System i

Работа в сети
Фильтрация IP-адресов и преобразование сетевых адресов

версия 6 выпуск 1

System i

Работа в сети
Фильтрация IP-адресов и преобразование сетевых адресов

версия 6 выпуск 1

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 33.

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

Содержание

Фильтрация IP-пакетов и преобразование сетевых адресов

Фильтрация IP-пакетов и преобразование сетевых адресов (NAT) выполняют роль брандмауэра, защищая внутренние системы, подключенные к защищенной сети, от несанкционированного доступа.

Фильтрация IP-пакетов позволяет контролировать входящие и исходящие IP-потоки сети. Служба фильтрации пропускает или отбрасывает пакеты на основе заданных правил. Применение NAT позволяет скрыть незарегистрированные частные IP-адреса за набором зарегистрированных IP-адресов. Это дает возможность защитить внутреннюю сеть от внешней. Кроме того, применение NAT решает проблему нехватки IP-адресов, поскольку большое число частных адресов могут быть представлены в виде ограниченного множества зарегистрированных адресов.

Примечание: *Правило обработки пакетов* представляет собой комбинацию фильтрации IP-пакетов и NAT. Термин Правила обработки пакетов употребляется в данном разделе по отношению к обеим службам.

В дополнение к информации из этого раздела можно пользоваться электронной справкой по Редактору правил обработки пакетов в System i Navigator. В электронной справке System i Navigator приведены советы по работе с правилами обработки пакетов, включая разделы Каким образом.., Что такое... и обширную контекстную справку.

Примечание: Используя примеры исходного кода, вы принимаете условия соглашения Лицензирование и отказ от гарантий на предоставляемый код.

Документ PDF о фильтрации IP-пакетов и преобразовании сетевых адресов

Файл PDF этой информации можно просмотреть и напечатать.

Для просмотра или загрузки документа в формате PDF выберите следующую ссылку: Фильтрация IP-пакетов и преобразование сетевых адресов (размер файла - около 621 Кб).

Сохранение PDF-файлов

Для сохранения файла PDF на своей рабочей станции:

1. Щелкните правой кнопкой мыши на приведенной ссылке на документ PDF.
2. Выберите опцию сохранения файла PDF на локальном диске.
3. Перейдите в каталог, в котором требуется сохранить документ PDF.
4. Нажмите **Сохранить**.

Загрузка Adobe Reader

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

Ссылки, связанные с данной

“Дополнительная информация о фильтрации IP-пакетов и преобразовании сетевых адресов” на стр. 32
Справочники IBM Redbooks содержат сведения о фильтрации IP-пакетов и преобразовании сетевых адресов. Документы в формате PDF можно просмотреть или распечатать.

Сценарии: Правила фильтрации пакетов

Для защиты локальной сети можно использовать преобразование сетевых адресов (NAT) и фильтрацию IP-пакетов.

Каждый пример сопровождается рисунком и описанием соответствующей конфигурации.

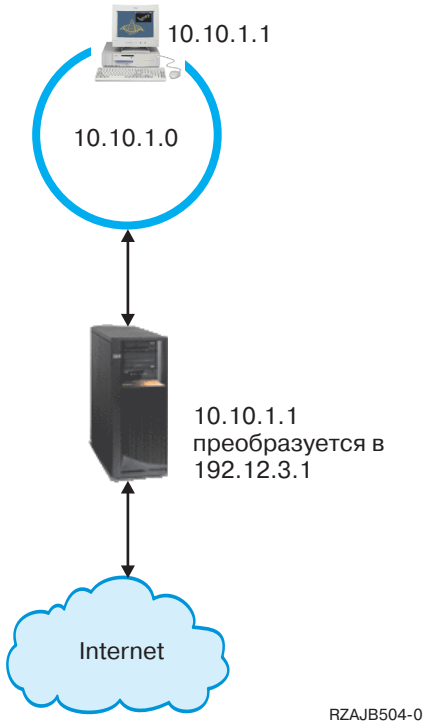
Совет: В каждом сценарии IP-адреса вида 192.*x*.*x*.*x* соответствуют внешним IP-адресам. Все адреса приводятся только в качестве примера.

Сценарий: преобразование IP-адресов с помощью NAT

В этом сценарии частные IP-адреса сети вашей компании преобразуются во внешние адреса с помощью статического преобразования сетевых адресов (NAT).

Ситуация

Вы решили создать частную сеть для своей компании. Однако у вас нет зарегистрированного внешнего IP-адреса. При подключении к Internet выясняется, что вы не можете использовать IP-адреса своей частной сети, так как они могут быть зарегистрированы другими пользователями внешней сети. Перед вами стоит задача обеспечить пользователям внешней сети доступ к своему Web-серверу. Как решить поставленную задачу?



Решение

Настройте статический NAT. Статический NAT связывает внутренний (частный) адрес с зарегистрированным (внешним) адресом. Ваша система преобразует этот зарегистрированный адрес во внутренний. Зарегистрированный адрес позволит системе, с ее внутренним адресом, соединяться с Internet. Фактически NAT образует мост между внутренней и внешней сетью. Соединение может быть открыто как из внешней, так и из внутренней сети.

Статический NAT позволяет подключиться к Internet, сохранив внутренние IP-адреса. Для каждой внутренней системы вам потребуется отдельный IP-адрес. Например, для сети с 12 пользователями вам потребуется 12 внешних IP-адресов для преобразования 12 внутренних адресов.

В приведенном примере адрес NAT 192.12.3.1 не используется, ожидая возврата данных. При получении информации NAT преобразует адрес во внутренний адрес персонального компьютера. Если включен статический NAT, то все пакеты с адресом назначения 192.12.3.1 будут поступать не в систему с таким адресом, а в систему с соответствующим внутренним адресом. Фактическим получателем таких пакетов будет система с внутренним адресом 10.10.1.1, хотя все внешние системы будут отправлять пакеты на IP-адрес 192.12.3.1.

Настройка

Для настройки правил обработки пакетов, описанных в этом сценарии, воспользуйтесь мастером **Преобразование адресов** в System i Navigator. Мастеру требуется следующая информация:

- Внутренний адрес для преобразования: 10.10.1.1
- Внешний адрес, в который преобразуется внутренний адрес: 192.12.3.1
- Имя линии, в соединениях которой выполняется преобразование адресов: TRNLINE

Для запуска мастера **Преобразование адресов** выполните следующие действия:

1. В System i Navigator выберите ***ваша система*** **→ Сеть → Стратегии IP**.
2. Щелкните правой кнопкой мыши на значке **Правила обработки пакетов** и выберите **Редактор правил**.
3. В окне Настройка правил обработки пакетов выберите **Создать новый файл правил обработки пакетов** и нажмите **OK**.
4. В меню Мастеры выберите **Преобразование адресов** и следуйте инструкциям мастера по настройке правил преобразования адресов.

Ниже приведен пример правил обработки пакетов.

```
Преобразовать 10.1.1.1 в 192.12.3.1 на TRNLINE

ADDRESS MAPPRIVATE1      IP = 10.1.1.1
ADDRESS MAPPUBLIC1       IP = 192.12.3.1 MAP
MAPPRIVATE1          TO MAPPUBLIC1   LINE = TRNLINE
```

RZAJB507-0

Создав эти правила, проверьте их, чтобы убедиться в отсутствии ошибок.

Примечание: В строке LINE=TRNLINE определяется линия Token-Ring, к которой подключен интерфейс с адресом 192.12.3.1. Статический NAT не будет работать, если к этой же линии подключена система с адресом 10.10.1.1. При использовании NAT необходимо настроить пересылку дейтаграмм IP.

Понятия, связанные с данным

“Статический NAT (преобразование адресов)” на стр. 13
Статическое преобразование сетевых адресов (NAT) выполняет взаимно однозначное преобразование внутренних IP-адресов во внешние. Это позволяет преобразовать IP-адрес внутренней сети во внешний IP-адрес.

Задачи, связанные с данной

“Проверка правил обработки пакетов” на стр. 26
Перед активизацией правил их необходимо проверить. Это позволит убедиться в том, что активизация пройдет без ошибок.

“Активация правил обработки пакетов” на стр. 27
Последним этапом настройки правил обработки пакетов является активизация созданных правил.

Ссылки, связанные с данной

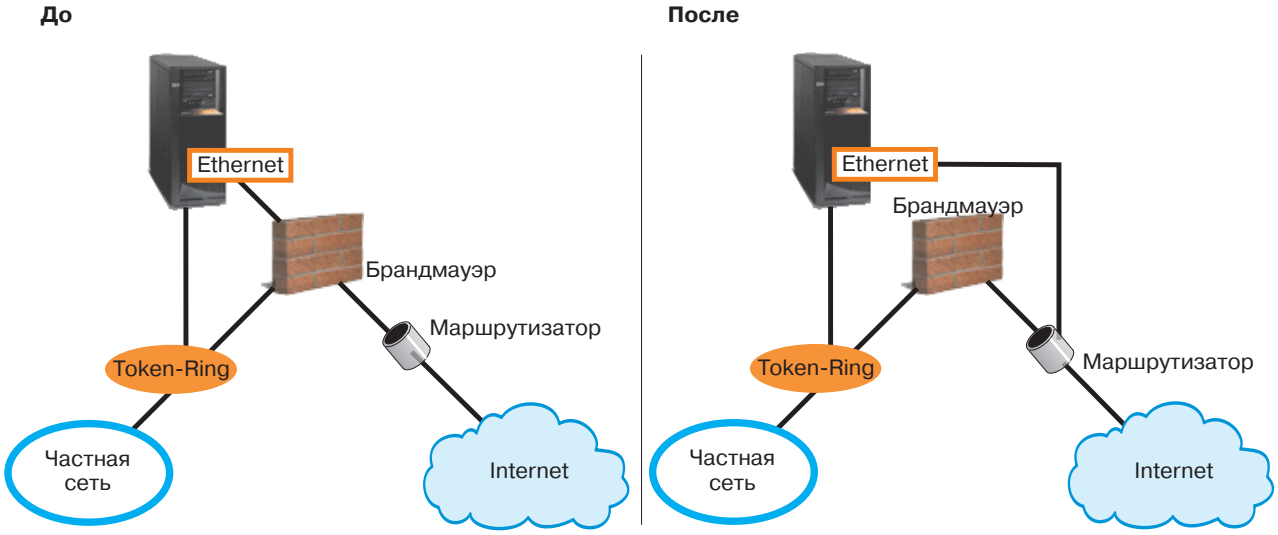
“Устранению ошибок в правилах обработки пакетов” на стр. 30
В этом разделе приведены советы по устранению ошибок в правилах обработки пакетов.

Сценарий: Создание правил фильтрации для работы с HTTP, Telnet и FTP

В этом сценарии вы посредством фильтрации ограничиваете поток IP-пакетов, которым доступен Web-сервер вашей компании, пакетами протоколов HTTP, Telnet и FTP (File Transfer Protocol).

Ситуация

Вы планируете предоставить своим клиентам возможность пользоваться Web-приложениями, однако брандмауэр перегружен и вы не хотите создавать дополнительную нагрузку на него. Ваши коллеги посоветовали запускать Web-приложения во внешней системе. Но вы хотите разрешить внешним пользователям работать на Web-сервере System i только через HTTP, FTP и Telnet. Как решить поставленную задачу?



Решение

Создайте правила фильтрации IP-пакетов, определяющие, какие данные могут быть переданы через Web-сервер. В данном сценарии можно добавить правила, разрешающие передачу данных (входящих и исходящих) по протоколам HTTP, FTP, and Telnet. Внешний IP-адрес сервера - 192.54.5.1, внутренний - 10.1.2.3.

Настройка

Для настройки правил обработки пакетов, описанных в этом сценарии, воспользуйтесь мастером **Разрешить службу** в System i Navigator. Мастеру требуется следующая информация:

- тип службы, которую вы хотите разрешить: HTTP
- внешний адрес Web-сервера: 192.54.5.1.
- адрес клиента: любой IP-адрес
- интерфейс службы: TRNLINE
- направление потока данных: INBOUND

- имя набора правил фильтрации для идентификации данного набора фильтров: external_files

Для запуска мастера **Разрешить службу** выполните следующие действия:

1. В System i Navigator выберите ***ваша система*** **→ Сеть → Стратегии IP**.
2. Щелкните правой кнопкой мыши на значке **Правила обработки пакетов** и выберите **Редактор правил**.
3. В окне Настройка правил обработки пакетов выберите **Создать новый файл правил обработки пакетов** и нажмите **OK**.
4. В меню Мастеры выберите **Разрешить службу** и следуйте инструкциям мастера по созданию правил фильтрации.

