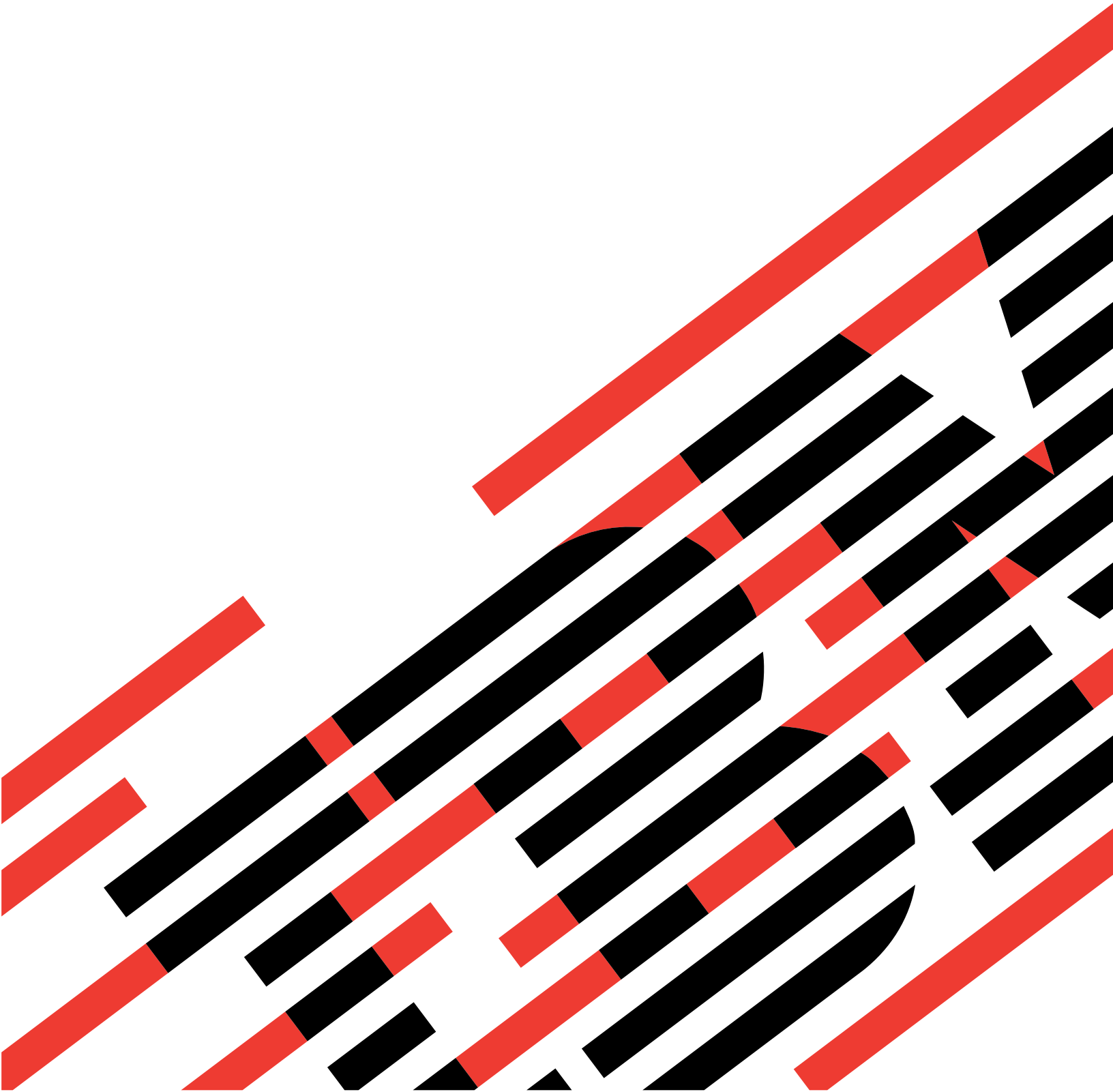
IBM

eserver

iSeries

Виртуальная частная сеть

Версия 5, выпуск 3



IBM

@server

iSeries

Виртуальная частная сеть

Версия 5, выпуск 3

Примечание

Перед началом работы с этой информацией и с описанным в ней продуктом обязательно ознакомьтесь со сведениями, приведенными в разделе “Примечания”, на стр. 73.

Шестое издание (август 2005 г.)

Это издание относится к версии 5, выпуску 3, модификации 2 IBM i5/OS (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

Виртуальная частная сеть

Виртуальная частная сеть (VPN) - это расширение сети вашей организации за счет уже существующей общей сети, например, Internet. VPN позволяет управлять сетевым потоком данных и предоставляет такие важные функции, как идентификация и защита данных.

VPN OS/400(R) является дополнительным компонентом Навигатора iSeries(TM) - графического пользовательского интерфейса (GUI) для OS/400. Она позволяет создавать защищенные соединения между двумя хостами, двумя шлюзами или хостом и шлюзом. Для защиты передаваемых данных в VPN OS/400 предусмотрены идентификация, шифрование и другие средства.

В многоуровневой модели TCP/IP VPN находится на сетевом уровне. В частности, VPN применяет открытую среду Архитектуры защиты IP (IPSec). IPSec предоставляет базовые функции для защиты данных, передаваемых по сети Internet, и различные гибкие средства, на основе которых можно создать надежную защищенную виртуальную частную сеть.

Кроме того, VPN поддерживает протокол L2TP. Соединения L2TP, которые иногда называются виртуальными линиями, - это сравнительно недорогой способ подключения удаленных пользователей, при котором IP-адресами удаленных пользователей управляет корпоративный сервер, подключенный к сети. С помощью функций IPSec можно создавать защищенные соединения L2TP.

Важно понимать, какой влияние оказывает на сеть функция VPN. Для успешной настройки этой функции важно тщательно спланировать конфигурацию, а затем правильно реализовать ее в сети. Для получения дополнительной информации о принципах работы функции VPN и способах ее применения ознакомьтесь со следующими разделами:

“Новое в V5R3” на стр. 2
В этом разделе указано, какая информация была добавлена или значительно изменена в этом выпуске.

“Как напечатать этот раздел” на стр. 3
Если вам удобнее работать с напечатанной версией документа, выполните приведенные инструкции для печати файла PDF.

“Сценарии применения VPN” на стр. 3
Ознакомьтесь с приведенными сценариями, в которых описаны основные типы VPN и приведены инструкции по настройке.

“Принципы работы VPN” на стр. 22
Этот раздел позволяет получить общее представление о стандартных технологиях VPN. В нем приведена основная информация о протоколах, применяемых в данной реализации VPN.

“Планирование конфигурации VPN” на стр. 33
Перед работой с VPN необходимо тщательно спланировать конфигурацию. В этом разделе содержится информация о переходе от старой версии, список требований к настройке и ссылки на советник по планированию, который создает необходимую форму планирования.

“Настройка VPN” на стр. 38
После того как конфигурация VPN будет спланирована, можно перейти к настройке. В этом разделе приведен обзор задач, которые необходимо выполнить для настройки VPN.

“Работа с функцией VPN” на стр. 47
В этом разделе описаны различные задачи по управлению активными соединениями VPN, в том числе процедуры изменения свойств, сбора данных и удаления соединений.

“Устранение неполадок VPN” на стр. 50
Обратитесь к этому разделу, если при работе с соединениями VPN возникла ошибка.

“Дополнительная информация о VPN” на стр. 72
В этом разделе приведены ссылки на другие источники информации о VPN и связанные разделы справки.

Новое в V5R3

Изменения в функциях
Ниже перечислены изменения, внесенные в функцию Виртуальная частная сеть (VPN) в операционной системе выпуска 5, версии 3 (V5R3). Появилось два новых типа идентификаторов, которые можно выбирать при определении стратегий обмена ключами и при настройке конечных точек данных для соединений. Этими типами являются локальный IP-адрес и имя хоста в IPv4. Дополнительная информация приведена в электронной справке Навигатора iSeries(TM).

- **Мой локальный IP-адрес**
  Тип идентификатора Мой локальный IP-адрес может быть выбран в качестве локального сервера ключей для стратегии IKE или в качестве локальной конечной точки данных в определении соединения. После выбора VPN использует доступный адрес IPv4. Этот тип идентификатора может применяться только в соединениях VPN, не использующих фильтр стратегий. Кроме того, инициатором соединения должна быть локальная система.
- **Имя хоста IPv4**
  Идентификатор Имя хоста IPv4 может быть выбран при настройке следующих параметров:
  – Удаленный сервер ключей в стратегии IKE
  – Удаленный адрес в свойствах соединения
  – Фильтр стратегий в свойствах группы соединений

  Имя хоста IPv4 принимает значение IP-адреса хоста, имя которого указано в типе идентификатора.

Примечание о защите VPN:
Если для идентификации применяется подготовленный ключ, то рекомендуется использовать основной режим согласования IKE. Тем самым обеспечивается более высокий уровень защиты передаваемых данных. Если вам приходится использовать подготовленные ключи с ускоренным режимом согласования, то используйте нетривиальные пароли, взлом которых путем сканирования словаря маловероятен. Инструкции по настройке основного режима согласования приведены в разделе Снижение уровня защиты при использовании подготовленных ключей. При создании и использовании стратегии IKE за более подробной информацией вы можете обращаться к электронной справке по Навигатору iSeries.

Новое в документации
Ниже перечислены изменения, внесенные в раздел VPN в V5R3 Information Center: Следующая ссылка позволяет просмотреть наглядную презентацию Туннели L2TP, защищенные с помощью IPSec. Для этого необходим встраиваемый модуль Flash .Вы также можете просмотреть эту презентацию в формате HTML.

Информация о новых возможностях и изменениях

Информация о технических изменениях, внесенных в данный выпуск, отмечена следующим образом:

- Начало нового или измененного раздела информации помечается значком »
- Конец нового или измененного раздела информации помечается значком «

Более подробная информация о новых и измененных функциях этого выпуска приведена в документе Информация для пользователей.

Как напечатать этот раздел

Для просмотра или печати этого документа в формате PDF щелкните на ссылке Виртуальная частная сеть (VPN) (примерно 95 страниц или 500 Кб).

Сохранение файлов PDF

Для просмотра или печати документа в формате PDF сохраните его на рабочей станции, выполнив следующие действия:

1. Щелкните правой кнопкой мыши на имени документа PDF в окне браузера (на приведенной выше ссылке).
2. Если вы работаете с Internet Explorer, то выберите опцию **Сохранить объект как...**. Если вы работаете с Netscape Communicator, то выберите опцию **Сохранить ссылку как...**
3. Выберите каталог для сохранения файла с документом PDF.
4. Нажмите кнопку **Сохранить**.

Загрузка программы Adobe Acrobat Reader

Для чтения и печати этих файлов необходима программа Adobe Acrobat Reader. Копию этой программы можно загрузить с Web-сайта Adobe (www.adobe.com/products/acrobat/readstep.html)  .

Сценарии применения VPN

Ознакомьтесь с приведенным ниже сценариями, в которых описаны основные типы соединений, а также приведена техническая информация и информация о настройке:

- **“Сценарий применения VPN: Основная информация о соединении между филиалами” на стр. 4**
  В этом сценарии фирме необходимо настроить соединение VPN между подсетями двух филиалов. Для этого планируется настроить два сервера iSeries(TM) в качестве шлюзов VPN.
- **“Сценарий применения VPN: Основная информация о соединении между фирмами” на стр. 9**
  В этом сценарии фирме требуется установить соединение VPN между клиентскими рабочими станциями, одна из которых находится в производственном отделе фирмы, а вторая - в отделе поставок делового партнера фирмы.
- **“Сценарий применения VPN: Защита необязательного туннеля L2TP с помощью IPSec” на стр. 14**
  В этом сценарии рассматривается соединение между хостом, расположенным в филиале фирмы, и корпоративным сервером. Соединение устанавливается по туннелю L2TP, защищенному с помощью IPSec. Хосту филиала IP-адрес назначается динамически, тогда как у корпоративного сервера есть постоянный внешний IP-адрес.
- **“Сценарий применения VPN: Применение преобразования сетевых адресов в VPN” на стр. 21**
  В этом сценарии функцию VPN OS/400(R) планируется применять для обмена конфиденциальными данными с деловым партнером. Для защиты сети фирмы применяется функция NAT VPN, позволяющая скрыть внутренний IP-адрес сервера iSeries, на котором находятся приложения, необходимые деловому партнеру.

Другие сценарии применения VPN

Другие сценарии применения VPN можно найти в дополнительных источниках информации о VPN:

- **Сценарий QoS: Надежные и предсказуемые результаты (VPN и QoS)**
  С помощью VPN можно создать стратегию QoS. В этом примере демонстрируется совместное применение VPN и QoS.
- **OS/400 V5R1 Virtual Private Networks: Remote Access to the IBM(R) e(logo)server iSeries Server with Windows(R) 2000 VPN Clients, REDP0153** 

Это руководство фирмы IBM содержит описание пошаговой процедуры настройки туннеля VPN, использующего функции VPN выпуска V5R1, а также функции L2TP и IPSec, предусмотренные в Windows 2000.

- **AS/400(R) Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00** 
  В этом руководстве приведена основная информация о функции VPN и ее реализации в OS/400, основанной на средствах защиты IP (IPSec) и протоколе L2TP.

- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00** 
  В этом руководстве описаны все средства защиты сетевых соединений, предусмотренные в системе OS/400, в том числе фильтры пакетов IP, NAT, VPN, сервер Proxy HTTP, SSL, DNS, функция передачи почты, функция контроля и функция ведения протокола. Приведены практические примеры применения этих средств защиты.

Сценарий применения VPN: Основная информация о соединении между филиалами

Предположим, что вашей фирме необходимо минимизировать издержки, связанные с передачей данных между основным офисом и филиалами. В настоящий момент для этого применяется Frame Relay или выделенные линии связи, однако вы планируете внедрить новые технологии для передачи внутренней конфиденциальной информации, которые требуют меньше затрат, обеспечивают более высокий уровень защиты и могут применяться в любой точке земного шара. Для этого будет создана виртуальная частная сеть (VPN), которая использует возможности сети Internet.

Необходимо защитить только ту часть соединения, установленного между фирмой и ее филиалом, которая проходит по сети Internet. Фрагменты соединения, расположенные во внутренних сетях, защищать не нужно. Предполагается, что внутренние сети достаточно надежно защищены, поэтому можно установить соединение VPN между двумя шлюзами. Такие шлюзы должны быть напрямую подключены к промежуточной сети. Другими словами, они должны быть *граничными* или *крайними* системами, не защищенными брандмауэром. Данный пример демонстрирует действия, которые выполняются при настройке основных параметров VPN. В данном сценарии под сетью *Internet* понимается промежуточная сеть, расположенная между двумя шлюзами VPN. Это может быть внутренняя сеть фирмы или общедоступная сеть Internet.

> **Важное примечание:**
> В данном сценарии рассматриваются шлюзы iSeries(TM), которые напрямую подключены к Internet. Для простоты предполагается, что брандмауэр отсутствует. Это не означает, что брандмауэр использовать не нужно. Вы должны тщательно оценить все опасности, связанные с подключением к Internet. Подробная информация о необходимых мерах безопасности приведена в руководстве AS/400(R) Internet Security Scenarios: A Practical Approach, SG24-5954-00  .

Достоинства

У этого сценария есть следующие достоинства:

- Применение сети Internet или существующей корпоративной сети снижает стоимость внутренних линий связи, установленных между удаленными подсетями.
- Применение сети Internet или существующей корпоративной сети упрощает процедуру создания и обслуживания внутренних линий и связанного с ними оборудования.
- Применение сети Internet позволяет устанавливать соединения между удаленными системами, расположенными в любой точке земного шара.
- С помощью VPN пользователи могут работать с любыми серверами и ресурсами, расположенными в сетях, между которыми установлено соединение. Работа с таким соединением ничем не отличается от применения выделенной линии или соединения, установленного по глобальной сети (WAN).
- Применение стандартных способов шифрования и идентификации гарантирует высокий уровень защиты конфиденциальной информации во время ее передачи между системами.

- Регулярный обмен ключами шифрования упрощает настройку и минимизирует вероятность того, что ключи будут расшифрованы, а защита взломана.
- Применение внутренних IP-адресов в удаленных подсетях дает возможность сэкономить на приобретении внешних IP-адресов для клиентов.

Цели

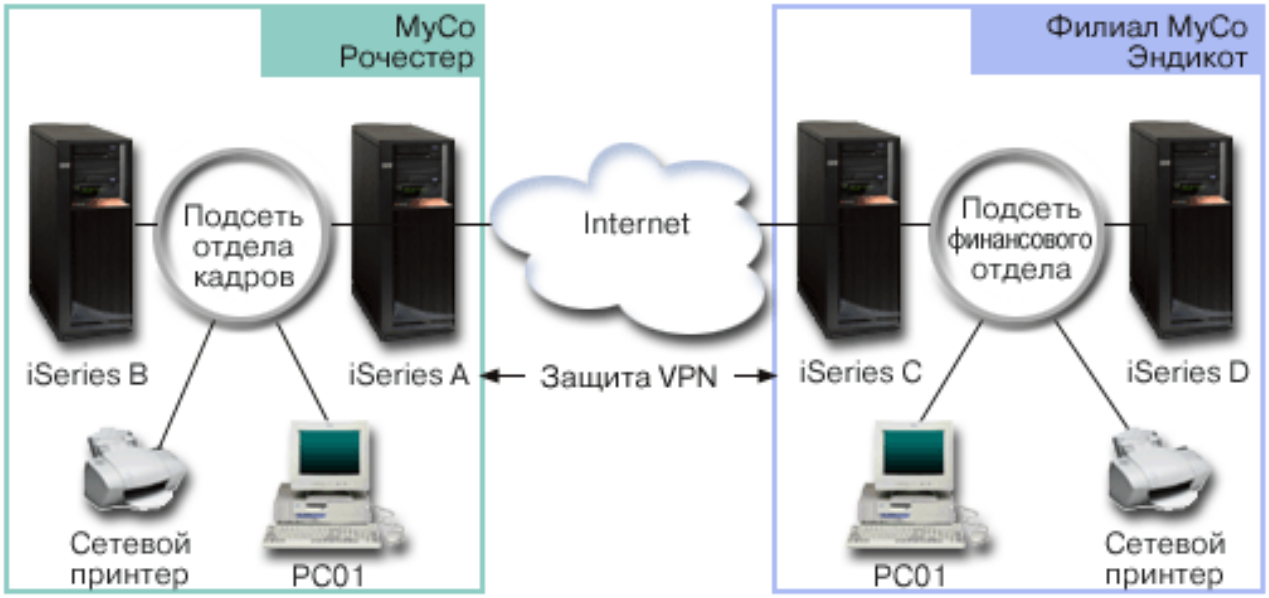
В данном сценарии фирме MyCo, Inc. необходимо настроить VPN между подсетями, принадлежащими отделу кадров и финансовому отделу. Для этой цели будут применяться серверы iSeries, расположенные в этих подсетях. Эти серверы будут играть роль шлюзов VPN. В VPN шлюз отвечает за управление ключами и применение правил IPSec к данным, которые передаются по туннелю. Шлюзы не являются конечными точками данных соединения.

В данном сценарии преследуются следующие цели:

- VPN будет применяться для защиты всех данных, передаваемых между подсетью отдела кадров и подсетью финансового отдела.
- Данные не нужно защищать с помощью VPN во время их передачи по внутренней подсети отдела.
- У всех клиентов и хостов одной подсети есть доступ ко всем ресурсам другой подсети. Ограничен лишь доступ к приложениям.
- Серверы шлюзов могут подключаться друг к другу и работать с приложениями друг друга.

Описание

На приведенном ниже рисунке показана схема сети фирмы MyCo.



Отдел кадров

- В системе iSeries-A установлена операционная система OS/400(R) версии 5, выпуска 2 (V5R2). Эта система играет роль шлюза VPN в отделе кадров.
- Адрес подсети равен 10.6.0.0, маска подсети равна 255.255.0.0. Эта подсеть является конечной точкой данных туннеля VPN в филиале фирмы MyCo, расположенном в городе Рочестер.
- В сети Internet системе iSeries-A присвоен IP-адрес 204.146.18.227. Этот адрес представляет конечную точку соединения. Это означает, что система iSeries-A отвечает за управление ключами и применение правил IPSec к принимаемым и отправляемым дейтаграммам IP.
- Во внутренней подсети системе iSeries-A присвоен IP-адрес 10.6.11.1.

- Система iSeries-B является рабочим сервером в подсети отдела кадров, на котором запущены стандартные приложения TCP/IP.

Финансовый отдел

- В системе iSeries-C установлена операционная система OS/400 версии 5, выпуска 2 (V5R2). Эта система играет роль шлюза VPN финансового отдела.
- Адрес подсети равен 10.196.8.0, маска подсети равна 255.255.255.0. Эта подсеть является конечной точкой данных туннеля VPN в филиале фирмы MyCo, расположенном в городе Эндикот.
- В сети Internet системе iSeries-C присвоен IP-адрес 208.222.150.250. Этот адрес представляет конечную точку соединения. Это означает, что система iSeries-C отвечает за управление ключами и применение правил IPSec к принимаемым и отправляемым дейтаграммам IP.
- Во внутренней подсети системе iSeries-C присвоен IP-адрес 10.196.8.5.

Задачи настройки

Для настройки соединения между филиалами, описанными в данном сценарии, необходимо выполнить следующие задачи:

1. Убедитесь, что в конфигурации TCP/IP определен маршрут, соединяющий два сервера шлюзов, по которому эти серверы могут обмениваться данными в сети Internet. Кроме того, хосты подсети должны правильно определять маршрут к соответствующему шлюзу для обращения к удаленной подсети. **Примечание:** Вопросы, связанные с маршрутизацией, не рассматриваются в данном разделе. Дополнительную информацию можно найти в разделе Маршрутизация и управление нагрузкой в TCP/IP справочной системы Information Center.
2. Заполните (стр. 6) формы и справочные таблицы в обеих системах, для того чтобы спланировать настройку соединения.
3. Настройте (стр. 7) VPN на шлюзе отдела кадров (в системе iSeries-A).
4. Настройте (стр. 8) VPN на шлюзе финансового отдела (в системе iSeries-C).
5. Убедитесь, что серверы VPN запущены (стр. 8).
6. Проверьте (стр. 9) соединение, установленное между двумя удаленными подсетями.

Подробная информация о настройке

После того как вы убедились, что маршруты TCP/IP настроены правильно, и серверы шлюзов могут подключаться друг к другу, можно приступить к настройке VPN.

Шаг 2: Заполните формы планирования

Приведенные ниже справочные таблицы помогут вам собрать информацию, необходимую для настройки VPN. К настройке VPN можно приступить только тогда, когда на все вопросы справочной таблицы предварительных требований будет дан положительный ответ.

Примечание: Приведенные ниже формы относятся к системе iSeries-A. Аналогичные формы нужно заполнить для системы iSeries-C, скорректировав IP-адреса.

Справочная таблица предварительных требований	**Ответы**
Установлена ли в системе операционная система OS/400(R) версии V5R2 (5722-SS1) или более поздней версии?	Да
Установлен ли в системе компонент Диспетчер цифровых сертификатов (5722-SS1, компонент 34)?	Да
Установлен ли в системе продукт Cryptographic Access Provider (5722-AC2 или AC3)?	Да
Установлен ли в системе продукт iSeries(TM) Access для Windows(R) (5722-XE1)?	Да
Установлен ли в системе Навигатор iSeries?	Да

Справочная таблица предварительных требований	Ответы
Установлен ли компонент Сеть программы Навигатор iSeries?	Да
Установлен ли в системе продукт TCP/IP Connectivity Utilities для OS/400 (5722-TC1)?	Да
Установлено ли системное значение Сохранять идентификационные данные на сервере (QRETSVRSEC *SEC) равным 1?	Да
Настроен ли в системе iSeries протокол TCP/IP (включая интерфейсы IP, маршруты, имя локального хоста и имя локального домена)?	Да
Установлено ли между конечными точками обычное соединение TCP/IP?	Да
Применены ли в системе последние версии временных исправлений программ (PTF)?	Да
Если туннель VPN будет проходить через брандмауэры или маршрутизаторы, выполняющие фильтрацию пакетов IP, то поддерживают ли эти брандмауэры и маршрутизаторы протоколы AH и ESP?	Да
Разрешено ли на брандмауэрах и маршрутизаторах применение протоколов IKE (порт UDP 500), AH и ESP?	Да
Разрешена ли на брандмауэрах пересылка пакетов IP?	Да

Для настройки VPN вам потребуется следующая информация	Ответы
Соединение какого типа будет создано?	Соединение между шлюзами
Какое имя будет присвоено группе соединений с динамическим ключом?	HRgw2FINgw
Какой способ защиты ключей, по отношению к производительности системы, будет применяться?	Сбалансированный
Применяются ли сертификаты для идентификации соединения? Если нет, какой подготовленный ключ будет применяться?	Нет topsecretstuff
Какой идентификатор связан с локальным сервером ключей?	IP-адрес: 204.146.18.227
Какой идентификатор связан с локальной конечной точкой данных?	Подсеть: 10.6.0.0 Маска: 255.255.0.0
Какой идентификатор присвоен удаленному серверу ключей?	IP-адрес: 208.222.150.250
Какой идентификатор связан с удаленной конечной точкой данных?	Подсеть: 10.196.8.0 Маска: 255.255.255.0
Пакеты каких протоколов будет разрешено передавать по соединению и через какие порты?	Любые
Какой способ защиты данных, по отношению к производительности системы, будет применяться?	Сбалансированный
К каким интерфейсам относится соединение?	TRLINE

Шаг 3: Настройте VPN в системе iSeries-A

Настройте VPN в системе iSeries-A, как описано ниже, используя информацию из заполненных ранее форм:

1. В окне программы Навигатор откройте iSeries-A **—>Сеть —>Стратегии IP**.
2. Для запуска мастера создания соединения щелкните правой кнопкой мыши на пункте **Виртуальная частная сеть** и выберите опцию **Создать соединение**.
3. Ознакомьтесь с описанием объектов, создаваемых мастером, приведенным на странице **Приветствие**.
4. Нажмите кнопку **Далее** для перехода к странице **Имя соединения**.
5. В поле **Имя** введите `HRgw2FINgw`.
6. При необходимости укажите описание группы соединений.
7. Нажмите кнопку **Далее** для перехода к странице **Сценарий подключения**.
8. Выберите опцию **Подключить локальный шлюз к другому шлюзу**.

9. Нажмите кнопку **Далее** для перехода к странице **Стратегия IKE**.
10. Выберите опцию **Создать стратегию**, а затем выберите вариант **Сбалансированная защита и производительность**.
11. Нажмите кнопку **Далее** для перехода к странице **Сертификат локальной конечной точки соединения**.
12. Выберите значение **Нет**, для того чтобы сертификат не применялся для идентификации соединения.
13. Нажмите кнопку **Далее** для перехода к странице **Локальный сервер ключей**.
14. В поле **Тип идентификатора** выберите значение **IP-адрес версии 4**.
15. В поле IP-адрес выберите значение **204.146.18.227**.
16. Нажмите кнопку **Далее** для перехода к странице **Удаленный сервер ключей**.
17. В поле **Тип идентификатора** выберите значение **IP-адрес версии 4**.
18. В поле Идентификатор введите значение **208.222.150.250**.
19. В поле Подготовленный ключ введите значение **topsecretstuff**.
20. Нажмите кнопку **Далее** для перехода к странице **Локальная конечная точка данных**.
21. В поле **Тип идентификатора** выберите значение **Подсеть IP версии 4**.
22. В поле Идентификатор введите значение **10.6.0.0**.
23. В поле Маска подсети введите значение **255.255.0.0**.
24. Нажмите кнопку **Далее** для перехода к странице **Удаленная конечная точка данных**.
25. В поле **Тип идентификатора** выберите значение **Подсеть IP версии 4**.
26. В поле Идентификатор введите значение **10.196.8.0**.
27. В поле Маска подсети введите значение **255.255.255.0**.
28. Нажмите кнопку **Далее** для перехода к странице **Службы данных**.
29. Оставьте значения по умолчанию и нажмите кнопку **Далее** для перехода к странице **Стратегия защиты данных**.
30. Выберите опцию **Создать стратегию**, а затем выберите вариант **Сбалансированная защита и производительность**. Выберите опцию **Применять алгоритм шифрования RC4**.
31. Нажмите кнопку **Далее** для перехода к странице **Допустимые интерфейсы**.
32. Выберите значение **TRLINE** в таблице **Линия связи**.
33. Нажмите кнопку **Далее** для перехода к странице **Обзор**. Проверьте все значения на этой странице.
34. Для завершения настройки нажмите кнопку **Готово**.
35. Когда появится окно **Активировать фильтры стратегии**, выберите значение **Да, активировать созданные фильтры стратегии**, а затем выберите опцию **Разрешить прочие данные**. Для завершения настройки нажмите кнопку **OK**. Когда появится соответствующее приглашение, укажите, что правила нужно активировать для всех интерфейсов.

