Сервер Proxy для протокола HTTP, входящий в комплект поставки продукта IBM HTTP Server для iSeries  , можно использовать для интеграции доступа к Web-ресурсам вашей организации. Кроме того, сервер Proxy может вести протокол всех полученных запросов. Такой протокол позволяет контролировать использование сетевых ресурсов.

Дополнительную информацию об этом вы можете найти в книге *Рекомендации по организации защиты в системе iSeries*. 

Защита при работе с Java и Internet

Программирование на Java сегодня становится все более популярным. Вполне возможно, что в своей системе вы разрабатываете приложения с помощью продуктов IBM Toolbox for Java или IBM Development Kit for Java . В этом случае вы должны быть готовы принять особые меры защиты, связанные с применением Java. Хотя брандмауэр - надежное средство защиты внутренней сети при работе с Internet, он не обеспечивает защиту от многих опасностей, связанных с применением Java. В вашей схеме защиты должны быть предусмотрены особые меры предосторожности в связи с использованием таких источников повышенной опасности, как приложения, аплеты и

сервлеты Java. Кроме того, вы должны изучить взаимосвязь между средствами Java и системой защиты ресурсов применительно к идентификации и разграничению доступа для программ на Java.

Приложения Java

Структура языка Java в определенной степени защищает программиста от случайных ошибок, способных нарушить целостность данных. (Другие распространенные языки программирования для PC - например, C или C++, не обеспечивают такой защиты от ошибок.) Например, в Java установлены строгие ограничения на преобразование типов данных, что не позволяет использовать объекты не по назначению. В Java запрещены операции над указателями, что предохраняет от случайного выхода за границы выделенной программе области памяти. С точки зрения разработки программ, Java можно рассматривать как язык высокого уровня. При разработке приложений на Java следует принимать такие же меры защиты, как и при работе с другими языками программирования системы iSeries 400.

Аплеты Java

Аплетами называются небольшие программы на Java, которые можно включать в документы на языке HTML. Аплеты запускаются на компьютере клиента, и поэтому их действия не относятся к системе, в которой работает Web-сервер. Однако аплет Java может получить доступ к системе iSeries 400. (К системе iSeries также могут обращаться программы, в которых используются интерфейсы ODBC и APPC.) Строго говоря, аплеты Java могут устанавливать связь только с теми серверами, с которых они загружены. Поэтому к вашей системе iSeries могут подключаться только те аплеты, которые с нее же и были загружены (например, если аплет был загружен и запущен на PC, подключенном к вашей локальной сети).

Аплет может попытаться подключиться к любому порту TCP/IP системы. Ему не обязательно взаимодействовать с сервером, написанным на Java. Однако в случае сервера, разработанного с помощью IBM Toolbox for Java, аплет при подключении к родительскому серверу обязан предъявить ИД пользователя и пароль. В данном контексте под сервером понимается система iSeries. (Сервер, написанный на Java, не обязательно использует IBM Toolbox for Java). Как правило, любой класс IBM Toolbox for Java при первом подключении пользователя к системе iSeries запрашивает ИД пользователя и пароль.

После подключения к системе iSeries аплет может выполнять только те операции, которые разрешены пользовательскому профайлу, под управлением которого аплет подключился к системе. Поэтому прежде чем использовать аплеты Java, необходимо аккуратно настроить систему защиты. При обработке запросов, поступающих от аплетов, система не учитывает параметр ограничения возможностей пользовательского профайла.

Программа запуска аплетов позволяет проверить работу аплетов в системе сервера, но она не учитывает ограничений прав доступа, установленных для браузера. Поэтому программу запуска аплетов следует использовать только для проверки собственных аплетов. Никогда не пользуйтесь этой программой для запуска аплетов, полученных из посторонних источников. Аплеты Java могут записывать информацию на жесткие диски, что теоретически позволяет им выполнять сколь угодно деструктивные действия. Для того чтобы предоставить аплету особые права доступа, его можно снабдить цифровой подписью, гарантирующей его идентификацию. Аплет с цифровой подписью может выполнять даже те операции, которые запрещены

браузеру по умолчанию, - например, записывать на локальные диски PC и даже на сетевые диски, которые теоретически могут быть дисками системы iSeries, подключенными к PC.