Следующие правила обработки пакетов разрешают отправку и прием пакетов HTTP в системе. Ниже приведен пример правил обработки пакетов.

Разрешить прием данных HTTP через TRNLINE

```
INCLUDE FILE = /QIBM/UserData/OS400/TCPIP/PacketRules/Services.i3p
FILTER SET external_files    ACTION = PERMIT DIRECTION = OUTBOUND          SRCADDR = 192.54.5.1DSTADDR = *
SERVICE = HTTP_80_FS         JRN = OFF
FILTER SET external_files    ACTION= PERMIT  DIRECTION = INBOUND           SRCADDR = *DSTADDR = 192.54.5.1
SERVICE= HTTP_80_FC          JRN = OFF
FILTER SET external_files    ACTION = PERMIT DIRECTION = OUTBOUND          SRCADDR = 192.54.5.1DSTADDR = *
SERVICE = HTTP_443_FS        JRN = OFF FILTER
SET external_files           ACTION = PERMIT DIRECTION = INBOUND           SRCADDR = *DSTADDR = 192.54.5.1
SERVICE = HTTP_443_FC        JRN = OFF
FILTER_INTERFACE             LINE = TRNLINE    SET = external_files
```

RZAJB508-0

С помощью того же мастера Разрешить службу вы можете настроить правила фильтрации, пропускающие пакеты FTP и Telnet.

Создав эти правила, проверьте их, чтобы убедиться в отсутствии ошибок.

Задачи, связанные с данной

“Проверка правил обработки пакетов” на стр. 26
Перед активизацией правил их необходимо проверить. Это позволит убедиться в том, что активизация пройдет без ошибок.

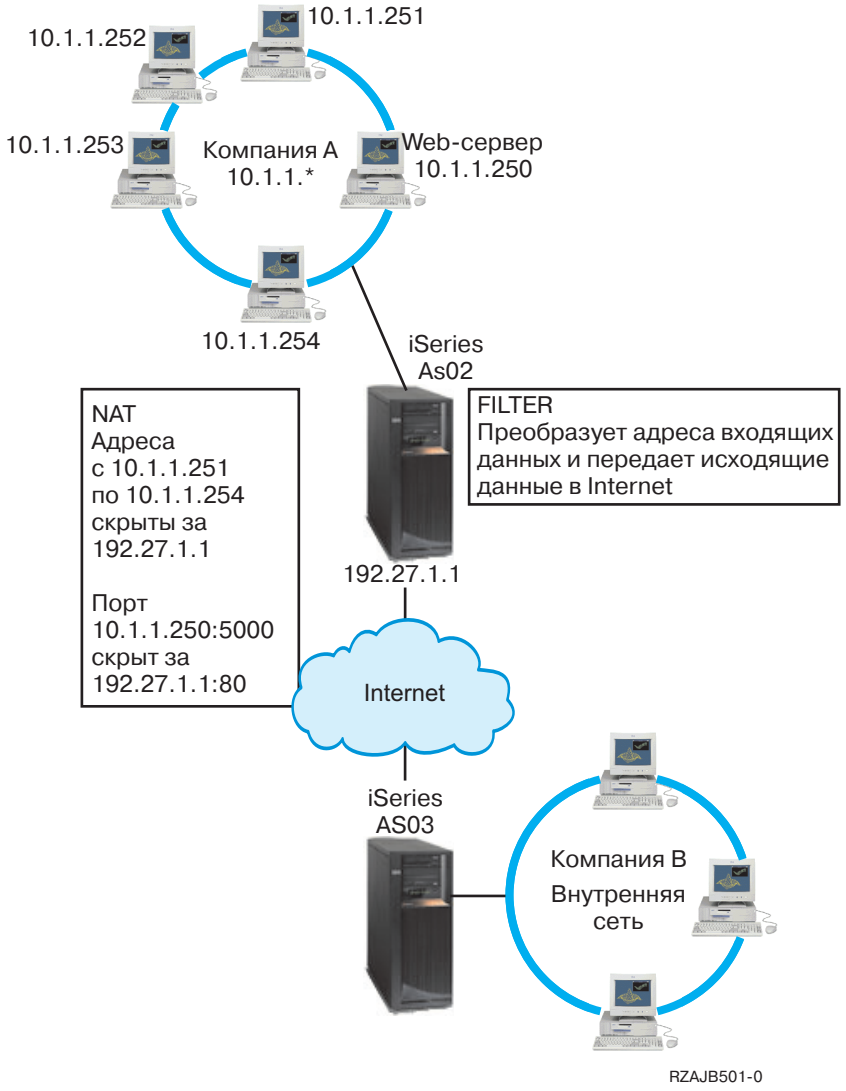
“Активация правил обработки пакетов” на стр. 27
Последним этапом настройки правил обработки пакетов является активизация созданных правил.

Сценарий: NAT в сочетании с фильтрацией пакетов IP

В этом сценарии ваша компания использует преобразование сетевых адресов (NAT) и фильтрацию IP-пакетов совместно. Требуется скрыть персональные компьютеры и Web-сервер за одним внешним IP-адресом, разрешая другим компаниям доступ к Web-серверу.

Ситуация

Предположим, что у вас есть внутренняя сеть среднего размера, в которой модель System i играет роль шлюза. Система-шлюз должна пересылать все пакеты выделенному внутреннему Web-серверу. Этот Web-сервер работает с портом 5000. Вы хотите скрыть все внутренние компьютеры и Web-сервер за адресом интерфейса System i interface (AS02 на рисунке). Тем не менее, у других компаний должен быть доступ к Web-серверу. Как решить поставленную задачу?



Решение

Используя совместно IP-фильтрацию и NAT, можно настроить персональные компьютеры и Web-сервер:

- Скрытый NAT, чтобы скрыть внутренние персональные компьютеры за внешним адресом 192.27.1.1 (это позволит им подключаться к Internet).
- NAT с преобразованием порта, чтобы скрыть адрес Web-сервера 10.1.1.250 и номер порта 5000 за внешним адресом 192.27.1.1 и номером порта 80. Обратите внимание, что в обоих правилах NAT указан один и тот же адрес 192.27.1.1. Это допустимо, так как соответствующие внутренние адреса не совпадают. Правило NAT преобразования порта разрешает передавать в систему только пакеты для порта 80. Поступившие пакеты с другим адресом или номером порта NAT преобразовывать не будет. Такие пакеты будет отброшены.
- Правила, которые разрешают принимать от внешних систем любые пакеты, обработанные NAT, и отправлять любые пакеты в Internet.

Настройка

Для настройки описанных в этом сценарии правил обработки пакетов с помощью скрытого NAT воспользуйтесь мастером Преобразования адресов в System i Navigator. Мастеру требуется следующая информация:

- Набор скрываемых адресов: с 10.1.1.251 по 10.1.1.254
- Адрес интерфейса, за которым следует скрыть этот набор адресов: 192.27.1.1

Для запуска мастера Преобразование адресов выполните следующие действия:

1. В System i Navigator выберите ***ваша система*** → **Сеть** → **Стратегии IP**.
2. Щелкните правой кнопкой мыши на значке **Правила обработки пакетов** и выберите **Редактор правил**.
3. В окне Настройка правил обработки пакетов выберите **Создать новый файл правил обработки пакетов** и нажмите **OK**.
4. В меню Мастеры выберите **Преобразование адресов** и следуйте инструкциям мастера по настройке правил преобразования скрытых адресов.

Следующее правило преобразует четыре адреса персональных компьютеров во внешний адрес. Это позволит им подключаться к Internet. Ниже приведен пример правил обработки пакетов с помощью скрытого NAT.

```
Скрыть адреса 10.1.1.251 - 10.1.1.254 как 192.27.1.1

ADDRESS HIDE1IP = 10.1.1.251 THROUGH 10.1.1.254
ADDRESS BEHIND1              IP = 192.27.1.1
HIDE HIDE1        BEHIND BEHIND1
```

RZAJB509-0

Для настройки NAT с преобразованием порта выполните следующие действия:

1. Из System i Navigator откройте Редактор правил обработки пакетов.
2. Создайте определенный адрес для представления адреса Web-сервера и порта 5000.
   a. В меню Вставить выберите **Адрес**.
   b. На странице Общие введите `Web250` в поле **Псевдоним адреса**.
   c. Выберите **IP-адреса** в списке **Определенный адрес**. Затем нажмите **Добавить** и введите IP-адрес Web-сервера `10.1.1.250` в соответствующем поле.
   d. Нажмите **OK**.
3. Создайте определенный адрес для представления внешнего адреса 192.27.1.1.

   Примечание: Поскольку вы уже создали определенный адрес для представления внешнего адреса 192.27.1.1 при настройке скрытого NAT, вы можете пропустить этот шаг в данном сценарии и перейти к шагу 4. Однако, если вы выполняете эти инструкции для настройки NAT с преобразованием порта для своей сети и вы не настраивали скрытый NAT, то продолжите выполнение этого шага:

   a. В меню Вставить выберите **Адрес**.
   b. На странице Общие введите или выберите `BEHIND1` в поле **Псевдоним адреса**.
   c. Выберите **IP-адреса** в списке **Определенный адрес**. Затем нажмите **Добавить** и введите `192.27.1.1` в поле **IP-адреса**.
   d. Нажмите **OK**.
4. Создайте правило NAT с преобразованием порта:
   a. В меню Вставить выберите **Скрыть**.
   b. На странице Общие выберите `Web250` в списке **Псевдоним скрытого адреса**.
   c. Выберите **BEHIND1** в списке **Псевдоним внешнего адреса**.
   d. Выберите **Разрешить входящие соединения** и введите `5000` в поле **Скрытый порт**.

e. Введите 80 в поле **Внешний порт**.
f. Введите 16 и выберите **секунды** в полях **Тайм-аут**.
g. Введите 64 в поле **Максимальное число диалогов**.
h. Выберите **OFF** в списке **Ведение журнала**.
i. Нажмите **OK**.

Следующий NAT с преобразованием порта преобразует адрес и порт Web-сервера во внешний адрес и номер порта. Обратите внимание, что в обоих правилах NAT указан один и тот же внешний IP-адрес. Это допустимо, так как соответствующие внутренние адреса не совпадают. Правило NAT преобразования порта разрешает передавать в систему только пакеты для порта 80.

Пример правила обработки пакетов с помощью NAT с преобразованием порта:

```
ADDRESS Web250   IP = 10.1.1.250
ADDRESS BEHIND1   IP = 192.27.1.1
HIDE Web250:5000   BEHIND BEHIND1:80   TIMEOUT = 16   MAXCON = 64   JRN = OFF
```

Для создания правил фильтрации, описанных в этом сценарии, выполните следующие действия:

1. Из System i Navigator откройте Редактор правил обработки пакетов.
2. Создайте правило фильтрации, пропускающее входящие пакеты, предназначенные для внутренней сети.
   a. В окне Настройка правил обработки пакетов выберите **Создать новый файл правил обработки пакетов** и нажмите **OK**.
   b. В меню Вставить выберите **Фильтр**.
   c. На странице Общие введите external_rules в поле **Имя набора**.
   d. Выберите **Пропускать** в списке **Действие**.
   e. Выберите **INBOUND** в списке **Направление**.
   f. Выберите **=** и ***** в списках **Псевдоним адреса отправителя**.
   g. Выберите **=** и введите 192.27.1.1 в полях **Псевдоним адреса получателя**.
   h. Выберите **OFF** в списке **Ведение журнала**.
   i. На странице Службы выберите **Служба**.
   j. Выберите **TCP** в списке **Протокол**.
   k. Выберите **=** и ***** в списках **Порт отправителя**.
   l. Выберите **=** и ***** в списках **Порт получателя**.
   m. Нажмите **OK**.
3. Создайте правило фильтрации, пропускающее исходящие пакеты, предназначенные для Internet:
   a. В окне Настройка правил обработки пакетов выберите **Открыть существующий файл правил обработки пакетов** и нажмите **OK**.
   b. В окне Открыть файл выберите файл **external_rules** и нажмите **Открыть**.
   c. В меню Вставить выберите **Фильтр**.
   d. На странице Общие выберите **external_rules** в выпадающем списке **Имя набора**.
   e. Выберите **Пропускать** в списке **Действие**.
   f. Выберите **OUTBOUND** в списке **Направление**.
   g. Выберите **=** и введите 192.27.1.1 в полях **Псевдоним адреса отправителя**.
   h. Выберите **=** и ***** в списках **Псевдоним адреса получателя**.
   i. Выберите **OFF** в списке **Ведение журнала**.
   j. На странице Службы выберите **Служба**.
   k. Выберите **TCP** в списке **Протокол**.
   l. Выберите **=** и ***** в списках **Порт отправителя**.
   m. Выберите **=** и ***** в списках **Порт получателя**.

n. Нажмите **OK**.