Настройка VPN в системе iSeries-A завершена. Перейдите к процедуре настройки VPN на шлюзе VPN финансового отдела (iSeries-C).

Шаг 4: Настройте VPN в системе iSeries-C

Выполните ту же процедуру настройки, что и в системе iSeries-A, изменив необходимые IP-адреса. За дополнительной информацией обратитесь к формам планирования. После выполнения процедуры настройки на шлюзе VPN финансового отдела соединение будет находиться в состоянии *по запросу*. Такое соединение активируется при отправке дейтаграммы IP, которая должна быть передана по защищенному соединению VPN. Далее необходимо запустить серверы VPN (если они еще не запущены).

Шаг 6: Запустите серверы VPN

Для запуска серверов VPN выполните следующие действия:

1. В окне программы Навигатор откройте **сервер —>Сеть —>Стратегии IP**.
2. Щелкните правой кнопкой мыши на значке **VPN** и выберите **Запустить**.

Шаг 7: Проверьте соединение

После настройки и запуска обоих серверов VPN необходимо проверить связь между удаленными подсетями. Для этого выполните следующие действия:

1. В окне программы Навигатор разверните **iSeries-A —>Сеть**.
2. Щелкните правой кнопкой мыши на пункте **Настройка TCP/IP**, выберите опцию **Утилиты**, а затем - **Проверить соединение**.
3. В окне **Проверить соединение** введите значение `iSeries-C` в поле **Проверить соединение**.
4. Нажмите кнопку **Отправить пробный пакет** для проверки связи между системами iSeries-A и iSeries-C.
5. После завершения проверки нажмите кнопку **OK**.

Сценарий применения VPN: Основная информация о соединении между фирмами

Для обмена данными с деловыми партнерами, дочерними фирмами и поставщиками многие фирмы применяют соединения Frame Relay или выделенные линии связи. Такие способы подключения дороги в обслуживании и накладывают ограничения на длину линии связи. Альтернативой для таких фирм может стать сеть VPN, которая позволяет с минимальными затратами обеспечить защиту конфиденциальной информации при ее передаче по открытой сети.

Предположим, что ваша фирма - основной поставщик комплектующих для изготовителя продукции. Для того чтобы у вас всегда было в наличии достаточное количество комплектующих, вам нужно знать, сколько комплектующих осталось у фирмы-изготовителя, и сколько комплектующих ей потребуется в ближайшее время. Получение такой информации занимает много времени и дорого стоит. Иногда полученная информация бывает неточной. Вы хотите найти более простой, быстрый и эффективный способ получения информации от фирмы-изготовителя. Учитывая, что требуемая информация носит конфиденциальный характер и постоянно изменяется, изготовитель не может опубликовать ее на своем Web-сайте или указать в ежемесячном открытом отчете. Для выполнения поставленной задачи можно создать виртуальную частную сеть (VPN), которая будет использовать возможности сети Internet.

Цели

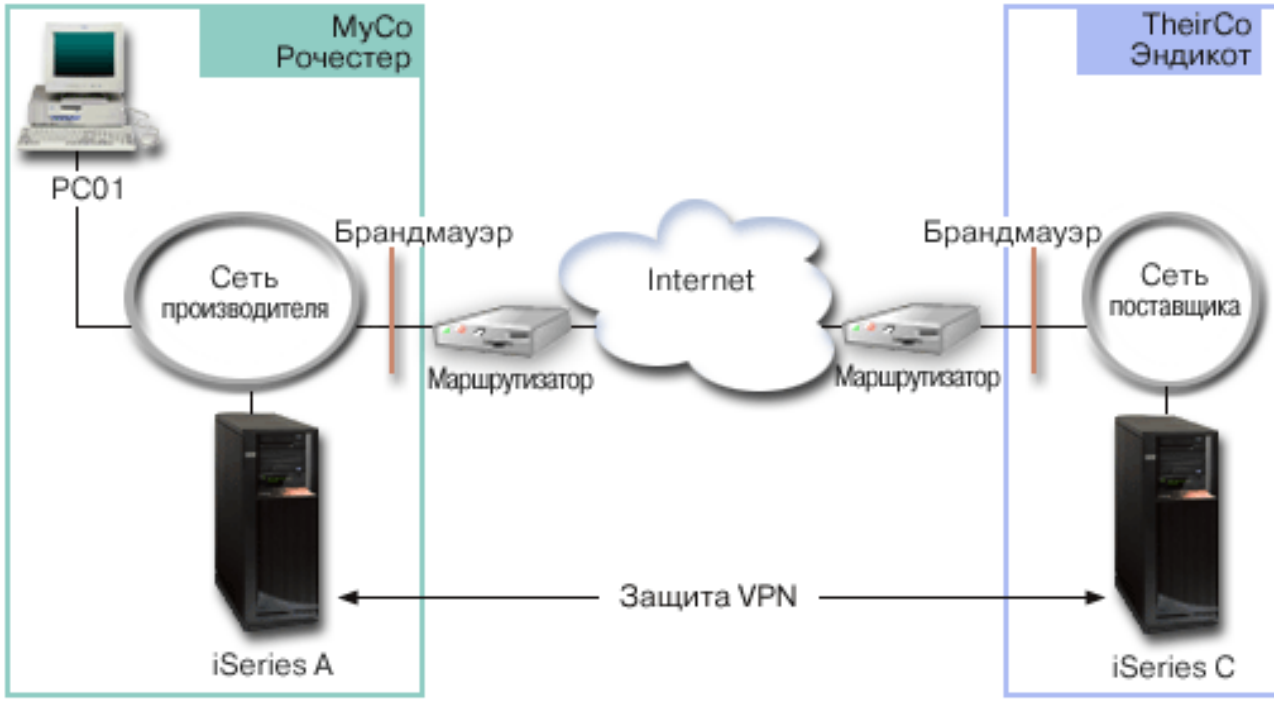
В данном сценарии фирме MyCo требуется установить соединение VPN между хостом, расположенным в отделе поставки комплектующих, и хостом, расположенным в производственном отделе одного из деловых партнеров, TheirCo.

Поскольку фирмы планируют обмениваться конфиденциальной информацией, эта информация должна быть защищена во время передачи по сети Internet. Кроме того, данные должны защищаться во время их передачи по внутренней сети фирмы, так как каждая фирма считает, что сеть другой фирмы не защищена. Для этого потребуются средства идентификации, обеспечения целостности и шифрования данных.

Важное примечание:
В данном сценарии будет рассматриваться настройка простого соединения VPN между двумя хостами. В реальной сети обычно требуется дополнительно настроить брандмауэр, IP-адреса и маршруты.

Описание

На приведенном ниже рисунке показаны сети фирм MyCo и TheirCo:



Сеть поставщика - фирмы MyCo

- В системе iSeries-A установлена операционная система OS/400(R) версии 5, выпуска 2 (V5R2).
- Системе iSeries-A присвоен IP-адрес 10.6.1.1. Этот адрес представляет собой конечную точку соединения и конечную точку данных. Это означает, что система iSeries-A выполняет согласование IKE и применяет правила IPSec к исходящим и входящим дейтаграммам IP, а также является отправителем и получателем данных, которые передаются по соединению VPN.
- Система iSeries-A расположена в подсети 10.6.0.0 с маской 255.255.0.0
- Соединение с системой iSeries-C разрешено устанавливать только системе iSeries-A.

Сеть изготовителя - фирмы TheirCo

- В системе iSeries-C установлена операционная система OS/400 версии 5, выпуска 2 (V5R2).
- Системе iSeries-C присвоен IP-адрес 10.196.8.6. Этот адрес представляет собой конечную точку соединения и конечную точку данных. Это означает, что система iSeries-A выполняет согласование IKE и применяет правила IPSec к исходящим и входящим дейтаграммам IP, а также является отправителем и получателем данных, которые передаются по соединению VPN.
- Система iSeries-C расположена в подсети 10.196.8.0 с маской 255.255.255.0

Задачи настройки

Для настройки соединения между двумя фирмами, описанными в данном сценарии, необходимо выполнить следующие действия:

1. Убедитесь, что в конфигурации TCP/IP определен маршрут между системами iSeries-A и iSeries-C, по которому эти системы могут обмениваться данными в сети Internet. В этом случае хосты подсети будут правильно направлять данные на соответствующий шлюз для их пересылки в удаленную подсеть. В данном сценарии предполагается, что в подсети применяются внутренние адреса.

   Примечание: Вопросы, связанные с маршрутизацией, не рассматриваются в данном разделе. Дополнительную информацию можно найти в разделе Маршрутизация и управление нагрузкой в TCP/IP справочной системы Information Center.

2. Заполните (стр. 11) формы и справочные таблицы в обеих системах, для того чтобы спланировать настройку соединения.
3. Настройте (стр. 12) VPN в системе iSeries-A, расположенной в сети поставщика (фирмы MyCo).
4. Настройте (стр. 13) VPN в системе iSeries-C, расположенной в сети изготовителя (фирмы TheirCo).
5. Активируйте (стр. 13) правила фильтрации на обоих серверах.
6. Запустите (стр. 13) соединение в системе iSeries-A.
7. Проверьте (стр. 14) связь между подсетями.

Подробная информация о настройке

После того как вы убедились, что маршруты TCP/IP настроены правильно, и серверы могут подключаться друг к другу, можно приступить к настройке VPN.

Шаг 2: Заполните формы планирования

Приведенные ниже справочные таблицы помогут вам собрать информацию, необходимую для настройки VPN. К настройке VPN можно приступить только тогда, когда на все вопросы справочной таблицы предварительных требований будет дан положительный ответ.

Примечание: Приведенные ниже формы относятся к системе iSeries-A. Аналогичные формы нужно заполнить для системы iSeries-C, скорректировав IP-адреса.

Справочная таблица предварительных требований	**Ответы**
Установлена ли в системе операционная система OS/400(R) V5R2 (5722-SS1) или более поздней версии?	Да
Установлен ли в системе компонент Диспетчер цифровых сертификатов (5722-SS1, компонент 34)?	Да
Установлен ли в системе продукт Cryptographic Access Provider (5722-AC2 или AC3)?	Да
Установлен ли в системе продукт iSeries(TM) Access для Windows(R) (5722-XE1)?	Да
Установлен ли в системе Навигатор iSeries?	Да
Установлен ли компонент Сеть программы Навигатор iSeries?	Да
Установлен ли в системе продукт TCP/IP Connectivity Utilities for OS/400 (5722-TC1)?	Да
Установлено ли системное значение Сохранять идентификационные данные на сервере (QRETSVRSEC *SEC) равным 1?	Да
Настроен ли в системе iSeries протокол TCP/IP (включая интерфейсы IP, маршруты, имя локального хоста и имя локального домена)?	Да
Установлено ли между конечными точками обычное соединение TCP/IP?	Да
Применены ли в системе последние версии временных исправлений программ (PTF)?	Да
Если туннель VPN будет проходить через брандмауэры или маршрутизаторы, выполняющие фильтрацию пакетов IP, то поддерживают ли эти брандмауэры и маршрутизаторы протоколы AH и ESP?	Да
Разрешено ли на брандмауэрах и маршрутизаторах применение протоколов IKE (порт UDP 500), AH и ESP?	Да
Разрешена ли на брандмауэрах пересылка пакетов IP?	Да

Для настройки VPN вам потребуется следующая информация	**Ответы**
Соединение какого типа будет создано?	Соединение между хостами
Какое имя будет присвоено группе соединений с динамическим ключом?	MyCo2TheirCo
Какой способ защиты ключей, по отношению к производительности системы, будет применяться?	Максимальный

Применяются ли сертификаты для идентификации соединения? Если нет, какой подготовленный ключ будет применяться?	Да
Какой идентификатор связан с локальным сервером ключей?	IP-адрес: 10.6.1.1
Какой идентификатор связан с локальной конечной точкой данных?	IP-адрес: 10.6.1.1
Какой идентификатор присвоен удаленному серверу ключей?	IP-адрес: 10.196.8.6
Какой идентификатор связан с удаленной конечной точкой данных?	IP-адрес: 10.196.8.6
Пакеты каких протоколов будет разрешено передавать по соединению и через какие порты?	Любые
Какой способ защиты данных, по отношению к производительности системы, будет применяться?	Максимальный
К каким интерфейсам относится соединение?	TRLINE

Шаг 3: Настройте VPN в системе iSeries-A

Настройте VPN в системе iSeries-A, как описано ниже, используя информацию из заполненных ранее форм:

1. В окне программы Навигатор разверните значок своего сервера **—>Сеть —>Стратегии IP**.
2. Для запуска мастера настройки соединения щелкните правой кнопкой мыши на пункте **Виртуальная частная сеть** и выберите **Создать соединение**.
3. Ознакомьтесь с описанием объектов, создаваемых мастером, приведенным на странице **Приветствие**.
4. Нажмите кнопку **Далее** для перехода к странице **Имя соединения**.
5. В поле **Имя** введите значение `MyCo2TheirCo`.
6. При необходимости укажите описание группы соединений.
7. Нажмите кнопку **Далее** для перехода к странице **Сценарий подключения**.
8. Выберите опцию **Подключить локальный хост к другому хосту**.
9. Нажмите кнопку **Далее** для перехода к странице **Стратегия IKE**.
10. Выберите опцию **Создать стратегию**, а затем выберите вариант **Максимальная защита, низкая производительность**.
11. Нажмите кнопку **Далее** для перехода к странице **Сертификат локальной конечной точки соединения**.
12. Выберите значение **Да**, для того чтобы сертификаты применялись для идентификации соединения. После этого выберите сертификат системы iSeries-A.
    Примечание: Если вы планируете применять сертификат для идентификации локальной конечной точки соединения, то сначала создайте сертификат с помощью Диспетчера цифровых сертификатов (DCM).
13. Нажмите кнопку **Далее** для перехода к странице **Идентификатор локальной конечной точки соединения**.
14. Выберите для типа идентификатора значение **IP-адрес версии 4**. В качестве IP-адреса необходимо указать значение 10.6.1.1. Эти значения также должны быть заданы в сертификате, созданном с помощью DCM.
15. Нажмите кнопку **Далее** для перехода к странице **Удаленный сервер ключей**.
16. В поле **Тип идентификатора** выберите значение **IP-адрес версии 4**.
17. В поле `Идентификатор` введите значение **10.196.8.6**.
18. Нажмите кнопку **Далее** для перехода к странице **Службы данных**.
19. Не изменяя значения по умолчанию, нажмите кнопку **Далее** для перехода к странице **Стратегия защиты данных**.
20. Выберите опцию **Создать стратегию**, а затем выберите вариант **Максимальная защита, низкая производительность**. Выберите опцию **Применять алгоритм шифрования RC4**.
21. Нажмите кнопку **Далее** для перехода к странице **Допустимые интерфейсы**.
22. Выберите значение **TRLINE**.
23. Нажмите кнопку **Далее** для перехода к странице **Обзор**. Проверьте все значения на этой странице.

24. Для завершения настройки нажмите кнопку **Готово**.
25. Когда появится окно диалога **Активировать фильтры стратегии**, выберите значение **Нет, активировать правила фильтрации позднее** и нажмите кнопку **OK**.

Теперь нужно указать, что это соединение может устанавливать только система iSeries-A. Для этого измените свойства группы соединений с динамическим ключом, которая была создана мастером (MyCo2TheirCo):

1. В интерфейсе VPN выберите опцию **Группы** на левой панели. На правой панели появится группа соединений с динамическим ключом MyCo2TheirCo. Щелкните на ней правой кнопкой мыши и выберите пункт **Свойства**.
2. Перейдите на страницу **Стратегия** и выберите опцию **Соединение устанавливается локальной системой**.
3. Нажмите **OK** для сохранения изменений.

Настройка VPN в системе iSeries-A завершена. Перейдите к процедуре настройки VPN в системе iSeries-C, расположенной в сети изготовителя, то есть фирмы TheirCo.

Шаг 4: Настройте VPN в системе iSeries-C

Выполните ту же процедуру настройки, что и в системе iSeries-A, изменив необходимые IP-адреса. За дополнительной информацией обратитесь к формам планирования. После выполнения процедуры настройки в системе iSeries-C активируйте на обоих серверах правила фильтрации, созданные мастером Соединение.

Шаг 5: Активируйте правила обработки пакетов

Мастер автоматически создает правила обработки пакетов, необходимые для правильной работы соединения. Перед запуском соединения VPN эти правила необходимо активировать в обеих системах. Для того чтобы активировать правила в системе iSeries-A, выполните следующие действия:

1. В Навигаторе разверните **iSeries-A —> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Правила обработки пакетов** и выберите опцию **Активировать**. Появится окно **Активировать правила обработки пакетов**.
3. Укажите, какие правила должны быть активированы: правила, созданные VPN, выбранный файл правил или и то, и другое. Последнюю опцию, например, можно выбрать в том случае, если помимо правил, созданных VPN, для интерфейса должны быть активированы некоторые правила PERMIT и DENY.
4. Выберите интерфейс, для которого должны быть активированы правила. В данном случае нужно выбрать опцию **Все интерфейсы**.
5. Нажмите кнопку **OK**, для того чтобы подтвердить, что нужно проверить и активировать правила для указанных интерфейсов. Система проверит правила на наличие синтаксических и семантических ошибок. Результаты проверки будут показаны в окне сообщений, расположенном в нижней области окна редактора. При наличии сообщения об ошибке щелкните правой кнопкой мыши на этом сообщении и выберите пункт **Перейти к строке**, чтобы была выделена строка файла правил, в которой была найдена ошибка.
6. Повторите описанную процедуру активации правил в системе iSeries-C.

Шаг 6: Запустите соединение

Для запуска соединения MyCo2TheirCo в системе iSeries-A выполните следующие действия:

1. В Навигаторе разверните **iSeries-A —> Сеть —> Стратегии IP**.
2. Если сервер VPN не запущен, щелкните правой кнопкой мыши на пункте **Виртуальная частная сеть** и выберите опцию **Запустить**. Будет запущен сервер VPN.
3. Разверните список **Виртуальная частная сеть —>Защищенные соединения**.
4. Выберите **Все соединения** для просмотра списка соединений в правой панели.
5. Щелкните правой кнопкой мыши на соединении **MyCo2TheirCo** и выберите опцию **Запустить**.

6. В меню **Вид** выберите пункт **Обновить**. После запуска соединения его состояние должно измениться с *Простаивает* на *Активно*. Запуск соединения может занять несколько минут. Если состояние соединения не изменилось на *Активно*, обновите содержимое окна еще раз.

Шаг 7: Проверьте соединение

После настройки серверов и запуска соединения необходимо убедиться в том, что удаленные хосты могут обмениваться данными по установленному соединению. Для этого выполните следующие действия:

1. В окне программы Навигатор разверните **iSeries-A —>Сеть**.
2. Щелкните правой кнопкой мыши на пункте **Настройка TCP/IP**, выберите опцию **Утилиты**, а затем - **Проверить соединение**.
3. В окне **Проверить соединение** введите значение `iSeries-C` в поле **Проверить соединение**.
4. Для проверки соединения между системами iSeries-A и iSeries-C нажмите кнопку **Отправить пробный пакет**.
5. После завершения проверки нажмите кнопку **OK**.

Сценарий применения VPN: Защита необязательного туннеля L2TP с помощью IPSec

Предположим, что у вашей фирмы открыт небольшой филиал в другом регионе страны. В любой момент в течение рабочего дня филиалу может потребоваться конфиденциальная информация, хранящаяся на сервере iSeries(TM), который подключен к корпоративной сети. Для подключения филиала к корпоративной сети применяется дорогая выделенная линия связи. Хотя защищенное соединение с корпоративной сетью фирмы необходимо для работы филиала, было бы желательно сократить стоимость такого соединения. Это можно сделать с помощью необязательного туннеля L2TP, за счет которого можно расширить корпоративную сеть таким образом, чтобы в нее входил филиал фирмы. Для защиты данных, передаваемых по туннелю L2TP, применяется функция VPN.

Применение необязательного туннеля L2TP дает возможность удаленному филиалу напрямую устанавливать защищенное соединение с сетевым сервером L2TP (LNS), расположенным в корпоративной сети. При этом на клиенте будет расположен концентратор L2TP (LAC). Туннель будет прозрачен для провайдера Internet (ISP) удаленного клиента, поэтому не требуется, чтобы ISP поддерживал протокол L2TP. Для получения дополнительной информации о протоколе L2TP обратитесь к разделу “Протокол L2TP” на стр. 27.

> **Важное примечание:**
> В данном сценарии рассматриваются шлюзы iSeries, которые напрямую подключены к Internet. Для простоты предполагается, что брандмауэр отсутствует. Это не означает, что брандмауэр использовать не нужно. Вы должны оценить все опасности, связанные с подключением к Internet. Подробная информация о необходимых мерах безопасности приведена в руководстве AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00  .

Цели

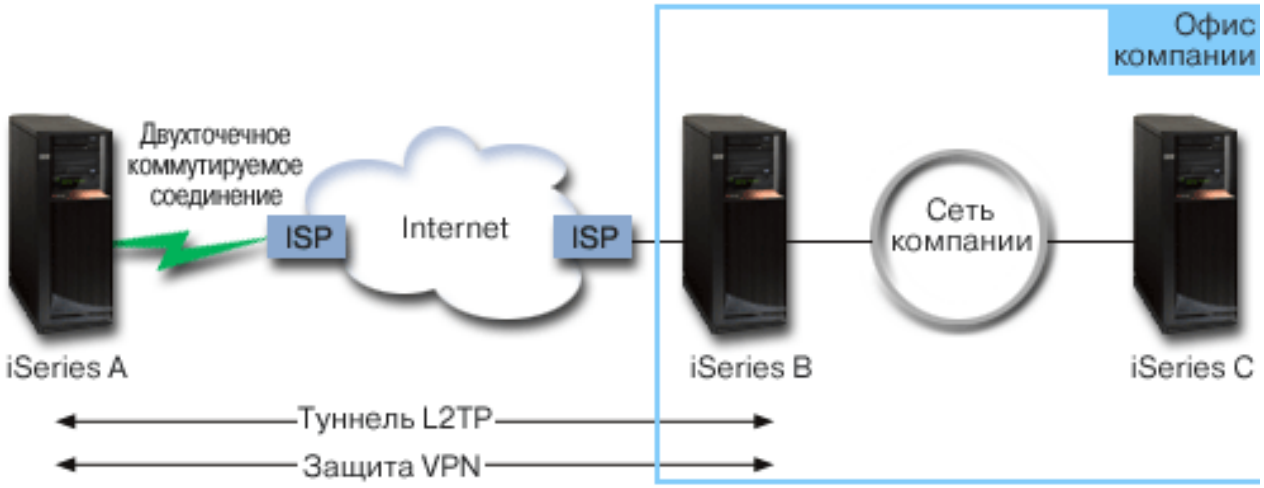
В данном сценарии система iSeries, расположенная в филиале фирмы, подключается к корпоративной сети с помощью защищенного туннеля L2TP, который устанавливается через шлюз iSeries.

В этом сценарии преследуются следующие цели:

- Соединение с корпоративной сетью всегда устанавливается системой, расположенной в филиале фирмы.
- В сети филиала фирмы есть только одна система, которой требуется доступ к корпоративной сети. Такая система играет в сети филиала роль хоста, а не шлюза.
- Корпоративный сервер - это хост, подключенный к корпоративной сети.

Описание

На приведенном ниже рисунке показана сеть, описанная в этом сценарии:



iSeries-A

- Есть права доступа к приложениям TCP/IP всех систем, подключенных к корпоративной сети.
- IP-адрес назначается динамически провайдером Internet.
- Поддерживает протокол L2TP.

iSeries-B

- Есть права доступа к приложениям TCP/IP системы iSeries-A.
- Адрес подсети равен 10.6.0.0, маска подсети равна 255.255.0.0. Эта подсеть является конечной точкой данных туннеля VPN в корпоративной сети.
- Для подключения к Internet применяется IP-адрес 205.13.237.6. Этот адрес представляет конечную точку соединения. Это означает, что система iSeries-B отвечает за управление ключами и применение правил IPSec к принимаемым и отправляемым дейтаграммам IP. Во внутренней подсети системе iSeries-B присвоен IP-адрес 10.6.11.1.

Если говорить в терминах L2TP, то система *iSeries-A* играет роль инициатора L2TP, а система *iSeries-B* играет роль конечной системы L2TP.

Задачи настройки

Предполагается, что в системах уже заданы правильные параметры TCP/IP. Необходимо выполнить следующие задачи:

1. Настроить VPN (стр. 16) в системе iSeries-A.
2. Настроить профайл соединения PPP (стр. 18) и виртуальную линию в iSeries-A.
3. Связать (стр. 19) группу соединений с динамическим ключом с профайлом PPP.
4. Настроить VPN (стр. 19) в iSeries-B.
5. Настроить профайл соединения PPP (стр. 19) и виртуальную линию в iSeries-B.
6. Активировать (стр. 20) правила обработки пакетов в iSeries-A и iSeries-B.
7. Запустить (стр. 20) соединение в iSeries-A.

Подробная информация о настройке

После того как вы убедились, что протокол TCP/IP настроен правильно, и серверы iSeries(TM) могут подключаться друг к другу, перейдите к настройке соединения, описанного в этом сценарии.

Шаг 1: Настройте VPN в системе iSeries-A

Для настройки VPN в системе iSeries-A выполните следующие действия:

1. **Настройте стратегию Internet Key Exchange**
   a. В окне программы Navigator разверните iSeries-A **—> Сеть—> Стратегии IP—> Виртуальная частная сеть—> Стратегии защиты IP**.
   b. Щелкните правой кнопкой мыши на пункте **Стратегии IKE** и выберите опцию **Создать стратегию IKE**
   c. На странице **Удаленный сервер** выберите в качестве типа идентификатора значение **IP-адрес версии 4** и введите значение `205.13.237.6` в поле **IP-адрес**.
   d. На странице **Конфигурации** выберите опцию **Подготовленный ключ**. Она означает, что для идентификации в стратегии будет применяться подготовленный ключ.
   e. Укажите подготовленный ключ в поле **Ключ**. Подготовленный ключ можно считать разновидностью пароля.
   f. Выберите в качестве типа идентификатора локального сервера ключей значение **Идентификатор ключа** и введите идентификатор ключа в поле **Идентификатор**. Например, `thisisthekeyid`. IP-адрес локального сервера ключей назначается динамически, поэтому его нельзя узнать заранее. С помощью указанного идентификатора система iSeries-B сможет идентифицировать систему iSeries-A, когда получит от нее запрос о подключении.
   g. На странице **Преобразование** нажмите кнопку **Добавить**. Добавьте преобразование, которое система iSeries-A будет предлагать системе iSeries-B для защиты ключей. Укажите, следует ли применять функцию защиты идентификаторов на первом этапе согласования.
   h. На странице **Преобразование стратегии IKE** выберите в качестве способа идентификации **Подготовленный ключ**, в качестве алгоритма хэширования - значение **SHA**, а в качестве алгоритма шифрования - значение **3DES-CBC**. Оставьте значения по умолчанию в полях Группа Diffie-Hellman и Срок действия ключей IKE.
   i. Нажмите кнопку **OK**, чтобы вернуться на страницу **Преобразования**.
   j. Выберите опцию **Ускоренный режим согласования IKE (без защиты идентификатора)**.

