IBM

eserver

iSeries

# Сетевая защита - Фильтрация IP-пакетов и преобразование сетевых адресов (NAT)

*Версия 5, выпуск 3*

IBM

@server

iSeries

# Сетевая защита - Фильтрация IP-пакетов и преобразование сетевых адресов (NAT)

*Версия 5, выпуск 3*

**Шестое издание (август 2005 года)**

Это издание относится к версии 5, выпуску 3, модификации 0 операционной системы OS/400 (код продукта 5722–SS1), а также ко всем последующим выпускам и модификациям, если в новых изданиях не будет указано обратное. Данная версия работает не на всех моделях систем с сокращенным набором команд (RISC) и не работает на моделях с полным набором команд (CISC).

# Содержание

# Часть 1. 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 защищает внутреннюю сеть от несанкционированного доступа из внешних сетей. Кроме того, применение NAT решает проблему нехватки IP-адресов, поскольку большое число частных адресов могут быть представлены в виде ограниченного множества зарегистрированных адресов.

**Примечание:** **Правила обработки пакетов** применяются и в фильтрации IP-пакетов, и в NAT. Этот термин употребляется в данном разделе по отношению к обоим службам.

Подробная информация о применении правил обработки пакетов приведена в перечисленных ниже разделах:

**Печать раздела**
Инструкции по печати справочного файла в формате PDF.

**Варианты использования правил обработки пакетов**
Описание некоторых наиболее употребительных сценариев применения правил обработки пакетов. Каждый сценарий снабжен рисунком и примером конфигурации.

**Общая концепция применения правил обработки пакетов**
Перед тем как приступить к работе, нужно усвоить основные принципы и концепции применения правил обработки пакетов. Этот раздел содержит информацию об IP-фильтрации и службе NAT. В частности, в нем обсуждаются вопросы преобразования и защиты адресов. Также в нем приведен список особых терминов, применяемых при работе с серверами iSeries.

**Планирование применения правил обработки пакетов**
Планирование - одна из наиболее важных процедур, в ходе которой определяются цели и выбираются способы защиты. В этом разделе приведены формы для планирования и прочая информация, которая поможет вам выбрать оптимальный способ защиты.

**Настройка правил обработки пакетов**
Информация о том, какие операции можно выполнять над правилами обработки пакетов и каким образом.

**Управление правилами обработки пакетов**
Описание различных задач по управлению правилами обработки пакетов. В частности, в этом разделе обсуждается ведение журнала, а также изменение и просмотр правил фильтрации.

**Устранение неполадок в правилах обработки пакетов**
Указания по локализации и устранению возможных неполадок.

**Связанная информация о правилах обработки пакетов**
Ссылки на другие источники информации о правилах обработки пакетов и связанные разделы документации.

В дополнение к информации из этого раздела можно пользоваться электронной справкой по правилам работы с пакетами, предусмотренной в Навигаторе iSeries. В электронной справке Навигатора iSeries приведены советы по работе с правилами обработки пакетов, включая разделы **Каким образом...**, **Что такое...** и обширную контекстную справку.

# Глава 1. Как напечатать этот раздел

Для просмотра или загрузки этого документа в формате PDF выберите ссылку Правила обработки пакетов (около 250 Кб).

Для сохранения файла PDF на своей рабочей станции выполните следующие действия:

1. Щелкните правой кнопкой мыши на PDF-файле (на вышеприведенной ссылке) в окне браузера.
2. Выберите **Сохранить как...**.
3. Перейдите в каталог, выбранный для хранения PDF.
4. Нажмите **Сохранить**.

**Загрузка Adobe Acrobat Reader**

Если для просмотра или печати файлов PDF вам необходима программа Adobe Acrobat Reader, то вы можете загрузить ее с Web-сайта фирмы Adobe (http://www.adobe.com/products/acrobat/readstep.html)  .

# Глава 2. Сценарии применения правил обработки пакетов

Ниже описано несколько сценариев организации защиты сети с помощью NAT и фильтрации IP-пакетов. Каждый пример сопровождается рисунком и описанием соответствующей конфигурации.

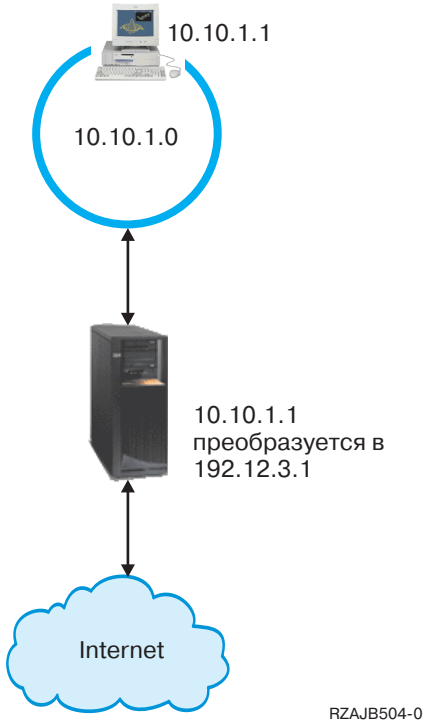
- **Сценарий применения правил обработки пакетов: Преобразование IP-адресов (статический NAT)**
  В этом сценарии частные IP-адреса вашей компании преобразуются во внешние адреса с помощью статического NAT.
- **Сценарий применения правил обработки пакетов: Создание правил фильтрации для работы с HTTP, 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.
- **Сценарий применения правил обработки пакетов: Совместное применение NAT и фильтрации IP-пакетов**
  В этом сценарии ваша компания с помощью и NAT, и фильтрации IP-пакетов скрывает свои PC и Web-сервер за одним внешним IP-адресом, разрешая другим компаниям доступ к Web-серверу.
- **Сценарий применения правил обработки пакетов: Сокрытие IP-адресов (маскирующий NAT)**
  В этом сценарии ваша компания скрывает частные адреса PC с помощью маскирующего NAT, вместе с тем разрешая своим сотрудникам доступ в Internet

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

## Сценарий применения правил обработки пакетов: Преобразование IP-адресов (статический NAT)

**Ситуация**

Вы создали частную сеть своей компании. Однако у вас нет зарегистрированного внешнего IP-адреса. В какой-то момент вам потребовалось подключиться к Internet. 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 ее решить?