4. Определите интерфейс для созданного набора фильтров:
   a. В меню Вставить выберите **Интерфейс фильтра**.
   b. Выберите **Имя линии** и затем **TRNLINE** в списке **Имя линии**.
   c. На странице Наборы фильтров выберите **external_rules** в списке **Набор фильтров** и нажмите **Добавить**.
   d. Нажмите **OK**.

Следующие фильтры в сочетании с оператором HIDE разрешают принимать от внешних систем любые пакеты, обработанные NAT, и отправлять любые пакеты в Internet. NAT пропускает в систему только те пакеты, которые предназначены для порта 80. NAT не будет преобразовывать адреса пакетов, которые не соответствуют правилу NAT преобразования порта. Пример правил фильтрации:

```
FILTER SET external_files   ACTION = PERMIT   DIRECTION = INBOUND   SRCADDR = *   DSTADDR = 192.27.1.1
   PROTOCOL = TCP   DSTPORT = *   SRCPORT = *   JRN = OFF
FILTER SET external_files   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = 192.27.1.1   DSTADDR = *
   PROTOCOL = TCP   DSTPORT = *   SRCPORT = *   JRN = OFF
```

Данный оператор связывает набор правил фильтрации 'external_rules' с физическим интерфейсом.

```
FILTER_INTERFACE   LINE = TRNLINE   SET = external_files
```

Создав эти правила, проверьте их, чтобы убедиться в отсутствии ошибок. После этого правила можно активизировать.

Задачи, связанные с данной

"Проверка правил обработки пакетов" на стр. 26
Перед активизацией правил их необходимо проверить. Это позволит убедиться в том, что активизация пройдет без ошибок.

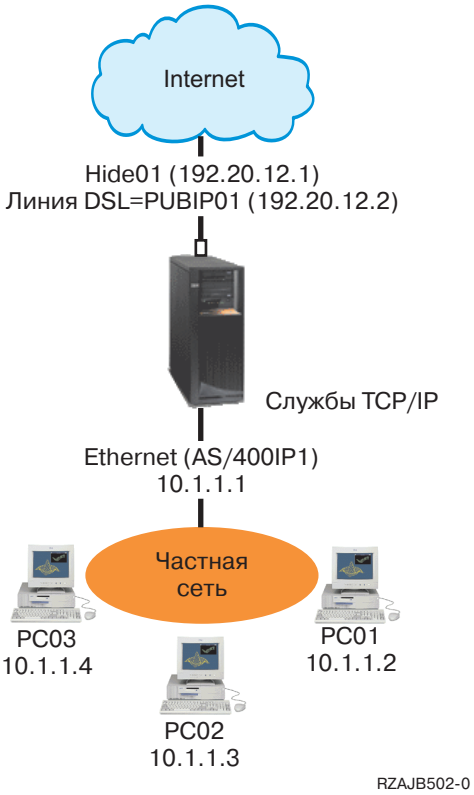
"Активация правил обработки пакетов" на стр. 27
Последним этапом настройки правил обработки пакетов является активизация созданных правил.

Сценарий: сокрытие IP-адресов с помощью маскирующего NAT

В этом сценарии ваша компания скрывает частные адреса персональных компьютеров с помощью маскирующего преобразования сетевых адресов (NAT). В то же время у этих компьютеров есть доступ к Internet.

Ситуация

Предположим, что в небольшой компании вы планируете запустить службу HTTP на платформе System i. В системе установлена одна карта Ethernet и подключены три персональных компьютера. Провайдер Internet (ISP) предоставил вам соединение DSL (Digital Subscriber Line) черед модем. Он назначил вам следующие внешние IP-адреса: 192.20.12.1 и 192.20.12.2. Всем компьютерам присвоены адреса вида 10.1.1.*x* во внутренней сети. Вы хотите скрыть частные адреса персональных компьютеров, чтобы предотвратить доступ внешних пользователей в свою сеть; вместе с тем вы хотите разрешить своим сотрудникам доступ в Internet. Как решить поставленную задачу?



Решение

Скройте адреса персональных компьютеров с 10.1.1.1 по 10.1.1.4 за внешним адресом 192.20.12.1. В этом случае пользователи системы с адресом 10.1.1.1 смогут работать со службами TCP/IP. NAT, преобразующий диапазон внутренних адресов, запрещает внешним системам устанавливать соединения с компьютерами внутренней сети, поскольку для запуска такого NAT передача должна быть инициализирована из внутренней сети. Однако такой NAT не защищает интерфейс System i. Для защиты системы от получения посторонней информации нужно применить соответствующие правила фильтрации.

Настройка

Для настройки правил обработки пакетов, описанных в этом сценарии, воспользуйтесь мастером Преобразование адресов в System i Navigator. Мастеру требуется следующая информация:

- Набор скрываемых адресов: с 10.1.1.1 по 10.1.1.4.
- Адрес интерфейса, за которым следует скрыть этот набор адресов: 192.20.12.1.

Для запуска мастера Преобразование адресов выполните следующие действия:

1. В System i Navigator выберите ***ваша система*** → **Сеть** → **Стратегии IP**.
2. Щелкните правой кнопкой мыши на значке **Правила обработки пакетов** и выберите **Редактор правил**.
3. В окне Настройка правил обработки пакетов выберите **Создать новый файл правил обработки пакетов** и нажмите **OK**.
4. В меню Мастеры выберите **Преобразование адресов** и следуйте инструкциям мастера по настройке правил преобразования скрытых адресов.

Ниже приведен пример правил обработки пакетов.

Скрыть 10.1.1.1 - 10.1.1.4 как 192.20.12.1

```
ADDRESS HIDE1 IP = 10.1.1.1 THROUGH 10.1.1.4
ADDRESS BEHIND1          IP = 192.20.12.1
HIDE HIDE1      BEHIND BEHIND1
```

RZAJB510-0

Создав эти правила, проверьте их, чтобы убедиться в отсутствии ошибок. После этого правила можно активизировать.

Понятия, связанные с данным

“Маскирующий NAT (сокрытие адресов)” на стр. 14
Маскирующий (скрытый) NAT позволяет скрыть фактический адрес персонального компьютера от внешних систем. NAT направляет данные от персонального компьютера системе, которая по существу выполняет функцию шлюза для персонального компьютера.

Задачи, связанные с данной

“Проверка правил обработки пакетов” на стр. 26
Перед активизацией правил их необходимо проверить. Это позволит убедиться в том, что активизация пройдет без ошибок.

“Активация правил обработки пакетов” на стр. 27
Последним этапом настройки правил обработки пакетов является активизация созданных правил.

Общая концепция применения правил обработки пакетов

Правила обработки пакетов подразделяются на правила преобразования сетевых адресов (NAT) и правила фильтрации IP-пакетов. Оба эти правила работают на уровне IP стека TCP/IP и защищают систему от потенциальной опасности, связанной с получением и передачей данных TCP/IP.

Для лучшего понимания правил обработки пакетов вам необходимо ознакомиться со следующими концепциями, применительно к вашей системе:

- Правила обработки пакетов в сравнении с другими способами обеспечения безопасности i5/OS
- NAT

Примечание: Используя примеры исходного кода, вы принимаете условия соглашения Лицензирование и отказ от гарантий на предоставляемый код.

Терминология правил обработки пакетов

Применяемые термины, связанные с обработкой пакетов.

border address
Граничный адрес. Внешний адрес, отделяющий защищенную сеть от незащищенной. Он представляет собой IP-адрес реально существующего интерфейса системы. При определении адреса в системе необходимо указать его тип. Например, IP-адреса компьютеров, подключенных к внутренней сети, являются защищенными, а внешний IP-адрес системы - граничным.

firewall
Брандмауэр. Логический барьер между внутренней и внешней сетью. Брандмауэр включает в себя программные и аппаратные компоненты, а также стратегию защиты, задающую правила доступа к информации и правила ее передачи между защищенными и незащищенными системами.

maxcon
Параметр, используемый в правилах маскирующего преобразования сетевых адресов. Он задает максимальное число одновременных диалогов. Этот параметр необходимо задать при настройке правил маскирующего NAT. Значение по умолчанию равно 128. Этот параметр применяется только в правилах маскирующего NAT.

NAT conversation

Диалог NAT. Диалог NAT задает взаимосвязь между следующими IP-адресами и номерами портов:

- Внутренним исходным IP-адресом и исходным номером порта (не обработанным NAT).
- Внешним исходным IP-адресом (обработанным NAT) и внешним исходным номером порта (обработанным NAT).
- Целевым IP-адресом и номером порта во внешней сети.

PPP filter identifier

ИД фильтра PPP. ИД фильтра PPP позволяет применять правила фильтрации к интерфейсу, определенному в профайле двухточечного соединения. Кроме того, идентификатор фильтра PPP связывает правила фильтрации с группами пользователей в двухточечном профайле. Поскольку двухточечный профайл связан с определенным IP-адресом, идентификатор фильтра неявно определяет интерфейс, к которому будут применяться правила.

timeout

Тайм-аут. Тайм-аут задает максимальный интервал, в течение которого может продолжаться диалог. Если тайм-аут будет недостаточным, то диалог будет слишком рано прерываться. Значение по умолчанию равно 16.

Информация, связанная с данной

Сценарий: Управление доступом удаленных пользователей к ресурсам с помощью групповых стратегий и фильтрации IP-пакетов

Правила обработки пакетов в сравнении с другими способами обеспечения безопасности i5/OS

В ситуациях повышенного риска, например, при организации защиты рабочей системы или соединений между вашей платформой System i и и другими системами в сети, возможно, вам понадобится рассмотреть дополнительные средства защиты.

В системе предусмотрен ряд встроенных компонентов, обеспечивающих защиту системы от нескольких типов внешних угроз. Правила обработки пакетов представляют собой простой и недорогой способ защиты системы. В ряде случаев вы можете с их помощью обеспечить необходимую защиту без приобретения дополнительных продуктов.

Информация о различных средствах защиты приведена в следующих разделах справочной системы Information Center:

- **Защита системы System i при работе с Internet**

  Этот раздел содержит информацию о типах внешних угроз и способах защиты данных, передаваемых по Internet.
- **Secure Sockets Layer (SSL)**

  Протокол SSL позволяет устанавливать защищенные соединения между приложениями сервера и их клиентами. Данный раздел посвящен применению SSL в приложениях i5/OS.
- **Виртуальные частные сети (VPN)**

  VPN позволяет вашему предприятию безопасно расширить свою частную сеть на основе существующей структуры открытой сети, такой как Internet. В этом разделе приведено описание VPN и способов ее применения в вашей системе.

Преобразование сетевых адресов

Преобразование сетевых адресов (NAT) позволяет установить защищенное соединение с Internet, не изменяя внутренние IP-адреса.

В связи с ростом популярности Internet число свободных IP-адресов быстро уменьшается. В рамках организаций создаются частные сети, в которых могут назначаться любые IP-адреса. Однако, если в сетях двух компаний применяются одинаковые IP-адреса, то при подключении к Internet могут возникнуть

ошибки. Для работы в Internet системе должен быть выделен уникальный, зарегистрированный адрес. Как следует из названия, функция преобразования сетевых адресов (NAT) обеспечивает преобразование одних IP-адресов в другие.

Правила обработки пакетов включают три метода NAT. NAT обычно используется для табличного преобразования адресов (статический NAT) или для их сокрытия (маскирующий NAT). NAT позволяет решить некоторые проблемы адресации путем преобразования или сокрытия адресов.

Пример: Сокрытие внутренних IP-адресов от внешних пользователей

Предположим, вы установили на платформе System i общедоступный Web-сервер. Однако вы не хотите, чтобы внешним пользователям был известен IP-адрес системы во внутренней сети. Вы можете создать правила NAT для преобразования внутренних адресов во внешние адреса, доступные в Internet. В данном случае действительный адрес системы скрыт и система будет защищена от внешних атак.

Пример: Преобразование IP-адреса внутреннего хоста в другой IP-адрес

Предположим, что хостам внутренней сети присвоены частные IP-адреса, и вы хотите обеспечить этим хостам доступ к Internet. Для этого настройте преобразование IP-адреса внутреннего хоста в другой IP-адрес. Для соединения с хостами Internet должен применяться внешний IP-адрес. Следовательно, с помощью NAT внутренние IP-адреса должны преобразовываться во внешние. Только в этом случае пакеты из внутренней сети смогут передаваться по Internet.