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

Аплеты, хранящиеся в системе iSeries, может потребоваться снабжать цифровыми подписями. Однако следует запретить пользователям принимать подписанные аплеты из непроверенных источников.

Начиная с выпуска V4R4 вы можете применять IBM Toolbox for Java для настройки среды Secure Sockets Layer (SSL). Кроме того, вы можете настроить SSL-защиту приложения Java с помощью IBM Developer Toolkit for Java. Применение SSL для защиты приложений Java обеспечивает шифрование данных, включая ИД пользователей и пароли, передаваемых между клиентом и сервером. Для настройки применения SSL в зарегистрированных программах на Java воспользуйтесь Диспетчером цифровых сертификатов.

Сервлеты Java

Сервлеты - это программы на Java, выполняемые в системе Web-сервера. Сервлеты позволяют динамически расширять возможности сервера без изменения его программного кода. Продукт IBM WebSphere Application Server, поставляемый вместе с IBM HTTP Server для iSeries, предусматривает поддержку сервлетов в системе iSeries.

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

Дополнительная информация о мерах защиты при работе с объектами Java приведена в следующих разделах:
- IBM Developer Kit for Java - Защита Java.
- IBM Toolbox for Java - классы защиты.
- Книга Рекомендации по организации защиты в системе iSeries  .

Средства идентификации и разграничения доступа в Java

В IBM Toolbox for Java предусмотрены классы защиты, обеспечивающие возможность идентификации пользователей и назначения соответствующих прав доступа нитям операционной системы, выполняющим приложение или сервлет в системе iSeries. Дальнейшее управление доступом осуществляется средствами операционной системы.Более подробную информацию о классах защиты см. в разделе IBM Toolbox for Java - Службы идентификации.

IBM Developer Kit for Java предоставляет поддержку Службы идентификации и разграничения доступа (JAAS) - стандартного расширения продукта Java 2 Software Development Kit (J2SDK), Standard Edition. В настоящее время J2SDK предоставляет средства управления доступом, основанные на определении источника и автора кода. Дополнительная информация о применении J2SDK приведена в разделе Служба идентификации и разграничения доступа.

Защита приложений Java с помощью протокола SSL

Для защиты данных, которыми обмениваются приложения, разработанные с помощью продукта IBM Developer Kit для Java, можно применять протокол SSL. Протокол SSL также можно применять для приложений-клиентов, использующих IBM Toolbox для Java. Настройка протокола SSL для приложений Java обладает рядом особенностей по сравнению с другими приложениями.

Дополнительная информация о применении протокола SSL для защиты приложений Java приведена в следующих разделах документации Information Center:
- IBM Toolbox for Java - Среда Secure Sockets Layer (SSL).
- IBM Developer Toolkit for Java - защита приложения Java с помощью SSL.

Защита электронной почты

Применение электронной почты в сети Internet и в любых других общедоступных сетях представляет собой определенную опасность, от которой вас не всегда сможет защитить брандмауэр. Для того чтобы разработать эффективную стратегию защиты, необходимо четко представлять характер этой опасности.

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

Распространенные способы нарушения нормальной работы электронной почты

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

получателю, оно пройдет через много неподконтрольных вам серверов. Если вы не зашифруете свое сообщение, злоумышленники могут перехватить и прочитать его в любой точке маршрута пересылки.

Средства защиты на уровне 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 позволяет, помимо прочего, шифровать весь документ или его отдельные поля.

Для шифрования электронной почты Lotus Notes Domino предоставляет каждому пользователю уникальные личный и общий ключи. 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 кто-то отправит вам зашифрованную почту, Lotus Notes Domino расшифрует предназначенное вам сообщение, используя общий ключ отправителя.

Информация о применении встроенных средств шифрования Lotus Notes приведена в электронной справке к этому продукту.

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

- Справочная библиотека Lotus Domino. 
- Web-сайт справочной информации Lotus Notes. 
- Lotus Notes and Domino R5.0 Security Infrastructure Revealed  (SG24-5341).
- Lotus Domino for AS/400 Internet Mail and More  (SG24-5990).