**Решение**

Настройте статический NAT. Статический NAT связывает внутренний (частный) адрес с зарегистрированным (внешним) адресом. Сервер iSeries преобразует этот зарегистрированный адрес во внутренний. Таким образом, внутренняя система будет подключаться к Internet через зарегистрированный адрес. Фактически NAT образует мост между внутренней и внешней сетью. Соединение могут устанавливать пользователи обеих сетей.

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

На приведенном рисунке адрес NAT 192.12.3.1 не используется, ожидая возврата данных. При получении информации NAT преобразует адрес во внутренний адрес PC. 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 в систему iSeries с IP-адресом 192.12.3.1.

**Настройка**

Для настройки правил обработки пакетов, описанных в этом сценарии, воспользуйтесь мастером **Преобразование адресов** в Навигаторе iSeries. 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 Навигаторе iSeries выберите **свой сервер–>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.

Правила обработки пакетов должны выглядеть так:

```
-----------------------------------------------------
Statements to map 10.1.1.1 to 192.12.3.1 over TRNLINE
-----------------------------------------------------
ADDRESS MAPPRIVATE1   IP = 10.1.1.1
ADDRESS MAPPUBLIC1   IP = 192.12.3.1
MAP MAPPRIVATE1   TO MAPPUBLIC1   LINE = TRNLINE
-----------------------------------------------------
```

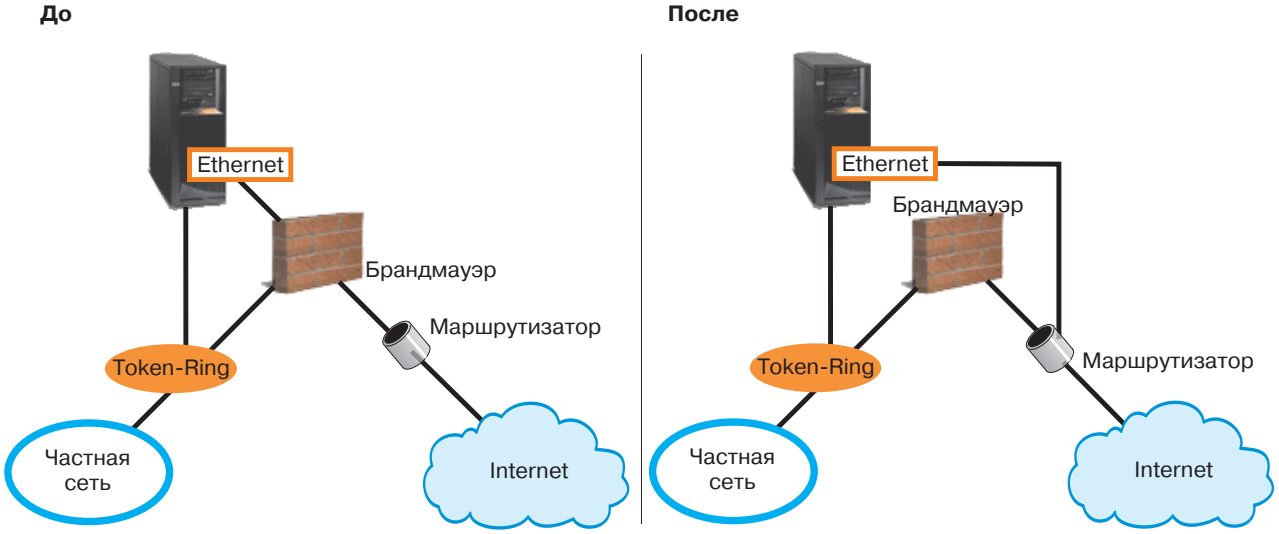
Создав эти, а также все остальные необходимые правила, проверьте их, чтобы убедиться в отсутствии ошибок. Затем вы можете активизировать правила.

**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. Более подробное описание приведено в разделе Устранение неполадок в правилах обработки пакетов.

## Сценарий применения правил обработки пакетов: Создание правил фильтрации для работы с HTTP, Telnet и FTP

**Ситуация**

Вы планируете предоставить пользователям доступ в Internet, однако брандмауэр перегружен, и вы не хотите создавать дополнительную нагрузку на него. Ваши коллеги посоветовали запускать Web-приложения во внешней системе. Вы хотите разрешить внешним пользователям работать на Web-сервере iSeries только с приложениями HTTP, FTP и Telnet. Как решить поставленную задачу?




**Решение**

Создайте правила фильтрации IP-пакетов, определяющие, какие данные разрешено передавать во внешнюю и внутреннюю сеть. Для решения поставленной задачи нужно добавить правила, разрешающие Web-серверу iSeries обмениваться данными HTTP, FTP и 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 Навигаторе iSeries. Мастеру требуется следующая информация:

- Тип службы, которую вы хотите разрешить: HTTP
- Внешний адрес сервера iSeries: 192.54.5.1
- Адрес клиента: Произвольный IP-адрес
- Интерфейс службы: TRNLINE
- Направление передачи пакетов службой: INBOUND
- Имя набора правил фильтрации: external_files

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

1. В Навигаторе iSeries выберите **свой сервер–> 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. Правила обработки пакетов должны выглядеть так:

```
-------------------------------------------
Statements to permit inbound HTTP over TRNLINE
-------------------------------------------
INCLUDE   FILE = /QIBM/UserData/OS400/TCPIP/PacketRules/Services.i3p
FILTER SET external_files   ACTION = PERMIT   DIRECTION = OUTBOUND   SRCADDR = 192.54.5.1   DSTADDR = *
  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 = 192.54.5.1   DSTADDR = *
   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
-------------------------------------------
```