      Примечание:Если вам приходится применять подготовленные ключи с ускоренным режимом согласования, то используйте нетривиальные пароли, взлом которых с помощью сканирования словаря маловероятен. Кроме того, рекомендуется периодически менять пароли.
   k. Нажмите кнопку **OK** для сохранения конфигурации.
2. **Настройте стратегию защиты данных**
   a. В интерфейсе VPN щелкните правой кнопкой мыши на пункте **Стратегии защиты данных** и выберите опцию **Создать стратегию защиты данных**.
   b. На странице **Общие** укажите имя стратегии защиты данных. Например, `l2tpremoteuser`.
   c. Перейдите на страницу **Планы**. План - это набор протоколов, применяемых инициатором и отвечающим сервером ключей для установления динамического соединения между двумя точками. Одну стратегию защиты данных можно задать для нескольких соединений. На удаленном сервере ключей VPN может не оказаться стратегии защиты данных с теми же свойствами. Для того чтобы не столкнуться с этой проблемой, задайте несколько планов в одной стратегии. При установлении соединения VPN с удаленным сервером ключей в стратегиях инициатора соединения и отвечающей стороны должен присутствовать хотя бы один совпадающий план.
   d. Нажмите кнопку **Добавить**, чтобы добавить преобразование плана защиты данных.
   e. Выберите в качестве режима передачи данных значение **Открытая передача**.
   f. Укажите срок действия ключа.
   g. Нажмите кнопку **OK**, чтобы вернуться на страницу **Преобразования**.
   h. Нажмите кнопку **OK** для сохранения новой стратегии защиты данных.
3. **Настройте группу соединений с динамическим ключом**
4.
   a. В интерфейсе VPN разверните список **Защищенные соединения**.

b. Щелкните правой кнопкой мыши на пункте **По группам** и выберите опцию **Создать группу с динамическим ключом**.

c. На странице **Общие** укажите имя группы. Например, `l2tptocorp`.

d. Выберите опцию **Защищает локально созданный туннель L2TP**.

e. В качестве роли системы выберите значение **Обе системы являются хостами**.

f. Перейдите на страницу **Стратегия**. Выберите в списке **Стратегия защиты данных** стратегию `l2tpremoteuser`, созданную на шаге 2.

g. Выберите опцию **Соединение устанавливается локальной системой**. Она означает, что соединение с системой iSeries-B может устанавливать только система iSeries-A.

h. Перейдите на страницу **Соединения**. Выберите опцию **Создать следующее правило фильтрации стратегии для этой группы**. Нажмите кнопку **Изменить** и задайте параметры фильтра стратегии.

i. На странице **Фильтр стратегии - Локальные адреса** выберите в качестве типа идентификатора значение **Идентификатор ключа**.

j. В качестве идентификатора выберите идентификатор ключа `thisisthekeyid`, заданный в стратегии IKE.

k. Перейдите на страницу **Фильтр стратегии - Удаленные адреса**. Выберите в списке **Тип идентификатора** значение **IP-адрес версии 4**.

l. Введите значение `205.13.237.6` в поле **Идентификатор**.

m. Перейдите на страницу **Фильтр стратегии - Службы**. Введите значение `1701` в полях **Локальный порт** и **Удаленный порт**. Порт 1701 применяется протоколом L2TP.

n. В списке **Протокол** выберите значение **UDP**.

o. Нажмите кнопку **OK** для возврата на страницу **Соединения**.

p. Перейдите на страницу **Интерфейсы**. Выберите любую линию связи или профайл PPP, с которым будет связана эта группа. Профайл PPP для этой группы еще не создан. После создания профайла вам потребуется изменить профайл PPP, с которым связана группа.

q. Нажмите кнопку **OK** для создания группы соединений с динамическим ключом, l2tptocorp.

Теперь необходимо добавить соединение в созданную группу.

5. **Настройте соединение с динамическим ключом**

a. В интерфейсе VPN разверните значок **По группам**. Появится список групп соединений с динамическим ключом, настроенных в системе iSeries-A.

b. Щелкните правой кнопкой мыши на группе **l2tptocorp** и выберите пункт **Создать соединение с динамическим ключом**.

c. На странице **Общие** укажите описание соединения, если это необходимо.

d. В качестве типа идентификатора удаленного сервера ключей выберите значение **IP-адрес версии 4**.

e. Выберите значение `205.13.237.6` в списке **IP-адрес**.

f. Отмените выбор опции **Запуск по запросу**.

g. Перейдите на страницу **Локальные адреса**. Выберите в качестве типа идентификатора значение **Идентификатор ключа**, а затем выберите значение `thisisthekeyid` в списке **Идентификатор**.

h. Перейдите на страницу **Удаленные адреса**. Выберите в качестве типа идентификатора значение **IP-адрес версии 4**.

i. Введите значение `205.13.237.6` в поле **Идентификатор**.

j. Перейдите на страницу **Службы**. Введите значение `1701` в полях **Локальный порт** и **Удаленный порт**. Порт 1701 применяется протоколом L2TP.

k. В списке **Протокол** выберите значение **UDP**.

l. Нажмите кнопку **OK** для сохранения свойств соединения с динамическим ключом.

Настройка VPN в системе iSeries-A завершена. Перейдите к процедуре настройки профайла PPP в системе iSeries-A.

Шаг 2: Настройте профайл соединения PPP и виртуальную линию в системе iSeries-A

В этом разделе описаны действия, которые необходимо выполнить для создания профайла PPP в системе iSeries-A. С профайлом PPP связана не физическая, а виртуальная линия связи. Это вызвано тем, что данные PPP передаются по туннелю L2TP, для защиты которого применяется VPN.

Для создания профайла соединения PPP в системе iSeries-A выполните следующие действия:

1. В окне программы Навигатор разверните iSeries-A **—>Сеть—>Службы удаленного доступа**.
2. Щелкните правой кнопкой мыши на пункте **Профайлы исходящих соединений** и выберите опцию **Создать профайл**.
3. На странице **Настройка** выберите в качестве типа протокола значение **PPP**.
4. В поле Режим укажите **L2TP (виртуальная линия)**.
5. В списке **Режим работы** выберите значение **Инициатор по запросу (необязательный туннель)**.
6. Нажмите кнопку **OK** для перехода к странице свойств профайлов PPP.
7. На странице **Общие** укажите имя соединения, характеризующее его тип и целевую систему. В данном случае введите значение `toCORP`. Длина имени не должна превышать 10 символов.
8. (необязательно) Укажите описание профайла.
9. Перейдите на страницу **Соединение**.
10. В поле **Имя виртуальной линии** выберите значение **tocorp**. С этой линией не связан физический интерфейс. Виртуальная линия задает некоторые свойства профайла PPP, например, максимальный размер кадра, идентификационную информацию, имя локального хоста и т.д. Появится окно диалога **Свойства линии L2TP**.
11. На странице **Общие** введите описание виртуальной линии.
12. Перейдите на страницу **Идентификация**.
13. В поле **Имя локального хоста** укажите имя хоста локального сервера ключей, `iSeriesA`.
14. Нажмите кнопку **OK** для сохранения описания виртуальной линии и возврата на страницу **Соединения**.
15. Введите в поле **Адрес удаленной конечной точки туннеля** адрес `205.13.237.6`.
16. Выберите опцию **Необходима защита IPSec**. В списке **Имя группы соединений** выберите группу соединений с динамическим ключом, созданную на шаге 1, `l2tptocorp`.
17. Перейдите на страницу **Параметры TCP/IP**.
18. В разделе **Локальный IP-адрес** выберите значение **Назначается удаленной системой**.
19. В разделе **Удаленный IP-адрес** выберите значение **Применять фиксированный IP-адрес**. Введите IP-адрес, который назначен удаленной системе в ее подсети: `10.6.11.1`.
20. В разделе параметров маршрутизации выберите опцию **Определить дополнительные статические маршруты** и нажмите кнопку **Маршруты**. Если в профайле PPP не будет задана информация о маршрутизации, то система iSeries-A сможет подключаться к удаленной конечной точке туннеля, но не сможет подключаться другим системам из подсети 10.6.0.0.
21. Нажмите кнопку **Добавить**, чтобы добавить статический маршрут.
22. Введите адрес подсети `10.6.0.0` и маску подсети `255.255.0.0`. В результате все данные, предназначенные для систем с адресами 10.6.*.*, будут передаваться по туннелю L2TP.
23. Нажмите кнопку **OK** для сохранения статического маршрута.
24. Нажмите кнопку **OK**, чтобы закрыть окно Маршрутизация.
25. Перейдите на страницу **Идентификация** и задайте имя и пароль пользователя для профайла PPP.
26. В разделе Идентификация локальной системы выберите опцию **Разрешить удаленной системе идентифицировать данную систему**.
27. В поле **Протокол идентификации** выберите значение **Применять зашифрованный пароль (CHAP-MD5)**.
28. Введите имя пользователя, `iSeriesA`, и пароль.
29. Нажмите кнопку **OK** для сохранения профайла PPP.

Шаг 3: Свяжите группу соединений l2tptocorp с профайлом PPP toCorp

После настройки профайла соединения PPP необходимо вернуться к свойствам созданной группы соединений l2tptocorp и задать для нее новый профайл PPP. Для этого выполните следующие действия:

1. В интерфейсе VPN разверните **Защищенные соединения—>По группам**.
2. Щелкните правой кнопкой мыши на имени группы соединений с динамическим ключом (l2tptocorp) и выберите пункт **Свойства**.
3. Перейдите на страницу **Интерфейсы** и выберите опцию **Использовать эту группу** для профайла PPP, созданного на шаге 2 (toCorp).
4. Нажмите кнопку **OK**, чтобы связать группу l2tptocorp с профайлом PPP toCorp.

Шаг 4: Настройте VPN в системе iSeries-B

Выполните ту же процедуру настройки, что и в системе iSeries-A. Поменяйте местами адреса и идентификаторы там, где это необходимо. Во время настройки следуйте следующим рекомендациям:

- В качестве идентификатора удаленного сервера ключей нужно задать идентификатор ключа, указанный для локального сервера ключей в системе iSeries-A. В данном примере он равен thisisthekeyid.
- Укажите *точно такой же* подготовленный ключ.
- Параметры указанных преобразований должны совпадать с параметрами, заданными в системе iSeries-A. В противном случае соединение не будет установлено.
- Не выбирайте опцию **Защищает локально созданный туннель L2TP** на странице **Общие** окна свойств группы соединений с динамическим ключом.
- Укажите, что инициатором соединения является удаленная система.
- Укажите, что соединение должно запускаться по запросу.

Шаг 5: Настройте профайл соединения PPP и виртуальную линию в системе iSeries-B

Для создания профайла соединения PPP в системе iSeries-B выполните следующие действия:

1. В окне программы Навигатор разверните iSeries-B **—>Сеть—> Службы удаленного доступа**.
2. Щелкните правой кнопкой мыши на пункте **Профайлы входящих соединений** и выберите опцию **Создать профайл**.
3. На странице **Настройка** выберите в качестве типа протокола значение **PPP**.
4. В поле Режим укажите **L2TP (виртуальная линия)**.
5. В списке **Режим работы** выберите значение **Конечная система (сетевой сервер)**.
6. Нажмите кнопку **OK** на странице свойств профайлов PPP.
7. На странице **Общие** укажите имя соединения, характеризующее его тип и целевую систему. В данном случае необходимо ввести значение tobranch. Длина имени не должна превышать 10 символов.
8. (необязательно) Укажите описание профайла.
9. Перейдите на страницу **Соединение**.
10. Выберите IP-адрес локальной конечной точки туннеля, 205.13.237.6.
11. В поле **Имя виртуальной линии** выберите значение **tobranch**. С этой линией не связан физический интерфейс. Виртуальная линия задает некоторые свойства профайла PPP, например, максимальный размер кадра, идентификационную информацию, имя локального хоста и т.д. Появится окно диалога **Свойства линии L2TP**.
12. На странице **Общие** введите описание виртуальной линии.
13. Перейдите на страницу **Идентификация**.
14. В поле **Имя локального хоста** укажите имя хоста локального сервера ключей, iSeriesB.
15. Нажмите кнопку **OK** для сохранения описания виртуальной линии и возврата на страницу **Соединения**.
16. Перейдите на страницу **Параметры TCP/IP**.
17. В разделе **Локальный IP-адрес** выберите фиксированный IP-адрес локальной системы, 10.6.11.1.

18. В разделе **Удаленный IP-адрес** выберите способ назначения адресов **Пул адресов**. Введите начальный адрес и укажите число адресов в пуле, из которого будет присваиваться адрес удаленной системе.
19. Выберите опцию **Разрешить удаленной системе доступ в другие сети (пересылка пакетов IP)**.
20. Перейдите на страницу **Идентификация** и задайте имя и пароль пользователя для профайла PPP.
21. В разделе Идентификация локальной системы выберите опцию **Разрешить удаленной системе идентифицировать данную систему**. Появится окно диалога **Идентификация локальной системы**.
22. В поле **Протокол идентификации** выберите значение **Применять зашифрованный пароль (CHAP-MD5)**.
23. Введите имя пользователя, `iSeriesB`, и пароль.
24. Нажмите кнопку **OK** для сохранения профайла PPP.

Шаг 6: Активируйте правила обработки пакетов

Функция VPN автоматически создает правила обработки пакетов, необходимые для правильной работы соединения. Перед запуском соединения VPN эти правила необходимо активировать в обеих системах. Для того чтобы активировать правила в системе iSeries-A, выполните следующие действия:

1. В Навигаторе разверните **iSeries-A —> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Правила обработки пакетов** и выберите опцию **Активировать**. Появится окно **Активировать правила обработки пакетов**.
3. Укажите, какие правила должны быть активированы: правила, созданные VPN, выбранный файл правил или и то, и другое. Последнюю опцию, например, можно выбрать в том случае, если помимо правил, созданных VPN, для интерфейса должны быть активированы некоторые правила PERMIT и DENY.
4. Выберите интерфейс, для которого должны быть активированы правила. В данном случае нужно выбрать опцию **Все интерфейсы**.
5. Нажмите кнопку **OK**, для того чтобы подтвердить, что нужно проверить и активировать правила для указанных интерфейсов. Система проверит правила на наличие синтаксических и семантических ошибок. Результаты проверки будут показаны в окне сообщений, расположенном в нижней области окна редактора. При наличии сообщения об ошибке щелкните правой кнопкой мыши на этом сообщении и выберите пункт **Перейти к строке**, чтобы была выделена строка файла правил, в которой была найдена ошибка.
6. Повторите описанную процедуру активации правил в системе iSeries-B.

Шаг 7: Запустите соединение

После завершения настройки необходимо запустить соединение. Перед запуском соединения L2TP необходимо настроить конечную систему L2TP таким образом, чтобы она отвечала на запросы инициатора. Убедитесь, что запущены все необходимые службы, а затем запустите соединение PPP в конечной системе. Ниже перечислены действия, которые необходимо выполнить для запуска соединения PPP в системе iSeries-B:

1. В окне программы Навигатор разверните iSeries-B **—> Сеть—> Службы удаленного доступа**.
2. Выберите опцию **Профайлы входящих соединений**. На правой панели появится список профайлов входящих соединений.
3. Щелкните правой кнопкой мыши на записи `tobranch` и выберите пункт **Запустить**. После запуска профайла соединения и обновления содержимого окна будет указано, что соединение находится в состоянии `Ожидание запроса на подключение`. Теперь система iSeries-A может отвечать на запросы об установлении соединения L2TP, отправленные системой iSeries-B.

Для запуска соединения L2TP в системе iSeries-A выполните следующие действия:

1. В окне программы Навигатор разверните iSeries-A **—> Сеть—> Службы удаленного доступа**.
2. Выберите опцию **Профайлы исходящих соединений**. На правой панели появится список профайлов исходящих соединений.
3. Щелкните правой кнопкой мыши на записи **toCORP** и выберите пункт **Запустить**. После запуска профайла соединения и обновления содержимого окна будет указано, что соединение находится в состоянии `Установление туннеля L2TP`.

4. Для обновления содержимого окна нажмите F5. Если туннель L2TP был установлен, то соединение будет находиться в состоянии Активное соединение.

Сценарий применения VPN: Применение преобразования сетевых адресов в VPN

Предположим, что вы являетесь администратором сети небольшой производственной фирмы, расположенной в Миннеаполисе. Один из ваших поставщиков, офис которого находится в Чикаго, предложил обмениваться деловой информацией по сети Internet. Для того чтобы вовремя доставлять необходимое количество комплектующих, поставщику необходимо знать, сколько комплектующих у вас осталось, и сколько комплектующих потребуется в ближайшее время. В настоящее время для получения такой информации поставщику требуется специально обращаться в вашу фирму, что занимает много времени и требует дополнительных затрат. Иногда полученная информация бывает неточной.

Учитывая то, что передаваемая информация носит конфиденциальный характер и требует срочной доставки, было решено создать соединение VPN между сетью поставщика и сетью вашей фирмы. Для защиты сети своей фирмы вы приняли решение скрыть внутренний IP-адрес сервера iSeries(TM), на котором запущены приложения, необходимые поставщику. Вам необходимо решить, какие средства позволяют создать такое соединение.

Таким средством является функция VPN OS/400(R). С ее помощью можно не только создать определение соединения на шлюзе VPN в сети фирмы, но и обеспечить преобразование адресов, необходимое для сокрытия локальных адресов. Обычная функция преобразования сетевых адресов (NAT) изменяет IP-адреса, указанные в конфигурациях защиты (SA), что приводит к ошибкам в работе VPN. В отличие от нее, функция VPN NAT преобразует адрес перед проверкой SA путем назначения адреса при запуске соединения.

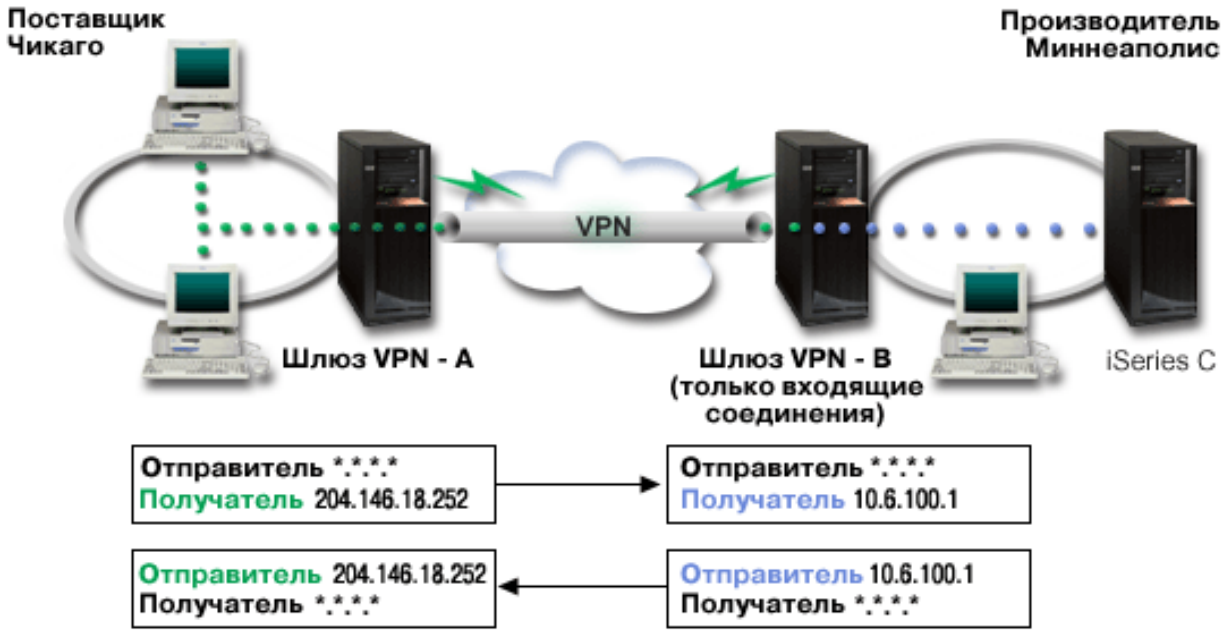
Цели

В этом сценарии преследуются следующие цели:

- предоставить всем клиентам сети поставщика доступ к системе iSeries в сети производственной фирмы по соединению VPN, установленному между шлюзами.
- скрыть внутренний IP-адрес системы iSeries из сети производственной фирмы путем его преобразования во внешний IP-адрес с помощью функции VPN NAT.

Описание

На приведенном ниже рисунке показана схема сети фирмы-поставщика и фирмы-производителя:



- Шлюз A всегда выступает инициатором соединения со шлюзом B.
- В качестве удаленной конечной точки соединения на шлюзе A задан адрес 204.146.18.252 (внешний адрес системы iSeries-C).
- В сети производителя системе iSeries-C присвоен внутренний IP-адрес 10.6.100.1.
- В пуле адресов локальных служб на шлюзе B внешнему адресу 204.146.18.252 соответствует внутренний адрес системы iSeries-C, 10.6.100.1.
- При получении дейтаграмм шлюз B преобразует внешний адрес системы iSeries-C в ее внутренний адрес, 10.6.100.1. При отправке дейтаграмм шлюз B преобразует адрес 10.6.100.1 во внешний адрес системы iSeries-C, 204.146.18.252. С точки зрения клиентов сети поставщика, IP-адрес системы iSeries-C равен 204.146.18.252. Им ничего не известно о выполняющемся преобразовании адресов.

Задачи настройки

Для настройки соединения, описанного в этом сценарии, выполните следующие задачи:

1. Настройте обычное соединение VPN между **шлюзом A** и **шлюзом B**.
2. Укажите в пуле адресов локальных служб **шлюза B**, что внутренний адрес системы **iSeries-C** необходимо скрыть за внешним адресом 204.146.18.252.
3. Настройте на **шлюзе B** преобразование локальных адресов с применением пула адресов локальных служб.

Принципы работы VPN

Виртуальная частная сеть (VPN) применяет несколько основных протоколов TCP/IP для защиты данных. Для того чтобы понять, как работает соединение VPN, необходимо ознакомиться с описанием этих протоколов и информацией об их применении в VPN OS/400(R):

- “Протоколы защиты IP (IPSec)” на стр. 23
  Протокол IPSec - это основа для защиты различных сетевых протоколов.
- “Управление ключами” на стр. 26
  Динамическое соединение VPN обеспечивает более высокий уровень защиты, так как для управления ключами в этом соединении применяется протокол IKE. Этот протокол позволяет серверам VPN, между которыми установлено соединение, согласовывать новые ключи через заданные интервалы времени.

- “Протокол L2TP” на стр. 27
  Если соединение VPN будет установлено между локальной сетью и удаленными клиентами, ознакомьтесь с описанием протокола L2TP.
- “Преобразование сетевых адресов в VPN” на стр. 28
  В VPN OS/400 предусмотрена функция преобразования сетевых адресов, которая называется VPN NAT. Эта функция отличается от обычного NAT тем, что она преобразует адреса до применения протоколов IKE и IPSec. Для получения дополнительной информации ознакомьтесь с этим разделом.
- “IPSec с поддержкой NAT” на стр. 29
  Функция инкапсуляции UDP позволяет передавать данные IPSec через обычные устройства NAT. Для получения дополнительной информации об этой функции и ее применении при работе с соединениями VPN ознакомьтесь с этим разделом.
- “Сжатие пакетов IP (IPComp)” на стр. 30
  Протокол IPComp уменьшает размер дейтаграмм IP путем их сжатия. Это позволяет повысить скорость передачи данных по соединению.
- “VPN и фильтрация пакетов IP” на стр. 31
  Функция фильтрации пакетов IP тесно связана с функцией VPN. Для работы большинства соединений VPN требуется правильно настроить правила фильтрации. В этом разделе приведена информация о необходимых правилах фильтрации и прочие сведения о применении фильтрации в VPN.

Протоколы защиты IP (IPSec)

Протокол IPSec - это основа для защиты различных сетевых протоколов. Этот протокол поддерживает все современные алгоритмы шифрования и допускает добавление новых. Протокол IPSec предназначен для решения следующих задач защиты:

Идентификация источника данных
Гарантирует, что дейтаграмма была отправлена ожидаемым отправителем.

Целостность данных
Гарантирует, что дейтаграмма не была изменена при передаче, случайно или намеренно.

Конфиденциальность передачи данных
Скрывает содержимое сообщения посредством шифрования.

Защита от воспроизведения информации
Гарантирует, что дейтаграмму нельзя перехватить и отправить через некоторое время.

Автоматическое управление ключами шифрования и конфигурациями защиты
Позволяет создать стратегию VPN для крупной сети автоматически или с минимальным объемом настройки вручную.

VPN применяет два протокола IPSec для защиты передаваемых данных: AH и ESP. Другая часть протокола IPSec, протокол IKE, обеспечивает управление ключами. Протокол IKE поддерживает автоматическое согласование конфигураций защиты (SA), а также автоматическое создание и обновление ключей шифрования.

Ниже описаны основные протоколы IPSec:

- “Протокол AH” на стр. 24
- “Протокол ESP” на стр. 25
- “Совместное применение AH и ESP” на стр. 26
- “Управление ключами” на стр. 26

Формальное описание протокола IPSec, созданное Рабочей группой Internet (IETF), содержится в документе RFC 2401, *Security Architecture for the Internet Protocol*. Этот документ RFC можно найти в Internet на следующем Web-сайте: http://www.rfc-editor.org  .

Протокол AH

Протокол Authentication Header (AH) позволяет идентифицировать отправителя данных, а также обеспечивает целостность данных и защиту от воспроизведения информации. Однако AH не гарантирует конфиденциальность данных, то есть все данные передаются по соединению открыто.

Целостность данных проверяется в протоколе AH с помощью контрольной суммы, созданный алгоритмом идентификации сообщения, например, MD5. Для идентификации отправителя данных протокол AH добавляет в алгоритм общий ключ. Для защиты от воспроизведения информации протокол AH указывает порядковый номер в поле заголовка AH. Часто все три функции смешиваются вместе и называются **идентификацией**. Проще говоря, протокол AH позволяет убедиться, что данные не были изменены во время их передачи получателю.

Хотя протокол AH позволяет идентифицировать большую часть дейтаграммы IP, значения некоторых полей заголовка IP получатель проверить не может. AH не защищает **изменяемые** поля дейтаграммы. Однако протокол AH всегда защищает поле данных пакета IP.

Рабочая группа Internet (IETF) формально определила протокол AH в документе RFC 2402, *IP Authentication Header*. Этот документ RFC можно найти в Internet на следующем Web-сайте: http://www.rfc-editor.org .

Способы применения протокола AH

Протокол AH может применяться двумя способами: в режиме открытой передачи и в режиме туннеля. В режиме открытой передачи самым внешним заголовком дейтаграммы является заголовок IP, за которым расположен заголовок AH, а затем - поле данных дейтаграммы. Протокол AH защищает всю дейтаграмму, за исключением изменяемых полей. Однако вся информация, содержащаяся в дейтаграмме, передается открыто, поэтому она может быть перехвачена. Для обмена данными в режиме открытой передачи требуется меньше ресурсов, чем при работе в режиме туннеля. Однако такой режим обеспечивает более низкий уровень защиты.

В режиме туннеля создается новый заголовок IP, который становится самым внешним заголовком дейтаграммы. Заголовок AH помещается после нового заголовка IP. Затем размещается сама дейтаграмма (заголовок IP и данные). В этом случае протокол AH позволяет идентифицировать всю дейтаграмму. Это означает, что получатель может определить, была ли изменена дейтаграмма во время передачи.

Если в конфигурации защиты одной из конечных систем является шлюз, рекомендуется использовать режим туннеля. В этом режиме адреса отправителя и получателя, указанные во внешнем заголовке IP, не обязательно должны совпадать с адресами, указанными в исходном заголовке IP. Например, туннель AH можно установить между двумя защищенными шлюзами, для того чтобы они могли идентифицировать все данные, передаваемые между двумя сетями. Такая конфигурация применяется очень часто.

Основное преимущество режима туннеля состоит в том, что в нем обеспечивается защита инкапсулированной дейтаграммы IP. Кроме того, при работе в режиме туннеля можно применять внутренние адреса.