Пример: Обеспечение совместимости IP-адресов двух сетей

Предположим, вы хотите предоставить удаленному хосту (например, из сети вендора) доступ к одному из внутренних хостов вашей сети. В обеих сетях применяются внутренние адреса в формате (10.*x*.*x*.*x*), что может привести к конфликту адресов и ошибкам в маршрутизации. Функция NAT позволяет избежать конфликта путем преобразования адресов внутренних хостов.

Ссылки, связанные с данной

“Создание правил фильтрации IP-пакетов” на стр. 23
При создании фильтра вы указываете правило для управления передачей данных IP.

Статический NAT (преобразование адресов)

Статическое преобразование сетевых адресов (NAT) выполняет взаимно однозначное преобразование внутренних IP-адресов во внешние. Это позволяет преобразовать IP-адрес внутренней сети во внешний IP-адрес.

Статический NAT позволяет устанавливать соединения как внутренним, так и внешним системам, например, хостам Internet. Этот тип преобразования особенно рекомендуется применять для организации общего доступа к системе, находящейся во внутренней сети. Для этого нужно создать правило NAT для преобразования фактического адреса системы во внешний адрес. Этот адрес будет доступен внешним пользователям. В этом случае никто не сможет получить информацию о внутренней сети для последующих атак извне.

Ниже перечислены особенности статического NAT:

- Это взаимно однозначное преобразование.
- Его можно инициировать как из внешней, так и из внутренней сети.
- Целевой адрес для преобразования может быть любым адресом.
- Целевой адрес для преобразования не может применяться в качестве интерфейса IP
- Нельзя применять NAT для преобразования портов.

Внимание: Будьте внимательны при использовании статического NAT для преобразования адреса персонального компьютера в стандартный адрес платформы System i. *Внешний адрес* - адрес, который чаще других применяется для обмена данными с Internet и внутренней сетью. Если этот IP-адрес будет применяться для преобразования внутреннего адреса, то все пакеты, обработанные NAT, будут передаваться на частный внутренний адрес. Поскольку этот интерфейс будет зарезервирован для NAT, система и интерфейс перестанут работать правильно.

Понятия, связанные с данным

“Сценарий: преобразование IP-адресов с помощью NAT” на стр. 2
В этом сценарии частные IP-адреса сети вашей компании преобразуются во внешние адреса с помощью статического преобразования сетевых адресов (NAT).

Маскирующий NAT (сокрытие адресов)

Маскирующий (скрытый) NAT позволяет скрыть фактический адрес персонального компьютера от внешних систем. NAT направляет данные от персонального компьютера системе, которая по существу выполняет функцию шлюза для персонального компьютера.

Маскирующий NAT позволяет преобразовывать несколько адресов в один IP-адрес. С помощью маскирующего NAT можно скрыть один или несколько внутренних адресов за одним внешним IP-адресом. Данный внешний адрес является целевым адресом для преобразования внутренних адресов и должен быть определен в качестве интерфейса в вашей системе. Для этого сам внешний адрес должен быть определен как граничный (BORDER).

Сокрытие нескольких адресов

Для того чтобы скрыть несколько адресов, необходимо задать диапазон адресов, преобразуемых NAT в системе. Ниже описан сценарий его работы:

1. Исходный IP-адрес заменяется на внешний IP-адрес. Такая замена выполняется в заголовке IP-пакета.
2. Номер исходного порта IP (если он есть) в заголовке TCP или UDP заменяется на временный номер порта.
3. Диалог - это связь между новым исходным IP-адресом и номером порта.
4. Существующий диалог позволяет серверу NAT выполнять обратное преобразование адресов IP-дейтаграмм, поступающих из внешней системы.

Маскирующий NAT обрабатывает только те пакеты, которые отправляются из внутренней сети. При этом IP-пакет преобразуется средствами NAT при передаче через сервер NAT. Маскирующий NAT запрещает пересылку внешних пакетов во внутреннюю сеть. Это обеспечивает дополнительную защиту от внешних атак. Кроме того, для подключения к Internet нескольких пользователей вам потребуется приобрести только один IP-адрес.

Ниже перечислены особенности маскирующего NAT:

- Внутренний IP-адрес или диапазон адресов связывается на рабочей станции NAT с внешним IP-адресом
- Маскирующий NAT можно инициировать только из внутренней сети.
- Номера портов связываются с временными номерами портов. Это означает, что от внешней сети скрывается не только адрес, но и номер порта.
- Адрес, зарегистрированный на рабочей станции NAT, может применяться и для других целей.

Примечание:

Если NAT настроен неправильно, преобразование адресов может работать неверно. Например, IP-адреса могут не преобразовываться, а пакеты, которые следует принять - отклоняться. В любом случае аппаратное и программное обеспечение не будет повреждено. При изменении параметров учитывайте следующие сведения:

- Параметр MAXCON должен быть достаточно большим, так как он определяет число одновременно работающих диалогов. Например, при работе с FTP (File Transfer Protocol) вам потребуется как минимум два активных диалога. В этом случае необходимо присвоить переменной MAXCON достаточно большое значение, чтобы обслуживать несколько диалогов на каждом компьютере. Подсчитайте, сколько параллельных диалогов может быть установлено в сети. Значение по умолчанию равно 128.
- Значение параметра TIMEOUT (применяется в операторе HIDE) должно предоставлять достаточное время для завершения диалога между компьютером и сервером. Для правильной работы маскирующего NAT должен быть запущен внутренний диалог. Тайм-аут определяет время ожидания ответа для внутреннего диалога. Значение по умолчанию - 16.
- Маскирующий NAT поддерживает только следующие протоколы: TCP, UDP (User Datagram Protocol) и ICMP (Internet Control Message Protocol).
- При использовании NAT необходимо также настроить пересылку дейтаграмм IP. С помощью команды Изменить атрибуты TCP/IP (CHGTCPA) убедитесь, что эта опция включена.

Понятия, связанные с данным

“Заголовок IP-пакета” на стр. 17
В правилах фильтрации критерием для сравнения пакетов могут служить поля заголовков IP, TCP, UDP и ICMP.

“Сценарий: сокрытие IP-адресов с помощью маскирующего NAT” на стр. 9
В этом сценарии ваша компания скрывает частные адреса персональных компьютеров с помощью маскирующего преобразования сетевых адресов (NAT). В то же время у этих компьютеров есть доступ к Internet.

Маскирующий NAT с преобразованием порта

NAT (преобразование сетевых адресов) с преобразованием порта является разновидностью маскирующего NAT.

NAT с преобразованием порта позволяет скрыть не только IP-адрес, но и номер порта. Это позволяет обрабатывать пакеты, которые поступают как от внутренних компьютеров, так и от внешних систем. Такой тип NAT применяется в том случае, если внешним компьютерам или клиентам нужно обеспечить доступ к рабочей станции или системе частной сети. В сеть пропускаются только те пакеты IP, в которых и IP-адрес, и порт совпадают с указанными.

Подключение внутреннего компьютера к внешнему

Если внутренний компьютер с *адресом 1: портом 1* отправляет пакет внешней рабочей станции, NAT попытается найти правило преобразования для *адреса 1: порта 1*. Если будет найдено правило NAT, заданное для исходного IP-адреса (адреса 1) и исходного номера порта (порт 1), то NAT активизирует диалог и выполнит преобразование. Исходный IP-адрес и исходный номер порта заменяются на значения, указанные в правиле NAT. *адрес 1: порт 1* заменяется на *адрес 2: порт 2*.

Подключение внешнего компьютера к внутреннему

Пусть внешний компьютер отправил пакет IP с целевым адресом *адрес 2* и целевым номером порта *порт 2*. Сервер NAT производит обратное преобразование дейтаграммы с существующим диалогом или без него. Это означает, что NAT автоматически создаст диалог, если его еще нет. *адрес 2: порт 2* будет преобразован в *адрес 1: порт 1*.

Ниже перечислены особенности маскирующего NAT с преобразованием порта:

- Маскирующий NAT с преобразованием порта производит взаимно однозначное преобразование.
- Маскирующий NAT с преобразованием порта можно инициировать как из внешней, так и из внутренней сети.

- Зарегистрированный адрес, который применяется для преобразования, должен быть определен на платформе System i, выполняющей преобразования NAT.
- Зарегистрированный адрес недоступен для потоков IP, не преобразуемых по правилам NAT. Однако, если этот адрес попытается использовать номер порта, заданный в правилах NAT в качестве скрытого порта, то поток будет преобразован. Работа с интерфейсом станет невозможной.
- Обычно номера портов преобразуются в номера стандартных портов, так что дополнительная информация не нужна. Например, вы можете запустить сервер HTTP, привязанный к порту 5123, а затем преобразовать его во внешний IP-адрес с портом 80. Если же вы хотите скрыть исходный номер порта за другим (нестандартным) номером порта, то клиенту должен быть передан номер целевого порта. В противном случае соединение не будет установлено.

Замечания:

- Параметр MAXCON должен быть достаточно большим, так как он определяет число одновременно работающих диалогов. Например, при работе с FTP (File Transfer Protocol) вам потребуется как минимум два активных диалога. Необходимо присвоить переменной MAXCON достаточно большое значение, чтобы обслуживать несколько диалогов на каждом компьютере. Значение по умолчанию равно 128.
- Маскирующий NAT поддерживает только следующие протоколы: TCP, UDP (User Datagram Protocol) и ICMP (Internet Control Message Protocol).
- При использовании NAT необходимо также настроить пересылку дейтаграмм IP. С помощью команды Изменить атрибуты TCP/IP (CHGTCPA) убедитесь, что эта опция включена.

Фильтрация IP-пакетов

Этот компонент фильтрации IP-пакетов правил обработки пакетов позволяет управлять потоками IP, поступающими в сеть и исходящими из сети.

Он позволяет пропускать или отбрасывать пакеты на основе заданных правил фильтрации.

Можно создать один набор правил, который будет применяться для нескольких линий связи, либо свой набор правил для каждой линии. Правила фильтрации связываются именно с линиями связи; например, Token-Ring, а не с интерфейсами или IP-адресами. Система последовательно просматривает список правил для текущей линии связи и проверяет соответствие пакета правилу. Сравнение выполняется до первого совпадения, после чего найденное правило применяется.

Это означает, что выполняется действие, заданное в правиле.

- PERMIT — разрешить обычную обработку пакета
- DENY — немедленно отклонить пакет
- IPSEC — отправить пакет по соединению виртуальной частной сети (VPN), указанному в правиле фильтрации

Примечание: В данном случае, Протокол безопасности IP (IPSec) - это действие, которое можно задать в правиле фильтрации. Хотя в этом разделе не рассматривается применение IPSec, важно понимать, что правила фильтрации и виртуальная частная сеть (VPN) тесно связаны между собой.

Сравнение выполняется до тех пор, пока не будут обработаны все пакеты. Если для пакета не будет найдено ни одного правила, он будет автоматически отброшен системой. Это достигается за счет применения правила запрета по умолчанию. Обратите внимание, что хотя обычные правила фильтрации предназначены для пропуска пакетов только в одном направлении, правило запрета по умолчанию применяется в обоих направлениях, т.е. будут отбрасываться и входящие, и исходящие пакеты.

Информация, связанная с данной

Виртуальная частная сеть (VPN)

Примеры фильтров

Данный пример оператора фильтра демонстрирует правильные синтаксические конструкции правил обработки пакетов в системе и совместную работу различных операторов в одном файле.

Файл следует применять только в качестве примера.

Обычный фильтр может выглядеть следующим образом:

```
FILTER SET TestFilter   ACTION = PERMIT   DIRECTION = INBOUND SRCADDR = 162.56.39.100   DSTADDR
= *   PROTOCOL = *   DSTPORT >= 1024  SRCPORT = 80
```

Этот фильтр пропускает любые входящие пакеты (INBOUND) с адресом отправителя 162.56.39.100, портом отправителя 80 и портом получателя 1024 или более.

Поскольку поток IP обычно передается в обоих направлениях (INBOUND и OUTBOUND) по соединению, в системе, как правило, создаются два связанных фильтра для обработки потоков в обоих направлениях. Эти два фильтра называются зеркальным отражением друг друга и показаны в следующем примере:

```
FILTER SET TestFilter   ACTION = PERMIT   DIRECTION = INBOUND SRCADDR = 162.56.39.100   DSTADDR
= *   PROTOCOL = *   DSTPORT >= 1024  SRCPORT = 80  FILTER SET TestFilter   ACTION = PERMIT
DIRECTION = OUTBOUND   SRCADDR = *   DSTADDR = 162.56.39.100   PROTOCOL = *   DSTPORT = 80
SRCPORT >= 1024
```

Вы, конечно, заметили, что у этих фильтров совпадает имя набора, TestFilter. Все фильтры с одинаковым именем набора считаются принадлежащими к одному набору. Число фильтров в наборе не ограничено. Когда вы активизируете фильтры из заданного набора, они просматриваются в том же порядке, в котором они записаны в файле.