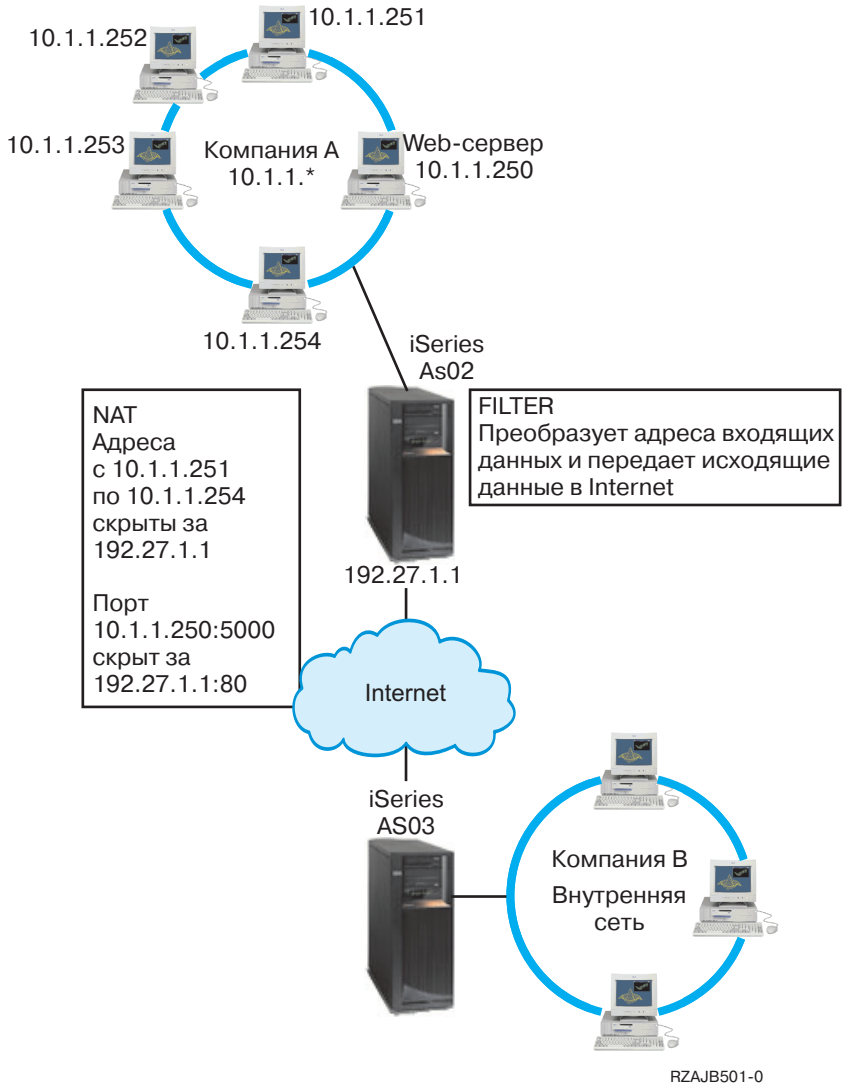
С помощью того же мастера **Разрешить службу** вы можете настроить правила фильтрации, пропускающие пакеты FTP и Telnet.

Создав эти правила, проверьте их, чтобы убедиться в отсутствии ошибок. Затем вы можете активизировать правила.

## Сценарий применения правил обработки пакетов: Совместное применение NAT и фильтрации IP-пакетов

**Ситуация**

Предположим, что у вас есть внутренняя сеть среднего размера, в которой сервер iSeries играет роль шлюза. Шлюз iSeries должен пересылать все пакеты выделенному внутреннему Web-серверу. Этот Web-сервер работает с портом 5000. Вы хотите скрыть адреса всех внутренних компьютеров и Web-сервера, заменив их адресом AS02 интерфейса шлюза iSeries (см. рисунок). Тем не менее, у других компаний должен быть доступ к Web-серверу. Как решить поставленную задачу?




**Решение**

Используя совместно IP-фильтрацию и NAT, вы можете настроить:

1. Скрытый NAT, чтобы скрыть внутренние PC за внешним адресом 192.27.1.1, что позволит им подключаться к Internet.
2. 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 просто разрешает передавать в систему пакеты с портом 80. Поступившие пакеты с другим адресом или номером порта NAT преобразовывать не будет. Такие пакеты будет отброшены.
3. Правила, которые разрешают принимать от внешних систем любые пакеты, обработанные NAT, и отправлять любые пакеты в Internet.

### Настройка

Для настройки правил обработки пакетов скрытого NAT, описанных в этом сценарии, воспользуйтесь мастером **Преобразование адресов** в Навигаторе iSeries. 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 Навигаторе iSeries выберите **свой сервер– > 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 PC во внешний адрес. Это позволит им подключаться к Internet. Правила обработки пакетов скрытого NAT должны выглядеть так:

```
------------------------------------------------------------
Statements to hide 10.1.1.251 - 10.1.1.254 behind 192.27.1.1
------------------------------------------------------------
ADDRESS HIDE1   IP = 10.1.1.251 THROUGH 10.1.1.254
ADDRESS BEHIND1   IP = 192.27.1.1
HIDE HIDE1   BEHIND BEHIND1
------------------------------------------------------------
```

Для настройки NAT с преобразованием порта выполните следующие действия:

1. Откройте Редактор правил обработки пакетов в Навигаторе iSeries.
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 выпадающем 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 выпадающем 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 выпадающем списке **Псевдоним скрытого адреса**.
   c. Выберите **BEHIND1** в выпадающем 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 **Выкл.** в выпадающем 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. Данное правило NAT просто разрешает передавать в систему пакеты с портом 80.

Правила обработки пакетов NAT с преобразованием порта должны выглядеть так:

```
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. Откройте Редактор правил обработки пакетов в Навигаторе iSeries.
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 выпадающем списке **Действие**.
   e. Выберите **Входящие** в выпадающем списке **Направление**.
   f. Выберите = и * в выпадающих списках **Псевдоним адреса отправителя**.
   g. Выберите = и введите 192.27.1.1 в полях **Псевдоним адреса получателя**.
   h. Выберите **Выкл.** в выпадающем списке **Ведение журнала**.
   i. На странице **Службы** выберите **Служба**.
   j. Выберите **TCP** в выпадающем списке **Протокол**.
   k. Выберите = и * в выпадающих списках **Порт отправителя**.
   l. Выберите = и * в выпадающих 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 выпадающем списке **Действие**.
   f. Выберите **Исходящие** в выпадающем списке **Направление**.
   g. Выберите = и введите 192.27.1.1 в полях **Псевдоним адреса отправителя**.
   h. Выберите = и * в выпадающих списках **Псевдоним адреса получателя**.
   i. Выберите **Выкл.** в выпадающем списке **Ведение журнала**.
   j. На странице **Службы** выберите **Служба**.
   k. Выберите **TCP** в выпадающем списке **Протокол**.
   l. Выберите = и * в выпадающих списках **Порт отправителя**.
   m. Выберите = и * в выпадающих 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 выпадающем списке **Имя линии**.
c. На странице **Наборы фильтров** выберите **external_rules** в выпадающем списке **Набор фильтров**. Затем 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 на сервер только те пакеты, которые предназначены для порта 80. NAT не будет преобразовывать адреса пакетов, которые не соответствуют правилу преобразования порта. Правила фильтрации должны выглядеть так:

```
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.