Достоинства протокола AH

Во многих случаях требуется только идентификация данных. В отличие от протокола “Протокол ESP” на стр. 25, который также может применяться для идентификации данных, протокол AH не влияет на производительность системы. Кроме того, протокол AH позволяет идентифицировать всю дейтаграмму. Протокол ESP не защищает внешний заголовок IP и любую другую информацию, указанную перед заголовком ESP.

Кроме этого, для применения протокола ESP требуются надежные алгоритмы шифрования. В некоторых странах применение таких алгоритмов запрещено, тогда как протокол AH может свободно применяться во всем мире.

Алгоритмы защиты информации, применяемые в протоколе AH
В протоколе AH применяются алгоритмы, которые называются **HMAC (хэшированные коды идентификации сообщений)**. В частности, в VPN применяются алгоритмы HMAC-MD5 и HMAC-SHA. Оба алгоритма получают на входе данные переменной длины и личный ключ, а на их основе создают данные фиксированной длины (или значение хэш-функции). Если значения хэш-функции, вычисленные для двух сообщений, совпадают, то с высокой вероятностью эти сообщения одинаковые. Алгоритм SHA считается более надежным, поскольку создает более длинное значение хэширования.

Формальное описание алгоритма HMAC-MD5, созданное Рабочей группой Internet (IETF), находится в документе RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. Формальное описание алгоритма HMAC-SHA, созданное Рабочей группой Internet (IETF), находится в документе RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Эти документы можно найти в Internet на следующем Web-сайте:

http://www.rfc-editor.org .

Протокол ESP
Протокол Encapsulating Security Payload (ESP) обеспечивает конфиденциальность данных. Кроме того, он позволяет идентифицировать отправителя данных, а также обеспечить целостность данных и защиту от воспроизведения информации. Отличие протокола ESP от протокола “Протокол AH” на стр. 24 состоит в том, что ESP выполняет шифрование данных. При этом оба протокола обеспечивают идентификацию, проверку целостности и защиту от воспроизведения информации. При работе с ESP для шифрования и расшифровки данных обе конечные системы применяют общий ключ.

Если одновременно применяются средства шифрования и идентификации данных, то отвечающая система вначале идентифицирует пакет, а если идентификация выполнена успешно, то расшифровывает пакет. Такой способ обработки пакетов снижает нагрузку на систему и уменьшает риск взлома защиты с помощью атаки типа ″отказ в обслуживании″.

Два способа применения ESP
Протокол ESP может применяться двумя способами: в режиме открытой передачи и в режиме туннеля. В режиме открытой передачи заголовок ESP указывается после заголовка IP дейтаграммы. Если у дейтаграммы уже есть заголовок IPSec, то заголовок ESP помещается перед этим заголовком. Концевик ESP и идентификационные данные, если они есть, указываются после поля данных.

В режиме открытой передачи заголовок IP не идентифицируется и не зашифровывается. В этом случае адреса, указанные в заголовке, могут быть перехвачены во время передачи дейтаграммы по сети. Для обмена данными в режиме открытой передачи требуется меньше ресурсов, чем при работе в режиме туннеля. Однако такой режим обеспечивает более низкий уровень защиты. В большинстве случаев при работе с протоколом ESP применяется режим открытой передачи.

В режиме туннеля создается новый заголовок IP, который становится самым внешним заголовком дейтаграммы. После него помещается заголовок ESP, а затем - сама дейтаграмма (заголовок IP и данные). Концевик ESP и идентификационные данные, если они есть, добавляются в конец поля данных. Если одновременно применяются средства шифрования и идентификации, то ESP полностью защищает исходную дейтаграмму, так как эта дейтаграмма становится полем данных в новом пакете ESP. Новый заголовок IP не защищается. При установлении соединения между шлюзами следует применять ESP в режиме туннеля.

Алгоритмы защиты информации, применяемые в протоколе ESP
В протоколе ESP применяется симметричный ключ, с помощью которого данные зашифровываются и расшифровываются конечными системами. Перед обменом данными отправитель и получатель должны согласовать ключ, который они будут применять. Функция VPN операционной системы OS/400(R) поддерживает способы шифрования DES, тройной DES (3DES), RC5, RC4 и AES.

Формальное описание алгоритма DES, созданное Рабочей группой Internet (IETF), находится в документе RFC 1829, *The ESP DES-CBC Transform*. Формальное описание алгоритма 3DES, созданное Рабочей группой

Internet (IETF), находится в документе RFC 1851, *The ESP Triple DES Transform*. Эти и другие документы RFC можно найти в Internet на следующем Web-сайте: http://www.rfc-editor.org .

Протокол ESP поддерживает алгоритмы идентификации HMAC-MD5 и HMAC-SHA. Оба алгоритма получают на входе данные переменной длины и личный ключ, а на их основе создают данные фиксированной длины (или значение хэш-функции). Если значения хэш-функции, вычисленные для двух сообщений, совпадают, то с высокой вероятностью эти сообщения одинаковые. Алгоритм SHA считается более надежным, поскольку создает более длинное значение хэширования.

Формальное описание алгоритма HMAC-MD5, созданное Рабочей группой Internet (IETF), находится в документе RFC 2085, *HMAC-MD5 IP Authentication with Replay Prevention*. Формальное описание алгоритма HMAC-SHA, созданное Рабочей группой Internet (IETF), находится в документе RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*. Эти и другие документы RFC можно найти в Internet на следующем Web-сайте: http://www.rfc-editor.org .

Совместное применение AH и ESP

Для защиты соединений, установленных между хостами и работающих в режиме открытой передачи, VPN позволяет применять протокол AH в сочетании с протоколом ESP. Применение обоих протоколов дает возможность защитить всю дейтаграмму IP. Это обеспечивает более высокую степень защиты, но требует значительно больше ресурсов системы.

Управление ключами

Если процедура согласования выполнена успешно, серверы VPN заново создают ключи, применяемые для защиты соединения. Это уменьшает вероятность того, что кто-либо сможет получить конфиденциальную информацию во время ее передачи по соединению. Если при пересылке информации обеспечивается ее секретность, то на основе передаваемых данных невозможно угадать новые ключи.

Диспетчер ключей VPN - это реализация протокола Internet Key Exchange (IKE), созданная фирмой IBM(TM). Диспетчер ключей поддерживает автоматическое согласование конфигураций защиты (SA), а также автоматическое создание и обновление ключей шифрования.

Конфигурация защиты (SA) содержит информацию, необходимую для работы протокола IPSec. В частности, SA задает алгоритмы, размер и срок действия ключей, конечные системы и режим передачи данных.

Ключи шифрования служат для защиты информации во время ее передачи целевой системе.

Примечание: Секретность ключей - это основное требование, которое необходимо соблюдать при установлении защищенного соединения. Если ключи станут известны другим пользователям, то будет бесполезно применять какие-либо способы идентификации и шифрования.

Этапы управления ключами

Работа диспетчера ключей VPN делится на два этапа.

Первый этап

На первом этапе создается основной секретный ключ, на основе которого вычисляются все последующие ключи шифрования, применяемые для защиты пользовательских данных. Этот этап не зависит от наличия защищенного соединения. Для идентификации и выбора ключей, предназначенных для защиты сообщений IKE на втором этапе согласования, на первом этапе согласования функция VPN применяет подпись RSA или подготовленный ключ.

Подготовленный ключ - это неочевидная строка (пароль) длиной до 128 символов ASCII. На обоих концах соединения должен быть задан один и тот же подготовленный ключ. Преимущество применения подготовленного ключа - простота, недостаток - необходимость предварительной

передачи ключа по надежному каналу связи, например, по телефону или по почте (не по сети). Подготовленный ключ можно считать разновидностью пароля.

Идентификация с помощью *подписи RSA* считается более надежным способом идентификации, так как в этом случае применяются цифровые сертификаты. Цифровые сертификаты можно настроить с помощью Диспетчера цифровых сертификатов (5722-SS1, компонент 34). Кроме того, в некоторых системах VPN подпись RSA обязательна для взаимодействия между системами. Например, в VPN Windows(R) 2000 по умолчанию применяется подпись RSA. Наконец, подписи RSA обеспечивают большую масштабируемость, чем подготовленные ключи. Оба сервера ключей должны доверять сертификатной компании, выдавшей применяемый сертификат.

Второй этап
На втором этапе согласуются конфигурации защиты и ключи, которые будут применяться для защиты данных приложения. До этого момента данные приложения не передавались по сети. Первый этап необходим для защиты сообщений, передаваемых на втором этапе.

После завершения второго этапа согласования VPN устанавливает защищенное сетевое соединение между указанными конечными точками. При передаче данных по соединению VPN обеспечивается их защита. Уровень защиты выбирается относительно уровня производительности на первом и втором этапах согласования.

Обычно первый этап согласования выполняется раз в день, а второй этап согласования выполняется каждые 60 - 5 минут. Чем чаще обновляются параметры защиты, тем выше уровень защиты данных, но ниже производительность системы. Для защиты наиболее важных данных установите минимальный срок действия ключа.

При создании динамического соединения VPN с помощью программы Навигатор iSeries(TM) требуется “Настройка стратегии Internet Key Exchange (IKE)” на стр. 41, применяемую на первом этапе согласования, а также “Настройка стратегии защиты данных” на стр. 41, применяемую на втором этапе согласования. При необходимости воспользуйтесь мастером Создать соединение. Этот мастер автоматически создает все необходимые объекты конфигурации VPN, в том числе стратегию IKE и стратегию защиты данных.

Рекомендуемая информация
Для получения дополнительной информации о протоколе Internet Key Exchange (IKE) и управлении ключами ознакомьтесь со следующими документами RFC, созданными Рабочей группой Internet (IETF):

- RFC 2407, *The Internet IP Security Domain of Interpretation for ISAKMP*
- RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*
- RFC 2409, *The Internet Key Exchange (IKE)*

Эти документы можно найти в Internet на следующем Web-сайте: http://www.rfc-editor.org  .

Протокол L2TP

Соединения L2TP, которые иногда называются виртуальными линиями, - это сравнительно недорогой способ подключения удаленных пользователей, при котором IP-адресами удаленных пользователей управляет корпоративный сервер, подключенный к сети. С помощью средств защиты IP (IPSec) можно обеспечить защиту данных, передаваемых по соединениям L2TP.

Протокол L2TP поддерживает туннели двух типов: обязательные и необязательные. Основное различие между этими туннелями состоит в том, какая система играет роль конечной точки туннеля. Конечной точкой необязательного туннеля является удаленный клиент, а конечной точкой обязательного туннеля - ISP.

В случае **обязательного туннеля** L2TP удаленный хост устанавливает соединение со своим провайдером Internet (ISP). После этого ISP устанавливает соединение L2TP между удаленным пользователем и

корпоративной сетью. При этом пользователь может самостоятельно выбрать необходимые средства защиты данных, предоставляемые функцией VPN. Для применения обязательного туннеля провайдер Internet должен поддерживать протокол LT2P.

В случае **необязательного туннеля** L2TP соединение устанавливается удаленным пользователем. Обычно для этого применяется клиент туннелей L2TP. Удаленный пользователь отправляет пакеты L2TP своему ISP, который пересылает их в корпоративную сеть. Для применения необязательного туннеля не требуется, чтобы провайдер Internet поддерживал протокол L2TP. В сценарии *"Сценарий применения VPN: Защита необязательного туннеля L2TP с помощью IPSec" на стр. 14* приведен пример настройки соединения между сервером iSeries, принадлежащим филиалу фирмы, и корпоративной сетью. Соединение устанавливается через шлюз iSeries(TM) и туннель L2TP, защищенный с помощью VPN.

» Вы можете просмотреть наглядную презентацию Туннели L2TP, защищенные с помощью IPSec. Для этого необходим встраиваемый модуль Flash  . Вы также можете просмотреть эту презентацию в формате HTML. «

Протокол L2TP является версией протокола инкапсуляции IP. При передаче данных по туннелю L2TP кадр L2TP помещается в пакет UDP, который, в свою очередь, помещается в пакет IP. В качестве адресов отправителя и получателя этого пакета указываются конечные точки соединения. Для защиты составного пакета IP могут применяться протоколы IPSec. С их помощью можно обеспечить защиту данных, передаваемых по туннелю L2TP. При работе с таким соединением можно напрямую применять протоколы AH, ESP и IKE.

Пример применения протокола L2TP при подключении к IBM(R) через Universal Connection приведен в разделе Сценарий: настройка удаленного коммутируемого соединения PPP.

Преобразование сетевых адресов в VPN

Функция преобразования сетевых адресов (NAT) служит для преобразования внутренних IP-адресов во внешние IP-адреса. Она позволяет предоставить хостам внутренней сети доступ к службам и удаленным хостам, расположенным в сети Internet (или другой внешней сети), используя небольшое количество внешних IP-адресов.

Применение внутренних IP-адресов за пределами локальной сети может привести к конфликтам, так как такие же адреса могут быть присвоены компьютерам другой сети. Например, если в обеих сетях применяются адреса вида 10.*.*.*, то все пакеты, передаваемые между хостами этих сетей, будут удаляться. Такую ошибку можно исправить путем применения NAT к адресам отправляемых пакетов. Однако при передаче данных по защищенному соединению VPN обычную функцию NAT применять нельзя, так как она изменяет IP-адреса, заданные в конфигурациях защиты (SA), что приводит к ошибкам в работе VPN. Специально для VPN была разработана особая версия функции преобразования сетевых адресов, которая называется VPN NAT. Эта функция преобразует адреса перед проверкой SA, назначая адрес при запуске соединения. Этот адрес будет связан с соединением до тех пор, пока оно не будет удалено.

Примечание: В данный момент FTP не поддерживает функцию VPN NAT.

Применение функции VPN NAT
Существует две разновидности функции VPN NAT. Это:

VPN NAT для устранения конфликтов между IP-адресами
Эта разновидность функции VPN NAT позволяет избежать конфликтов при настройке соединения VPN между сетями или системами, в которых применяются похожие схемы адресации. Обычно она используется в том случае, когда соединение VPN устанавливается между подсетями с одинаковыми диапазонами внутренних IP-адресов. Например, 10.*.*.*. Способ настройки такой функции VPN NAT зависит от того, какую роль играет сервер по отношению к соединению VPN: роль инициатора или роль отвечающей стороны. Если сервер является инициатором соединения VPN, вы можете преобразовать локальные адреса в адреса, не совпадающие с адресами удаленной подсети. Если сервер

выступает в роли отвечающей стороны, вы можете преобразовать адреса удаленной подсети в адреса, не совпадающие с локальными адресами. Такой способ преобразования адресов может применяться только при работе с динамическими соединениями.

VPN NAT для сокрытия локальных адресов
Эта разновидность функции VPN NAT применяется для того, чтобы скрыть IP-адрес локальной системы путем его преобразования во внешний адрес, который будет известен другим системам. При настройке VPN NAT можно указать, что внешний IP-адрес должен преобразовываться в один из скрытых адресов из заданного пула адресов. За счет этого можно распределить нагрузку между несколькими системами. VPN NAT можно применять для локальных адресов лишь в том случае, если при установлении соединения сервер играет роль отвечающей стороны.

Настройте функцию VPN NAT для сокрытия локальных адресов, если вы дадите положительный ответ на все приведенные ниже вопросы:

1. Вы хотите предоставить пользователям доступ к одному или нескольким серверам по соединениям VPN?
2. Часто ли изменяются фактические IP-адреса локальных систем?
3. Есть ли у вас хотя бы один внешний IP-адрес?

В сценарии *"Сценарий применения VPN: Применение преобразования сетевых адресов в VPN" на стр. 21* приведен пример настройки VPN NAT для сокрытия локальных адресов системы iSeries(TM).

Пошаговые инструкции по настройке функции VPN NAT в системе iSeries можно найти в электронной справке по интерфейсу VPN, предусмотренному в программе Навигатор.

IPSec с поддержкой NAT

Проблема: Обычная функция NAT не совместима с VPN

Функция преобразования сетевых адресов (NAT) позволяет скрыть незарегистрированные частные IP-адреса за набором зарегистрированных IP-адресов. Это дает возможность защитить внутреннюю сеть от внешних хостов. Кроме того, применение NAT частично решает проблему нехватки IP-адресов, поскольку для представления большого количества частных адресов применяется небольшой набор зарегистрированных адресов.

Обычная функция NAT не подходит для обработки пакетов IPSec, так как при прохождении пакета через устройство NAT в нем изменяется адрес отправителя, в результате чего пакет становится недостоверным. Система-получатель, с которой установлено соединение VPN, отклоняет такой пакет, в результате чего не удается согласовать параметры соединения VPN.

Решение: функция инкапсуляции UDP
В двух словах, функция инкапсуляции UDP добавляет к пакету IPSec еще одну копию заголовка IP/UDP. Во время прохождения такого пакета через устройство NAT преобразуется адрес в новом заголовке IP. При получении этого пакета система, с которой установлено соединение VPN, удаляет лишний заголовок, получая в итоге исходный пакет IPSec. Все процедуры проверки выполняются по отношению к этому исходному пакету.

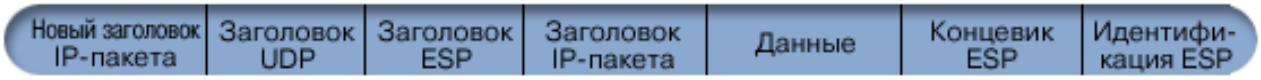
Функция инкапсуляции UDP может применяться только с теми соединениями VPN, для которых включена опция применения протокола ESP в режиме открытой передачи или в режиме туннеля. Кроме того, в выпуске V5R2 система iSeries(TM) по отношению к функции инкапсуляции UDP может играть только роль клиента. Другими словами, она может только *инициировать* передачу инкапсулированных пакетов UDP.

На приведенном ниже рисунке показан формат пакета ESP, инкапсулированного в дейтаграмму UDP, в режиме туннеля:

Исходная дейтаграмма IPv4:

После применения протокола ESP в режиме туннеля:

После применения функции инкапсуляции UDP:



На приведенном ниже рисунке показан формат пакета ESP, инкапсулированного в дейтаграмму UDP, в режиме открытой передачи:

Исходная дейтаграмма IPv4:

После применения протокола ESP в режиме открытой передачи:

После применения функции инкапсуляции UDP:

» После инкапсуляции пакета в дейтаграмму UDP система iSeries отправляет дейтаграмму системе, расположенной на другом конце соединения VPN, через порт UDP с номером 4500. Для обмена данными во время согласования IKE обычно применяется порт UDP с номером 500. Однако, если IKE обнаруживает функцию NAT при согласовании ключей, то последующие пакеты IKE будут пересылаться через порт 4500 на целевой порт 4500. Это также означает, что порт 4500 должен быть свободен от каких-либо ограничений, накладываемых правилами фильтрации. Получатель всегда может отличить пакет IKE от инкапсулированного пакета UDP. Первые 4 байта в поле данных пакета IKE равны нулю. Функцию инкапсуляции UDP можно применять лишь в том случае, если ее поддерживают обе конечные системы. «

Сжатие пакетов IP (IPComp)

Протокол IP Payload Compression (IPComp) уменьшает размер дейтаграмм IP путем их сжатия. Это позволяет повысить скорость передачи данных по соединению. Сжатие пакетов может применяться при работе с медленными или перегруженными линиями связи. Протокол IPComp не предоставляет никаких средств защиты, поэтому при работе с соединением VPN вместе с этим протоколом должно применяться преобразование AH или ESP.

Формальное описание протокола IPComp, созданное Рабочей группой Internet (IETF), содержится в документе RFC 2393, *IP Payload compression Protocol (IPComp)*. Этот документ RFC можно найти в Internet на следующем Web-сайте: http://www.rfc-editor.org .

VPN и фильтрация пакетов IP

Для работы большинства соединений VPN требуется правильно настроить правила фильтрации. Набор необходимых правил фильтрации зависит от типа соединения VPN и типа данных, которые вы планируете передавать по этому соединению. Обычно для соединения требуется настроить фильтр стратегии. Фильтр стратегии задает адреса, протоколы и порты, связанные с соединением VPN. Если соединение будет поддерживать протокол IKE, то для него требуется явно задать правила фильтрации, разрешающие передавать данные IKE по соединению.

Начиная с выпуска V5R1, в функции VPN появилась возможность автоматически создавать правила фильтрации. Рекомендуется всегда использовать фильтры стратегий, созданные VPN автоматически. Это позволит избежать ошибок и избавит вас от необходимости настраивать эти правила с помощью редактора правил обработки пакетов программы Навигатор iSeries(TM).

Конечно, существует ряд исключений. Информация о других особенностях применения правил фильтрации при работе с соединениями VPN приведена в следующих разделах:

- **“Перенос фильтров стратегий в текущий выпуск”**
  В операционной системе выпусков V4R4 и V4R5 правила фильтрации пакетов VPN настраиваются отдельно. Они не создаются автоматически во время настройки соединения VPN. В этом разделе приведены подробные рекомендации по переносу фильтров стратегий из выпуска V4R4 или V4R5 в текущий выпуск.
- **“Соединения VPN без фильтров стратегий” на стр. 32**
  Если конечными точками соединения VPN являются конечные системы с фиксированными IP-адресами, и вы не хотите настраивать и активировать правила фильтрации, настройте динамический фильтр стратегии. В этом разделе описаны случаи, в которых может применяться динамический фильтр, и приведены рекомендации по его настройке.
- **“Неявная передача данных IKE” на стр. 33**
  Для того чтобы параметры соединения VPN могли согласовываться в соответствии с протоколом IKE, необходимо разрешить передавать дейтаграммы UDP через порт 500. Если в системе не заданы правила фильтрации, разрешающие передавать данные IKE, то по умолчанию считается, что передача таких данных разрешена. Для получения дополнительной информации о неявной передаче данных IKE в системе iSeries ознакомьтесь с этим разделом.

Перенос фильтров стратегий в текущий выпуск

В операционной системе выпусков V4R4 и V4R5 правила фильтрации пакетов VPN настраиваются отдельно с помощью интерфейса Правила обработки пакетов программы Навигатор iSeries(TM). Они не создаются автоматически во время настройки соединения VPN. Начиная с выпуска V5R1, в интерфейсе VPN появилась возможность автоматически создавать правила фильтрации пакетов.

Существуют некоторые особенности, которые следует учесть, если вы планируете применять в текущем выпуске правила фильтрации стратегии (правила с действием IPSEC), созданные в выпуске V4R4 или V4R5. Это же следует учесть и в том случае, если правила фильтрации стратегии *будут* созданы функцией VPN, но вы планируете добавить правила, разрешающие передавать по соединению другие данные IP, например, данные протокола Telnet. Для того чтобы избежать ошибок во время настройки, следуйте следующим рекомендациям.

Пояснение: Под файлом правил *заказчика* далее будет пониматься любой файл правил, созданный с помощью редактора правил обработки пакетов программы Навигатор. Не следует путать этот файл с файлом правил *VPNPOLICYFILTERS.I3P*, который автоматически создается во время настройки VPN.

- Если вы не планируете применять никакие соединения VPN, за исключением тех, которые были созданы в выпуске V4R4 или V4R5, активируйте правила фильтрации и запустите соединения обычным образом.
- Если помимо соединений VPN, созданных в выпуске V4R4 или V4R5, в текущем выпуске будут применяться другие соединения VPN, воспользуйтесь мастером **Перенести фильтры стратегии**. Этот

мастер удаляет фильтры стратегии из созданных файлов правил обработки пакетов и добавляет аналогичные фильтры стратегии в файл VPNPOLICYFILTERS.I3P, созданный функцией VPN. Для запуска мастера выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—>Сеть —>Стратегии IP**.
2. Щелкните правой кнопкой мыши на опции **Виртуальная частная сеть**и выберите пункт **Перенести фильтры стратегий**.
3. После выполнения всех инструкций мастера нажмите кнопку **Готово**.
4. Для просмотра дополнительной информации о любой странице и ее полях нажмите на этой странице кнопку **Справка**.

- Если правила фильтрации стратегии были созданы функцией VPN, и вы планируете добавить некоторые другие правила фильтрации, настройте эти правила с помощью редактора правил обработки пакетов программы Навигатор. Если некоторые из этих правил нужно поместить перед фильтрами VPN, укажите в именах соответствующих наборов правил префикс `PREIPSEC`. Например, `PREIPSECMYRULES`. В этом случае система правильно определит порядок обработки правил фильтрации. Имена всех остальных наборов правил, отличных от VPN, не должны начинаться с префикса `PREIPSEC`. Примером имени набора может служить `MORERULES`.
- Рекомендуется разрешить функции VPN автоматически создать правила фильтрации стратегии. Все правила фильтрации, не связанные с VPN, должны располагаться в файле правил заказчика. Если некоторые из этих правил фильтрации необходимо разместить перед фильтрами стратегии, определенными в файле VPNPOLICYFILTERS.I3P, добавьте префикс `PREIPSEC` к имени набора правил. В этом случае правила заказчика и правила VPN будут обрабатываться ожидаемым образом. Предположим, что функция VPN создала правила фильтрации стратегии (наборы VPN), и вы добавили правила, разрешающие передавать другие данные IP по соединению (пользовательские наборы). При загрузке правил в систему они будут упорядочены следующим образом:
  1. Пользовательские наборы правил, имена которых начинаются с префикса PREIPSEC
  2. Наборы правил VPN, имена которых начинаются с префикса PREIPSEC
  3. Наборы правил VPN, в которых указано ACTION=IPSEC (фильтры стратегии)
  4. Пользовательские наборы правил, в которых указано ACTION=IPSEC (фильтры стратегии)
  5. Прочие пользовательские наборы правил.
  6. Прочие наборы правил VPN.

  Порядок применения правил фильтрации можно просмотреть в файле вывода EXPANDED.OUT. Файл EXPANDED.OUT сохраняется в том каталоге, в котором расположены файлы правил заказчика.
- С помощью программы Навигатор можно активировать следующие правила:
  – только файл правил VPNPOLICYFILTERS.I3P, созданный функцией VPN
  – только файл правил заказчика
  – Файл правил VPN и файл правил заказчика
- Правила фильтрации следует активировать сразу для всех интерфейсов, а не для отдельных интерфейсов. Это гарантирует, что правила фильтрации будут активированы, а фильтры стратегий будут загружены в правильном порядке.
- Перед активацией правил фильтрации их необходимо проверить. Если во время проверки ошибки не будут найдены, просмотрите файл EXPANDED.OUT и убедитесь, что правила расположены в правильном порядке. После этого можно активировать правила.

Соединения VPN без фильтров стратегий

Правило фильтрации стратегии задает адреса, протоколы и порты, которым разрешено применять VPN, и указывает, какие данные должны передаваться по соединению. В некоторых случаях требуется настроить соединение, при работе с которым не должно применяться правило фильтрации стратегии. Например, если для интерфейса, связанного с соединением VPN, активированы правила обработки пакетов, не относящиеся к VPN, то вместо того чтобы деактивировать эти правила можно настроить VPN таким образом, чтобы система динамически управляла всеми фильтрами соединения. Фильтр стратегии для такого типа

соединения называется **динамическим фильтром стратегии**. Динамический фильтр стратегии можно настроить для соединения VPN, если выполнены следующие условия:

- Соединение устанавливается только локальным сервером.
- Конечные точки данных этого соединения представляют собой отдельные системы. Другими словами, конечные точки не являются подсетями и диапазонами адресов.
- Для соединения не загружается правило фильтрации стратегии.

Если все перечисленные выше условия выполнены, то можно настроить соединение, не требующее фильтр стратегии. После установления такого соединения по нему будут передаваться все данные, которыми обмениваются конечные точки данных, независимо от того, какие правила обработки пакетов загружены в системе.

Пошаговые инструкции по настройке соединения, не требующего применения фильтра стратегии, приведены в электронной справке по VPN.

Неявная передача данных IKE

Обычно для установления соединения VPN требуется выполнить процедуру согласования IKE. После этого выполняется обработка IPSec. Протокол IKE применяет стандартный порт 500, поэтому для правильной работы IKE требуется разрешить передачу дейтаграмм UDP этого протокола через порт 500. Если в системе не заданы правила фильтрации, разрешающие передавать данные IKE, то по умолчанию считается, что передача таких данных разрешена. Однако все правила, созданные для порта UDP с номером 500, обрабатываются с учетом того, что задано в активных правилах фильтрации.