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

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

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

Защита FTP

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

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

  Рассмотрим следующий пример. Предположим, что в вашей системе ограничен доступ пользователей к меню, и при этом для всех объектов установлены общие права доступа *USE. (Ограничением доступа к меню называется режим, при котором пользователям недоступны некоторые пункты меню.) Поскольку на пользователей FTP не распространяются ограничения, связанные с меню, им автоматически становятся доступны все объекты системы.Во избежание такой ситуации вам следует воспользоваться следующими возможностями:
  - Задействовать систему защиты iSeries на уровне объектов (иными словами, перейти от концепции ″защиты меню″ к концепции ″защиты объектов″). Этот вариант обеспечивает максимальную защиту.
  - Написать для FTP программы выхода, запрещающие передачу определенных файлов. Эти программы выхода должны обеспечить по крайней мере тот же уровень защиты, что и программа меню. Однако в большинстве случаев требования к таким программам будут еще выше. Кроме того, такой подход обеспечивает защиту только при работе с протоколом FTP; он никак не влияет на другие интерфейсы - например, ODBC, DDM или DRDA.

    Примечание: Права доступа *USE допускают загрузку файлов из системы. Права доступа *CHANGE позволят пользователю FTP изменять файлы из удаленной системы.
- Злоумышленник может попытаться нарушить работу FTP посредством отключения пользовательских профайлов системы. Для этого ему достаточно несколько раз попытаться войти в систему с неверным паролем, и соответствующий пользовательский профайл будет отключен. Обычно профайл отключается после трех неудачных попыток входа в систему.

  Действия, которые вы можете предпринять во избежание такой ситуации, определяются компромиссом между надежностью защиты и простотой доступа пользователей к системе. В протоколе FTP обычно применяется системное значение QMAXSIGN, так как в противном случае злоумышленник может постепенно подобрать пароль. Ниже приведены некоторые рекомендации:
  - Воспользуйтесь программой выхода для процедуры подключения к серверу по протоколу FTP. Эта программа выхода должна отклонять попытки входа в систему с посторонних систем и под управлением пользовательских профайлов, которым при обычной работе не нужен доступ по протоколу FTP. (Такие отклоненные попытки **не** будут учитываться при проверке ограничения QMAXSIGN.)

- Воспользуйтесь программой выхода для сервера FTP, которая будет разрешать клиентам входить в систему только с определенных удаленных систем. Например, если вы разрешаете сотруднику бухгалтерии подключаться к системе по протоколу FTP, сервер FTP должен принимать соединения только с тех IP-адресов, которые относятся к компьютерам, установленным в бухгалтерии.
- Воспользуйтесь программой выхода для сервера FTP, которая будет записывать в журнал ИД пользователя и IP-адрес при каждой попытке входа в систему по протоколу FTP. Если вы будете регулярно просматривать протоколы, у вас будут высокие шансы обнаружить злоумышленников и предпринять соответствующие меры.

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.

Начиная с выпуска V5R1 вы можете применять протокол Secure Sockets Layer (SSL) для защиты сеансов FTP. 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.

Дополнительная информация о протоколе FTP, возможных опасностях при его применении и соответствующих мерах защиты приведена в следующих разделах:
- Реализация защиты FTP.
- Анонимный FTP.
- Применение SSL для защиты FTP.
- Рекомендации по организации защиты в системе iSeries  .

Глава 8. Средства защиты на уровне передачи данных

Напомним, что в нашем примере компании JKL Toys принадлежат две системы iSeries. Одна из них применяется для разработки продуктов, а вторая используется в производственных целях. Обе системы работают с крайне важными данными и программами. Поэтому компания решила приобрести третью систему iSeries и использовать ее в качестве управляющего звена для работы с приложениями внутренней сети и Internet.

За счет этого компании удастся организовать физическое отделение внутренней сети от Internet, что снижает вероятность причинения какого-либо ущерба со стороны Internet. Кроме того, применение специальной системы iSeries в качестве сервера Internet упрощает управление защитой сети.

Поскольку современные компьютерные злоумышленники становятся с каждым днем все изобретательнее, фирма IBM постоянно развивает и совершенствует средства защиты, направленные на ведение электронной коммерции 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.

Для минимизации риска, связанного с передачей данных по открытым сетям, можно воспользоваться следующими встроенными средствами защиты системы iSeries на уровне передачи данных: протоколом SSL и поддержкой виртуальных частных сетей (VPN).