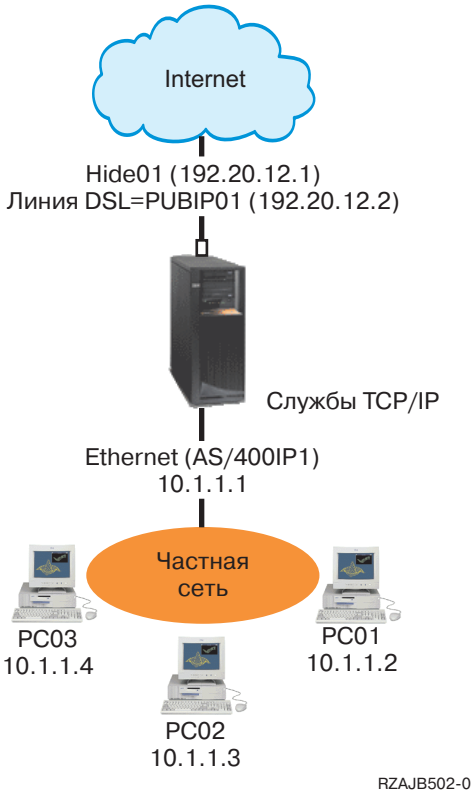
```
FILTER_INTERFACE   LINE = TRNLINE   SET = external_files
```

Создав эти правила, проверьте их, чтобы убедиться в отсутствии ошибок. Затем вы можете активизировать правила.

## Сценарий применения правил обработки пакетов: Сокрытие IP-адресов (маскирующий NAT)

**Ситуация**

Предположим, что в небольшой компании вы планируете запустить службу HTTP на сервере iSeries. У вас есть система модели 170e с одной картой Ethernet и три PC. Провайдер Internet (ISP) предоставил вам соединение DSL черед модем. Он назначил вам следующие внешние IP-адреса: 192.20.12.1 и 192.20.12.2. Всем PC присвоены адреса вида 10.1.1.x во внутренней сети. Вы хотите скрыть частные адреса PC, 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 PC 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, запретит внешним системам устанавливать соединения с PC внутренней сети, поскольку для запуска такого NAT передача должна быть инициализирована из внутренней сети. Однако такой NAT не защищает интерфейс iSeries. Для защиты iSeries от получения пакетов с непреобразованным адресом нужно настроить соответствующие правила фильтрации.

**Настройка**

Для настройки правил обработки пакетов, описанных в этом сценарии, воспользуйтесь мастером **Преобразование адресов** в Навигаторе iSeries. 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 Навигаторе iSeries выберите **свой сервер– > 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.

Правила обработки пакетов должны выглядеть так:

```
-------------------------------------------------------
Statements to hide 10.1.1.1 - 10.1.1.4 behind 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
-------------------------------------------------------
```

Создав эти правила, проверьте их, чтобы убедиться в отсутствии ошибок. Затем вы можете активизировать правила.

# Глава 3. Концепция применения правил обработки пакетов

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

Для успешного применения правил обработки пакетов вам необходимо ознакомиться с этими концепциями и их влиянием на работу iSeries:

- **Терминология правил обработки пакетов**
  Список терминов iSeries, которые вы должны знать.
- **Сравнение правил обработки пакетов с другими способами защиты iSeries**
  В чем преимущества правил обработки пакетов перед другими средствами защиты iSeries? Ответ на этот вопрос вы найдете в данном разделе.
- **Преобразование сетевых адресов (NAT)**
  Существует несколько типов преобразования адресов. С помощью этого раздела вы сможете сделать правильный выбор для своей сети.
- **Фильтрация IP-пакетов**
  Информация о том, как работает фильтрация IP-пакетов.
- **Применение правил NAT в сочетании с правилами фильтрации IP-пакетов**
  Правила NAT и правила фильтрации IP-пакетов можно применять как по отдельности, так и вместе. В этом разделе рассматривается совместное применение этих двух компонентов.
- **Применение нескольких правил фильтрации IP-пакетов**
  Если вы создали несколько правил фильтрации, система обрабатывает их в определенном порядке. В этом разделе указано, каким образом обрабатываются несколько правил фильтрации, и приводится пример.
- **Защита от несанкционированного доступа путем имитации**
  Дано определение защиты от несанкционированного доступа путем имитации и приведены доводы в пользу ее применения.

## Терминология правил обработки пакетов

Ниже приведен список терминов iSeries, применяемых в этом разделе Information Center.

**Граничный адрес**

Внешний адрес, отделяющий защищенную сеть от незащищенной. Этот IP-адрес соответствует физическому интерфейсу iSeries. При определении адреса в системе требуется указать его тип. Например, IP-адреса компьютеров, подключенных к внутренней сети, являются защищенными, а внешний IP-адрес сервера - граничным.

**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.

**Максимальное число диалогов**

Максимальное число диалогов - это параметр, задающий максимальное число одновременных диалогов. Этот параметр задается при настройке правил маскирующего NAT. Значение по умолчанию равно 128. Этот параметр применяется только в правилах маскирующего NAT.

**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

**ИД фильтра PPP**

ИД фильтра PPP позволяет применять правила фильтрации к интерфейсу, определенному в профайле двухточечного соединения. Кроме того, ИД фильтра PPP связывает правила фильтрации с группами пользователей, заданными в этом профайле. Так как профайл двухточечного соединения связан с некоторым IP-адресом, идентификатор фильтра неявно определяет интерфейс, к которому применяются правила. Дополнительная информация приведена в сценарии Управление доступом удаленных пользователей к ресурсам с помощью стратегий для групп и фильтрации IP-пакетов в разделе *Службы удаленного доступа: Соединения PPP*.

**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.

## Сравнение правил обработки пакетов с другими способами защиты iSeries

В iSeries предусмотрен ряд встроенных компонентов, обеспечивающих защиту системы от нескольких типов внешних атак. Правила обработки пакетов, с одной стороны, представляют собой достаточно простой и недорогой способ защиты системы. В ряде случаев вы можете с их помощью обеспечить необходимую защиту без приобретения дополнительных продуктов. Однако надежность применяемой системы защиты важнее ее стоимости.

В ситуациях повышенного риска, например при организации защиты рабочей системы или соединений между системой iSeries и другими системами в сети, вам следует установить другие средства защиты iSeries.