Планирование конфигурации VPN

Планирование конфигурации - это обязательный этап настройки соединения VPN. Правильность работы соединения будет зависеть от того, какие решения вы примете на этом этапе. Для получения всей необходимой информации ознакомьтесь со следующими разделами:

- “Требования к настройке VPN”
  Перед созданием VPN необходимо убедиться, что выполнены все необходимые требования.
- “Выбор типа VPN” на стр. 34
  На одном из первых шагов планирования необходимо определить назначение соединения VPN. В этом разделе описаны разные типы соединений, которые можно настроить.
- **Применение советника по планированию конфигурации VPN**
  При работе с советником по планированию вам потребуется ответить на ряд вопросов относительно локальной сети. На основании ваших ответов советник предложит рекомендации по созданию соединения VPN.
  Примечание: Советник по планированию VPN следует применять только в тех случаях, если вы планируете настроить соединение с поддержкой протокола IKE. Если вы планируете настроить статическое соединение, заполните формы планирования.
- “Заполнение форм планирования конфигурации VPN” на стр. 35
  При необходимости напечатайте и заполните формы планирования, которые позволят вам собрать необходимую информацию о применении будущего соединения VPN.

После завершения планирования конфигурации VPN перейдите к ее “Настройка VPN” на стр. 38.

Требования к настройке VPN

Для применения функции VPN в системе iSeries(TM) и на PC-клиентах необходимо, чтобы были выполнены следующие требования:

Требования к системе iSeries выпуска V5R2

- Операционная система OS/400(R) версии 5, выпуска 2 (5722-SS1) или более позднего выпуска.
- Диспетчер цифровых сертификатов (5722-SS1, компонент 34)
- Продукт Cryptographic Access Provider (5722-AC2 или AC3)
- Программы iSeries Access для Windows(R) (5722-XE1) и Навигатор iSeries
  - Компонент Сеть программы Навигатор iSeries
- Системное значение Сохранять идентификационные данные на сервере (QRETSVRSEC *SEC) должно быть равно 1
- В системе должен быть настроен протокол TCP/IP, включая интерфейсы IP, маршруты, имя локального хоста и имя локального домена

Требования к клиенту

- Рабочая станция с 32-разрядной операционной системой Windows(R), подключенная к системе iSeries и настроенная для работы в сети TCP/IP
- Процессор с тактовой частотой 233 МГц
- Оперативная память объемом 32 Мб (для клиентов Windows 95/98)
- Оперативная память объемом 64 Мб (для клиентов Windows(R) NT и 2000)
- На PC-клиенте должна быть установлена программа iSeries Access для Windows и Навигатор iSeries
- Необходимо программное обеспечения для работы с протоколом Защита IP (IPSec)
- Если удаленные пользователи будут подключаться к системе с помощью протокола L2TP, то необходимо программное обеспечение для работы с этим протоколом

Выбор типа VPN

На одном из первых шагов планирования необходимо определить назначение соединения VPN. Для этого необходимо знать, какую роль по отношению к соединению будут играть локальный и удаленный сервер ключей. Например, будут ли конечные точки *соединения* совпадать с конечными точками *данных*. Конечные точки соединения и данных могут отличаться. Конечные точки соединения отвечают за идентификацию и шифрование данных, а также за управление ключами в соответствии с протоколом Internet Key Exchange (IKE). Конечные точки данных - это системы, между которыми передаются пакеты IP по соединению VPN. Например, по такому соединению могут передаваться все данные TCP/IP, которыми обмениваются системы с адресами 123.4.5.6 и 123.7.8.9. Обычно, если конечные точки данных и соединения не совпадают, то сервер VPN играет роль шлюза. Если они совпадают, то сервер VPN играет роль хоста.

Ниже перечислены возможные типы соединений VPN, которые могут применяться в разных ситуациях:

Соединение между двумя шлюзами
Конечные точки соединения отличаются от конечных точек данных. Протокол защиты IP (IPSec) применяется для защиты данных во время их передачи между шлюзами. Однако он не применяется для защиты данных во время их передачи по внутренней сети. Обычно этот вариант конфигурации применяется для защиты соединений между различными филиалами одной фирмы, поскольку внутреннюю сеть фирмы можно считать защищенной.

Соединение между шлюзом и хостом
Протокол IPSec применяется для защиты данных во время их передачи между шлюзом и хостом удаленной сети. VPN не защищает данные во время их передачи по локальной сети, так как эта сеть считается защищенной.

Соединение между хостом и шлюзом
VPN защищает данные во время их передачи между хостом локальной сети и удаленным шлюзом. VPN не защищает данные во время их передачи по удаленной сети.

Соединение между хостами
Конечные точки соединения совпадают с конечными точками данных. VPN защищает данные во время их передачи между хостом локальной сети и хостом удаленной сети. При этом пакеты IP будут защищены на всем протяжении их передачи по сети.

Заполнение форм планирования конфигурации VPN

Формы планирования конфигурации VPN позволяют собрать всю необходимую информацию о будущем соединении VPN. Эта информация потребуется при планировании стратегии VPN. Кроме того, ей можно руководствоваться при настройке соединения VPN. Выберите форму планирования с учетом типа создаваемого соединения.

- “Форма планирования конфигурации динамических соединений”
  Заполните эту форму перед настройкой динамического соединения.
- “Форма планирования конфигурации статических соединений” на стр. 36
  Заполните эту форму перед настройкой статического соединения.
- **Советник по планированию конфигурации VPN**
  Для получения рекомендаций по планированию и настройке можно обратиться к советнику по планированию. При работе с советником по планированию вам потребуется ответить на ряд вопросов относительно локальной сети. На основании ваших ответов советник предложит рекомендации по созданию соединения VPN.

  Примечание: Советник по планированию VPN может применяться только для динамических соединений. Если вы планируете настроить статическое соединение, заполните формы планирования.

Если вы планируете создать несколько соединений со схожими свойствами, рекомендуется задать значения атрибутов VPN по умолчанию. Значения по умолчанию автоматически указываются на страницах свойств VPN. Вам не потребуется вводить одни и те же значения несколько раз. Для того чтобы задать значения по умолчанию для параметров VPN, выберите в главном меню VPN пункт **Правка**, а затем выберите опцию **Значения по умолчанию**.

Форма планирования конфигурации динамических соединений

Перед созданием динамических соединений VPN заполните приведенную ниже форму. В этой форме предполагается, что соединение будет создано с помощью мастера Создать соединение. Этот мастер позволяет настроить VPN исходя из основных требований к защите системы. В большинстве случаев после завершения работы с мастером требуется изменить некоторые параметры соединения. Например, вы можете включить функцию ведения журнала или разрешить автоматический запуск сервера VPN при запуске TCP/IP. Для изменения параметров щелкните правой кнопкой мыши на значке группы соединений с динамическим ключом или соединения, созданного мастером, и выберите пункт **Свойства**.

Перед настройкой VPN ответьте на указанные ниже вопросы.

Справочная таблица предварительных требований	**Ответы**
Установлена ли в системе операционная система OS/400(R) версии V5R2 (5722-SS1) или более поздней версии?	
Установлен ли в системе компонент Диспетчер цифровых сертификатов (5722-SS1, компонент 34)?	
Установлен ли в системе продукт Cryptographic Access Provider (5722-AC2 или AC3)?	
Установлен ли в системе продукт iSeries Access (5722-XE1)?	
Установлен ли в системе Навигатор iSeries?	
Установлен ли компонент Сеть программы Навигатор iSeries?	
Установлен ли в системе продукт TCP/IP Connectivity Utilities для OS/400 (5722-TC1)?	
Установлено ли системное значение Сохранять идентификационные данные на сервере (QRETSVRSEC *SEC) равным 1?	
Настроен ли в системе iSeries протокол TCP/IP (включая интерфейсы IP, маршруты, имя локального хоста и имя локального домена)?	
Установлено ли между конечными точками обычное соединение TCP/IP?	
Применены ли в системе последние версии временных исправлений программ (PTF)?	

Справочная таблица предварительных требований	Ответы
Если туннель VPN будет проходить через брандмауэры или маршрутизаторы, выполняющие фильтрацию пакетов IP, то поддерживают ли эти брандмауэры и маршрутизаторы протоколы AH и ESP?	
Разрешено ли на брандмауэрах и маршрутизаторах применение протоколов IKE (порт UDP 500), AH и ESP?	
Разрешена ли на брандмауэрах пересылка пакетов IP?	

Для настройки динамического соединения VPN вам потребуется следующая информация	Ответы
Соединение какого типа будет создано? • Соединение между шлюзами • Соединение между хостом и шлюзом • Соединение между шлюзом и хостом • Соединение между хостами	
Какое имя будет присвоено группе соединений с динамическим ключом?	
Какой способ защиты ключей, по отношению к производительности системы, будет применяться? • Максимальная защита, низкая производительность • Средняя защита и средняя производительность • Минимальная защита, высокая производительность	
Применяются ли сертификаты для идентификации соединения? Если нет, какой подготовленный ключ будет применяться?	
Какой идентификатор связан с локальным сервером ключей?	
Какой идентификатор связан с локальной конечной точкой данных?	
Какой идентификатор присвоен удаленному серверу ключей?	
Какой идентификатор связан с удаленной конечной точкой данных?	
Какой способ защиты данных, по отношению к производительности системы, будет применяться? • Максимальная защита, низкая производительность • Средняя защита и средняя производительность • Минимальная защита, высокая производительность	

Форма планирования конфигурации статических соединений

Заполните эту форму перед созданием соединений VPN, не применяющих функции управления ключами IKE.

Перед настройкой VPN ответьте на указанные ниже вопросы:

Справочная таблица предварительных требований	Ответы
Установлена ли в системе операционная система OS/400(R) версии V5R2 (5722-SS1) или более поздней версии?	
Установлен ли в системе компонент Диспетчер цифровых сертификатов (5722-SS1, компонент 34)?	
Установлен ли в системе продукт Cryptographic Access Provider (5722-AC2 или AC3)?	
Установлен ли в системе продукт iSeries Access (5722-XE1)?	
Установлен ли в системе Навигатор iSeries?	
Установлен ли компонент Сеть программы Навигатор iSeries?	
Установлен ли в системе продукт TCP/IP Connectivity Utilities для OS/400 (5722-TC1)?	

Справочная таблица предварительных требований	Ответы
Установлено ли системное значение Сохранять идентификационные данные на сервере (QRETSVRSEC *SEC) равным 1?	
Настроен ли в системе iSeries протокол TCP/IP (включая интерфейсы IP, маршруты, имя локального хоста и имя локального домена)?	
Установлено ли между конечными точками обычное соединение TCP/IP?	
Применены ли в системе последние версии временных исправлений программ (PTF)?	
Если туннель VPN будет проходить через брандмауэры или маршрутизаторы, выполняющие фильтрацию пакетов IP, то поддерживают ли эти брандмауэры и маршрутизаторы протоколы AH и ESP?	
Разрешено ли на брандмауэрах и маршрутизаторах передавать пакеты протоколов AH и ESP?	
Разрешена ли на брандмауэрах пересылка пакетов IP?	

Для настройки статического соединения VPN вам потребуется следующая информация	Ответы
Соединение какого типа будет создано? • Соединение между хостами • Соединение между хостом и шлюзом • Соединение между шлюзом и хостом • Соединение между шлюзами	
Какое имя будет присвоено соединению?	
Какой идентификатор связан с локальной конечной точкой соединения?	
Какой идентификатор связан с удаленной конечной точкой соединения?	
Какой идентификатор связан с локальной конечной точкой данных?	
Какой идентификатор связан с удаленной конечной точкой данных?	
Какие данные будет разрешено передавать по соединению (список локальных портов, удаленных портов и протоколов)?	
Требуется ли применять функцию преобразования адресов при работе с этим соединением? Дополнительная информация приведена в разделе “Преобразование сетевых адресов в VPN” на стр. 28.	
Какой режим передачи будет применяться: режим открытой передачи или режим туннеля?	
Какие протоколы IPSec будут применяться для защиты соединения (AH, ESP или AH и ESP)? За дополнительной информацией обратитесь к разделу “Протоколы защиты IP (IPSec)” на стр. 23.	
Какой алгоритм идентификации будет применяться при работе с соединением (HMAC-MD5 или HMAC-SHA)?	
Какой алгоритм шифрования будет применяться при работе с соединением (DES-CBC или 3DES-CBC)? **Примечание:** Алгоритм шифрования нужно выбирать лишь в том случае, если в качестве протокола защиты выбран протокол ESP.	
Какой ключ AH будет применяться для обработки входящих данных? Если применяется алгоритм MD5, то ключ представляет собой шестнадцатеричную строку длиной 16 байт. Если применяется алгоритм SHA, то ключ представляет собой шестнадцатеричную строку длиной 20 байт. Ключ для обработки входящих данных должен совпадать с ключом для обработки исходящих данных, заданным на удаленном сервере.	

Для настройки статического соединения VPN вам потребуется следующая информация	Ответы
Какой ключ AH будет применяться для обработки исходящих данных? Если применяется алгоритм MD5, то ключ представляет собой шестнадцатеричную строку длиной 16 байт. Если применяется алгоритм SHA, то ключ представляет собой шестнадцатеричную строку длиной 20 байт. Ключ для обработки исходящих данных должен совпадать с ключом для обработки входящих данных, заданным на удаленном сервере.	
Какой ключ ESP будет применяться для обработки входящих данных? Если применяется алгоритм DES, ключ представляет собой шестнадцатеричное значение длиной 8 байт. Если применяется алгоритм 3DES, то ключ представляет собой шестнадцатеричное значение длиной 24 байта. Ключ для обработки входящих данных должен совпадать с ключом для обработки исходящих данных, заданным на удаленном сервере.	
Какой ключ ESP будет применяться для обработки исходящих данных? Если применяется алгоритм DES, ключ представляет собой шестнадцатеричное значение длиной 8 байт. Если применяется алгоритм 3DES, то ключ представляет собой шестнадцатеричное значение длиной 24 байта. Ключ для обработки исходящих данных должен совпадать с ключом для обработки входящих данных, заданным на удаленном сервере.	
Чему равен индекс стратегии защиты (SPI) для входящих данных? SPI для входящих данных представляет собой шестнадцатеричное значение размером 4 байта, в котором первый байт равен 00. SPI для входящих данных должен совпадать с SPI для исходящих данных, заданным на удаленном сервере.	
Чему равен SPI для исходящих данных? SPI для исходящих данных представляет собой шестнадцатеричное значение размером 4 байта. SPI для исходящих данных должен совпадать с SPI для входящих данных, заданным на удаленном сервере.	

Настройка VPN

В интерфейсе VPN предусмотрено несколько способов настройки соединений VPN. Далее в этом разделе описаны различные типы соединений и способы их настройки.

Выбор типа соединения

Динамическим называется соединение, ключи которого создаются и согласуются во время работы соединения с помощью протокола IKE. Динамическое соединение обеспечивает высокий уровень защиты данных, так как ключи автоматически регулярно обновляются. Это сокращает срок действия ключей и, следовательно, снижает вероятность взлома защиты.

Статическим (стр. 40) называется соединение, которое не поддерживает процедуру согласования IKE и автоматическое управление ключами. Значения некоторых параметров на обоих концах этого соединения должны совпадать. Ключи статического соединения не обновляются автоматически. Их нельзя изменить во время работы соединения. Для замены ключа необходимо прервать соединение. Это ослабляет защиту соединения, поэтому в тех случаях, когда требуется максимально надежная защита, рекомендуется создать динамическое соединение.

Настройка динамического соединения VPN

VPN представляет собой группу объектов конфигурации, задающих различные свойства соединения. Для

применения динамического соединения VPN необходимо правильно настроить все объекты. Более подробная информация о настройке отдельных объектов конфигурации VPN приведена в следующих разделах:

Совет:
“Настройка соединений VPN с помощью мастера Создать соединение” на стр. 40
Обычно для создания динамических соединений применяется мастер Соединение. Этот мастер автоматически создает все необходимые объекты конфигурации VPN, включая правила обработки пакетов. Если при работе с мастером вы выберете опцию автоматической активации правил обработки пакетов VPN, вы можете сразу перейти к шагу 6, *Запуск соединения*. В противном случае после завершения работы с мастером вам потребуется активировать правила обработки пакетов. После этого вы сможете запустить соединение.

Если вы решите настроить динамическое соединение VPN без помощи мастера, выполните следующие действия:

1. “Настройка стратегий защиты VPN” на стр. 40
   Для всех динамических соединений необходимо определить стратегии защиты VPN. В стратегии IKE и стратегии защиты данных указывается, какие средства защиты будут применяться на первом и втором этапе согласования IKE.
2. “Настройка защищенного соединения VPN” на стр. 42
   После определения стратегий защиты необходимо настроить защищенное соединение. При настройке динамического соединения задаются параметры группы соединений с динамическим ключом и соединения с динамическим ключом. **Группа соединений с динамическим ключом** задает общие свойства одного или нескольких соединений VPN. **Соединение с динамическим ключом** определяет свойства отдельного соединения, установленного между двумя конечными точками. Соединение с динамическим ключом входит в группу соединений с динамическим ключом.

   Примечание: Следующие два действия, то есть *настройку правил обработки пакетов* и *выбор интерфейса для правил*, следует выполнять только в том случае, если на странице **Группа с динамическим ключом - Соединения** выбрана опция **Правило фильтрации стратегии будет определено в правилах обработки пакетов**. В противном случае такое правило будет создано во время настройки VPN и связано с указанным интерфейсом.

   Правила фильтрации стратегий рекомендуется создавать автоматически с помощью интерфейса VPN. Для этого выберите опцию **Создать следующий фильтр стратегии для группы** на странице **Группа с динамическим ключом - Соединения**.
3. “Настройка правил фильтрации пакетов VPN” на стр. 43
   После завершения настройки VPN необходимо создать и применить правила фильтрации, разрешающие передачу данных по соединению. Правила VPN, **применяемые до IPSec**, разрешают передавать все данные IKE по указанным интерфейсам. Это дает возможность согласовывать параметры соединения с помощью протокола IKE. **Правило фильтрации стратегии** задает адреса, протоколы и порты, связанные с новой группой соединений с динамическим ключом.

   Если вы планируете применять соединения VPN и фильтры стратегии, которые были определены в старом выпуске (V4R4 или V4R5), убедитесь, что они не будут конфликтовать с новыми фильтрами стратегии. Дополнительная информация приведена в разделе “Перенос фильтров стратегий в текущий выпуск” на стр. 31.
4. “Определение интерфейса для правил фильтрации VPN” на стр. 46
   После настройки правил фильтрации пакетов и других правил, необходимых для работы соединения VPN, определите интерфейс, к которому должны применяться эти правила.
5. “Активация правил фильтрации пакетов VPN” на стр. 46
   После выбора интерфейса, связанного с правилами обработки пакетов, активируйте эти правила. Это необходимо сделать до запуска соединения.
6. “Запуск соединения VPN” на стр. 47
   Выполните эту задачу для запуска соединения.

Настройка статического соединения VPN
Все свойства статического соединения VPN задаются пользователем, включая ключи для исходящих и входящих данных. Для настройки статического соединения необходимо выполнить следующие действия:

1. “Настройка статического соединения” на стр. 43
   В определении статического соединения задаются все свойства соединения, в том числе протоколы защиты, а также конечные точки соединения и данных.

   Примечание: Следующие два действия, то есть *настройку правил фильтрации пакетов* и *выбор интерфейса для правил*, требуется выполнять лишь в том случае, если на странице **Статическое соединение - Соединение** была выбрана опция **Правило фильтрации стратегии будет определено в правилах обработки пакетов**. В противном случае такое правило будет создано во время настройки VPN.

   Правила фильтрации стратегий рекомендуется создавать автоматически с помощью интерфейса VPN. Для этого выберите опцию **Создать фильтр стратегии, соответствующий конечным точкам данных** на странице **Статическое соединение - Соединение**.
2. “Настройка правила фильтрации стратегии” на стр. 45
   После настройки свойств статического соединения необходимо создать и применить правило фильтрации стратегии, разрешающее передавать данные по соединению. **Правило фильтрации стратегии** задает адреса, протоколы и порты, связанные с соединением.
3. “Определение интерфейса для правил фильтрации VPN” на стр. 46
   После настройки правил фильтрации пакетов и других правил, необходимых для работы соединения VPN, определите интерфейс, к которому должны применяться эти правила.
4. “Активация правил фильтрации пакетов VPN” на стр. 46
   После выбора интерфейса, связанного с правилами обработки пакетов, активируйте эти правила. Это необходимо сделать до запуска соединения.
5. “Запуск соединения VPN” на стр. 47
   Выполните эту задачу для запуска соединений, которые устанавливаются локальной системой.

Настройка соединений VPN с помощью мастера Создать соединение

Мастер Создать соединение позволяет настроить виртуальную частную сеть (VPN) между хостами или шлюзами. Например, соединение можно установить между двумя хостами, между шлюзом и хостом, между хостом и шлюзом или между двумя шлюзами.

Этот мастер автоматически создает все необходимые объекты конфигурации VPN, включая правила обработки пакетов. Если вы хотите настроить дополнительные функции VPN, например, функцию ведения журнала или преобразование сетевых адресов для VPN (VPN NAT), измените некоторые свойства соответствующей группы соединений с динамическим ключом или отдельного соединения. Для этого завершите соединение, если оно активно. Затем щелкните правой кнопкой мыши на значке группы соединений с динамическим ключом или значке соединения и выберите пункт **Свойства**.

Перед настройкой соединения заполните формы советника по планированию конфигурации VPN. Советник поможет вам собрать всю необходимую информацию для настройки VPN.

Для создания VPN с помощью мастера Создать соединение выполните следующие действия:

1. В Навигаторе разверните значок своего сервера и выберите **—> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Виртуальная частная сеть** и выберите опцию **Создать соединение**. Будет запущен мастер.
3. Задайте основные параметры соединения VPN, следуя инструкциям мастера. Для просмотра дополнительной информации нажмите кнопку **Справка**.

Настройка стратегий защиты VPN

После принятия решения относительно назначения VPN необходимо определить стратегии защиты VPN. В частности, необходимо выполнить следующие действия:

- “Настройка стратегии Internet Key Exchange (IKE)”
  Стратегия IKE определяет способы идентификации и шифрования, которые применяются протоколом IKE на первом этапе согласования. На этом этапе выбираются ключи для защиты второго этапа согласования. Стратегия IKE не нужна для создания статического соединения. Если для настройки соединения применяется мастер Создать соединение, стратегия IKE создается автоматически.
- “Настройка стратегии защиты данных”
  Стратегия защиты данных управляет идентификацией и шифрованием данных, передаваемых по соединению VPN. Соответствующие атрибуты принимаются конечными точками соединения на втором этапе согласования протокола IKE. При создании статического соединения не нужно определять стратегию защиты данных. Если для настройки соединения VPN применяется мастер Создать соединение, то стратегия защиты данных будет создана автоматически.

После настройки стратегий защиты VPN перейдите к настройке “Настройка защищенного соединения VPN” на стр. 42.

Настройка стратегии Internet Key Exchange (IKE)

Стратегия IKE определяет способы идентификации и шифрования, которые применяются протоколом “Управление ключами” на стр. 26 на первом этапе согласования. На этом этапе выбираются ключи для защиты второго этапа согласования. Для идентификации на первом этапе согласования функция VPN применяет подписи RSA или подготовленные ключи. Если для идентификации серверов ключей планируется применять цифровые сертификаты, настройте их с помощью Диспетчера цифровых сертификатов (5722-SS1, компонент 34). В стратегии IKE указан идентификатор удаленного сервера ключей, для которого предназначена эта стратегия.

Для создания новой или изменения существующей стратегии IKE выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Стратегии защиты IP**.
2. Для создания новой стратегии щелкните правой кнопкой мыши на значке **Стратегии IKE** и выберите **Создать стратегию IKE**. Для изменения существующей стратегии выберите **Стратегии IKE** на левой панели, затем щелкните правой кнопкой мыши на значке нужной стратегии на правой панели и выберите **Свойства**.
3. Заполните поля на всех страницах свойств. Для просмотра дополнительной информации о любой странице и ее полях нажмите на этой странице кнопку **Справка**.
4. Нажмите **OK** для сохранения изменений.

Примечание: Если для идентификации применяется подготовленный ключ, то рекомендуется использовать основной режим согласования IKE. Тем самым обеспечивается более высокий уровень защиты передаваемых данных. Если вам приходится использовать подготовленные ключи с ускоренным режимом согласования, то используйте нетривиальные пароли, взлом которых путем сканирования словаря маловероятен. Кроме того, рекомендуется периодически менять пароли. Более подробная информация приведена в электронной справке по Навигатору iSeries.

Настройка стратегии защиты данных

Стратегия защиты данных управляет идентификацией и шифрованием данных, передаваемых по соединению VPN. Значения соответствующих параметров принимаются конечными системами на втором этапе согласования “Управление ключами” на стр. 26.

Для создания новой или изменения существующей стратегии защиты данных выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Стратегии защиты IP**.

2. Для создания новой стратегии щелкните правой кнопкой мыши на значке **Стратегии защиты данных** и выберите **Создать стратегию защиты данных**. Для изменения существующей стратегии выберите **Стратегии защиты данных** (на левой панели), затем щелкните правой кнопкой мыши на значке нужной стратегии (на правой панели) и выберите **Свойства**.
3. Заполните поля на всех страницах свойств. Для просмотра дополнительной информации о любой странице и ее полях нажмите на этой странице кнопку **Справка**.
4. Нажмите **OK** для сохранения изменений.

Настройка защищенного соединения VPN

После настройки стратегий защиты можно определить защищенное соединение. При настройке динамического соединения задаются параметры группы соединений с динамическим ключом и соединения с динамическим ключом.

Группа соединений с динамическим ключом задает общие параметры одного или нескольких соединений VPN. Такая группа объединяет соединения, установленные между разными конечными точками данных, но использующие одинаковые стратегии. Группа соединений с динамическим ключом позволяет согласовать параметры с удаленным инициатором соединения в тех случаях, когда заранее неизвестны конечные точки данных, которые будут предложены удаленной системой. Для этого информация о стратегиях, заданная в группе соединений с динамическим ключом, связывается с правилом фильтрации стратегии, тип действия которого равен IPSEC. Если конечные точки данных, предложенные удаленной системой, попадают в диапазон значений, заданных в правиле фильтрации IPSEC, то считается, что к ним применима стратегия, определенная в группе соединений с динамическим ключом.

Соединение с динамическим ключом определяет свойства отдельного соединения, установленного между конкретными конечными точками данных. Соединение с динамическим ключом входит в группу соединений с динамическим ключом. После определения стратегий в группе соединений с динамическим ключом необходимо задать параметры тех соединений с динамическим ключом, которые будут устанавливаться локальной системой.

Для настройки защищенного соединения выполните следующие действия:

Шаг 1: Настройте группу соединений с динамическим ключом

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Защищенные соединения**.
2. Щелкните правой кнопкой мыши на пункте **По группам** и выберите опцию **Создать группу с динамическим ключом**.
3. Для просмотра дополнительной информации о любой странице и ее полях нажмите на этой странице кнопку **Справка**.
4. Нажмите **OK** для сохранения изменений.

Шаг 2: Настройте соединение с динамическим ключом

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть—> Стратегии IP—> Виртуальная частная сеть—> Защищенные соединения—> По группам**.
2. На левой панели окна программы Навигатор щелкните правой кнопкой мыши на значке группы соединений с динамическим ключом, созданной на первом шаге, и выберите опцию **Создать соединение с динамическим ключом**.
3. Для просмотра дополнительной информации о любой странице и ее полях нажмите на этой странице кнопку **Справка**.
4. Нажмите **OK** для сохранения изменений.

После выполнения описанных действий “Активация правил фильтрации пакетов VPN” на стр. 46 правила обработки пакетов, необходимые для работы соединения.