Защита приложений с помощью SSL

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

- Сервер IBM HTTP Server for iSeries (оригинальный и на основе Apache)
- Сервер FTP
- Сервер Telnet
- Сервер Архитектуры распределенных реляционных баз данных (DRDA) и Управления распределенными данными
- (DDM)
- Централизованное управление
- Сервер служб каталогов (LDAP)
- Приложения Client Access Express, включая Навигатор AS/400, и приложения, предназначенные для набора интерфейсов прикладных программ (API) Client Access Express
- Программы, разработанные с помощью Developer Kit for Java, и клиентские приложения, использующие 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 создать защищенное соединение.

Виртуальные частные сети (VPN) системы iSeries

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

Что выбрать?

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

Учтите также следующее обстоятельство: протокол SSL может применяться только теми приложениями, которые специально рассчитаны на его применение. Хотя таких приложений много и в их число входят Telnet и Client Access Express, все же SSL поддерживают не все продукты. 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 вы можете 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.

Применение цифровых сертификатов для SSL

Цифровые сертификаты - это основной инструмент для надежной идентификации и защищенного обмена данными с помощью протокола SSL. Для создания и управления цифровыми сертификатами систем и пользователей в системе iSeries 400 применяется Диспетчер цифровых сертификатов (DCM) - встроенный продукт с простым и удобным интерфейсом.

Кроме того, некоторые приложения (например, IBM HTTP Server для iSeries) могут применять цифровые сертификаты вместо имен и паролей для идентификации пользователей.

Что такое цифровой сертификат?

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

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

Хотя протокол SSL по-прежнему поддерживается не всеми приложениями, самые распространенные на сегодня продукты и протоколы (например Telnet и Client Access Express) уже поддерживают SSL. Информация о применении SSL с приложениями with iSeries приведена в разделе **Защита приложений с помощью SSL** документации iSeries Information Center:

Применение SSL для защиты Telnet

Начиная с выпуска V4R4 вы можете настроить на сервере Telnet 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 по соединениям Telnet будет передаваться очень важная или конфиденциальная информация, рекомендуется применять в соединениях Telnet протокол SSL. Если приложению Telnet системы iSeries будет выдан цифровой сертификат, то сервер Telnet сможет работать как с незащищенными клиентами, так и с клиентами SSL. Если ваша стратегия защиты предполагает обязательное шифрование сеансов Telnet, вы можете запретить применение незащищенных сеансов Telnet. Когда необходимость применения SSL с Telnet отпадет, порт SSL можно отключить. (Для отключения портов применяется команда ADDTCPPORT.) В этом случае сервер Telnet будет поддерживать только незащищенные соединения Telnet.

Более подробная информация о Telnet и рекомендации по защите данных в случае применения Telnet без SSL приведены в следующих разделах:

- Раздел Telnet документации Information Center содержит необходимые сведения для применения Telnet в системе iSeries.

- Раздел Защита Telnet посвящен совместному применению SSL и Telnet для защиты сеансов Telnet.
- Книга Рекомендации по организации защиты в системе iSeries  содержит подробную информацию о защите Telnet (раздел, посвященный TCP/IP).

Применение SSL для защиты Client Access Express

Начиная с выпуска V4R4 вы можете настроить на сервере Client Access Express применение протокола Secure Sockets Layer (SSL) для защиты сеансов Client Access Express. Компания JKL Toys разрослась, и у нее появилось несколько региональных агентов, не привязанных к какому-либо конкретному офису. Этим агентам требуется доступ к внутренней сети компании из любого места, где они могут находиться. По причине конфиденциальности данных компания JKL Toys решила предоставить своим агентам доступ к информации только через защищенный Client Access Express.

Протокол SSL обеспечивает шифрование всех данных, передаваемых в сеансах Client Access Express, что гарантирует конфиденциальность связи.

Дополнительную информацию о применении Client Access Express с SSL вы найдете в следующих разделах:

- Управление протоколом SSL
- Организация защиты Client Access Express и Навигатора AS/400
- Применение SSL с IBM Developer Kit for Java
- Применение SSL с IBM Java Toolbox

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

С появлением и развитием виртуальных частных сетей (VPN) компания JKL Toys решила начать обмен данными через Internet. Она недавно приобрела другую небольшую фирму по производству игрушек, которая будет выполнять функции филиала. Фирме JKL потребуется передавать информацию из филиала в головное отделение и обратно. В обеих фирмах применяются системы iSeries, и соединение VPN обеспечит необходимую защиту передаваемых данных. Затраты на обслуживание обычных выделенных линий существенно выше, чем затраты на организацию VPN.