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

- **IBM SecureWay®: iSeries и Internet**
  Этот раздел содержит информацию о типах внешних атак 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 iSeries.
- **Виртуальная частная сеть (VPN)**
  VPN позволяет распространить внутреннюю сеть, не нарушая ее защиту, на часть внешней сети, например Internet. В этом разделе приведено описание VPN и способов ее применения в iSeries.
- **Советы по организации защиты iSeries**
  Этот PDF-файл предоставляет обширную информацию о средствах защиты iSeries.

## Преобразование сетевых адресов (NAT)

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. Преобразование сетевых адресов (NAT) позволяет установить защищенное соединение с Internet, не изменяя внутренние IP-адреса. 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). Ниже приведены ссылки на разделы с дополнительной информацией о различных типах NAT:

- Статический NAT (преобразование адресов)
- Маскирующий NAT (сокрытие адресов)
- Маскирующий, или скрывающий NAT с преобразованием порта

NAT позволяет решить некоторые проблемы адресации путем преобразования или сокрытия адресов. Ниже приведены примеры применения NAT.

**Пример 1:** Сокрытие внутреннего IP-адреса от внешних систем

Предположим, вы установили в системе iSeries общий Web-сервер. Однако вы не хотите, чтобы внешним пользователям был известен IP-адрес сервера во внутренней сети. Вы можете создать правила NAT для преобразования внутренних адресов во внешние адреса, доступные в Internet. В итоге система будет защищена от внешних атак.

**Пример 2:** 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 3:** 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 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.

## Статический NAT (преобразование адресов)

Статический 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 применяется для организации общего доступа к внутреннему серверу. Для этого нужно создать правило преобразования фактического адреса сервера во внешний адрес. Этот адрес будет применяться внешними пользователями. В этом случае никто не сможет получить информацию о внутренней сети для последующих атак извне.

Ниже перечислены особенности статического NAT:

- Взаимно-однозначное преобразование адресов
- Возможность подключения как из внешней, так и из внутренней сети
- Возможность выбрать любой адрес в качестве целевого адреса преобразования
- Целевой адрес для преобразования не может применяться в качестве интерфейса IP
- Не преобразовывает номера портов

**Внимание**

Адрес PC не рекомендуется преобразовывать во внешний адрес iSeries. Для обмена данными с Internet чаще всего применяется именно внешний IP-адрес. Если этот IP-адрес будет применяться для преобразования

внутреннего адреса, то все пакеты, обработанные NAT, будут передаваться внутреннему компьютеру. Таким образом, интерфейс будет зарезервирован для NAT, поэтому интерфейс iSeries не будет работать правильно.

Сценарий применения статического NAT и его иллюстрация приведены в разделе Сценарий применения правил обработки пакетов: Преобразование IP-адресов.

## Маскирующий NAT (сокрытие адресов)

Маскирующий NAT позволяет скрыть фактические адреса защищенных PC от внешних по отношению к iSeries систем. PC передает все пакеты системе iSeries; таким образом, iSeries выполняет роль шлюза. Ниже описан сценарий работы такой функции.

Маскирующий NAT позволяет преобразовывать несколько адресов в один IP-адрес. Он применяется для того, чтобы *скрыть* один или несколько внутренних адресов за одним внешним IP-адресом. Внешний адрес должен быть определен в качестве интерфейса на сервере iSeries. Для этого сам внешний адрес должен быть определен как граничный - `BORDER`.

**Сокрытие нескольких адресов**

Для того чтобы скрыть несколько адресов, задается диапазон адресов, преобразуемых NAT на сервере iSeries. 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. Диалог позволяет серверу NAT выполнять обратное преобразование адресов IP-дейтаграмм, поступающих из внешней сети.

Для того чтобы узнать структуру заголовка IP-дейтаграммы, щелкните на ссылке заголовок IP-пакета.

Маскирующий NAT обрабатывает только те пакеты, которые отправляются из внутренней сети. При этом IP-пакет преобразуется средствами NAT при передаче через сервер NAT системы iSeries. 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 компьютере NAT с внешним IP-адресом
- Обрабатываются только пакеты, поступающие от внутренних систем
- Номера портов связываются с временными номерами портов. Это означает, что от внешней сети скрывается не только адрес, но и номер порта.
- Адрес, зарегистрированный на компьютере NAT, может применяться и для других целей

**Внимание**

- Параметр `MAXCON` должен быть достаточно большим, так как он определяет число одновременно работающих диалогов. Например, при работе с FTP вам потребуется как минимум два активных диалога. В этом случае необходимо присвоить переменной `MAXCON` достаточно большое значение, чтобы обслуживать несколько диалогов на каждом PC. 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 PC. Для правильной работы маскирующего NAT должен быть запущен внутренний диалог. Тайм-аут определяет время ожидания ответа для внутреннего диалога. Значение по умолчанию равно 16.
- Маскирующий NAT поддерживает следующие протоколы: TCP, UDP и ICMP.

- При использовании NAT необходимо также настроить пересылку дейтаграмм IP. Введите команду CHGTCPA (Изменить атрибуты TCP/IP), указав в параметре пересылки дейтаграмм IP значение YES.

Пример применения маскирующего NAT и его иллюстрация приведены в разделе Сокрытие IP-адресов (маскирующий NAT).

## Маскирующий NAT с преобразованием порта

NAT с преобразованием порта является разновидностью маскирующего NAT. В чем отличие? NAT с преобразованием порта позволяет скрыть не только IP-адрес, но и номер порта. Это позволяет обрабатывать пакеты, которые поступают как от внутренних PC, так и от внешних компьютеров. Такой тип NAT применяется в том случае, если внешним компьютерам или клиентам нужно обеспечить доступ к компьютеру или серверу частной сети. В сеть пропускаются только те пакеты IP, в которых и IP-адрес, и порт совпадают с указанными. Ниже описан сценарий работы NAT.

**Подключение внутреннего компьютера к внешнему**

Если внутренний PC с *адресом 1: портом 1* отправляет пакет внешнему компьютеру, 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 преобразует эти значения в заголовке дейтаграммы, даже если диалог для них еще не существует. 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:

- Взаимно однозначное соответствие.
- Возможность подключения как из внешней, так и из внутренней сети.
- Зарегистрированный адрес, который применяется для преобразования, должен быть определен в системе iSeries, выполняющей преобразование 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.