Примечание: В большинстве случаев следует разрешить функции VPN автоматически создать правила обработки пакетов, выбрав опцию **Создать следующий фильтр стратегии для группы** на странице **Группа с динамическим ключом - Соединения**. Если вы выберете опцию **Правило фильтрации стратегии будет определено в правилах обработки пакетов**, то перед активацией правил вам потребуется "Настройка правил фильтрации пакетов VPN" с помощью редактора правил обработки пакетов.

Настройка статического соединения

Статическим называется соединение VPN, все свойства которого задаются пользователем. Значения некоторых параметров на обоих концах соединения должны *совпадать*. Например, ключи для обработки входящих данных, заданные в локальной системе, должны совпадать с ключами для обработки исходящих данных, заданными в удаленной системе.

Ключи статического соединения не обновляются автоматически. Их нельзя изменить во время работы соединения. Для смены ключа необходимо прервать соединение. Поскольку применение одного и того же ключа в течение длительного времени ослабляет защиту, в тех случаях, когда обе конечные системы поддерживают протокол IKE, рекомендуется создавать динамическое соединение.

Для того чтобы задать свойства статического соединения, выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Защищенные соединения**.
2. Щелкните правой кнопкой мыши на значке **Все соединения** и выберите опцию **Создать статическое соединение**.
3. Заполните поля на всех страницах свойств. Для просмотра дополнительной информации о любой странице и ее полях нажмите на этой странице кнопку **Справка**.
4. Нажмите **OK** для сохранения изменений.

Примечание: В большинстве случаев следует разрешить функции VPN автоматически создать правила обработки пакетов, выбрав опцию **Создать фильтр стратегии, соответствующий конечным точкам данных** на странице **Статическое соединение - Соединение**. Если вы выберете опцию **Правило фильтрации стратегии будет определено в правилах обработки пакетов**, то вам потребуется вручную "Настройка правила фильтрации стратегии" на стр. 45, а затем активировать его.

Настройка правил фильтрации пакетов VPN

Если вы впервые создаете соединение VPN, включите опцию автоматического создания правил фильтрации пакетов VPN. Это можно сделать при настройке соединения с помощью мастера Создать соединение или страниц свойств VPN.

Если вы решили создать правила фильтрации пакетов VPN с помощью редактора правил обработки пакетов программы Навигатор iSeries(TM), все остальные правила должны быть созданы аналогичным образом. Если правила фильтрации стратегии будут созданы функцией VPN, все дополнительные правила фильтрации стратегии должны быть созданы с помощью редактора правил.

Обычно для работы VPN требуются правила фильтрации двух типов: правила, применяемые до IPSec, и правила фильтрации стратегии. Информация о настройке этих правил с помощью редактора правил программы Навигатор приведена в указанных ниже разделах. Для получения информации о других возможностях функции VPN и функции фильтрации обратитесь к разделу "VPN и фильтрация пакетов IP" на стр. 31, приведенному в главе с описанием принципов работы VPN.

- "Настройка правил фильтрации, применяемых до IPSec" на стр. 44
  Правила, применяемые до IPSec, - это любые правила обработки пакетов, которые размещаются перед правилами с действием IPSEC. В этом разделе описаны только те правила, применяемые до IPSec, которые необходимы для работы VPN. Это два правила, которые разрешают выполнять согласование IKE по соединению. Протокол IKE позволяет динамически создавать ключи защиты и согласовывать параметры соединения. Вы можете создать и другие правила, применяемые до IPSec, необходимые для реализации стратегии защиты в вашей сети.

Примечание: Эти правила, применяемые до IPSec, следует настраивать только в том случае, если для различных систем уже созданы правила, разрешающие передавать данные IKE. Если в системе не заданы правила фильтрации, разрешающие передавать данные IKE, то по умолчанию считается, что передача таких данных разрешена.

- “Настройка правила фильтрации стратегии” на стр. 45
  Правило фильтрации стратегии определяет, какие данные разрешено передавать по соединению VPN и какая стратегия будет применяться для защиты этих данных.

Ряд особенностей, которые необходимо учесть
При добавлении правила фильтрации для интерфейса система автоматически добавляет правило DENY для этого интерфейса. Это правило означает, что запрещены все пакеты, которые явно не разрешены. Вы не можете просмотреть или изменить это правило. В результате после активизации правил фильтрации VPN некоторые соединения могут перестать работать. Если помимо данных VPN по интерфейсу будут передаваться другие данные, необходимо явно разрешить (PERMIT) передачу соответствующих пакетов.

После настройки правил фильтрации необходимо “Определение интерфейса для правил фильтрации VPN” на стр. 46, к которому будут применяться эти правила, а затем “Активация правил фильтрации пакетов VPN” на стр. 46 правила.

Важно не допустить ошибки при настройке правил фильтрации. Такая ошибка может привести к тому, что системе iSeries будет запрещено отправлять и принимать любые данные IP. В частности, будут заблокированы соединения с Навигатором iSeries, которые применяются для настройки правил фильтрации.

Если правила фильтрации запрещают передавать данные Навигатора iSeries, Навигатор не сможет подключиться к системе iSeries. В этом случае войдите в систему iSeries с помощью другого интерфейса, который по-прежнему работает, например, с помощью консоли управления. Удалите все фильтры из системы с помощью команды RMVTCPTBL. Эта команда также перезапустит серверы *VPN. Заново настройте фильтры и активируйте их.

Настройка правил фильтрации, применяемых до IPSec

Внимание: Эту задачу следует выполнять только в том случае, если вы выключили опцию автоматического создания правил фильтрации стратегий с помощью VPN.

Пара серверов IKE динамически согласовывает и обновляет ключи. IKE применяет стандартный порт 500. Для правильной работы IKE необходимо разрешить передачу дейтаграмм UDP через порт 500. Для этого нужно создать два правила фильтрации: одно для входящих данных, а одно - для исходящих. В этом случае ключи для защиты соединения будут выбираться динамически:

1. В Навигаторе iSeries(TM) разверните значок своего сервера и выберите **—> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Правила обработки пакетов** и выберите пункт **Редактор правил**. Появится окно редактора правил обработки пакетов, предназначенного для создания и изменения правил фильтрации и правил NAT в системе iSeries.
3. На странице с приветствием выберите опцию **Создать файл правил обработки пакетов** и нажмите **OK**.
4. В меню редактора правил обработки пакетов выберите **Вставить —> Фильтр**.
5. На странице **Общие** укажите имя набора правил фильтрации VPN. Рекомендуется создать по крайней мере три различных набора: один для правил фильтрации, применяемых до IPSec, второй для правил фильтрации стратегий и третий для различных правил фильтрации PERMIT и DENY. Имя набора, содержащего правила фильтрации, применяемые до IPSec, должно начинаться с префикса *preipsec*. Например, preipsecfilters.
6. В поле **Действие** выберите значение **PERMIT**.
7. В поле **Направление** выберите значение **OUTBOUND**.
8. Для того чтобы задать **Адрес отправителя**, выберите в первом поле значение **=** и введите во втором поле IP-адрес локального сервера ключей. IP-адрес локального сервера ключей задан в стратегии IKE.
9. Для того чтобы задать **Адрес получателя**, выберите в первом поле значение **=** и введите во втором поле IP-адрес удаленного сервера ключей. Этот адрес указан в стратегии IKE.

10. На странице **Службы** выберите опцию **Служба**. В результате станут доступными поля **Протокол**, **Исходный порт** и **Целевой порт**.
11. В поле **Протокол** выберите значение **UDP**.
12. Для того чтобы задать **Исходный порт**, выберите в первом поле значение **=** и введите во втором поле значение `500`.
13. Укажите соответствующие значения в поле **Целевой порт**.
14. Нажмите кнопку **OK**.
15. Повторите описанные действия для настройки фильтра INBOUND. Укажите то же имя набора и поменяйте адреса местами.

Примечание: для того чтобы разрешить передачу данных IKE по соединению, достаточно задать только одно правило фильтрации, применяемое до IPSec, указав символ подстановки (*) в полях **Направление**, **Адрес отправителя** и **Адрес получателя**. Такой способ настройки более простой, но менее надежный.

“Настройка правила фильтрации стратегии”, чтобы определить данные IP, которые должны будут передаваться по защищенному соединению VPN.

Настройка правила фильтрации стратегии

Внимание: Эту задачу следует выполнять только в том случае, если вы выключили опцию автоматического создания правил фильтрации стратегий с помощью VPN.

Правило фильтрации стратегии (правило с действием IPSEC) указывает, для каких адресов, протоколов и портов будет применяться VPN. Кроме того, оно задает стратегию, которая будет применяться для защиты данных, передаваемых по соединению VPN. Для настройки правила фильтрации стратегии выполните следующие действия:

Примечание: Если вы только что настроили правило фильтрации, применяемое до IPSec (требуется только для динамических соединений), то редактор правил обработки пакетов должен быть по-прежнему открыт. Перейдите к шагу 4.

1. В Навигаторе iSeries(TM) разверните значок своего сервера и выберите **—> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Правила обработки пакетов** и выберите пункт **Редактор правил**. Появится окно редактора правил обработки пакетов, предназначенного для создания и изменения правил фильтрации и правил NAT в системе iSeries.
3. На странице с приветствием выберите опцию **Создать файл правил обработки пакетов** и нажмите **OK**.
4. В меню редактора правил обработки пакетов выберите **Вставить —> Фильтр**.
5. На странице **Общие** укажите имя набора правил фильтрации VPN. Рекомендуется создать по крайней мере три различных набора: один для правил фильтрации, применяемых до IPSec, второй для правил фильтрации стратегий и третий для различных правил фильтрации PERMIT и DENY. Например, можно указать имя `policyfilters`
6. В поле **Действие** выберите значение **IPSEC**. В поле **Направление** будет установлено значение по умолчанию, OUTBOUND, которое изменить нельзя. Несмотря на это, правило фильтрации относится к пакетам, передаваемым в обоих направлениях. Значение OUTBOUND просто поясняет смысл введенных значений. Так, исходные значения являются локальными, а целевые - удаленными.
7. Для того чтобы задать **Адрес отправителя**, выберите в первом поле значение **=** и введите во втором поле IP-адрес локальной конечной точки данных. Этот адрес может представлять диапазон IP-адресов или IP-адрес и маску подсети, если ранее он был определен с помощью функции **Определить адрес**.
8. Для того чтобы задать **Адрес получателя**, выберите в первом поле значение **=** и введите во втором поле IP-адрес удаленной конечной точки данных. Этот адрес может представлять диапазон IP-адресов или IP-адрес и маску подсети, если ранее он был определен с помощью функции **Определить адрес**.
9. В поле **Журнал** укажите уровень ведения журнала.
10. В поле **Имя соединения** выберите определение соединения, для которого должны применяться эти правила фильтрации.

11. (необязательно) Введите описание.
12. На странице **Службы** выберите опцию **Служба**. В результате станут доступными поля **Протокол**, **Исходный порт** и **Целевой порт**.
13. Укажите значения в полях **Протокол**, **Исходный порт** и **Целевой порт**. При необходимости выберите в выпадающем списке звездочку (*). В этом случае VPN будет применяться для передачи данных всех протоколов, работающих через любые порты.
14. Нажмите кнопку **OK**.

Далее вам нужно “Определение интерфейса для правил фильтрации VPN”, для которого должны применяться правила фильтрации.

Примечание: При добавлении правил фильтрации для интерфейса система автоматически добавляет правило DENY для этого интерфейса. Это правило означает, что запрещены все пакеты, которые явно не разрешены. Вы не можете просмотреть или изменить это правило. В результате после активизации правил фильтрации VPN некоторые соединения могут перестать работать. Если помимо данных VPN по интерфейсу будут передаваться другие данные, необходимо явно разрешить (PERMIT) передачу соответствующих пакетов.

Определение интерфейса для правил фильтрации VPN

После настройки правил фильтрации VPN и других правил, необходимых для работы соединений VPN, нужно определить интерфейс, к которому должны применяться эти правила.

Для того чтобы определить интерфейс, к которому должны применяться правила фильтрации VPN, выполните следующие действия:

Примечание: Если вы только что настроили правила обработки пакетов VPN, окно Правила обработки пакетов должно быть по-прежнему открыто. Перейдите к шагу 4.

1. В Навигаторе iSeries(TM) разверните значок своего сервера и выберите **—> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Правила обработки пакетов** и выберите пункт **Редактор правил**. Появится окно редактора правил обработки пакетов, предназначенного для создания и изменения правил фильтрации и правил NAT в системе iSeries.
3. На странице с приветствием выберите опцию **Создать файл правил обработки пакетов** и нажмите **OK**.
4. В окне редактора обработки пакетов выберите **Вставить —> Интерфейс фильтра**.
5. На странице **Общие** укажите **Имя линии**, выбрав в выпадающем списке описание линии, с которой будут связаны правила обработки пакетов VPN.
6. (необязательно) Введите описание.
7. На странице **Наборы фильтров** нажмите кнопку **Добавить** и добавьте созданные наборы правил фильтрации.
8. Нажмите **OK**.
9. Сохраните файл правил. Файл будет сохранен в интегрированной файловой системе с расширением .i3p.
   Примечание: Не сохраняйте файл в следующем каталоге:

   `/QIBM/UserData/OS400/TCPIP/RULEGEN`

   Этот каталог предназначен для внутреннего использования. Если вам впоследствии потребуется выполнить команду RMVTCPTBL *ALL для деактивации правил обработки пакетов, то она удалит все файлы из этого каталога.

После определения интерфейса для правил фильтрации необходимо “Активация правил фильтрации пакетов VPN” правила. После этого вы сможете запустить VPN.

Активация правил фильтрации пакетов VPN

Перед запуском соединений VPN необходимо активировать правила фильтрации пакетов VPN. Эти правила нельзя активировать (или деактивировать), если в системе установлены соединения VPN. Перед активацией правил фильтрации VPN обязательно убедитесь, что с ними не связаны активные соединения.

При настройке соединений VPN с помощью мастера Создать соединение можно выбрать опцию автоматической активации связанных правил фильтрации. Обратите внимание, что если для указанных интерфейсов применяются какие-то другие правила фильтрации, то они будут заменены на правила фильтрации стратегии VPN.

Для того чтобы активировать правила, с помощью редактора правил обработки пакетов, выполните следующие действия:

1. В Навигаторе iSeries(TM) разверните значок своего сервера и выберите **—> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Правила обработки пакетов** и выберите опцию **Активировать**. Появится окно **Активировать правила обработки пакетов**.
3. Укажите, какие правила должны быть активированы: правила, созданные VPN, выбранный файл правил или и то, и другое. Последнюю опцию, например, можно выбрать в том случае, если помимо правил, созданных VPN, для интерфейса должны быть активированы некоторые правила PERMIT и DENY.
4. Выберите интерфейс, для которого должны быть активированы правила. Можно выбрать конкретный интерфейс, идентификатор двухточечной линии, все интерфейсы или все идентификаторы двухточечной линии.
5. Нажмите кнопку **OK**, для того чтобы подтвердить, что нужно проверить и активировать правила для указанных интерфейсов. Система проверит правила на наличие синтаксических и семантических ошибок. Результаты проверки будут показаны в окне сообщений, расположенном в нижней области окна редактора. При наличии сообщения об ошибке щелкните правой кнопкой мыши на этом сообщении и выберите пункт **Перейти к строке**, чтобы была выделена строка файла правил, в которой была найдена ошибка.

После активации правил фильтрации можно “Запуск соединения VPN”.

Запуск соединения VPN

В этом разделе предполагается, что соединение VPN уже настроено. Для запуска соединения VPN выполните следующие действия:

1. В Навигаторе iSeries(TM) разверните значок своего сервера и выберите **—> Сеть —> Стратегии IP**.
2. Если сервер VPN не запущен, щелкните правой кнопкой мыши на пункте **Виртуальная частная сеть** и выберите опцию **Запустить**. Будет запущен сервер VPN.
3. Убедитесь, что правила обработки пакетов “Активация правил фильтрации пакетов VPN” на стр. 46.
4. Разверните список **Виртуальная частная сеть—> Защищенные соединения**.
5. Выберите **Все соединения** для просмотра списка соединений в правой панели.
6. Щелкните правой кнопкой мыши на имени соединения и выберите **Запустить**. Для запуска нескольких соединений выделите их имена, щелкните правой кнопкой мыши и выберите пункт **Запустить**.

Работа с функцией VPN

Все необходимые задачи при работе с VPN можно выполнить с помощью интерфейса, предусмотренного в программе Навигатор iSeries(TM). Ниже перечислены некоторые из них:

- “Запуск соединения VPN”
  Выполните эту задачу для запуска соединений, устанавливаемых локальной системой.
- “Выбор атрибутов по умолчанию для соединений” на стр. 48
  В полях, указанных на страницах создания стратегий и соединений, задаются значения по умолчанию. Вы можете не изменять значения по умолчанию, указанные для уровня защиты, параметров управления ключами сеанса, срока действия ключей и срока действия соединений.
- “Сброс соединений, при работе с которыми возникла ошибка” на стр. 48
  Сброс соединения позволяет перевести его из состояния Ошибка в состояние простоя.
- “Просмотр информации об ошибках” на стр. 48
  Выполните эту задачу для определения причин, по которым не работает соединение.

- “Просмотр атрибутов активного соединения” на стр. 49
  Выполните эту задачу, для того чтобы просмотреть состояние и другие атрибуты активных соединений.
- “Применение функции трассировки сервера VPN” на стр. 49
  Функция трассировки сервера VPN позволяет настроить, включить, выключить и просмотреть результаты трассировки сервера Диспетчера соединений VPN и Диспетчера ключей VPN. Эта функция аналогична команде TRCTCPAPP *VPN, которую можно вызвать в текстовом меню. Однако в отличие от этой команды, данная функция позволяет просматривать результаты трассировки во время работы соединения.
- “Просмотр протоколов заданий сервера VPN” на стр. 50
  Следуя приведенным в этом разделе инструкциям, можно просмотреть протоколы заданий Диспетчера ключей VPN и Диспетчера соединений VPN.
- “Завершение соединения VPN” на стр. 50
  Выполните эту задачу, чтобы завершить активные соединения.
- “Просмотр атрибутов конфигураций защиты (SA)” на стр. 50
  Выполните эту задачу для просмотра атрибутов конфигураций защиты (SA), связанных с активным соединением.
- “Удаление объектов конфигурации VPN” на стр. 50
  Перед удалением объекта конфигурации VPN из базы данных стратегий VPN убедитесь, что это не скажется на работе других соединений и групп соединений VPN.

Выбор атрибутов по умолчанию для соединений

При создании объектов VPN в некоторых полях указываются значения параметров защиты по умолчанию.

Для того чтобы задать значения параметров защиты по умолчанию для соединений VPN, выполните следующие действия:

1. В Навигаторе разверните значок своего сервера и выберите **—> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на значке **VPN** и выберите **Параметры по умолчанию**.
3. Для просмотра дополнительной информации о любой странице и ее полях нажмите на этой странице кнопку **Справка**.
4. После заполнения всех страниц свойств нажмите кнопку **OK**.

Сброс соединений, при работе с которыми возникла ошибка

Для того чтобы сбросить состояние соединения, при работе с которым возникла ошибка, выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Защищенные соединения**.
2. Выберите **Все соединения** для просмотра списка соединений в правой панели.
3. Щелкните правой кнопкой мыши на имени соединения и выберите пункт **Сбросить**. В результате соединение перейдет в состояние простоя. Для того чтобы сбросить несколько соединений, при работе с которыми возникла ошибка, выделите имена этих соединений, щелкните правой кнопкой мыши и выберите пункт **Сбросить**.

Просмотр информации об ошибках

Для просмотра информации об ошибках соединений выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Защищенные соединения**.
2. Выберите **Все соединения** для просмотра списка соединений в правой панели.
3. Щелкните правой кнопкой мыши на значке соединения, ошибки которого вы хотите просмотреть, и выберите пункт **Информация об ошибках**.

Просмотр атрибутов активного соединения

Для просмотра атрибутов активного соединения или соединения по запросу выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Защищенные соединения**.
2. Выберите **Все соединения** для просмотра списка соединений в правой панели.
3. Щелкните правой кнопкой мыши на имени активного соединения или соединения по запросу и выберите пункт **Свойства**
4. Откройте страницу **Текущие атрибуты** для просмотра атрибутов соединения.

В окне программы Навигатор можно просмотреть атрибуты всех соединений. По умолчанию указываются атрибуты Состояние, Описание и Тип соединения. Для того чтобы изменить список показанных атрибутов, выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть—> Стратегии IP—> Виртуальная частная сеть—> Защищенные соединения**.
2. Выберите **Все соединения** для просмотра списка соединений в правой панели.
3. В меню **Объекты** выберите пункт **Столбцы**. Появится окно диалога, позволяющее выбрать атрибуты, которые должны быть показаны в окне программы Навигатор.

Обратите внимание, что внесенные изменения будут сохранены не для отдельного пользователя или PC, а для всей системы.

Применение функции трассировки сервера VPN

Для просмотра результатов трассировки сервера VPN выполните следующие действия:

1. В Навигаторе разверните значок своего сервера и выберите **—> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Виртуальная частная сеть**, выберите **Диагностические средства**, а затем - **Трассировка сервера**.

Для изменения типа данных трассировки, собираемых Диспетчером ключей и Диспетчером соединений VPN, выполните следующие действия:

1. В окне **Виртуальная частная сеть** нажмите

   (Опции).
2. На странице **Диспетчер соединений** укажите тип трассировки, которую должен выполнять диспетчер соединений.
3. В окне **Страница Диспетчера ключей**, укажите тип трассировки, которую должен выполнять Диспетчер ключей.
4. Для просмотра дополнительной информации о любой странице и ее полях нажмите на этой странице кнопку **Справка**.
5. Нажмите **OK** для сохранения изменений.
6. Для включения трассировки нажмите

   (Запустить). Для просмотра свежих данных трассировки нажмите

   (Обновить).

Просмотр протоколов заданий сервера VPN

Для просмотра текущих протоколов заданий Диспетчера ключей VPN или Диспетчера соединений VPN выполните следующие действия:

1. В Навигаторе iSeries(TM) разверните значок своего сервера и выберите **—> Сеть —> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Виртуальная частная сеть**, выберите **Диагностические средства**, а затем выберите задание сервера для просмотра.

Просмотр атрибутов конфигураций защиты (SA)

Вы можете просмотреть атрибуты конфигураций защиты (SA), связанных с активным соединением. Для этого выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Защищенные соединения**.
2. Выберите **Все соединения** для просмотра списка соединений в правой панели.
3. Щелкните правой кнопкой на соответствующем активном соединении и выберите **Конфигурации защиты.** В появившемся окне будут показаны свойства всех SA, связанных с выбранным соединением.

Завершение соединения VPN

Для того чтобы завершить активное соединение или соединение, устанавливаемое по запросу, выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Защищенные соединения**.
2. Выберите **Все соединения** для просмотра списка соединений в правой панели.
3. Щелкните правой кнопкой мыши на имени соединения и выберите пункт **Завершить**. Для того чтобы завершить несколько соединений, выделите их имена, щелкните правой кнопкой мыши и выберите пункт **Завершить**.

Удаление объектов конфигурации VPN

Для того чтобы удалить соединение VPN из базы данных стратегий VPN, выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть —> Стратегии IP —> Виртуальная частная сеть —> Защищенные соединения**.
2. Выберите **Все соединения** для просмотра списка соединений в правой панели.
3. Щелкните правой кнопкой мыши на нужном соединении и выберите пункт **Удалить**.

Устранение неполадок VPN

VPN представляет собой сложную, динамически изменяющуюся технологию, для работы с которой необходимо иметь представление о стандартных технологиях IPSec. Кроме того, необходимо уметь работать с правилами обработки пакетов IP, так как для применения VPN требуется настроить некоторые правила фильтрации. С учетом этого, при работе с соединениями VPN иногда могут возникать ошибки. Некоторые ошибки VPN устранить весьма непросто. Необходимо хорошо знать конфигурацию системы и сети, а также уметь работать с функциями, применяемыми для изменения конфигурации. В приведенных ниже разделах приведены некоторые рекомендации по устранению различных неполадок, которые могут возникнуть при работе с VPN:

- “Устранение неполадок VPN - Введение” на стр. 51
  В этом разделе описаны действия, которые нужно выполнить прежде всего при возникновении неполадки в работе соединения VPN.
- “Часто встречающиеся ошибки в конфигурации VPN и способы их исправления” на стр. 52
  В этом разделе описаны ошибки, возникающие чаще всего, а также способы их исправления.
- “Устранение неполадок VPN с помощью журнала QIPFILTER” на стр. 58
  В этом разделе приведена информация о правилах фильтрации VPN.

- “Устранение неполадок VPN с помощью журнала QVPN” на стр. 60
  В этом разделе приведена информация о передаче данных IP по соединениям.
- “Устранение неполадок VPN с помощью протоколов заданий VPN” на стр. 62
  В этом разделе описаны различные протоколы заданий, которые применяются функцией VPN.
- “Устранение неполадок VPN путем трассировки соединений OS/400” на стр. 70
  В этом разделе описана функция трассировки данных, передаваемых по линии связи.

Устранение неполадок VPN - Введение

Анализ неполадок VPN можно выполнить несколькими способами:

1. Убедитесь, что в системе применена последняя версия временных исправлений программ (PTF).
2. Убедитесь, что в системе выполнены минимальные “Требования к настройке VPN” на стр. 33.
3. Ознакомьтесь со всеми сообщениями об ошибках, содержащимися в окне “Просмотр информации об ошибках” на стр. 48 и “Устранение неполадок VPN с помощью протоколов заданий VPN” на стр. 62 в локальной и удаленной системе. Причина ошибки, возникшей при работе с соединением VPN, может быть связана с любой конечной системой. Проверку следует выполнять для четырех адресов: конечных точек соединения, представляющих адреса, которые функция IPSec указывает в пакетах IP, и конечных точек данных, которые представляют адреса отправителя и получателя пакетов IP.
4. Если для устранения неполадки недостаточно сообщений об ошибках, просмотрите журнал “Устранение неполадок VPN с помощью журнала QIPFILTER” на стр. 58.
5. С помощью “Устранение неполадок VPN путем трассировки соединений OS/400” на стр. 70 системы iSeries(TM) можно получить общую информацию о том, отправляла ли система запросы на подключение и принимала ли система такие запросы.
6. Для локализации неполадки можно воспользоваться командой Трассировка приложения TCP (TRCTCPAPP). Обычно эта команда применяется сотрудниками сервисного представительства IBM(R) для анализа ошибок соединений с помощью данных трассировки.

Другие возможные источники ошибки

Если ошибка возникла после установления соединения, и вы не знаете, с чем она связана, постарайтесь упростить конфигурацию соединения. Например, вместо того чтобы искать причину ошибки сразу во всех компонентах соединения VPN, начните с самого соединения IP. Ниже приведены некоторые рекомендации по пошаговому анализу неполадки VPN, начиная с простого соединения IP и заканчивая сложным соединением VPN:

1. Начните проверку с конфигурации соединения IP, установленного между локальным и удаленным хостом. Удалите все фильтры IP, связанные с интерфейсом в локальной и удаленной системе. Проверьте соединение между локальным и удаленным хостом с помощью команды PING. Успешно ли выполнена проверка?

   Примечание: Откройте приглашение команды PING; введите адрес удаленной системы, нажмите PF10 для просмотра дополнительных параметров и введите IP-адрес локальной системы. Это обязательно нужно сделать в тех случаях, когда в системе существует несколько физических или логических интерфейсов. Если вы не укажете локальный адрес, то в пакетах PING может быть указан неверный адрес.

   Если **да**, перейдите к шагу 2. Если **нет**, проверьте правильность конфигурации IP, состояние интерфейса и записи маршрутизации. Если конфигурация задана правильно, включите трассировку соединения и убедитесь, что запрос PING передается за пределы системы. Если ответ на запрос PING не был получен, то, скорее всего, неполадка связана с сетью или удаленной системой.

   Примечание: Возможно, пакеты PING передаются через промежуточные маршрутизаторы и брандмауэры, выполняющие фильтрацию пакетов IP, которые отбрасывают пакеты PING. Обычно функция PING основана на протоколе ICMP. Если команда PING выполнена, значит соединение

работает правильно. Если команда PING не выполнена, то никаких выводов сделать нельзя. В этом случае рекомендуется установить соединение между двумя системами с помощью другого протокола IP, например, Telnet или FTP.