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

Преимущества VPN особенно актуальны для следующих пользователей:
- Пользователи, работающие вне офиса и находящиеся в командировках.
- Филиал, соединенный с головным предприятием и другими отделениями фирмы.
- Деловые партнеры.

Если вы не ограничиваете доступ пользователей к областям, где хранится конфиденциальная информация, то вы сильно рискуете. В такой ситуации высока вероятность утечки важной для вас информации. Вам необходимо разработать схему предоставления доступа к важным файлам вашей системы. 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 данные передаются по внутренним сетям, между которыми установлено соединение, то VPN не шифрует их. Следовательно, вам необходимо тщательно планировать настройку каждого конкретного соединения VPN. Убедитесь в том, что вы предоставили партнеру по VPN права доступа именно к тем хостам и ресурсам в вашей внутренней сети, к которым вы хотели их предоставить.

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

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

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

Глава 9. Терминология, применяемая в средствах защиты информации Internet

Для обсуждения средств защиты информации в Internet нам потребуется определить некоторые понятия. Если вы уже знакомы с терминологией Internet, можете пропустить этот раздел.

Идентификация

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

Взломщик

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

Криптография

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

Методы шифрования можно разделить на два класса:

- При шифровании с закрытым ключом **(симметричном шифровании)** при шифровании и дешифровании данных используется один и тот же ключ, известный обеим сторонам.
- При шифровании с открытым ключом **(асимметричном шифровании)** при шифровании и дешифровании данных используются различные ключи. У каждой стороны есть два ключа: общий и личный. Они математически связаны между собой, но получить один из другого практически невозможно. Сообщение, зашифрованное с помощью общего ключа, можно расшифровать только с помощью соответствующего личного ключа. Двойное шифрование данных с применением личного ключа отправителя и общего ключа получателя позволяет не только обеспечить конфиденциальность, но и гарантировать подлинность отправителя.

Цифровой сертификат

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

- Проверка ИД пользователя
- Идентификации пользователей
- Проверки подлинности документов, полученных по сети, по цифровой подписи отправителей

- Подтверждения того, что пользователь действительно отправил какую-либо информацию. Например, у покупателя, оплатившего товары по сети Internet с помощью кредитной карты, не должно быть возможности оспорить факт оплаты.

Цифровая подпись

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

Диспетчер цифровых сертификатов (DCM)

Диспетчер цифровых сертификатов (DCM) - это продукт, позволяющий системе OS/400 выступать в роли сертификатной компании (CA). С помощью DCM можно создавать цифровые сертификаты для серверов и пользователей. Помимо этого, можно импортировать сертификаты, выданные другими CA. Каждому пользовательскому профайлу OS/400 можно назначить собственный цифровой сертификат. DCM позволяет программам применять протокол SSL для организации защищенного обмена данными по сети.

Отличительное имя

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

Сервер имен доменов (DNS)

Хост, определяющий IP-адреса хостов по их доменным именам в Internet. Серверам DNS часто приходится обмениваться информацией между собой. Например, многие DNS знают адрес хоста

```
vnet.ibm.com
```

Однако далеко не все из них могут определить IP-адрес следующего хоста:

```
system1.vnet.ibm.com
```

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

Шифрование

Шифрованием называется преобразование данных, в результате которого их правильная интерпретация становится невозможной для посторонних лиц. Шифрование не защищает данные от перехвата, однако для использования перехваченных данных их требуется дешифровать.

Extranet

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

Брандмауэр

Логический барьер, отделяющий внутреннюю сеть организации от внешней сети - например, Internet. Брандмауэр может состоять из одной или

нескольких аппаратных и программных систем. Он управляет доступом к внутренней сети и передачей информации между внутренними (надежными) и внешними (ненадежными) системами.

Хакер Любое лицо, пытающееся получить несанкционированный доступ к системе.

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

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

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

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

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

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

Обмен ключами Internet (IKE)
Протокол IKE используется вместе с протоколом IPSec и позволяет заинтересованным сторонам автоматически согласовывать параметры защиты, а также автоматически генерировать и обновлять ключи шифрования. Обычно протокол IKE применяется в виртуальных частных сетях (VPN).