**Внимание**

- Параметр MAXCON должен быть достаточно большим, так как он определяет число одновременно работающих диалогов. Например, при работе с FTP вам потребуется как минимум два активных диалога. Необходимо присвоить переменной MAXCON достаточно большое значение, чтобы обслуживать несколько диалогов на каждом PC. Значение по умолчанию равно 128.
- Маскирующий NAT поддерживает следующие протоколы: TCP, UDP и ICMP.
- При использовании NAT необходимо также настроить пересылку дейтаграмм IP. Для этого воспользуйтесь командой CHGTCPA (Изменить атрибуты TCP/IP), указав в параметре пересылки дейтаграмм IP значение YES.

## Фильтрация IP-пакетов

В правилах обработки пакетов реализованы не все функции брандмауэра. Тем не менее, в них предусмотрен компонент для фильтрации IP-пакетов в iSeries. Этот компонент предназначен для управления потоками IP, поступающими в сеть и исходящими из сети. Он позволяет пропускать или отбрасывать пакеты на основе заданных правил фильтрации. Пакет пропускается или отбрасывается в зависимости от информации, указанной в заголовке IP-пакета.

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. В iSeries предусмотрено 3 варианта действий (начиная с версии V4R4):

1. PERMIT — разрешает обычную обработку пакета
2. DENY — немедленно отклоняет пакет
3. IPSEC — отправляет пакет по соединению VPN, указанному в правиле фильтрации

**Примечание:** В данном случае, 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. Дополнительная информация о VPN приведена в разделе Виртуальная частная сеть (VPN).

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.

## Примеры фильтров

Файл демонстрирует правильные синтаксические конструкции создания правил обработки пакетов в iSeries и совместную работу различных операторов. 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 не позволяет добиться нужного эффекта. 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. По этой причине, когда вы добавляете правила в интерфейс, посредством которого вы настраиваете iSeries, не забудьте внести разрешающее правило для своей рабочей станции или рабочей станции другого пользователя, также участвующего в настройке iSeries. Если вы не сделаете этого, то вам не удастся установить соединение с iSeries.

Фильтр может состоять из нескольких наборов, например:

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

Эти наборы будут обработаны в указанном порядке (set1, затем set2, затем set3). Учтите, что фильтры из каждого набора просматриваются в том же порядке, в котором они записаны в файле. Это означает, что взаимное расположение фильтров из разных наборов не играет никакой роли. Важно лишь расположение фильтров 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. Это называется правилом 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 iSeries. 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.

## Применение правил NAT в сочетании с правилами фильтрации IP-пакетов

Правила NAT и правила фильтрации работают независимо друг от друга. Тем не менее, они могут применяться вместе. 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*. Пусть 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. Дополнительная информация по этому вопросу приведена в разделе Объединение файлов в правилах обработки пакетов.