2. Проверьте правила фильтрации VPN и убедитесь, что они активированы. Запущена ли функция фильтрации? Если **да**, перейдите к шагу 3. Если **нет**, просмотрите сообщения об ошибках, показанные в окне Правила обработки пакетов программы Навигатор. Убедитесь, что в правилах фильтрации не задано применение функции NAT для данных VPN.
3. “Запуск соединения VPN” на стр. 47. Было ли запущено соединение? Если **да**, перейдите к шагу 4. Если **нет**, просмотрите сообщения об ошибках, приведенные в протоколах заданий QTOVMAN и QTOKVPNIKE.
   Для применения VPN необходимо, чтобы провайдер Internet (ISP) и все защищенные шлюзы в сети поддерживали протоколы AH и ESP. Применение протоколов AH и ESP оговаривается в планах защиты, связанных с соединением VPN.
4. Удалось ли установить сеанс пользователя по соединению VPN? Если **да**, значит соединение VPN работает правильно. Если **нет**, убедитесь, что в правилах обработки пакетов, определении группы соединений с динамическим ключом и определении соединения с динамическим ключом не заданы правила фильтрации, отклоняющие данные пользователя.

Часто встречающиеся ошибки в конфигурации VPN и способы их исправления

В этом разделе описаны ошибки, которые чаще всего возникают при работе с VPN, а также действия по их исправлению.

Примечание: Во время настройки VPN создается несколько отдельных объектов конфигурации, каждый из которых необходим для установления соединения VPN. В графическом интерфейсе VPN эти объекты называются стратегиями защиты IP и защищенными соединениями. Когда в этом разделе идет речь об объекте, имеется в виду один из указанных объектов VPN.

Часто встречающиеся сообщения об ошибках

Сообщение	Признак
“Сообщение об ошибке VPN: TCP5B28” на стр. 53	Во время активации правил фильтрации для интерфейса было получено следующее сообщение: TCP5B28 Нарушен порядок CONNECTION_DEFINITION
“Сообщение об ошибке VPN: Объект не найден” на стр. 53	Когда вы щелкаете правой кнопкой мыши на объекте VPN и выбираете пункт **Свойства** или **Удалить**, появляется следующее сообщение: **Объект не найден**.
“Сообщение об ошибке VPN: Значение параметра PINBUF недопустимо” на стр. 54	При запуске соединения появляется следующее сообщение: **Недопустимое значение параметра PINBUF...**
“Сообщение об ошибке VPN: Объект не найден, Удаленный сервер ключей...” на стр. 55	При выборе пункта **Свойства** для соединения с динамическим ключом появляется сообщение о том, что не удалось найти указанный удаленный сервер ключей.
“Сообщение об ошибке VPN: Не удалось обновить объект” на стр. 55	При нажатии кнопки **OK** на странице свойств группы соединений с динамическим ключом или статического соединения появляется сообщение о том, что системе не удалось обновить объект.
“Сообщение об ошибке VPN: Не удалось зашифровать ключ...” на стр. 55	Получено сообщение о том, что системе не удалось зашифровать ключи, так как значение QRETSVRSEC не равно 1.

“Сообщение об ошибке VPN: CPF9821” на стр. 56	При попытке развернуть или открыть контейнер Стратегии IP в окне Навигатора iSeries(TM) появляется сообщение CPF9821 - Нет прав доступа к программе QTFRPRS из библиотеки QSYS.

Прочие ошибки

Ошибка	**Признак**
“Ошибка VPN: Не показан ни один ключ” на стр. 56	При просмотре свойств статического соединения не показаны подготовленные ключи и ключи алгоритмов.
“Ошибка VPN: При работе с правилами обработки пакетов появляется приглашение на вход в другую систему” на стр. 56	При первом запуске интерфейса Правила обработки пакетов в программе Навигатор появилось приглашение на вход в систему, отличную от текущей системы.
“Ошибка VPN: В окне программы Навигатор не указано состояние соединения” на стр. 56	Для соединения не задано значение в столбце **Состояние** окна программы Навигатор.
“Ошибка VPN: После завершения соединения оно по-прежнему осталось активным” на стр. 57	Несмотря на то, что вы завершили соединение, в окне программы Навигатор по-прежнему указано, что соединение активно.
“Ошибка VPN: недоступен алгоритм шифрования 3DES” на стр. 57	При работе с преобразованием стратегии IKE, преобразованием стратегии защиты данных или статическим соединением нельзя выбрать алгоритм шифрования 3DES.
“Ошибка VPN: В окне Навигатора показаны неправильные столбцы данных” на стр. 57	Вы задали список столбцов, которые должны быть показаны в окне программы Навигатор при работе с соединениями VPN, однако в окне показаны другие столбцы.
“Ошибка VPN: Не удалось деактивировать правила фильтрации” на стр. 57	При попытке деактивировать текущий набор правил фильтрации в окне результатов появляется сообщение `Не удалось деактивировать правила фильтрации`.
“Ошибка VPN: Изменена группа соединений, связанная с соединением” на стр. 57	При создании соединения с динамическим ключом была задана группа соединений с динамическим ключом и идентификатор удаленного сервера ключей. Позднее при просмотре свойств соединения вы обнаружили, что на странице Общие задан правильный идентификатор удаленного сервера ключей, но другая группа соединений с динамическим ключом.

Сообщение об ошибке VPN: TCP5B28

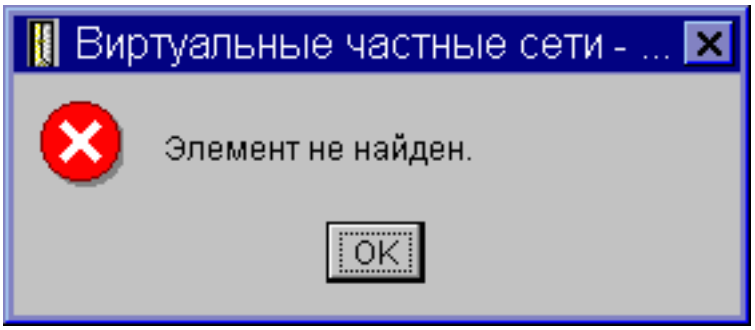
Признак:
Во время активации правил фильтрации для интерфейса было получено следующее сообщение:

```
TCP5B28: Нарушен порядок CONNECTION_DEFINITION
```

Возможные причины:
Правила фильтрации, выбранные для активации, содержат определения соединений, порядок которых не совпадает с порядком определений в наборе правил, активированных ранее. Для исправления ошибки проще всего активировать файл правил для **всех интерфейсов**, а не для отдельного интерфейса.

Сообщение об ошибке VPN: Объект не найден

Признак:
Когда вы щелкнули правой кнопкой мыши на значке объекта, расположенном в окне Виртуальная частная сеть, и выбрали пункт **Свойства** или **Удалить**, появилось следующее сообщение:

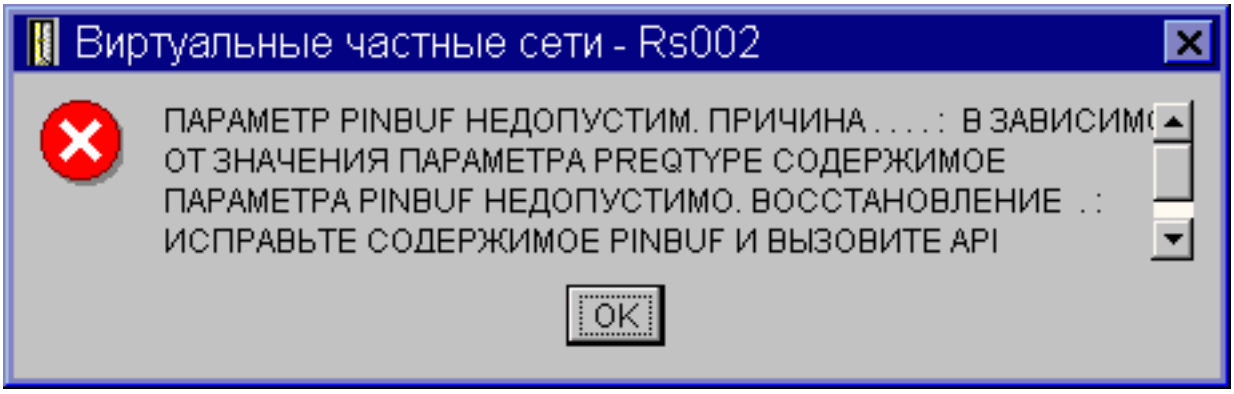


Возможные причины:

- Возможно, объект был удален или переименован, а в окне показана старая информация. В этом случае объект по-прежнему будет показан в окне Виртуальная частная сеть. Выберите в меню **Вид** пункт **Обновить**. Если объект по-прежнему показан в окне Виртуальная частная сеть, перейдите к следующему объекту в списке.
- Во время настройки свойств объекта могла возникнуть ошибка соединения, установленного между сервером VPN и системой iSeries(TM). Большинство объектов, показанных в окне Виртуальная частная сеть, представляют несколько объектов из базы данных стратегий VPN. Это означает, что из-за ошибки связи некоторые объекты базы данных могут быть по-прежнему связаны с объектом VPN. При создании или обновлении объекта возникнет ошибка, так как данные не будут синхронизированы. Для исправления ошибки нажмите кнопку **OK** в окне сообщения об ошибке. Появится окно свойств объекта, с которым связана ошибка. Значение будет указано только в поле Имя. Во всех остальных полях значение не будет указано или будет указано значение по умолчанию. Задайте правильные атрибуты объекта и нажмите **OK** для сохранения изменений.
- Аналогичная ошибка возникнет при попытке удалить объект. Для исправления ошибки заполните поля в окне свойств, которое появится после нажатия кнопки **OK** в окне сообщения об ошибке. В результате будут восстановлены все ссылки на базу данных стратегий VPN. После этого можно удалить объект.

Сообщение об ошибке VPN: Значение параметра PINBUF недопустимо

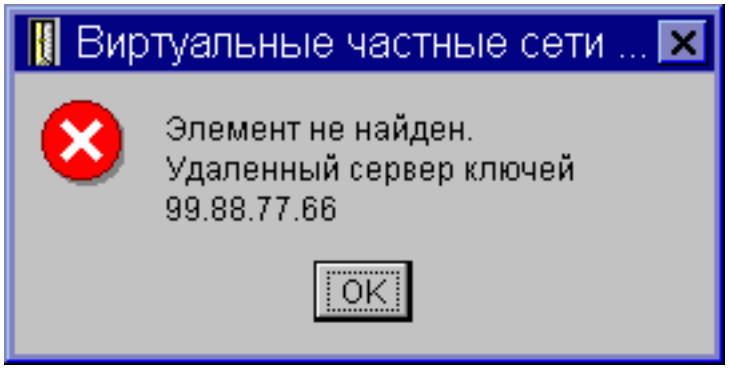
Признак:
При запуске соединения появилось следующее сообщение:



Возможные причины:
Эта ошибка возникает в том случае, если в системе выбрана локаль, не поддерживающая строчные символы. Для исправления ошибки убедитесь, что имена всех объектов содержат только прописные символы, либо измените локаль системы.

Сообщение об ошибке VPN: Объект не найден, Удаленный сервер ключей...

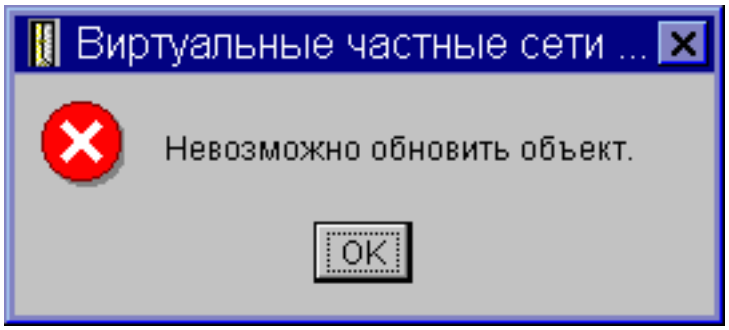
Признак:
При выборе пункта **Свойства** для соединения с динамическим ключом появилось следующее сообщение:



Возможные причины:
Эта ошибка возникает в том случае, если при создании соединения был задан идентификатор удаленного сервера ключей, а этот сервер был впоследствии удален из группы соединений с динамическим ключом. Для исправления ошибки нажмите кнопку **OK** в окне сообщения об ошибке. Появится окно свойств соответствующей группы соединений с динамическим ключом. В этом окне добавьте удаленный сервер ключей в группу или выберите другой идентификатор удаленного сервера ключей. Для сохранения внесенных изменений нажмите кнопку **OK**.

Сообщение об ошибке VPN: Не удалось обновить объект

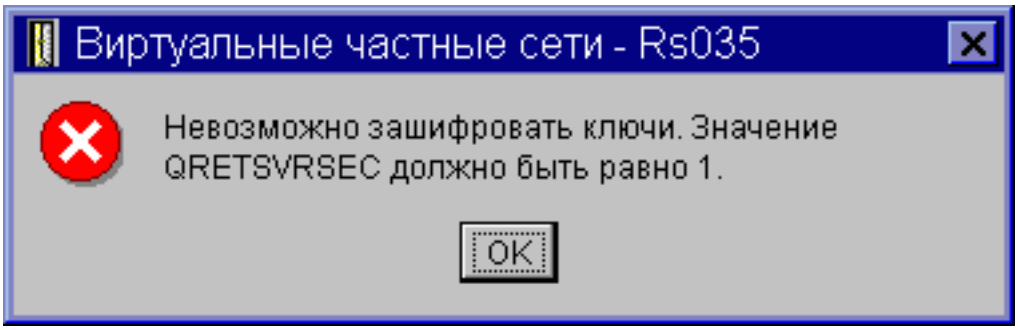
Признак:
При нажатии кнопки **OK** на странице свойств группы соединений с динамическим ключом или статического соединения появилось следующее сообщение:



Возможные причины:
Эта ошибка возникает в том случае, если изменяемый объект применяется активным соединением. Такие объекты изменять нельзя. Для изменения объекта определите, к какому активному соединению он относится, щелкните правой кнопкой мыши на значке этого соединения и выберите пункт **Завершить**.

Сообщение об ошибке VPN: Не удалось зашифровать ключ...

Признак:
Появилось следующее сообщение об ошибке:



Возможные причины:
Системное значение QRETSVRSEC определяет, разрешено ли в системе хранить зашифрованные ключи. Если это значение равно 0, то подготовленные ключи и ключи алгоритмов статического соединения нельзя сохранить в базе данных стратегий VPN. Для исправления этой ошибки откройте сеанс эмуляции 5250. Введите в командной строке `wrksysval` и нажмите **Enter**. Найдите в списке значение QRETSVRSEC и введите напротив него опцию 2 (изменить). На следующей панели введите 1 и нажмите **Enter**.

Сообщение об ошибке VPN: CPF9821

Признак:
При попытке развернуть контейнер Стратегии IP в Навигаторе iSeries(TM), появляется сообщение `CPF9821 Нет прав доступа к программе QTFRPRS из библиотеки QSYS`.

Возможные причины:
У вас нет прав доступа на просмотр правил обработки пакетов или на работу с диспетчером соединений VPN. После получения прав доступа *IOSYSCFG вы сможете работать с функциями из раздела Правила обработки пакетов в программе Навигатор.

Ошибка VPN: Не показан ни один ключ

Признак:
Для статического соединения не показаны подготовленные ключи и ключи алгоритмов.

Возможные причины:
Такая ошибка возникает в том случае, когда системное значение QRETSVRSEC снова становится равным 0. При обнулении этого системного значения из базы данных стратегий VPN удаляются все ключи. Для исправления ошибки установите системное значение равным 1 и заново укажите все ключи. За дополнительной информацией обратитесь к разделу “Сообщение об ошибке VPN: Не удалось зашифровать ключ...” на стр. 55.

Ошибка VPN: При работе с правилами обработки пакетов появляется приглашение на вход в другую систему

Признак:
При первом запуске интерфейса Правила обработки пакетов появилось приглашение на вход в систему, отличную от текущей.

Возможные причины:
Правила обработки пакетов хранятся в интегрированной файловой системе в формате Unicode. Вход в другую систему необходим программе iSeries(TM) Access для получения необходимых таблиц преобразования Unicode. Такое приглашение не будет появляться в дальнейшем.

Ошибка VPN: В окне программы Навигатор не указано состояние соединения

Признак:
Для соединения не показано значение в столбце **Состояние** окна программы Навигатор.

Возможные причины:
Если состояние соединения не указано, значит соединение находится в процессе запуска. Другими словами, соединение еще не запущено, и ошибки не обнаружены. После обновления содержимого окна в качестве состояния соединения будет указано одно из следующих значений: Ошибка, Активно, По запросу или Простаивает.

Ошибка VPN: После завершения соединения оно по-прежнему осталось активным

Признак:
Несмотря на то, что вы завершили соединение, в окне программы Навигатор по-прежнему указано, что соединение активно.

Возможные причины:
Обычно такая ситуация возникает в том случае, если пользователь не обновил содержимое окна программы Навигатор. В окне показана устаревшая информация. Для того чтобы обновить содержимое окна, выберите в меню **Вид** пункт **Обновить**.

Ошибка VPN: недоступен алгоритм шифрования 3DES

Признак:
При работе с преобразованием стратегии IKE, преобразованием стратегии защиты данных или статическим соединением нельзя выбрать алгоритм шифрования 3DES.

Возможные причины:
Скорее всего, в системе установлен продукт Cryptographic Access Provider AC2 (5722-AC2), а не продукт Cryptographic Access Provider AC3 (5722-AC3). Продукт AC2 поддерживает только алгоритм шифрования DES, так как в нем установлено ограничение на длину ключа.

Ошибка VPN: В окне Навигатора показаны неправильные столбцы данных

Признак:
Вы задали список столбцов, которые должны быть показаны в окне программы Навигатор при работе с соединениями VPN, однако в окне показаны другие столбцы.

Возможные причины:
Изменения, внесенные в список столбцов, сохраняются не для отдельного пользователя или компьютера, а для всей системы. Вероятно, другой пользователь изменил список столбцов, показанных в окне. Эти изменения действуют на всех пользователей, работающих с соединениями в данной системе.

Ошибка VPN: Не удалось деактивировать правила фильтрации

Признак:
При попытке деактивировать текущий набор правил фильтрации в окне результатов появляется сообщение Не удалось деактивировать правила фильтрации.

Возможные причины:
Обычно это сообщение об ошибке означает, что в системе есть по крайней мере одно активное соединение VPN. Необходимо завершить все соединения, которые находятся в состоянии Активно. Для этого щелкните правой кнопкой мыши на активном соединении и выберите пункт **Завершить**. После завершения всех активных соединений можно деактивировать правила фильтрации.

Ошибка VPN: Изменена группа соединений, связанная с соединением

Признак:
При создании соединения с динамическим ключом была задана группа соединений с динамическим ключом и идентификатор удаленного сервера ключей. Позднее при просмотре свойств соединения с помощью пункта меню **Свойства** вы обнаружили, что на странице свойств **Общие** указан правильный идентификатор удаленного сервера ключей, но другая группа соединений с динамическим ключом.

Возможные причины:
В базе данных стратегий VPN хранится только идентификатор удаленного сервера ключей, связанный с соединением с динамическим ключом. При поиске стратегии для удаленного сервера ключей VPN находит первую группу соединений с динамическим ключом, в свойствах которой задан идентификатор удаленного сервера ключей. При просмотре свойств соединения будет указано имя найденной группы соединений с динамическим ключом. Если вы не хотите связывать идентификатор удаленного сервера ключей с группой соединений с динамическим ключом, выполните одно из следующих действий:

1. Удалите идентификатор удаленного сервера ключей из определения группы соединений с динамическим ключом.
2. На левой панели интерфейса VPN разверните список **По группам**, выберите необходимую группу соединений с динамическим ключом и перенесите ее в начало таблицы, расположенной на правой панели. В этом случае VPN начнет поиск идентификатора удаленного сервера ключей с этой группы.

Устранение неполадок VPN с помощью журнала QIPFILTER

Журнал QIPFILTER расположен в библиотеке QUSRSYS и содержит информацию о наборах правил фильтрации, а также о пропущенных и отклоненных дейтаграммах IP. Опция ведения журнала задается в правилах фильтрации.

Включение опции ведения журнала фильтрации пакетов IP
Ведение журнала QIPFILTER можно активизировать с помощью редактора правил обработки пакетов программы Навигатор iSeries(TM). Опция ведения протокола настраивается для каждого правила фильтрации отдельно. Ведение протокола нельзя включить сразу для всех дейтаграмм IP, отправляемых и принимаемых системой.

Примечание: Перед включением функции ведения журнала QIPFILTER необходимо деактивировать правила фильтрации.

Для того чтобы включить функцию ведения журнала для отдельного правила фильтрации, выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть—> Стратегии IP**.
2. Щелкните правой кнопкой мыши на пункте **Правила обработки пакетов** и выберите опцию **Настройка**. Появится окно Правила обработки пакетов.
3. Откройте файл правил фильтрации.
4. Дважды щелкните на правиле фильтрации, для которого нужно включить опцию ведения журнала.
5. На странице **Общие** укажите значение **Полное** в поле **Ведение журнала**, как показано в приведенном выше окне диалога. Для выбранного правила фильтрации будет включена функция ведения протокола.
6. Нажмите кнопку **OK**.
7. Сохраните и активируйте измененный файл правил фильтрации.

При обнаружении дейтаграммы IP, соответствующей правилу фильтрации, в журнал QIPFILTER будет добавлена запись.

Применение журнала QIPFILTER
OS/400(R) автоматически создает журнал, когда правила фильтрации пакетов IP активируются в первый раз. Для просмотра записей журнала откройте журнал или сохраните его в файле вывода.

Скопировав записи журнала в файл вывода, можно легко просматривать различные записи с помощью таких утилит создания запросов, как Query/400 или SQL. При необходимости вы можете написать собственные программы на языке высокого уровня для обработки записей в файле вывода.

Ниже приведен пример применения команды Показать журнал (DSPJRN):

```
DSPJRN JRN(QIPFILTER) JRNCDE((M)) ENTTYP((TF)) OUTPUT(*OUTFILE)
    OUTFILFMT(*TYPE4) OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

Для того чтобы скопировать записи журнала QIPFILTER в файл вывода, выполните следующие действия:

1. Создайте копию системного файла вывода QSYS/QATOFIPF в пользовательской библиотеке с помощью команды Создать копию объекта (CRTDUPOBJ). Ниже приведен пример применения команды CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOFIPF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
        NEWOBJ(myfile)
   ```

2. С помощью команды Показать журнал (DSPJRN) скопируйте записи из журнала QUSRSYS/QIPFILTER в файл вывода, созданный на предыдущем шаге.

Если в команде DSPJRN будет указан несуществующий файл вывода, система создаст этот файл, однако он не будет содержать правильных описаний полей.

Примечание: В журнал QIPFILTER заносятся записи о пропущенных и отклоненных пакетах для тех правил фильтрации, в которых выбран полный режим ведения журнала. Например, если заданы только разрешающие правила фильтрации, все дейтаграммы IP, передача которых явно не разрешена, отклоняются. Информация о таких дейтаграммах не заносится в журнал. В целях анализа неполадок можно добавить правило фильтрации, запрещающее передачу всех пакетов, и указать в этом правиле полный режим ведения журнала. В этом случае в журнал будут добавляться записи обо всех дейтаграммах IP, которые были отклонены системой. Не рекомендуется включать опцию ведения журнала для всех правил фильтрации, так как это может негативно сказаться на производительности. После проверки наборов правил сократите число правил, для которых включена опция ведения журнала.

В разделе “Поля журнала QIPFILTER” приведена таблица с описанием файла вывода QIPFILTER.

Поля журнала QIPFILTER

В приведенной ниже таблице описаны поля файла вывода QIPFILTER:

Имя поля	Длина поля	Числовое	Описание	Комментарий
TFENTL	5	Да	Длина записи	
TFSEQN	10	Да	Порядковый номер	
TFCODE	1	Нет	Код журнала	Всегда равен M
TFENTT	2	Нет	Тип записи	Всегда равен TF
TFTIME	26	Нет	Системное время SAA	
TFJOB	10	Нет	Имя задания	
TFUSER	10	Нет	Пользовательский профайл	
TFNBR	6	Да	Номер задания	
TFPGM	10	Нет	Имя программы	
TFRES1	51	Нет	Зарезервировано	
TFUSPF	10	Нет	Пользователь	
TFSYMN	8	Нет	Имя системы	
TFRES2	20	Нет	Зарезервировано	
TFRESA	50	Нет	Зарезервировано	
TFLINE	10	Нет	Описание линии	*ALL, если TFREVT равно U*; пустое значение, если TFREVT равно L*; имя линии, если TFREVT равно L

Имя поля	Длина поля	Числовое	Описание	Комментарий
TFREVT	2	Нет	Событие правила	L* или L, если правила загружены. U*, если правила не загружены; A, если выполнено действие, указанное в фильтре
TFPDIR	1	Нет	Направление передачи пакетов IP	O - исходящее, I - входящее
TFRNUM	5	Нет	Номер правила	Номер правила в активном файле правил
TFACT	6	Нет	Выполненное действие	PERMIT, DENY или IPSEC
TFPROT	4	Нет	Транспортный протокол	1 - ICMP 6 - TCP 17 - UDP 50 - ESP 51 - AH
TFSRCA	15	Нет	IP-адрес отправителя	
TFSRCP	5	Нет	Исходный порт	Произвольное значение, если TFPROT= 1 (ICMP)
TFDSTA	15	Нет	IP-адрес получателя	
TFDSTP	5	Нет	Целевой порт	Произвольное значение, если TFPROT= 1 (ICMP)
TFTEXT	76	Нет	Дополнительный текст	Содержит описание, если TFREVT= L* или U*

Устранение неполадок VPN с помощью журнала QVPN

Информация о данных и соединениях IP заносится в отдельный журнал VPN, который называется QVPN. Этот журнал расположен в библиотеке QUSRSYS. Код журнала равен M, тип журнала равен TS. Этот журнал не нужен для повседневной работы. Он применяется для устранения неполадок и проверки правильности конфигурации системы, ключей и соединений. Например, по содержимому протокола можно определить, какие операции выполняются над передаваемыми пакетами, а также узнать текущее состояние VPN.

Включение функции ведения журнала VPN

Журнал VPN можно активизировать с помощью интерфейса виртуальной частной сети, предусмотренного в программе Навигатор iSeries(TM). Журнал нельзя активизировать сразу для всех соединений VPN. Опция ведения журнала отдельно настраивается для каждой группы соединений с динамическим ключом и каждого статического соединения.

Для того чтобы включить функцию ведения журнала для отдельной группы соединений с динамическим ключом или статического соединения, выполните следующие действия:

1. В окне программы Навигатор разверните значок своего сервера **—> Сеть—> Стратегии IP—> Виртуальная частная сеть—> Защищенные соединения.**
2. Для работы с группой соединений разверните список **По группам** и щелкните правой кнопкой мыши на имени группы соединений с динамическим ключом, для которой нужно включить опцию ведения журнала. Выберите пункт **Свойства.**
3. Для работы со статическим соединением разверните список **Все соединения** и щелкните правой кнопкой мыши на имени статического соединения, для которого нужно включить опцию ведения журнала.

4. На странице **Общие** выберите уровень ведения журнала. Существует четыре уровня. Они перечислены ниже:
   Нет
   Журнал не будет вестись для этой группы соединений.
   Все
   В журнал будет заноситься информация обо всех действиях над соединениями, в том числе о запуске и завершении соединений, а также сведения об изменении ключа и передаче данных IP.
   Действия над соединениями
   В журнал будет заноситься информация о таких действиях над соединениями, как запуск и завершение соединений.
   Передача пакетов IP
   В журнал будет заноситься информация обо всех данных VPN, передаваемых по этому соединению. Новая запись будет заноситься в журнал при каждом применении правила фильтрации. Информация о потоке данных IP записывается в журнал QIPFILTER в библиотеке QUSRSYS.
5. Нажмите **OK**.
6. Для включения функции ведения журнала запустите соединение.