Отдельный фильтр при активизации правил не работает. Вы должны применять набор фильтров в интерфейсе. Ниже приведен пример применения набора, TestFilter, к интерфейсу линии Ethernet:

```
FILTER_INTERFACE   LINE = ETH237   SET = TestFilter
```

После активизации этих правил по линии ETH237 будут передаваться только IP-пакеты, разрешенные набором TestFilter.

Примечание: Система добавляет правило запрета по умолчанию DENY ALL TRAFFIC в конец всех активизированных фильтров интерфейса. При добавлении правил в интерфейс, через который происходит настройка платформы System i, следует обязательно разрешить доступ к платформе System i для вашей рабочей станции или рабочей станции пользователя, настраивающего систему. В противном случае соединения с системой не будет.

Фильтр может состоять из нескольких наборов, например:

```
 FILTER_INTERFACE   LINE = ETH237   SET = set1, set2, set3
```

Эти наборы будут обработаны в указанном порядке (set1, set2 и set3). Правила, входящие в набор, просматриваются в том же порядке, в котором они записаны в файле. Это означает, что взаимное расположение фильтров из разных наборов не играет никакой роли. Очередность фильтров имеет значение только внутри одного набора.

Заголовок IP-пакета

В правилах фильтрации критерием для сравнения пакетов могут служить поля заголовков IP, TCP, UDP и ICMP.

Ниже приведен полный список таких полей:

- Исходный IP-адрес

- Протокол (например, TCP, UDP)
- Целевой IP-адрес
- Исходный порт
- Целевой порт
- Направление (для принимаемых, отправляемых или любых дейтаграмм)
- Бит SYN заголовка TCP

Например, вы можете задать правило на основе целевого IP-адреса, исходного IP-адреса и направления (для принимаемых пакетов). Этому правилу будут соответствовать все полученные пакеты с заданным исходным и целевым адресом. Для них будет выполнено действие, указанное в правиле. Система отбрасывает все пакеты, для которых не найдено ни одно правило фильтрации. Это называется *правило запрета по умолчанию*.

Примечание: Правило запрета по умолчанию действует в том случае, если для физического интерфейса активно хотя бы одно правило фильтрации. Это правило может быть добавлено пользователем или создано Навигатором System i Navigator. Независимо от направления, в котором действует фильтр, правило запрета по умолчанию применяется в обоих направлениях. Если для физического интерфейса не активизировано ни одно правило фильтрации, то правило запрета по умолчанию не применяется.

Понятия, связанные с данным

“Маскирующий NAT (сокрытие адресов)” на стр. 14
Маскирующий (скрытый) NAT позволяет скрыть фактический адрес персонального компьютера от внешних систем. NAT направляет данные от персонального компьютера системе, которая по существу выполняет функцию шлюза для персонального компьютера.

Совместное использование правил NAT и правил фильтрации IP-пакетов

Службы преобразования сетевых адресов (NAT) и фильтрации IP-пакетов работают независимо друг от друга, поэтому их можно использовать одновременно.

Если включена только функция NAT, система будет преобразовывать адреса пакетов без их фильтрации. Аналогично, если включена только фильтрация IP-пакетов, система будет только фильтровать IP-пакеты. Если вы зададите как правила NAT, так и правила фильтрации, то система будет преобразовывать адреса пакетов и фильтровать пакеты. Эти действия выполняются в определенном порядке. При приеме пакетов сначала применяются правила NAT. При отправке пакетов сначала применяются правила фильтрации.

Рекомендуется хранить правила NAT и правила фильтрации в отдельных файлах, хотя это и не обязательно. Это облегчает просмотр файлов и исправление ошибок в правилах. Способ хранения правил не влияет на число ошибок. Даже если правила фильтрации и NAT будут храниться в отдельных файлах, вы сможете активизировать оба набора правил. В этом случае вам потребуется убедиться, что правила логически непротиворечивы.

Для того чтобы активизировать оба набора правил, укажите оператор *include*. Допустим, правила фильтрации хранятся в файле A, а правила NAT - в файле B. С помощью оператора include вы можете вставить содержимое файла B в файл A, не переписывая все правила заново.

Задачи, связанные с данной

“Включение файлов в правила обработки пакетов” на стр. 25
Используя утилиту **Include** (включить) Редактора правил обработки пакетов, можно активизировать в системе несколько файлов правил обработки пакетов.

Совместное использование нескольких правил фильтрации IP-пакетов

Объединение правил фильтрации называется *набором*. Фильтры, содержащиеся в наборе, обрабатываются по порядку, сверху вниз. Несколько наборов обрабатываются в том порядке, в котором они указаны в операторе FILTER_INTERFACE.

Ниже приведен пример набора, содержащего три фильтра. При любой ссылке на этот набор будут включены все три правила. Часто проще бывает включить все правила фильтрации в один набор.

Примечание: Используя примеры исходного кода, вы принимаете условия соглашения Лицензирование и отказ от гарантий на предоставляемый код.

```
FILTER SET all ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR  %
        = * PROTOCOL = TCP/STARTING DSTPORT = * SRCPORT = * FRAGMENTS  %
        = HEADERS JRN = FULL
FILTER SET all ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR  %
        = * PROTOCOL = TCP DSTPORT = * SRCPORT = * FRAGMENTS = NONE  %
        JRN = OFF
FILTER SET all ACTION = PERMIT DIRECTION = INBOUND SRCADDR = * DSTADDR  %
        = * PROTOCOL = ICMP TYPE = * CODE = * FRAGMENTS = NONE JRN  %
        = OFF
FILTER_INTERFACE LINE = ETHLINE SET = all
###Ethernet line ETHLINE
```

Защита от несанкционированного доступа путем имитации

Под несанкционированным доступом путем имитации понимают попытку другого пользователя получить доступ к вашей системе, выдавая свою систему за надежную. Рекомендуется защищать любые интерфейсы, связанные с внешней сетью, от подобных атак.

Вы можете настроить защиту от несанкционированного доступа путем имитации с помощью соответствующего мастера, запускаемого из Редактора правил обработки пакетов навигатора System i Navigator. Мастер поможет вам создать подходящие правила защиты для уязвимых интерфейсов. После активизации таких правил никакая система из внешней сети не сможет выдавать себя за надежную систему из внутренней сети.

Планирование правил обработки пакетов

Перед подключением сетевых ресурсов к Internet следует составить план защиты с учетом возможных угроз безопасности системы.

Вы должны в деталях представлять себе, каким образом вы собираетесь использовать Internet; кроме того, вы должны располагать подробным описанием конфигурации внутренней сети. На основе этого вы сможете правильно определить необходимые меры по защите системы. Информация, приведенная в разделе Защита System i при подключении к Internet, поможет вам составить план защиты сети.

После составления плана вы можете приступить к настройке правил обработки пакетов.

Задачи, связанные с данной

“Настройка правил обработки пакетов” на стр. 21
Данная справочная таблица содержит описание задач, которые необходимо выполнить для проверки правил.

Правила обработки пакетов: Требования к правам доступа пользователя

Прежде чем приступить к настройке правил обработки пакетов на платформе System i, убедитесь в том, что у вас есть необходимые права доступа. Для вашего профайла необходимы специальные права доступа *IOSYSCFG.

Если вы собираетесь настраивать правила обработки пакетов под управлением ИД пользователя QSECOFR или аналогичного (типа *SECOFR), либо у вас есть права доступа *ALLOBJ, то этого будет достаточно. Если у вас нет прав требуемого ИД пользователя или *ALLOBJ, то вам потребуется доступ к следующим каталогам, файлам и к ИД пользователя QSYS:

1. Права на добавление объектов, *RXW, и права доступа к данным, OBJMGT, к следующим трем файлам:

   ```
   /QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.i3p
   /QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.txt
    /QIBM/ProdData/OS400/TCPIP/PacketRules/Template4PacketRules.tcpipml
   ```

2. Права на добавление объектов, *RWX, к следующим каталогам:

   ```
   /QIBM/UserData/OS400/TCPIP/PacketRules
   /QIBM/UserData/OS400/TCPIP/OpNavRules
   ```

3. Права на добавление объектов, *RWX, к следующим файлам:

   ```
   /QIBM/UserData/OS400/TCPIP/OpNavRules/VPNPolicyFilters.i3p
   /QIBM/UserData/OS400/TCPIP/OpNavRulesPPPFilters.i3p
   ```

4. Кроме того, вам понадобятся права доступа ADD к профайлу QSYS, поскольку ему будут принадлежать вновь созданные файлы правил.

Выше перечислены каталоги и файлы, которые Редактор правил обработки пакетов применяет по умолчанию. Если вы хотите хранить файлы в других каталогах, то вам будут необходимы права доступа к этим каталогам.

Правила обработки пакетов: Требования к системе

Убедитесь в том, что система соответствует минимальным требованиям, позволяющим применять правила обработки пакетов.

Для применения правил обработки пакетов необходимо, чтобы в системе были установлены следующие продукты:

- OS/400 V5R2, i5/OS V5R3 или выше.
- IBM System i Access for Windows (5761-XE1) и System i Navigator.
  - Сетевой компонент программы System i Navigator.
- Следует настроить IBM TCP/IP Connectivity Utilities for i5/OS (5761-TC1), включая интерфейсы IP, маршруты, имя локального хоста и имя локального домена.

Информация, связанная с данной

TCP/IP Tutorial and Technical Overview

V4 TCP/IP для AS/400: Больше отличных возможностей чем когда-либо

Правила обработки пакетов: Форма для планирования

Форма для планирования поможет вам собрать подробную информацию для составления плана применения правил обработки пакетов.

Эта информация позволит четко сформулировать требования к защите. Кроме того, она упростит настройку правил обработки пакетов. Ответьте на все вопросы, прежде чем приступать к настройке правил.

Эта информация необходима для разработки плана применения правил обработки пакетов	**Ответы**
Как выглядит схема сети и соединений? Нарисуйте ее.	
Какие маршрутизаторы и IP-адреса вы собираетесь применять?	

Эта информация необходима для разработки плана применения правил обработки пакетов	Ответы
Какие правила будут применяться для управления потоками TCP/IP, проходящими через системы? Для каждого из таких правил укажите следующие параметры потока TCP/IP: • служба, пакеты который будут разрешены или запрещены (например, HTTP, File Transfer Protocol (FTP) и т.д.); • стандартный номер порта для этой службы; • направление потока данных; • будут ли данные передаваться в качестве вызова или в ответ на вызов; • IP-адреса пакетов (исходный и целевой).	
Какие IP-адреса следует преобразовывать или скрывать? (Этот список нужен только в том случае, если вы планируете применять NAT).	

Настройка правил обработки пакетов

Данная справочная таблица содержит описание задач, которые необходимо выполнить для проверки правил.

В электронной справке Редактора правил обработки пакетов приведены соответствующие пошаговые инструкции.

После составления плана правил обработки пакетов можно приступить к фактическому созданию и применению правил.

__ Откройте Редактор правил обработки пакетов. Для того чтобы открыть Редактор правил обработки пакетов в окне System i Navigator, выполните следующие инструкции.

__ С помощью мастеров, входящих в состав Редактора правил обработки пакетов (версии V5R2 и выше), создайте файлы правил:

- Мастер **Разрешить службу**

  Этот мастер создаст и установит набор правил, пропускающий пакеты для данной службы TCP или UDP (User Datagram Protocol).

- Мастер **Защита от несанкционированного доступа путем имитации**

  Этот мастер создаст и установит набор правил, отклоняющий любые пакеты, поступающие на сервер не из предполагаемого интерфейса.

- Мастер **Преобразование адресов**

  Этот мастер создаст и установит набор правил преобразования или сокрытия адресов.

В зависимости от типа настраиваемых правил, эти мастеры создают все необходимые операторы фильтрации и преобразования сетевых адресов (NAT). Вы можете запустить мастеры из меню Мастеры Редактора правил обработки пакетов. Если вы предпочитаете самостоятельное создание правил, перейдите к следующему пункту справочной таблицы.

__ Определите псевдонимы адресов и служб, с которыми будут работать правила.
Примечание: При создании правил NAT определение псевдонимов адресов обязательно.