## Применение нескольких правил фильтрации IP-пакетов

При создании правил фильтрации фильтр ссылается на один из операторов правила. Набор ссылается на группу фильтров. Фильтры, содержащиеся в наборе, обрабатываются по порядку, сверху вниз. Несколько наборов также 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.

```
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 iSeries. 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.

# Глава 4. Планирование применения правил обработки пакетов

Перед подключением сетевых ресурсов к Internet вы должны 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. В зависимости от конкретных особенностей предстоящей работы с Internet вы сможете правильно оценить потребности в защите. Раздел IBM SecureWay: iSeries и Internet содержит подробную информацию, необходимую для составления общего плана защиты сети. Если вы собираетесь применять правила обработки пакетов, ознакомьтесь со следующими разделами:

- **Правила обработки пакетов: Требования к правам доступа пользователя**
  Убедитесь, что у вас есть необходимые права доступа для создания и применения правил обработки пакетов.
- **Правила обработки пакетов: Требования к системе**
  Убедитесь, что система iSeries отвечает минимальным требованиям, позволяющим применять правила обработки пакетов.
- **Правила обработки пакетов: Форма для планирования**
  Эта форма предназначена для записи информации, необходимой при настройке правил обработки пакетов.

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

## Правила обработки пакетов: Требования к правам доступа пользователя

Прежде чем приступить к настройке правил обработки пакетов в системе iSeries, вы должны убедиться, что у вас есть соответствующие права доступа. Вам 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. В противном случае вам необходимы права доступа к следующим каталогам, файлам и 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

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

1. OS/400 версии 5, выпуска 2 (5722-SS1) или более позднего выпуска.
2. iSeries Access for Windows (5722-XE1) и Навигатор iSeries
   - Компонент Навигатора, предназначенный для поддержки сети
3. Настроенная поддержка TCP/IP (5722-TC1), включая интерфейсы IP, маршруты, имя локального хоста и имя локального домена.

**Примечание:** Если вы испытываете затруднения при работе с TCP/IP, сетевой поддержкой или IP-адресами, прочтите разделы TCP/IP Tutorial and Technical Overview  и V4 TCP/IP for AS/400: More Cool Things Than Ever  .

## 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? | |
| Какие правила будут применяться для управления потоками TCP/IP, проходящими через системы? Для каждого из таких правил укажите следующие параметры потока TCP/IP:<br>• служба, пакеты который будут разрешены или запрещены (например, HTTP, FTP и т.д.)<br>• стандартный номер порта для этой службы<br>• направление передачи данных<br>• будут ли данные передаваться в качестве вызова или в ответ на вызов<br>• 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). | |

# Глава 5. Настройка правил обработки пакетов

После разработки плана настройки правил обработки пакетов вы можете приступать к фактическому созданию и применению правил. В электронной справке Редактора правил обработки пакетов приведены соответствующие пошаговые инструкции. Кроме того, в следующей справочной таблице приведен обзор предстоящих задач по настройке правил:

__ 1. Открытие Редактора правил обработки пакетов.
Для того чтобы открыть Редактор правил обработки пакетов в окне Навигатора iSeries, выполните следующие инструкции.

__ 2. 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.
- 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 скрытия адресов.

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

__ 3. Определение псевдонимов адресов и служб
Укажите псевдонимы адресов и служб, с которыми будут работать правила.

**Примечание:** При создании правил NAT определение псевдонимов адресов *обязательно*.

__ 4. Создание правил NAT.
Это необходимо *только* в том случае, если вы собираетесь применять функцию NAT.

__ 5. Создание правил фильтрации.
Определите, какие фильтры будут применяться к сети, контролируемой данной системой.

__ 6. Добавление файлов
Укажите дополнительные файлы, которые вы хотите включить в ″главный″ файл правил. Это нужно сделать *только* в том случае, если вы планируете повторно применять созданные ранее правила.

__ 7. Определение интерфейсов
Примените правила к интерфейсу.

__ 8. Ввод комментариев
Введите текстовое описание каждого файла правил.

__ 9. Проверка файлов правил
Убедитесь, что активизация файлов пройдет без ошибок и сбоев.

__ 10. Активизация файлов правил.
Для того чтобы правила обработки пакетов вступили в силу, их необходимо активизировать.

__ 11. Управление правилами обработки пакетов
После активизации правил обработки пакетов вы должны отслеживать их, чтобы обеспечивать защиту системы. В этом разделе приведена информация о редактировании файлов правил, ведении журналов и контроле действий над правилами обработки пакетов, а также советы и приемы по выполнению резервного копирования и восстановления.

## Открытие Редактора правил обработки пакетов

Откройте Редактор правил обработки пакетов с помощью Навигатора iSeries - графического интерфейса, предназначенного для работы с ресурсами iSeries. Открыв Редактор, вы сможете приступить к созданию правил обработки пакетов в системе. Вы можете создать новый файл, отредактировать существующий файл или модифицировать примеры файлов, предусмотренные в системе.

Для открытия Редактора правил обработки пакетов выполните следующие действия:
1. В окне Навигатора iSeries откройте свой сервер -->**Сеть -->Стратегии IP**.
2. Щелкните правой кнопкой мыши на **Правила обработки пакетов** и выберите **Редактор правил**.

Выполните все задачи, описанные в параграфе Настройка правил обработки пакетов этого раздела, согласно пошаговым инструкциям, приведенным в электронной справке.

## Определение псевдонимов 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 два преимущества:

1. Снижается вероятность появления опечаток.
2. Уменьшается число создаваемых правил фильтрации.

Предположим, что в сети работает 31 пользователь, и у каждого из них должен быть доступ к Internet. При этом им разрешено работать только с WWW. В этом случае правила можно создать двумя способами.

1. Создайте правило фильтрации для каждого IP-адреса.
2. 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 и ICMP, которые должны применяться в качестве критерия для сравнения пакетов. Например, можно выбрать исходный и целевой порт.

**Примечание:** Помните, что при создании правил NAT определение псевдонимов адресов *обязательно*. В правилах NAT могут применяться только псевдонимы адресов.

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

**Следующий шаг**
Если вы собираетесь применять преобразование сетевых адресов, перейдите к шагу Создание правил NAT. В противном случае перейдите к шагу Создание правил фильтрации IP-пакетов.

## Создание правил NAT

Если вы решили воспользоваться NAT, то *обязательно* определите псевдонимы преобразуемых IP-адресов. 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**
Вы можете скрыть внутренние адреса, сделав их недоступными во внешней сети. В правилах, скрывающих адреса, можно указать один IP-адрес для нескольких внутренних адресов. Такой тип NAT 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 называется *статическим* NAT.

Пошаговые инструкции по настройке сокрытия или преобразования адресов приведены в электронной справке Редактора правил обработки пакетов.

**Следующий шаг**
Если вы собираетесь настроить фильтрацию входящих и исходящих пакетов в сети, перейдите к разделу Создание правил фильтрации IP-пакетов. В противном случае перейдите к разделу Ввод комментариев к правилам обработки пакетов.

## 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.

**Примечание:** Когда вы добавляете правила в интерфейс, посредством которого вы настраиваете iSeries, не забудьте внести разрешающее правило для своей рабочей станции или рабочей станции другого пользователя, также участвующего в настройке iSeries. Если вы не сделаете этого, то вам не удастся установить соединение с iSeries. Вам придется войти в систему iSeries 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**. Создавайте 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:
  1. В операторе FILTER_INTERFACE имена наборов фильтров должны быть перечислены в том порядке, в котором они определены в файле.
  2. 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. См. приведенный ниже пример.
- **Создавайте только разрешающие правила фильтрации**. Пакеты, не соответствующие этим правилам, будут отбрасываться автоматически.
- **Сначала создайте правила, которые будут применяться чаще всего.**.

Пример к приведенному выше совету *Создавайте 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 вы можете 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.

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

**Следующий шаг**
После создания фильтров вы можете добавить один или несколько файлов в фильтр. Если это не требуется, перейдите к шагу определение интерфейсов (к которым применяются правила).

## Определение интерфейсов для фильтра

Для того чтобы задать правила для конкретных интерфейсов, *необходимо* 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.

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

**Следующий шаг**
После определения интерфейсов фильтров переходите к шагу ввод комментариев к правилам обработки пакетов.