Примечание: Перед выключением функции ведения журнала для соединения убедитесь, что это соединение не активно. Перед включением или выключением функции ведения журнала для группы соединений, убедитесь, что ни одно соединение из этой группы не активно.

Применение журнала VPN
Для просмотра записей журнала VPN откройте журнал или сохраните его в файле вывода.

Скопировав записи журнала в файл вывода, можно легко просматривать различные записи с помощью таких утилит создания запросов, как Query/400 или SQL. При необходимости вы можете написать собственные программы на языке высокого уровня для обработки записей в файле вывода. Ниже приведен пример применения команды Показать журнал (DSPJRN):

```
DSPJRN JRN(QVPN) JRNCDE((M)) ENTTYP((TS)) OUTPUT(*OUTFILE) OUTFILFMT(*TYPE4)
    OUTFILE(mylib/myfile) ENTDTALEN(*VARLEN *CALC)
```

Для того чтобы скопировать записи журнала VPN в файл вывода, выполните следующие действия:

1. Создайте копию системного файла вывода QSYS/QATOVSOF в пользовательской библиотеке. Для этого вызовите команду Создать копию объекта (CRTDUPOBJ). Ниже приведен пример применения команды CRTDUPOBJ:

   ```
   CRTDUPOBJ OBJ(QATOVSOF) FROMLIB(QSYS) OBJTYPE(*FILE) TOLIB(mylib)
        NEWOBJ(myfile)
   ```

2. С помощью команды Показать журнал (DSPJRN) скопируйте записи из журнала QUSRSYS/QVPN в файл вывода, созданный на предыдущем шаге. Если в команде DSPJRN будет указан несуществующий файл вывода, система создаст этот файл, однако он не будет содержать правильных описаний полей.

В разделе “Поля журнала QVPN” описаны поля файла вывода QVPN.

Поля журнала QVPN

В приведенной ниже таблице описаны поля файла вывода QVPN:

Имя поля	Длина поля	Числовое	Описание	Комментарий
TSENTL	5	Да	Длина записи	
TSSEQN	10	Да	Порядковый номер	
TSCODE	1	Нет	Код журнала	Всегда равен M
TSENTT	2	Нет	Тип записи	Всегда равен TS
TSTIME	26	Нет	Системное время записи SAA	
TSJOB	10	Нет	Имя задания	

Имя поля	Длина поля	Числовое	Описание	Комментарий
TSUSER	10	Нет	Пользователь, запустивший задание	
TSNBR	6	Да	Номер задания	
TSPGM	10	Нет	Имя программы	
TSRES1	51	Нет	Не применяется	
TSUSPF	10	Нет	Пользовательский профайл	
TSSYNM	8	Нет	Имя системы	
TSRES2	20	Нет	Не применяется	
TSRESA	50	Нет	Не применяется	
TSESDL	4	Да	Длина данных	
TSCMPN	10	Нет	Компонент VPN	
TSCONM	40	Нет	Имя соединения	
TSCOTY	10	Нет	Тип соединения	
TSCOS	10	Нет	Состояние соединения	
TSCOSD	8	Нет	Дата запуска	
TSCOST	6	Нет	Время запуска	
TSCOED	8	Нет	Дата завершения	
TSCOET	6	Нет	Время завершения	
TSTRPR	10	Нет	Транспортный протокол	
TSLCAD	43	Нет	Адрес локального клиента	
TSLCPR	11	Нет	Локальные порты	
TSRCAD	43	Нет	Адрес удаленного клиента	
TSCPR	11	Нет	Удаленные порты	
TSLEP	43	Нет	Локальная конечная точка	
TSREP	43	Нет	Удаленная конечная точка	
TSCORF	6	Нет	Число обновлений	
TSRFDA	8	Нет	Дата следующего обновления	
TSRFTI	6	Нет	Время следующего обновления	
TSRFLS	8	Нет	Срок действия обновления	
TSSAPH	1	Нет	Этап SA	
TSAUTH	10	Нет	Способ идентификации	
TSENCR	10	Нет	Способ шифрования	
TSDHGR	2	Нет	Группа Diffie-Hellman	
TSERRC	8	Нет	Код ошибки	

Устранение неполадок VPN с помощью протоколов заданий VPN

Если при работе с соединением VPN возникла ошибка, рекомендуется проанализировать протоколы заданий. Информация об ошибках и прочая информация о среде VPN содержится в нескольких протоколах заданий.

Если соединение установлено между двумя серверами iSeries(TM), проанализируйте протоколы заданий на обоих серверах. Если вам не удалось запустить динамическое соединение, необходимо узнать, что произошло в удаленной системе.

Задания VPN (QTOVMAN и QTOKVPNIKE) выполняются в подсистеме QSYSWRK. “Просмотр протоколов заданий сервера VPN” на стр. 50 с помощью Навигатора.

В этом разделе описаны основные задания, связанные с VPN. Ниже указаны имена и назначение этих заданий:

QTCPIP
Основное задание, запускающее все интерфейсы TCP/IP. Если возникла общая неполадка TCP/IP, проанализируйте протокол задания QTCPIP.

QTOKVPNIKE
Задание QTOKVPNIKE является заданием диспетчера ключей VPN. Диспетчер ключей VPN применяет порт UDP с номером 500 для работы с протоколом IKE.

QTOVMAN
Это задание диспетчера соединений VPN. В протокол этого задания заносятся “Часто встречающиеся сообщения об ошибках Диспетчера соединений VPN” обо всех неудачных попытках установить соединение.

QTPPANSxxx
Это задание применяется для обслуживания коммутируемых соединений PPP. Оно отвечает на запросы о подключении, если в профайле PPP указано значение *ANS.

QTPPPCTL
Это задание PPP для обслуживания коммутируемых соединений.

QTPPPL2TP
Это задание диспетчера L2TP. Если при настройке туннеля L2TP возникла ошибка, просмотрите сообщения из протокола этого задания.

Часто встречающиеся сообщения об ошибках Диспетчера соединений VPN

В этом разделе описаны наиболее часто встречающиеся сообщения об ошибках Диспетчера соединений VPN.

Обычно при возникновении ошибки, связанной с соединением VPN, Диспетчер соединений VPN заносит в протокол задания QTOVMAN два сообщения. В первом сообщении приведены сведения об ошибке. Эти сведения можно просмотреть в программе Навигатор, щелкнув правой кнопкой мыши на имени соединения и выбрав пункт **Информация об ошибках**.

Второе сообщение содержит описание операции, при выполнении которой возникла ошибка. Примером такой операции может служить запуск или завершение соединения. В число таких сообщений входят, в частности, TCP8601, TCP8602 и TCP860A.

Сообщения об ошибках Диспетчера соединений VPN

Сообщение	Причина	Исправление
TCP8601 Не удалось установить соединение VPN [*имя соединения*]	Ниже перечислены коды возможных причин, по которым не удалось установить соединение VPN: *0* - Подробная информация содержится в предыдущем сообщении протокола задания, связанном с этим соединением VPN. *1* - Конфигурация стратегии VPN. *2* - Сбой в сети. *3* - Диспетчеру ключей VPN не удалось согласовать новую конфигурацию защиты. *4* - Неправильно настроена удаленная конечная точка соединения. *5* - Диспетчер ключей VPN не ответил на запрос Диспетчера соединений VPN. *6* - Не удалось загрузить компонент защиты IP, связанный с соединением VPN. *7* - Ошибка компонента PPP.	1. Просмотрите остальные сообщения в “Просмотр протоколов заданий сервера VPN” на стр. 50. 2. Устраните причины возникновения ошибок и повторите операцию. 3. С помощью программы Навигатор “Просмотр атрибутов активного соединения” на стр. 49. Если соединение не удалось запустить, оно находится в состоянии Ошибка.
TCP8602 Не удалось завершить соединение VPN [*имя соединения*]	Был получен запрос на завершение соединения VPN, однако соединение не было завершено или было завершено с ошибкой. Ниже перечислены коды возможных причин: *0* - Подробная информация содержится в предыдущем сообщении протокола задания, связанном с этим соединением VPN. *1* - Соединение VPN не существует. *2* - Внутренняя ошибка связи Диспетчера ключей VPN. *3* - Внутренняя ошибка связи компонента IPSec. *4* - Ошибка связи удаленной конечной точки соединения VPN.	1. Просмотрите остальные сообщения в “Просмотр протоколов заданий сервера VPN” на стр. 50. 2. Устраните причины возникновения ошибок и повторите операцию. 3. С помощью программы Навигатор “Просмотр атрибутов активного соединения” на стр. 49. Если соединение не удалось запустить, оно находится в состоянии Ошибка.

Сообщение	Причина	Исправление
TCP8604 При запуске соединения VPN [*имя соединения*] возникла ошибка	Не удалось установить соединение VPN. Ниже перечислены коды возможных причин: *1* - Не удалось преобразовать имя удаленного хоста в IP-адрес. *2* - Не удалось преобразовать имя локального хоста в IP-адрес. *3* - Не загружено правило фильтрации стратегии VPN, связанное с данным соединением VPN. *4* - Указанный пользователем ключ недопустим для связанного с ним алгоритма. *5* - Значение инициализации соединения VPN запрещает выполнение указанного действия. *6* - Роль системы, заданная для соединения VPN, не совпадает с информацией, заданной в группе соединений. *7* - Зарезервировано. *8* - Конечные точки данных соединения VPN (локальные и удаленные адреса и службы) не совпадают с информацией, заданной в группе соединений. *9* - Неверный тип идентификатора.	1. Просмотрите остальные сообщения в “Просмотр протоколов заданий сервера VPN” на стр. 50. 2. Устраните причины возникновения ошибок и повторите операцию. 3. С помощью программы Навигатор проверьте и при необходимости скорректируйте конфигурацию стратегии VPN. Убедитесь, что правильно заданы параметры группы соединений с динамическим ключом, связанной с этим соединением.
TCP8605 Диспетчеру соединений VPN не удалось обратиться к Диспетчеру ключей VPN	Для выбора конфигурации защиты для динамического соединения VPN Диспетчеру соединений VPN требуется обратиться к службам Диспетчера ключей VPN. Диспетчеру соединений VPN не удалось подключиться к Диспетчеру ключей VPN.	1. Просмотрите остальные сообщения в “Просмотр протоколов заданий сервера VPN” на стр. 50. 2. С помощью команды NETSTAT OPTION(*IFC) убедитесь, что интерфейс *LOOPBACK активен. 3. Завершите работу сервера VPN с помощью команды ENDTCPSVR SERVER(*VPN). Снова запустите сервер VPN с помощью команды STRTCPSRV SERVER(*VPN). **Примечание:** при выполнении этой операции будут завершены все текущие соединения VPN.

Сообщение	Причина	Исправление
TCP8606 Диспетчеру ключей VPN не удалось установить конфигурацию защиты, запрошенную для соединения [*имя соединения*]	Диспетчеру ключей VPN не удалось установить запрошенную конфигурацию защиты. Ниже перечислены коды возможных причин: *24* - Диспетчеру ключей VPN не удалось идентифицировать соединение обмена ключами. *8300* - При согласовании параметров соединения обмена ключами Диспетчера ключей VPN возникла ошибка. *8306* - Не найден локальный подготовленный ключ. *8307* - Не найдена удаленная стратегия IKE этапа 1. *8308* - Не найден удаленный подготовленный ключ. *8327* - При согласовании параметров соединения обмена ключами Диспетчера ключей VPN возник тайм-аут. *8400* - Во время согласования параметров соединения VPN Диспетчера ключей VPN возникла ошибка. *8407* - Не найдена удаленная стратегия IKE этапа 2. *8408* - При согласовании параметров соединения VPN Диспетчера ключей VPN возник тайм-аут. *8500 и 8509* - В сети Диспетчера ключей VPN возникла ошибка.	1. Просмотрите остальные сообщения в “Просмотр протоколов заданий сервера VPN” на стр. 50. 2. Устраните причины возникновения ошибок и повторите операцию. 3. С помощью программы Навигатор проверьте и при необходимости скорректируйте конфигурацию стратегии VPN. Убедитесь, что правильно заданы параметры группы соединений с динамическим ключом, связанной с этим соединением.
TCP8608 Соединению VPN [*имя соединения*] не удалось назначить адрес NAT	В параметрах группы соединений с динамическим ключом или соединения обмена данными было указано, что для некоторых адресов требуется выполнить преобразование NAT. Это преобразование выполнить не удалось. Ниже перечислены коды возможных причин: *1* - Адрес, который должен быть преобразован с помощью NAT, не является единичным IP-адресом. *2* - Заняты все доступные адреса.	1. Просмотрите остальные сообщения в “Просмотр протоколов заданий сервера VPN” на стр. 50. 2. Устраните причины возникновения ошибок и повторите операцию. 3. С помощью программы Навигатор проверьте и при необходимости скорректируйте стратегию VPN. Убедитесь, что для группы соединений с динамическим ключом, связанной с этим соединением, заданы правильные адреса.
TCP8620 Локальная конечная точка соединения недоступна	Не удалось установить соединение VPN, так как локальная конечная точка соединения недоступна.	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. С помощью команды NETSTAT OPTION(*IFC) убедитесь, что локальная конечная точка соединения определена и запущена. 3. Устраните причины возникновения ошибок и повторите операцию.

Сообщение	Причина	Исправление
TCP8621 Локальная конечная точка данных недоступна	Не удалось установить соединение VPN, так как локальная конечная точка данных недоступна.	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. С помощью команды NETSTAT OPTION(*IFC) убедитесь, что локальная конечная точка соединения определена и запущена. 3. Устраните причины возникновения ошибок и повторите операцию.
TCP8622 Режим открытой передачи не поддерживается шлюзом	Не удалось установить соединение VPN, так как в согласованной стратегии выбран режим открытой передачи, но соединение устанавливается через защищенный шлюз.	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. С помощью программы Навигатор скорректируйте стратегию VPN, связанную с этим соединением VPN. 3. Устраните причины возникновения ошибок и повторите операцию.
TCP8623 Соединение VPN уже существует	Не удалось создать соединение VPN, так как такое соединение уже существует. Это соединение установлено между локальной конечной точкой данных [*локальная конечная точка данных*] и удаленной конечной точкой данных [*удаленная конечная точка данных*].	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. С помощью программы Навигатор найдите активные соединения, которые установлены между теми же конечными точками данных, что и запрошенное соединение. Для того чтобы установить второе соединение между этими точками данных, измените стратегию существующего соединения. 3. Устраните причины возникновения ошибок и повторите операцию.

Сообщение	Причина	Исправление
TCP8624 Соединение VPN не относится к области действия правила фильтрации соответствующей стратегии	Не удалось установить соединение VPN, так как конечные точки данных не определены в правиле фильтрации заданной стратегии.	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. С помощью программы Навигатор просмотрите ограничения на конечные точки данных, установленные для этого соединения или группы соединений с динамическим ключом. Если отмечена опция **Подмножество фильтра стратегии** или **Изменить в соответствии с фильтром стратегии**, убедитесь, что конечные точки данных соединения заданы правильно. Они должны соответствовать активному правилу фильтрации, с которым связано действие IPSEC и которое задано для этого соединения VPN. Измените существующую стратегию соединения или правило фильтрации. 3. Устраните причины возникновения ошибок и повторите операцию.
TCP8625 При проверке соединения VPN с помощью алгоритма ESP обнаружена ошибка	Не удалось установить соединение VPN, так как с ним связан неправильный личный ключ.	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. С помощью программы Навигатор просмотрите стратегию, связанную с этим соединением, и задайте другой личный ключ. 3. Устраните причины возникновения ошибок и повторите операцию.

Сообщение	Причина	Исправление
TCP8626 Конечная точка соединения VPN не совпадает с конечной точкой данных	Не удалось установить соединение VPN, так как в стратегии указано, что оно устанавливается с хостом, но конечная точка соединения VPN не совпадает с конечной точкой данных.	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. С помощью программы Навигатор просмотрите ограничения на конечные точки данных, установленные для этого соединения или группы соединений с динамическим ключом. Если отмечена опция **Подмножество фильтра стратегии** или **Изменить в соответствии с фильтром стратегии**, убедитесь, что конечные точки данных соединения заданы правильно. Они должны соответствовать активному правилу фильтрации, с которым связано действие IPSEC и которое задано для этого соединения VPN. Измените существующую стратегию соединения или правило фильтрации. 3. Устраните причины возникновения ошибок и повторите операцию.
TCP8628 Не загружено правило фильтрации стратегии	Правило фильтрации стратегии, связанное с этим соединением, не активно.	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. С помощью программы Навигатор просмотрите активные фильтры стратегии. Убедитесь, что среди них есть правило фильтрации стратегии для данного соединения. 3. Устраните причины возникновения ошибок и повторите операцию.
TCP8629 Пакет IP, который требовалось передать по соединению VPN, был удален	Для соединения VPN настроена функция NAT. Число необходимых адресов NAT превысило число доступных адресов NAT.	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. С помощью программы Навигатор увеличьте число адресов NAT, выделенных соединению VPN. 3. Устраните причины возникновения ошибок и повторите операцию.

Сообщение	Причина	Исправление
TCP862A Не удалось установить соединение PPP	Это соединение VPN связано с профайлом PPP. Во время установления соединения была сделана попытка запустить профайл PPP, однако при этом возникла ошибка.	1. Найдите в “Просмотр протоколов заданий сервера VPN” на стр. 50 другие сообщения об этом соединении. 2. Просмотрите протокол задания, связанный с соединением PPP. 3. Устраните причины возникновения ошибок и повторите операцию.

Устранение неполадок VPN путем трассировки соединений OS/400

В системе iSeries(TM) предусмотрена возможность трассировки данных, передаваемых по линии связи, например, по интерфейсу локальной сети (LAN) или глобальной сети (WAN). Вы можете не понять смысл некоторых записей трассировки. Однако с их помощью вы всегда сможете определить, выполнялся ли обмен данными между локальной и удаленной системами.

Запуск трассировки соединений
Для включения трассировки соединений в системе вызовите команду Запустить трассировку соединений (STRCMNTRC). Ниже приведен пример команды STRCMNTRC:

```
STRCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) MAXSTG(2048) TEXT('VPN Problems')
```

Ниже приведено описание параметров команды:

CFGOBJ (Объект конфигурации)
Имя объекта конфигурации, для которого должна быть включена трассировка. В качестве такого объекта можно задать описание линии связи, описание сетевого интерфейса или описание сетевого сервера.

CFGTYPE (Тип конфигурации)
Возможные варианты: линия связи (*LIN), сетевой интерфейс (*NWI), сетевой сервер (*NWS).

MAXSTG (Размер буфера)
Размер буфера трассировки. Значение по умолчанию составляет 128 Кб. Допустимы значения от 128 Кб до 64 Мб. Системное ограничение на размер буфера задается с помощью Системного инструментария (SST). Если размер буфера, указанный в команде STRCMNTRC, будет больше ограничения, заданного в SST, будет выдано сообщение об ошибке. Обратите внимание, что суммарный размер буферов всех активных сеансов трассировки соединений не должен превосходить максимальный размер буфера, заданный в SST.

DTADIR (Направление передачи данных)
Направление потока данных, для которого необходимо включить трассировку. Предусмотрены следующие значения: только исходящие данные (*SND), только входящие данные (*RCV), оба потока данных (*BOTH).

TRCFULL (Переполнение буфера трассировки)
Действие, выполняемое при переполнении буфера трассировки. Допустимы два значения параметра. По умолчанию применяется значение *WRAP. Оно означает, что при переполнении буфера трассировки новые данные начинают записываться поверх старых. По мере поступления новых записей они заменяют старые записи трассировки.

Второе значение - *STOPTRC. Оно означает, что когда размер буфера трассировки достигает значения параметра MAXSTG, трассировка должна быть выключена. В общем случае рекомендуется задавать такой размер буфера, чтобы в него поместились все записи трассировки. Если будет начат новый цикл

записи данных в буфер, вы рискуете потерять важную информацию. Если возникла очень серьезная неполадка, укажите такой размер буфера, чтобы записи трассировки не заменялись, и была сохранена вся информация.

USRDTA (Число обрабатываемых пользовательских байт)
Задает число байт пользовательских данных, содержащихся в кадре данных, для которых должна выполняться трассировка. Для интерфейсов LAN по умолчанию копируются только первые 100 байт пользовательских данных. Для остальных интерфейсов копируются все пользовательские данные. Если вы считаете, что ошибка связана с пользовательскими данными, содержащимися в кадре, укажите значение *MAX.

TEXT (Описание трассировки)
Описание сеанса трассировки.

Завершение сеанса трассировки соединений
Если не указано иное, то трассировка прекращается при выполнении отслеживаемого условия. Для выключения трассировки вызовите команду Завершить трассировку соединений (ENDCMNTRC). Ниже приведен пример команды ENDCMNTRC:

```
ENDCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN)
```

У команды есть два параметра:

CFGOBJ (Объект конфигурации)
Имя объекта конфигурации, для которого выполняется трассировка. В качестве такого объекта можно задать описание линии связи, описание сетевого интерфейса или описание сетевого сервера.

CFGTYPE (Тип конфигурации)
Возможные варианты: линия связи (*LIN), сетевой интерфейс (*NWI), сетевой сервер (*NWS).

Печать данных трассировки
После выключения трассировки соединений можно напечатать данные, собранные функцией трассировки. Для этого вызовите команду Печать данных трассировки соединений (PRTCMNTRC). Поскольку функция трассировки копирует всю информацию, передаваемую по соединению, вы можете задать различные фильтры для отбора данных, которые должны быть включены в вывод команды. Размер буферного файла должен быть как можно меньше. Это значительно упростит последующий анализ данных. Для анализа ошибок VPN достаточно включить в вывод только данные IP. По возможности рекомендуется указать IP-адрес отправителя или получателя. Кроме того, можно указать номер порта IP. Ниже приведен пример команды PRTCMNTRC:

```
PRTCMNTRC CFGOBJ(TRNLINE) CFGTYPE(*LIN) FMTTCP(*YES) TCPIPADR('10.50.21.1)
    SLTPORT(500) FMTBCD(*NO)
```

В данном примере вывод будут содержать только те данные IP, которые были отправлены или получены хостом с адресом 10.50.21.1 через порт IP с номером 500.

Ниже описаны параметры команды, которые указываются при анализе неполадок VPN:

CFGOBJ (Объект конфигурации)
Имя объекта конфигурации, для которого выполняется трассировка. В качестве такого объекта можно задать описание линии связи, описание сетевого интерфейса или описание сетевого сервера.

CFGTYPE (Тип конфигурации)
Возможные варианты: линия связи (*LIN), сетевой интерфейс (*NWI), сетевой сервер (*NWS).

FMTTCP (Форматировать данные TCP/IP)
Указывает, какие данные трассировки должны быть отформатированы: данные TCP/IP или UDP/IP. Для того чтобы были отформатированы данные IP, собранные функцией трассировки, укажите значение *YES.

TCPIPADR (Форматировать данные TCP/IP по адресу)
Этот параметр состоит из двух элементов. Если в обоих элементах будут указаны IP-адреса, то вывод команды будет содержать только те данные IP, которыми обменивались хосты с указанными адресами.

SLTPORT (Номер порта IP)
Номер порта IP, который будет применяться в качестве фильтра.

FMTBCD (Форматировать данные оповещения)
Указывает, следует ли включать в вывод кадры оповещения. По умолчанию применяется значение Да. Если вы не хотите, чтобы вывод содержал такую информацию, в частности, запросы протокола ARP, укажите значение *NO. Число оповещающих сообщений может быть очень велико.

Дополнительная информация о VPN

Дополнительную информацию о VPN и другие сценарии настройки можно найти в следующих источниках:

- **OS/400(R) V5R1 Virtual Private Networks: Remote Access to the IBM(R) e(logo)server iSeries(TM) Server with Windows(R) 2000 VPN Clients, REDP0153** 
  Это руководство фирмы IBM содержит описание пошаговой процедуры настройки туннеля VPN, использующего функции VPN выпуска V5R1, а также функции L2TP и IPSec, предусмотренные в Windows 2000.

- **AS/400(R) Internet Security: Implementing AS/400 Virtual Private Networks, SG24-5404-00** 
  В этом руководстве приведена основная информация о функции VPN и ее реализации в OS/400, основанной на средствах защиты IP (IPSec) и протоколе L2TP.

- **AS/400 Internet Security Scenarios: A Practical Approach, SG24-5954-00** 
  В этом руководстве описаны все средства защиты сетевых соединений, предусмотренные в системе OS/400, в том числе фильтры пакетов IP, NAT, VPN, сервер Proxy HTTP, SSL, DNS, функция передачи почты, функция контроля и функция ведения протокола. Приведены практические примеры применения этих средств защиты.

- **Virtual Private Networking: Securing Connections** 
  На этом Web-сайте приведены свежие новости о VPN, список новых PTF и ссылки на другие полезные Web-сайты.
- **Другие книги и руководства, посвященные средствам защиты**
  В этом разделе приведен список электронных источников информации о средствах защиты.

Для просмотра или печати документа в формате PDF сохраните его на рабочей станции, выполнив следующие действия:

1. Щелкните правой кнопкой мыши на имени документа PDF в окне браузера (на приведенной выше ссылке).
2. Выберите пункт **Сохранить как...**.
3. Выберите каталог для сохранения файла с документом PDF.
4. Нажмите кнопку **Сохранить**.

Для просмотра и печати документов в формате PDF применяется программа Adobe Acrobat Reader. Эту программу можно загрузить с Web-сайта Adobe (www.adobe.com/prodindex/acrobat/readstep.html)  .

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.

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

```
IBM Director of Licensing
IBM Corporation
500 Columbus Avenue
Thornwood, NY  10594-1785
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, 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 информации по данному продукту IBM и ответственность за применение этих материалов лежит на пользователе.

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

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

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

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

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

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

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

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

Все приведенные цены на продукты IBM - это рекомендованные IBM текущие розничные цены, которые могут быть изменены без предварительного уведомления. Цены у дилеров могут отличаться от указанных.

Приведенная информация предназначена только для планирования. Она может быть изменена до выхода описанного продукта.

Настоящая документация содержит примеры данных и отчетов, применяемых в повседневной деятельности компаний. Для обеспечения наглядности эти примеры могут включать имена людей, названия компаний, товарных знаков и наименования товаров. Все эти имена являются вымышленными, и любые сходства с именами и адресами действительных коммерческих предприятий абсолютно случайны.

Товарные знаки

Ниже перечислены товарные знаки International Business Machines Corporation в США и/или других странах:
Application System/400
AS/400
e (logo)
IBM
iSeries
Operating System/400
OS/400
400

Lotus, Freelance, и WordPro являются товарными знаками International Business Machines Corporation и Lotus Development Corporation в США и/или других странах.

C-bus является товарным знаком Corollary, Inc. в США и/или других странах.

ActionMedia, LANDesk, MMX, Pentium, и ProShare являются товарными знаками или зарегистрированы как товарные знаки корпорации Intel в США и/или других странах.

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

SET и логотип SET являются товарными знаками, принадлежащими SET Secure Electronic Transaction LLC.

Java и Java-based являются товарным знаком Sun, Inc. в США и/или других странах.

UNIX - зарегистрированный товарный знак The Open Group в США и других странах.

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

Условия загрузки и печати публикаций

Разрешение на использование выбранных для загрузки публикаций предоставляется в соответствии с следующими условиями и при подтверждении вашего с ними согласия.

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

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

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

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

Вы можете загружать, экспортировать и реэкспортировать эту информацию только в полном соответствии со всеми применимыми законами и правилами, включая все законы США в отношении экспорта. IBM не несет ответственности за содержание этих публикаций. Публикации предоставляются на условиях ″как есть″, без предоставления каких-либо явных или подразумеваемых гарантий, включая, но не ограничиваясь этим, подразумеваемые гарантии коммерческой ценности или применения для каких-либо конкретных целей.

Авторские права на все материалы принадлежат IBM Corporation.

Загружая или печатая публикации с этого сайта, вы тем самым подтверждаете свое согласие с приведенными условиями.

Напечатано в Дании