__ Создайте правила NAT. Это необходимо только в том случае, если вы собираетесь применять функцию NAT.

__ Определите, какие фильтры будут применяться к сети, контролируемой данной системой (задайте правила фильтрации).

__ Укажите дополнительные файлы, которые вы хотите включить в главный файл правил. Это нужно сделать только в том случае, если в новом файле правил планируется применять созданные ранее файлы правил.

__ Определите интерфейсы, к которым будут применяться правила.

__ Введите текстовое описание каждого файла правил.

__ Убедитесь, что активизация файлов пройдет без ошибок и сбоев - проверьте правила фильтрации.

__ Активизируйте файл с правилами фильтрации. Для того чтобы правила обработки пакетов вступили в силу, их необходимо активизировать.

__ Управляйте правилами обработки пакетов. После активизации правил обработки пакетов вы должны отслеживать их, чтобы обеспечивать защиту системы.

Задачи, связанные с данной

“Планирование правил обработки пакетов” на стр. 19
Перед подключением сетевых ресурсов к Internet следует составить план защиты с учетом возможных угроз безопасности системы.

“Управление правилами обработки пакетов” на стр. 28
Следует использовать все возможные средства для эффективного управления правилами обработки пакетов. Защита системы в значительной мере зависит от того, насколько точны и актуальны эти правила.

Доступ к редактору правил обработки пакетов

Для начального создания правил обработки пакетов в системе можно использовать Редактор правил обработки пакетов. Можно создать новый файл, отредактировать существующий файл или модифицировать примеры файлов, предусмотренные в системе.

Редактор правил обработки пакетов открывается через System i Navigator.

Для открытия Редактора правил обработки пакетов выполните следующие действия:

1. В System i Navigator откройте ***ваша система*** → **Сеть** → **Стратегии IP**.
2. Щелкните правой кнопкой мыши на **Правила обработки пакетов** и выберите **Редактор правил**.

Выполнение этих задач описано в электронной справке.

Ссылки, связанные с данной

“Устранению ошибок в правилах обработки пакетов” на стр. 30
В этом разделе приведены советы по устранению ошибок в правилах обработки пакетов.

Определение адресов и служб

При создании правил обработки пакетов необходимо указать, к каким IP-адресам и службам они будут применяться.

Определенные адреса (множества адресов, псевдонимы адресов) - это спецификации интерфейса, которым присвоены символьные имена. Вы должны определить псевдонимы адресов, когда соответствующие адреса образуют диапазон, подсеть, список идентификаторов двухточечных соединений или список несмежных адресов. Оператор определения адреса обязателен при создании правил преобразования адресов. Если адрес, который вы хотите представить, - это отдельный IP-адрес в фильтре, то оператор определения адреса необязателен. Псевдонимы служб позволяют определить службы и затем использовать их в любом количестве фильтров. Кроме того, псевдонимы служб позволяют отслеживать применение различных определений служб.

Определение псевдонимов адресов и служб упрощает обслуживание правил обработки пакетов. При создании правил вместо конкретных адресов и служб будут применяться псевдонимы. У псевдонимов есть несколько преимуществ:

- Снижается вероятность появления опечаток.
- Уменьшается число создаваемых правил фильтрации.

Предположим, что в сети работает несколько пользователей, у которых должен быть доступ к Internet. При этом им разрешено работать только с WWW. В этом случае правила можно создать двумя способами.

- Создайте правило фильтрации для каждого IP-адреса.
- Создайте псевдоним для всего набора адресов.

Так как число создаваемых правил велико, существует большая вероятность появления опечаток. Кроме того, создание правил займет значительное время. Во втором случае потребуется создать только два правила фильтрации. В каждом из них весь набор адресов будет заменен на псевдоним.

Аналогичным образом можно создавать и использовать псевдонимы для служб. Псевдоним службы определяет поля заголовков TCP, UDP (User Datagram Protocol) и ICMP (Internet Control Message Protocol), которые должны применяться в качестве критерия для сравнения пакетов. Например, можно выбрать исходный и целевой порт.

Напоминание: Для использования преобразование сетевых адресов (NAT) определение псевдонимов адресов обязательно. В правилах NAT могут применяться только псевдонимы адресов.

Инструкции определения адресов, псевдонимов служб и служб ICMP приведены в электронной справке Редактора правил обработки пакетов.

Если вы собираетесь применять преобразование сетевых адресов, перейдите к разделу Создание правил NAT. В противном случае перейдите к разделу "Создание правил фильтрации IP-пакетов" (фильтрация принимаемых и отправляемых IP-пакетов).

Задачи, связанные с данной

"Включение комментариев в правила обработки пакетов" на стр. 26
В комментариях к файлам правил обработки пакетов можно отразить цель создания правил.

Создание правил NAT

Для того чтобы можно было применять преобразование сетевых адресов (NAT), необходимо определить псевдонимы IP-адресов, которые планируется использовать.

В правилах NAT нельзя задавать обычные 32-разрядные адреса. Вместо фактического адреса, например 193.112.14.90, вы должны указать его псевдоним. Вместо указанных псевдонимов система будет преобразовывать связанные с ними IP-адреса. Таким образом, перед применением правил NAT необходимо определить адреса.

Редактор правил обработки пакетов позволяет создавать правила NAT двух типов. Один из них позволяет скрыть данный адрес, а второй - преобразовать данный адрес в другой адрес.

Сокрытие адресов

Можно скрыть внутренние адреса, сделав их недоступными во внешней сети. В правиле, скрывающем адреса, можно указать один IP-адрес для нескольких внутренних адресов. Такой тип NAT также называется маскирующим NAT.

Преобразование адресов

Правила преобразования адресов применяются в том случае, когда необходимо обеспечить однозначную пересылку пакетов, предназначенных для определенного внешнего адреса, на определенный внутренний адрес. Такой тип NAT также называется статическим NAT.

Инструкции по настройке сокрытия и преобразования адресов приведены в электронной справке Редактора правил обработки пакетов.

Следующий раздел

Если вы собираетесь настроить фильтрацию входящих и исходящих пакетов в сети, перейдите к разделу Создание правил фильтрации IP-пакетов. Иначе перейдите к разделу "Включение комментариев в правила обработки пакетов" на стр. 26.

Создание правил фильтрации IP-пакетов

При создании фильтра вы указываете правило для управления передачей данных IP.

Такие правила устанавливают критерии, по которым будут пропускаться или отбрасываться пакеты, поступающие в систему. Решение о направлении пакетов IP принимается на основе информации, указанной в заголовке пакета, и действия, заданного в правиле фильтрации. Система удаляет все пакеты, для которых не найдено ни одно правило. Это называется *правилом запрета по умолчанию*. Расположенное в конце файла, правило запрета по умолчанию автоматически применяется в случае, когда пакет не подпадает ни под одно из предыдущих правил. Правило запрета по умолчанию действует только в том случае, когда активизировано хотя бы одно правило фильтрации.

Важное замечание: Когда вы добавляете правила в интерфейс, посредством которого вы настраиваете платформу System i, не забудьте внести разрешающее правило для своей рабочей станции или рабочей станции другого пользователя, также участвующего в настройке системы. В противном случае соединения с системой не будет. Вам придется войти в систему с помощью другого интерфейса, которому система доступна, например с Консоли управления. После этого с помощью команды RMVTCPTBL удалите все фильтры в системе.

Перед созданием правил фильтрации решите, будете ли вы применять преобразование сетевых адресов (NAT). Если да, то вы обязательно должны определить псевдонимы адресов и служб. Эти псевдонимы необходимы только для функции NAT, однако они могут применяться и другими функциями. Определение псевдонимов адресов и служб позволяет сократить число правил и снизить вероятность опечатки при вводе правила.

Ниже приведено несколько советов о том, как быстро и безошибочно создать правила фильтрации:

- Не создавайте одновременно несколько правил фильтрации. Например, создайте сначала все правила для Telnet, а затем все правила для FTP. Это позволяет объединить правила в логические группы, на которые вы можете ссылаться в дальнейшем.
- Правила фильтрации просматриваются в том порядке, в котором они записаны в файле. Указывайте правила в том порядке, в котором они должны применяться. Если порядок правил неправильный, то система не будет защищена от атак, так как пакеты не будут обрабатываться так, как вы запланировали. Ниже перечислены некоторые рекомендации:
  - В операторе FILTER_INTERFACE имена наборов фильтров должны быть перечислены точно в таком же порядке, в котором они определены в файле.
  - Во избежание проблем, вызванных неправильным порядком наборов, поместите все правила фильтрации в один набор.
- Проверяйте синтаксис правил в процессе создания. Проверять все правила сразу намного тяжелее.
- Создавайте наборы групп логически связанных файлов. Это важно, так как активным может быть только один файл правил. Ниже приведен соответствующий пример.
- Создавайте только разрешающие правила фильтрации. Пакеты, не соответствующие этим правилам, будут отбрасываться автоматически.
- Сначала создайте правила, которые будут применяться чаще всего.

Пример:

Совет: Создавайте именованные наборы. Допустим, вы планируете разрешить доступ к Telnet только избранным пользователям. Для того чтобы упростить работу с соответствующими правилами, объедините их в набор с именем `TelnetOK`. В качестве дополнительного критерия сравнения можно указать имя интерфейса, по которому разрешена передача данных Telnet. Для этого потребуется создать второй набор правил, полностью блокирующих передачу данных по Telnet. Эти правила можно объединить в набор с именем `TelnetNever`. Имя набора отражает его назначение. Кроме того, имя набора указывает, для каких интерфейсов он создан. Для того чтобы упростить задачу создания правил, следуйте приведенным выше советам.

Инструкции по настройке правил фильтрации IP-пакетов приведены в электронной справке Редактора правил обработки пакетов.

После создания фильтров вы можете включить файлы из правил обработки наборов в оператор фильтрации. Если это не требуется, перейдите к определению интерфейсов, к которым применяются правила (раздел “Определение интерфейсов для фильтра”).

Понятия, связанные с данным

“Преобразование сетевых адресов” на стр. 12
Преобразование сетевых адресов (NAT) позволяет установить защищенное соединение с Internet, не изменяя внутренние IP-адреса.

Ссылки, связанные с данной

“Устранению ошибок в правилах обработки пакетов” на стр. 30
В этом разделе приведены советы по устранению ошибок в правилах обработки пакетов.

Определение интерфейсов для фильтра

Для того чтобы иметь возможность создавать правила для отдельных интерфейсов, можно определить интерфейсы фильтра.

Перед этим нужно создать фильтры, которые система будет применять для различных интерфейсов. Если вы решите задать собственный адрес при определении интерфейса, в дальнейшем вы будете ссылаться на этот интерфейс по имени, а не по IP-адресу. Если вы решите не определять свой адрес, то будете ссылаться на интерфейс по IP-адресу.

При создании фильтров вы можете объединять несколько фильтров в один набор. Затем вы должны добавить имя набора в оператор FILTER_INTERFACE. В операторе должно быть указано то же имя набора, которое вы определили в фильтре. Например, если набору присвоено имя ALL и все фильтры входят в этот набор, то вы должны добавить имя набора ALL в оператор FILTER_INTERFACE. Вы можете не только указать несколько фильтров в наборе, но и несколько наборов в операторе FILTER_INTERFACE.

Кроме того, перед определением интерфейсов необходимо включить все дополнительные файлы правил, которые будут использоваться. После этого вы можете приступить к определению интерфейсов. Учтите, что наборы фильтров применяются в том порядке, в котором они перечислены в операторе определения интерфейса фильтров. Таким образом, в операторе FILTER_INTERFACE имена наборов фильтров должны быть перечислены в том порядке, в котором они определены в файле.

Инструкции по определению интерфейса фильтров приведены в электронной справке Редактора правил обработки пакетов.

Включение файлов в правила обработки пакетов

Используя утилиту **Include** (включить) Редактора правил обработки пакетов, можно активизировать в системе несколько файлов правил обработки пакетов.

Создание нескольких файлов упрощает управление правилами, особенно в тех случаях, когда требуется создать большое число правил для нескольких интерфейсов. Например, некоторые правила могут применяться для нескольких интерфейсов.

Вы можете создать эту группу внутри отдельного файла. Вместо того чтобы указывать правила заново в каждом новом файле, вы можете включить их в главный файл. Главный файл - это файл, который может быть активен в любой момент времени. Для добавления правил в главный файл предназначена функция объединения.

Кроме того, такой подход позволяет отделить правила NAT от правил фильтрации пакетов, заданных для интерфейса. Тем не менее, в каждый момент времени может быть активен только один файл.

Вы можете создать новый файл правил на основе уже существующего. Однако перед этим нужно создать новые правила фильтрации. Созданные правила нужно объединять по типу. В этом случае не потребуется создавать дублирующие правила. Вы сможете просто включать и исключать правила по мере надобности.