Доменное имя
Псевдоним, используемый вместо IP-адреса хоста. Поскольку IP-адреса представляют собой длинные последовательности цифр (например: 10.5.100.75), их трудно запоминать. Поэтому IP-адресам присваивают доменные имена, например:

```
system1.vnet.ibm.com
```

Эти имена называют доменными, потому что в них последовательно указаны имена всех вложенных доменов, в которых находится хост. В большинстве случаев на объявлениях вида “посетите нашу страницу в Internet” указаны именно доменные имена, а не IP-адреса хостов.

Полное доменное имя состоит из нескольких частей. Например, следующее имя:

system1.vnet.ibm.com

состоит из следующих частей:

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

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

vnet: Группа систем в пределах домена ibm.com

Этот идентификатор определяется внутри организации. Администратор домена ibm.com может создать несколько таких групп по своему усмотрению.

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

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

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

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

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

IP-адрес
IP-адреса - это адреса, применяемые в сетях TCP/IP. Большинству серверов Internet присвоены уникальные фиксированные IP-адреса. Клиенты Internet могут использовать временные адреса, выделенные провайдером, но эти адреса также должны быть уникальными.

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

Фильтры IP

Фильтры IP применяются брандмауэрами в качестве основного механизма защиты. Фильтры позволяют определять характер информации, передаваемой через брандмауэр, на основании данных о структуре заголовков дейтаграмм. Благодаря этому внутреннюю сеть можно защитить от несанкционированного доступа извне с применением как простых, так и очень сложных методов. Фильтрацию IP-пакетов можно рассматривать как основу, на которой базируются все остальные средства защиты.

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

Подмена IP-адресов

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

Служба преобразования сетевых адресов (NAT)

Служба преобразования сетевых адресов (NAT) - это хорошая альтернатива серверам Proxy и SOCKS. Эта служба упрощает настройку сетей, поскольку она позволяет устанавливать соединения между сетями с несовместимыми структурами адресов. NAT реализует две важнейшие функции: во-первых, защиту внешнего Web-сервера, управление которым осуществляется из внутренней сети организации. Для этого фактический адрес сервера скрывается и заменяется на внешний адрес, к которому открыт общий доступ. Во-вторых, NAT позволяет пользователям внутренней сети работать с Internet, не раскрывая IP-адреса внутренних хостов. Благодаря этому NAT обеспечивает доступ к Internet из внутренней сети, не разглашая IP-адреса ваших компьютеров.

Неоспоримость

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

Пакет Дейтаграмма, в которой указана информация о протоколе линии связи - например, Ethernet, Token-Ring или Frame Relay.

Сервер Proxy

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

Инфраструктура общих ключей (PKI)

Система цифровых сертификатов, сертификатных компаний и других регистрационных служб, обеспечивающих идентификацию участников транзакций в сети Internet.

Secure Sockets Layer (SSL)

Протокол SSL был разработан компанией Netscape для шифрования сеансов связи между клиентами и серверами, и на сегодня стал стандартным

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

Перехват информации

Перехватом называется несанкционированное прослушивание сеансов обмена данными по сети. На пути от отправителя к получателю информация может пройти через множество маршрутизаторов. Изготовители маршрутизаторов, провайдеры Internet и разработчики операционных систем предпринимают максимальные усилия по предотвращению перехвата данных в магистральных сетях Internet. Случаи успешного перехвата данных встречаются все реже. Большинство таких случаев приходится не на магистральные линии, а на частные локальные сети, подключенные к Internet. Тем не менее, поскольку в подавляющем большинстве случаев информация передается в незашифрованном виде, следует все же учитывать возможность ее перехвата.

Протокол SOCKS

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

Подмена адресов

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

TCP/IP

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

Троянский конь

Троянский конь - это компьютерная программа, на первый взгляд предназначенная для выполнения полезных и не вызывающих подозрений функций. При этом такая программа содержит скрытые функции, в которых используются права доступа запустившего ее пользователя. Например, она может скопировать с вашего компьютера конфиденциальную информацию и переслать ее своему разработчику.

Виртуальная частная сеть (VPN)

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

- Удаленных пользователей
- Филиалов компании
- Деловых партнеров и поставщиков

Браузер

Программа-клиент протокола HTTP. Браузеры позволяют просматривать

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

World Wide Web (WWW)

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

Напечатано в Дании