## Добавление файлов к правилам обработки пакетов

Вы можете активизировать несколько файлов правил обработки пакетов в системе, если воспользуетесь опцией *Добавить* Редактора 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 вы не будете создавать дублирующие правила. Вы сможете просто включать и исключать правила по мере надобности.

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

**Следующий шаг**
После добавления всех файлов правил переходите к шагу Определение интерфейсов для фильтров.

## Ввод комментариев к правилам обработки пакетов

Очень полезно включать в файлы комментарии. В них вы можете 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 восстановить всю структуру защиты. 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.

**Следующий шаг**
Выполнив все шаги по настройке правил обработки пакетов, предшествующие данному, переходите к шагу Проверка правил обработки пакетов.

## Проверка правил обработки пакетов

Перед активизацией правил их необходимо проверить. Это позволит убедиться, 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. Она 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. Перед активизацией правил убедитесь в том, что они не содержат ошибок и расположены в правильном порядке.

Пошаговые инструкции по проверке правил обработки пакетов приведены в электронной справке Редактора правил обработки пакетов.

**Предупреждения:** При активизации правил система автоматически их проверяет. В ходе проверки выдаются различные предупреждения и сообщения об ошибках. Предупреждение представляет собой информационное сообщение. После его отправки проверка продолжается. Внимательно изучите все сообщения. Последним появляется сообщение об успешной проверке или активизации сообщений. Последнее сообщение может также говорить о том, что загрузка правила была неудачной, в том случае, если произошли ошибки.

**Следующий шаг**
После успешной проверки правил переходит к шагу Активизация правил.

## Активизация 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 их проверить. 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 всегда также проверять правила защиты вручную.

Если правила неприменимы к интерфейсу (например, если вы применяете только правила NAT), появится предупреждение (TCP5AFC). Оно не сигнализирует об ошибке. С его помощью система проверяет, что вы действительно планируете применять один интерфейс. 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.

**Последний шаг**
После настройки и успешной активизации правил обработки пакетов рекомендуется периодически

обращаться к ним для контроля. Список задач по отслеживанию и обслуживанию правил обработки пакетов приведен в разделе Управление правилами обработки пакетов.

# Глава 6. Управление правилами обработки пакетов

В целях обеспечения защиты системы и целостности правил обработки пакетов рекомендуется периодически выполнять следующие задачи управления:

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

- Резервное копирование правил обработки пакетов для защиты от потери файлов.
- Деактивизация правил обработки пакетов в случае приостановки действия NAT и правил фильтрации по любой причине. Учтите, однако, что если правила обработки пакетов деактивизированы, то система не защищена.
- Редактирование правил обработки пакетов при изменении схемы управления передачей данных IP.
- Ведение журнала и контроль действий над правилами обработки пакетов для отслеживания изменений в правилах. Это упрощает отладку правил.
- Просмотр правил обработки пакетов для устранения ошибок.

Следует регулярно выполнять все описанные задачи. Защита системы в значительной мере зависит от того, насколько хорошо организовано управление правилами защиты. Если вам потребуется помощь в устранении неполадок, обратитесь к разделу Устранение неполадок в правилах обработки пакетов.

## Деактивизация 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.

Пошаговые инструкции по деактивизации правил обработки пакетов приведены в электронной справке Редактора правил обработки пакетов.

## Просмотр правил обработки пакетов

Перед активизацией правил фильтрации их следует просмотреть, чтобы убедиться в отсутствии ошибок. 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 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 вы должны убедиться в отсутствии ошибок, просмотрев правила вручную, не полагаясь полностью на эту функции. Это позволит сэкономить 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 окне Навигатора iSeries выберите **свой сервер —> 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:** в этом окне нельзя редактировать правила. Для редактирования правил их нужно деактивизировать, а затем открыть соответствующий файл в Редакторе правил обработки пакетов.

Вернитесь к разделу Работа с правилами фильтрации и NAT.

## Редактирование правил обработки пакетов

При изменении требований к защите системы вы *должны* 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 Навигатора iSeries. По окончании редактирования не забудьте проверить и затем вновь активизировать правила.

Пошаговые инструкции по редактированию правил обработки пакетов приведены в электронной справке Редактора правил обработки пакетов.

## Резервное копирование правил обработки пакетов

Хотя поначалу это может показаться ненужным, рекомендуется всегда создавать резервную копию правил обработки пакетов. При сбое в системе резервные копии позволят сэкономить время и усилия, требуемые для восстановления правил.

Ниже приведены общие рекомендации по резервному копированию и восстановлению файлов правил:

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

Пошаговые 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 iSeries копирует информацию на жесткий диск, а не на дискету. Файлы правил хранятся в файловой системе IFS iSeries, а не на PC. Для защиты данных, расположенных на системном диске, могут применяться средства защиты дисков.

При работе с системой iSeries необходимо спланировать стратегию резервного копирования и восстановления. Дополнительная информация о резервном копировании и восстановлении файлов приведена в разделе Резервное копирование и восстановление.

## Ведение журнала и контроль действий над правилами 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. Такой протокол значительно упрощает отладку правил и обновление SPOT. 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 iSeries. 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 чаще всего.

Для просмотра журналов выполните следующие действия:
1. Введите в командной строке iSeries: DSPJRN JRN(QIPNAT) для просмотра журналов NAT, либо DSPJRN JRN(QIPFILTER) для просмотра журналов фильтрации пакетов IP.

# Глава 7. Устранение неполадок в правилах обработки пакетов

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

- Средство **трассировки соединений iSeries** позволяет получить информацию обо всех пакетах, переданных по конкретному соединению. Для сбора и печати информации предназначены 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. В результате система будет уязвима для внешних атак. В операторе FILTER_INTERFACE имена наборов фильтров должны быть перечислены в том порядке, в котором они определены в файле.

  Дополнительная информация о создании правил фильтрации приведена в разделе Создание правил фильтрации IP-пакетов. 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**. Для этого введите в системе iSeries команду RMVTCPTBL (Удалить таблицу TCP/IP). Эту же команду можно использовать для возврата в Навигатор iSeries с целью исправления ошибок в правилах.

  **Примечание:** Команда Удалить таблицу TCP/IP помимо описанных действий запускает серверы VPN, однако только в том случае, если серверы VPN (IKE и ConMgr) были запущены ранее.
- **Разрешение пересылки IP-дейтаграмм** - это важная опция конфигурации TCP/IP в системе iSeries, в том случае, если вы используете NAT. С помощью команды CHGTCPA (Изменить атрибуты TCP/IP) убедитесь, что она 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 iSeries по маршруту возврата, а затем - отправлен по правильной линии связи.

  **Примечание:** Если к системе iSeries подключено несколько линий связи, нужно особенно тщательно проверять все принимаемые пакеты. 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 активизации набора фильтров эти фильтры объединяются со всеми правилами, созданными Навигатором iSeries. После этого 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.
  1. Открытие Редактора правил обработки пакетов в окне Навигатора iSeries.
  2. В меню **Файл** выберите **Открыть**.
  3. Перейдите к каталогу `QIBM/UserData/OS400/TCPIP/PacketRules/`, либо к тому 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 его и нажмите **Открыть**.

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

# Глава 8. Связанная информация о правилах обработки пакетов

Ниже перечислены руководства и справочники IBM (в формате PDF), содержащие дополнительную информацию о фильтрации IP-пакетов и службе NAT.

**Руководства**

- **Tips and Tools for Securing your iSeries** (около 254 страниц)
  Этот файл в формате PDF содержит обширную информацию о средствах защиты iSeries.

**Справочники**

- **TCP/IP Tutorial and Technical Overview**
  Информация о средствах защиты сетей TCP/IP.
- **TCP/IP for AS/400 : More Cool Things Than Ever**
  Несколько сценариев применения преобразования сетевых адресов (NAT) и фильтрации IP-пакетов.

Для сохранения файла PDF на своей рабочей станции:

1. Щелкните правой кнопкой мыши на файле в формате PDF (на вышеприведенной ссылке) в окне браузера.
2. Выберите **Сохранить как...**.
3. Перейдите в каталог, выбранный для хранения PDF.
4. Нажмите **Сохранить**.

Если вам требуется программа Adobe Acrobat Reader для просмотра или печати файлов в формате PDF, ее можно загрузить с Web-сайта фирмы Adobe (www.adobe.com/prodindex/acrobat/readstep.html) .

Напечатано в Дании