Инструкции по добавлению файла в правила обработки пакетов приведены в электронной справке Редактора правил обработки пакетов.

Понятия, связанные с данным

“Совместное использование правил NAT и правил фильтрации IP-пакетов” на стр. 18
Службы преобразования сетевых адресов (NAT) и фильтрации IP-пакетов работают независимо друг от друга, поэтому их можно использовать одновременно.

Включение комментариев в правила обработки пакетов

В комментариях к файлам правил обработки пакетов можно отразить цель создания правил.

Например, вы можете указать, что именно разрешает или запрещает то или иное правило. В будущем эта информация поможет вам быстро понять назначение того или иного правила. Если вам потребуется быстро исправить ошибку в защите, эти комментарии позволят вам вспомнить назначение используемых правил. Часто в таких случаях не хватает времени на выяснение назначения правил, поэтому настоятельно рекомендуется создавать комментарии.

Во всех окнах диалога, связанных с созданием и применением правил работы с пакетами, есть поле **Описание**. Это поле отведено для комментариев. Система игнорирует содержимое данного поля. Комментарий можно задать на любом этапе создания правила. Это снижает вероятность того, что вы забудете внести важный комментарий. Лучше всего записывать комментарии во время создания правил. Однако вы можете добавить комментарии и после создания всех правил.

Пошаговые инструкции по указанию комментариев в файле правил обработки пакетов приведены в электронной справке Редактора правил обработки пакетов.

Задачи, связанные с данной

“Определение адресов и служб” на стр. 22
При создании правил обработки пакетов необходимо указать, к каким IP-адресам и службам они будут применяться.

Проверка правил обработки пакетов

Перед активизацией правил их необходимо проверить. Это позволит убедиться в том, что активизация пройдет без ошибок.

Когда вы запускаете функцию проверки, система проверяет правила на наличие синтаксических и семантических ошибок и выдает результаты в окне сообщений, расположенном в нижней части Редактора правил обработки пакетов. Для перехода к сообщению, относящемуся к конкретному файлу и номеру строки, щелкните правой кнопкой мыши на ошибке и выберите **Перейти к строке** - строка с этой ошибкой в редактируемом файле будет выделена.

Перед запуском функции проверки рекомендуется просмотреть правила обработки пакетов, чтобы устранить явные ошибки. Правила с синтаксическими ошибками не будут активизированы. Функция проверки позволяет найти и устранить только синтаксические ошибки. Система не позволяет проверить правильность порядка правил. Это нужно проверить вручную. Помните, что правила применяются в том порядке, в котором они расположены. Неверный порядок правил может привести к неправильному выполнению фильтрации.

Инструкции по проверке правил обработки пакетов приведены в электронной справке Редактора правил обработки пакетов.

Понятия, связанные с данным

“Сценарий: преобразование IP-адресов с помощью NAT” на стр. 2
В этом сценарии частные IP-адреса сети вашей компании преобразуются во внешние адреса с помощью статического преобразования сетевых адресов (NAT).

“Сценарий: Создание правил фильтрации для работы с HTTP, Telnet и FTP” на стр. 4
В этом сценарии вы посредством фильтрации ограничиваете поток IP-пакетов, которым доступен Web-сервер вашей компании, пакетами протоколов HTTP, Telnet и FTP (File Transfer Protocol).

“Сценарий: NAT в сочетании с фильтрацией пакетов IP” на стр. 5
В этом сценарии ваша компания использует преобразование сетевых адресов (NAT) и фильтрацию IP-пакетов совместно. Требуется скрыть персональные компьютеры и Web-сервер за одним внешним IP-адресом, разрешая другим компаниям доступ к Web-серверу.

“Сценарий: сокрытие IP-адресов с помощью маскирующего NAT” на стр. 9
В этом сценарии ваша компания скрывает частные адреса персональных компьютеров с помощью маскирующего преобразования сетевых адресов (NAT). В то же время у этих компьютеров есть доступ к Internet.

Задачи, связанные с данной

“Просмотр правил обработки пакетов” на стр. 28
Перед активизацией правил не забудьте проверить их правильность.

Активация правил обработки пакетов

Последним этапом настройки правил обработки пакетов является активизация созданных правил.

Для того чтобы правила вступили в силу, вы должны их активизировать, или загрузить. Однако перед активизацией правил не забудьте проверить их правильность. Перед тем как активизировать правила, необходимо исправить все найденные ошибки. Активизация неверных правил может привести к тому, что система окажется незащищенной. В системе предусмотрена функция проверки синтаксиса, которая автоматически запускается при активизации правил. В связи с тем, что эта функция отслеживает только основные синтаксические ошибки, вы не должны полагаться только на нее. Рекомендуется также всегда проверять файлы правил вручную.

Если правила неприменимы к интерфейсу (например, если вы применяете только правила NAT), появится предупреждение (TCP5AFC). Оно не сигнализирует об ошибке. Оно просто обращает ваше внимание на факт возможно неправильного использования интерфейса. Прежде всего обращайте внимание на последнее сообщение. Если в нем говорится, что правила успешно активизированы, то все предыдущие сообщения являются предупреждениями.

Примечание: Активизация новых правил для всех интерфейсов приводит к замене предыдущего набора правил для всех физических интерфейсов. Это относится и к тем физическим интерфейсам, которые не упоминаются в новых правилах. Однако если вы активизируете набор правил для одного конкретного интерфейса, то будут заменены только правила для этого конкретного интерфейса. Существующие правила для других интерфейсов не изменятся.

После настройки и активизации правил обработки пакетов рекомендуется периодически обращаться к ним для контроля.

Понятия, связанные с данным

“Сценарий: преобразование IP-адресов с помощью NAT” на стр. 2
В этом сценарии частные IP-адреса сети вашей компании преобразуются во внешние адреса с помощью статического преобразования сетевых адресов (NAT).

“Сценарий: Создание правил фильтрации для работы с HTTP, Telnet и FTP” на стр. 4
В этом сценарии вы посредством фильтрации ограничиваете поток IP-пакетов, которым доступен Web-сервер вашей компании, пакетами протоколов HTTP, Telnet и FTP (File Transfer Protocol).

“Сценарий: NAT в сочетании с фильтрацией пакетов IP” на стр. 5
В этом сценарии ваша компания использует преобразование сетевых адресов (NAT) и фильтрацию IP-пакетов совместно. Требуется скрыть персональные компьютеры и Web-сервер за одним внешним IP-адресом, разрешая другим компаниям доступ к Web-серверу.

“Сценарий: сокрытие IP-адресов с помощью маскирующего NAT” на стр. 9
В этом сценарии ваша компания скрывает частные адреса персональных компьютеров с помощью маскирующего преобразования сетевых адресов (NAT). В то же время у этих компьютеров есть доступ к Internet.

Задачи, связанные с данной

“Управление правилами обработки пакетов”
Следует использовать все возможные средства для эффективного управления правилами обработки пакетов. Защита системы в значительной мере зависит от того, насколько точны и актуальны эти правила.

Управление правилами обработки пакетов

Следует использовать все возможные средства для эффективного управления правилами обработки пакетов. Защита системы в значительной мере зависит от того, насколько точны и актуальны эти правила.

Примечание: Инструкции по выполнению этих задач приведены в электронной справке Редактора правил обработки пакетов, если не указано иное.

Задачи, связанные с данной

“Настройка правил обработки пакетов” на стр. 21
Данная справочная таблица содержит описание задач, которые необходимо выполнить для проверки правил.

“Активация правил обработки пакетов” на стр. 27
Последним этапом настройки правил обработки пакетов является активизация созданных правил.

Деактивация правил обработки пакетов

Если требуется внести изменения в существующие активные правила обработки пакетов или активизировать вновь созданные правила, то сначала нужно деактивизировать текущие активные правила.

Можно деактивизировать правила, относящиеся к конкретному интерфейсу, конкретному идентификатору двухточечного соединения или ко всем интерфейсам и всем идентификаторам двухточечных соединений.

Инструкции по деактивизации правил обработки пакетов приведены в электронной справке Редактора правил обработки пакетов.

Просмотр правил обработки пакетов

Перед активизацией правил не забудьте проверить их правильность.

При просмотре созданных правил фильтрации вы сможете обнаружить явные ошибки. Рекомендуется просматривать правила не только перед активацией и тестированием, но также перед распечаткой и резервным копированием правил. Просмотр правил не является единственным способом поиска ошибок. Однако эта процедура позволяет устранить некоторые ошибки перед началом тестирования.

Для удобного просмотра правил защиты рекомендуется их распечатать. Это позволит найти явные ошибки и убедиться в том, что вы включили все требуемые файлы правил.

В системе предусмотрена функция проверки. Однако не следует полностью полагаться на эту функцию. Вы должны сами просмотреть правила, принять все необходимые меры и убедиться в отсутствии ошибок. Таким образом вы сбережете свое время и ресурсы системы.

Для просмотра неактивных правил необходимо открыть соответствующий файл в Редакторе правил обработки пакетов.

Если требуется отредактировать активные правила фильтрации, сначала нужно просмотреть их и определить, каким образом их нужно изменить.

Для просмотра активных правил фильтрации выполните следующие действия:

1. В System i Navigator выберите ***ваша система*** **→ Сеть → Стратегии IP → Правила обработки пакетов**.
2. Выберите интерфейс, соответствующий тем активным правилам обработки пакетов, которые нужно просмотреть.
3. Просмотрите список активных правил обработки пакетов, показанный в правом окне.

Примечание: Изменять правила с помощью этого окна невозможно. Для редактирования правил их нужно деактивизировать, а затем открыть соответствующий файл в Редакторе правил обработки пакетов.

Задачи, связанные с данной

"Проверка правил обработки пакетов" на стр. 26
Перед активизацией правил их необходимо проверить. Это позволит убедиться в том, что активизация пройдет без ошибок.

"Редактирование правил обработки пакетов"
При изменении требований к защите системы необходимо соответствующим образом отредактировать файлы правил.

Редактирование правил обработки пакетов

При изменении требований к защите системы необходимо соответствующим образом отредактировать файлы правил.

Учтите, однако, что перед редактированием правил их необходимо деактивизировать. После этого вы можете внести требуемые изменения в правила, открыв их в Редакторе правил обработки пакетов в окне System i Navigator. По окончании редактирования не забудьте проверить и затем вновь активизировать правила.

Инструкции по редактированию правил обработки пакетов приведены в электронной справке Редактора правил обработки пакетов.

Задачи, связанные с данной

"Просмотр правил обработки пакетов" на стр. 28
Перед активизацией правил не забудьте проверить их правильность.

Создание резервных копий правил обработки пакетов

Создавая резервные копий правил обработки пакетов, вы сбережете время и свой труд в случае необходимости восстановить потерянные данные.

Ниже приведены советы общего характера, позволяющие быстро восстановить утраченные файлы:

Напечатайте правила фильтрации

Сохраните печатную копию правил и при необходимости введите правила повторно. Кроме того, распечатки позволят найти явные ошибки в правилах фильтрации.

Инструкции по печати правил обработки пакетов приведены в электронной справке Редактора правил обработки пакетов.

Скопируйте информацию на диск

В этом случае вместо ввода правил вручную вы сможете просто скопировать файлы. Кроме этого, путем копирования файлов вы можете переносить параметры защиты из одной системы в другую.

Примечание: Система копирует информацию на системный диск, а не на дискету. Файлы правил хранятся в интегрированной файловой системе на платформе System i, а не на персональном компьютере. Для защиты данных, хранящихся на системном диске, можно воспользоваться соответствующими средствами защиты диска.

При работе с платформой System i необходимо спланировать стратегию резервного копирования и восстановления.

Информация, связанная с данной

Создание резервной копии системы

Ведения журнала и проверка работы правил обработки пакетов

В правилах обработки пакетов предусмотрена функция ведения журнала. Она позволяет исправлять ошибки в правилах фильтрации и NAT.

С ее помощью вы можете создать протокол, содержащий информацию о применении правил — для каждого правила отдельно. Эта функция позволяет отлаживать и проверять отдельные правила. Просматривая создаваемые протоколы и журналы, вы можете контролировать, какие пакеты отправляются и поступают в систему.

Функция ведения журнала включается отдельно для каждого правила. При создании правила фильтрации или NAT вы можете задать одну из следующих опций ведения журнала: полный или выключен. Более подробно эти опции описаны в приведенной ниже таблице.

Опция	**Определение**
Полный	В протокол заносится информация о всех обрабатываемых пакетах.
Выключен	Журнал не ведется.

Если функция ведения журнала включена, то в журнал заносятся записи о всех правилах фильтрации и NAT, примененных к дейтаграммам. Единственное исключение делается для правила запрета по умолчанию. Информация о нем не заносится в журнал, так как это правило создано системой.

Информация журналов хранится в общем файле в системе. С ее помощью вы можете узнать, к каким функциям системы обращались пользователи. Кроме того, на основе этих данных вы сможете решить, нужно ли изменить стратегию защиты системы.

В этом режиме информация о применении правила в журнал заноситься не будет. Опцию ведения журнала выключать не рекомендуется, хотя это делать не запрещено. Если у вас нет опыта создания правил фильтрации и NAT, рекомендуется заносить в протокол информацию о всех случаях применения правил. Впоследствии вы сможете использовать протокол для поиска и исправления ошибок. Однако такую опцию следует выбирать только для наиболее важных правил. Ведение журнала отнимает значительную часть ресурсов системы. В первую очередь обратите внимание на те правила, которые применяются для обработки наиболее интенсивного обмена данных.

Для просмотра журналов выполните следующее действие:

1. В командной строке введите `DSPJRN JRN(QIPNAT)` для просмотра журналов NAT, либо `DSPJRN JRN(QIPFILTER)` для просмотра журналов фильтрации пакетов IP.

Устранению ошибок в правилах обработки пакетов

В этом разделе приведены советы по устранению ошибок в правилах обработки пакетов.

- Средство **i5/OS трассировки соединений** позволяет получить информацию обо всех пакетах, переданных по указанному соединению. Для сбора и печати информации используются команды STRCMNTRC (запустить трассировку соединений) и PRTCMNTRC (напечатать информацию о трассировке соединений).
- **Порядок правил фильтрации и NAT** совпадает с порядком их обработки. Другими словами, правила просматриваются в том же порядке, в котором они записаны в файле. Если порядок правил неправильный, то пакеты не будут обрабатываться так, как вы запланировали. Таким образом система

остается незащищенной от внешних атак. В операторе FILTER_INTERFACE имена наборов фильтров должны быть перечислены точно в таком же порядке, в котором они определены в файле.

Запомните порядок, в котором применяются правила фильтрации и NAT. Он описан в следующей таблице:

Обработка принимаемых пакетов	Обработка отправляемых пакетов
1. Правила NAT	1. Правила фильтрации IP-пакетов
2. Правила фильтрации IP-пакетов	2. Правила NAT

- Лучший способ исправить все ошибки - **удалить все правила**. Если используется i5/OS, запустите команду Удалить таблицу TCP/IP (RMVTCPTBL). Находясь вне приложения System i Navigator, можно также использовать данную команду для возврата и исправления ошибок в правилах.

  Примечание: Команда Удалить таблицу TCP/IP также запускает серверы виртуальной частной сети (VPN), если только серверы VPN (IKE и ConMgr) уже запускались.
- Если используется NAT, то опция **Разрешение пересылки IP-дейтаграмм** конфигурации TCP/IP в системе является обязательной. С помощью команды Изменить атрибуты TCP/IP (CHGTCPA) убедитесь, что эта опция включена.
- **Проверка маршрутов возврата по умолчанию** позволяет убедиться, что для преобразования выбран правильный адрес. Для того чтобы этот адрес был преобразован NAT обратно во внутренний адрес, он должен быть передан в систему по маршруту возврата, а затем отправлен по правильной линии связи.

  Примечание: Если к платформе System i подключено несколько линий связи, нужно особенно тщательно проверять настройки перенаправления принимаемых пакетов. Пакет может поступить не по той линии связи, для которой он предназначен.
- **Просмотр сообщений об ошибках и предупреждений** из файла `EXPANDED.OUT` позволяет убедиться, что правила расположены в требуемом порядке. После подтверждения и активации набора фильтров эти фильтры объединяются со всеми правилами, созданными навигатором System i Navigator. Затем объединенные правила помещаются в новый файл с именем `EXPANDED.OUT`, расположенный в том же каталоге, в котором хранятся ваши правила (обычно /QIBM). Сообщения об ошибках и предупреждения ссылаются на этот файл. Для просмотра этого файла откройте его в Редакторе правил обработки пакетов. Для этого необходимо выполнить следующие действия:
  1. В System i Navigator откройте Редактор правил обработки пакетов.
  2. В меню Файл выберите **Открыть**.
  3. Перейдите к каталогу `QIBM/UserData/OS400/TCPIP/PacketRules/`, либо к иному каталогу, в котором вы сохранили файл правил обработки пакетов.
  4. В окне Открыть файл выберите файл **EXPANDED.OUT** . Файл `EXPANDED.OUT` должен появиться на экране.
  5. Выберите файл `EXPANDED.OUT` и нажмите **Open**.

  Файл EXPANDED.OUT показан только в информационных целях. Редактировать его нельзя.

Понятия, связанные с данным

“Сценарий: преобразование IP-адресов с помощью NAT” на стр. 2
В этом сценарии частные IP-адреса сети вашей компании преобразуются во внешние адреса с помощью статического преобразования сетевых адресов (NAT).

Задачи, связанные с данной

“Доступ к редактору правил обработки пакетов” на стр. 22
Для начального создания правил обработки пакетов в системе можно использовать Редактор правил обработки пакетов. Можно создать новый файл, отредактировать существующий файл или модифицировать примеры файлов, предусмотренные в системе.

Ссылки, связанные с данной

“Создание правил фильтрации IP-пакетов” на стр. 23
При создании фильтра вы указываете правило для управления передачей данных IP.

Дополнительная информация о фильтрации IP-пакетов и преобразовании сетевых адресов

Справочники IBM Redbooks содержат сведения о фильтрации IP-пакетов и преобразовании сетевых адресов. Документы в формате PDF можно просмотреть или распечатать.

IBM Redbooks

- **Учебно-технический обзор TCP/IP**
  Информация о средствах защиты сетей TCP/IP.
- **V4 TCP/IP for AS/400 — Больше отличных возможностей чем когда-либо**
  Несколько сценариев применения преобразования сетевых адресов (NAT) и фильтрации IP-пакетов.

Ссылки, связанные с данной

“Документ PDF о фильтрации IP-пакетов и преобразовании сетевых адресов” на стр. 1
Файл PDF этой информации можно просмотреть и напечатать.

Лицензия на исходный код и отказ от обязательств

IBM предоставляет вам неисключительную лицензию на использование всех примеров программного кода. Разрешается создавать на их основе программный код, необходимый вам.

ПРИ УСЛОВИИ СОБЛЮДЕНИЯ ВСЕХ НЕ ДОПУСКАЮЩИХ ИСКЛЮЧЕНИЙ ГАРАНТИЙ, ПРЕДУСМОТРЕННЫХ ЗАКОНОМ, IBM, РАЗРАБОТЧИКИ ПРОГРАММ И ПОСТАВЩИКИ НЕ ПРЕДОСТАВЛЯЮТ КАКИХ-ЛИБО ЯВНЫХ ИЛИ ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ, НО НЕ ОГРАНИЧИВАЯСЬ ЭТИМ, ПОДРАЗУМЕВАЕМЫЕ ГАРАНТИИ СОБЛЮДЕНИЯ ПРАВ, КОММЕРЧЕСКОЙ ЦЕННОСТИ ИЛИ ПРИМЕНЕНИЯ ДЛЯ КАКИХ-ЛИБО КОНКРЕТНЫХ ЦЕЛЕЙ.

IBM, РАЗРАБОТЧИКИ ПРОГРАММ ИЛИ ПОСТАВЩИК НИ ПРИ КАКИХ УСЛОВИЯХ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА:

1. ПОТЕРЮ ИЛИ ПОВРЕЖДЕНИЕ ДАННЫХ;
2. ПРЯМОЙ, ЧАСТНЫЙ, СВЯЗАННЫЙ ИЛИ КОСВЕННЫЙ УЩЕРБ И ВЫЗВАННЫЙ ИМ ЭКОНОМИЧЕСКИЙ УЩЕРБ; ЛИБО
3. УПУЩЕННУЮ ВЫГОДУ, ПОТЕРЮ КЛИЕНТОВ, ДОХОДОВ, ДЕЛОВОЙ РЕПУТАЦИИ ИЛИ ИСТРАЧЕННЫЕ СБЕРЕЖЕНИЯ.

В НЕКОТОРЫХ ЮРИСДИКЦИЯХ НЕ ДОПУСКАЮТСЯ ИСКЛЮЧЕНИЯ ИЛИ ОГРАНИЧЕНИЯ ПРЯМОГО, СВЯЗАННОГО ИЛИ КОСВЕННОГО УЩЕРБА, ПОЭТОМУ НЕКОТОРЫЕ ИЛИ ВСЕ УКАЗАННЫЕ ВЫШЕ ОГРАНИЧЕНИЯ И ИСКЛЮЧЕНИЯ МОГУТ К ВАМ НЕ ОТНОСИТЬСЯ.

Приложение. Примечания

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

IBM может не предлагать продукты и услуги, упомянутые в этом документе, в других странах. Информацию о продуктах и услугах, предлагаемых в вашей стране, вы можете получить в местном представительстве IBM. Ссылка на продукт, программу или услугу IBM не означает, что может применяться только этот продукт, программа или услуга IBM. Вместо них можно использовать любые другие функционально эквивалентные продукты, программы или услуги, не нарушающие прав IBM на интеллектуальную собственность. Однако в этом случае ответственность за проверку работы этих продуктов, программ и услуг возлагается на пользователя.

Продукты и технологии, описанные в документе, могут быть запатентованы IBM. Предоставление настоящего документа не означает предоставления каких-либо лицензий на патенты. Запросы на приобретение лицензий можно отправлять по следующему адресу:

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

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

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

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

В данной публикации могут встретиться технические неточности и типографские опечатки. В информацию периодически вносятся изменения, которые будут учтены во всех последующих изданиях настоящей публикации. IBM оставляет за собой право в любое время и без дополнительного уведомления исправлять и обновлять продукты и программы, упоминаемые в настоящей публикации.

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

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

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

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

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

Описанная в этом документе лицензионная программа и все связанные с ней лицензионные материалы предоставляются IBM в соответствии с условиями Соглашения с заказчиком IBM, Международного соглашения о лицензии на программу IBM, Соглашения о лицензии на машинный код или любого другого эквивалентного соглашения.

Данные о быстродействии, приведенные в документах, были получены на системах, настроенных особым образом. В связи с этим результаты, полученные в реальной среде, могут существенно отличаться от приведенных. Некоторые измерения могли быть выполнены в системах, находящихся на этапе разработки, поэтому результаты измерений, полученные в серийных системах, могут отличаться от приведенных. Более того, некоторые значения могли быть получены в результате экстраполяции. Фактические результаты могут различаться. Систему следует настроить в соответствии с рекомендациями, приведенными в документе.

Информация о продуктах других изготовителей получена от поставщиков этих продуктов, из их официальных сообщений и других общедоступных источников. Эти продукты не были проверены IBM. Точность приводимых данных о быстродействии, совместимости и других сведений о продуктах, выпущенных сторонними компаниями, не гарантируется. Запросы на получение дополнительной информации об этих продуктах должны направляться их поставщикам.

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

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ:

Эта информация содержит примеры приложений на исходном языке, иллюстрирующие приемы программирования в различных операционных платформах. Разрешается копировать, изменять и распространять эти примеры программ в любой форме без какой-либо платы IBM, в целях разработки, использования, продажи или распространения прикладных программ, соответствующих интерфейсу программирования приложений тех операционных систем, для которых примеры были созданы. Работа примеров не была проверена во всех возможных условиях. Поэтому IBM не может гарантировать или подразумевать надежность, пригодность и функциональность этих программ.

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

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

В электронной версии этих документов фотографии и цветные иллюстрации могут отсутствовать.

Информация об интерфейсе программирования

В документах, связанных с фильтрацией IP-адресов и преобразованием сетевых адресов, приведена информация о программных интерфейсах, с помощью которой можно создавать программы, взаимодействующие с IBM i5/OS.

Товарные знаки

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

AS/400
i5/OS
IBM
IBM (logo)
OS/400
Справочники
System i

Adobe, логотип Adobe, PostScript и логотип PostScript являются зарегистрированными товарными знаками или товарными знаками Adobe Systems Incorporated в США и/или в других странах.

Microsoft, Windows и логотип Windows являются товарными знаками корпорации Microsoft в США и/или других странах.

Другие названия фирм, продуктов и услуг могут являться товарными знаками или знаками обслуживания других фирм.

Условия и соглашения

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

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

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

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

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

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

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

применения для каких-либо конкретных целей.

Напечатано в Дании