Семинарское занятие №15

Тема «Настройка брандмауэра Windows для разрешения доступа к SQL Server»

Настройка брандмауэра Windows для разрешения доступа к SQL Server

SQL Server 2014
Другие версии

Системы брандмауэров предотвращают несанкционированный доступ к ресурсам компьютера.Если брандмауэр включен, но настроен неправильно, попытка соединения с SQL Server может оказаться заблокированной.
Чтобы разрешить доступ к экземпляру SQL Server через брандмауэр, его необходимо настроить на компьютере, на котором работает SQL Server.Брандмауэр является компонентом Корпорация Майкрософт Windows.Вместо него можно установить брандмауэр другой компании.В данном разделе обсуждается настройка брандмауэра Windows, однако общие принципы применимы к любым другим брандмауэрам.

Примечание

В разделе содержатся общие сведения о настройке брандмауэра и сводные сведения, представляющие интерес для администратора SQL Server.Дополнительные сведения и официальные данные о брандмауэрах см. в документации по брандмауэру, например в разделе Брандмауэр Windows в режиме повышенной безопасности и IPsec.

Пользователи, хорошо знакомые с элементом **Брандмауэр Windows** на панели управления и оснасткой «Брандмауэр Windows в режиме повышенной безопасности» консоли управления (MMC) и умеющие настраивать параметры брандмауэра, могут перейти непосредственно к разделам, приведенным в следующем списке.

- Настройка брандмауэра Windows для доступа к компоненту Database Engine
- Настройка брандмауэра Windows на разрешение доступа к службам Analysis Services
- настроить брандмауэр для доступа к серверу отчетов

В этом разделе

Этот раздел содержит следующие подразделы.
Основные сведения о брандмауэрах
Параметры брандмауэра по умолчанию

Основные сведения о брандмауэрах

Брандмауэр проверяет входящие пакеты на соответствие набору правил.Если правила разрешают передачу пакета, то брандмауэр передает его протоколу TCP/IP для дальнейшей обработки.Если передача пакета правилами не разрешена, то брандмауэр отвергает его и, если включено ведение журнала, создает в файле журнала соответствующую запись.

Список разрешенного трафика заполняется одним из следующих способов.

- Когда защищенный брандмауэром компьютер открывает соединение, брандмауэр добавляет в список элемент, разрешающий ответ по этому соединению.Полученный ответ рассматривается как ожидаемый и не требует настройки.
- Работа администратора заключается в настройке исключений в работе брандмауэра.Это дает возможность разрешать доступ определенным программам, запущенным на компьютере, либо доступ к определенным портам.В этом случае компьютер принимает весь входящий трафик, выполняя роль сервера, прослушивателя или одноранговогo узла.Для соединения с SQL Server должна быть выполнена именно такая настройка.

Выбор стратегии брандмауэра является более сложной задачей и не сводится лишь к открытию или закрытию портов.При выборе стратегии брандмауэра для предприятия необходимо обязательно рассмотреть все доступные правила и параметры конфигурации.В этом разделе все возможные параметры брандмауэра не рассматриваются.Рекомендуется ознакомиться со следующими документами.

Руководство по началу работы с брандмауэром Windows в режиме повышенной безопасности
Руководство разработчика по брандмауэру Windows в режиме повышенной безопасности
Основные сведения об изоляции серверов и доменов

Параметры брандмауэра по умолчанию

Первым шагом при планировании конфигурации брандмауэра является определение его текущего состояния в операционной системе.Если операционная система была обновлена с предыдущей версии, в ней могли сохраниться старые настройки брандмауэра.Кроме того, параметры брандмауэра могли быть изменены другим администратором или групповой политикой домена.

Примечание
Включение брандмауэра может повлиять на общий доступ к файлам и принтерам, подключения к удаленному рабочему столу и работу других программ, которым

необходим доступ к компьютеру.Администратор должен просмотреть все приложения, которые работают на компьютере, прежде чем приступать к настройке параметров брандмауэра.

Программы для настройки брандмауэра

Существует три способа настройки параметров брандмауэра Windows.

- **Элемент «Брандмауэр Windows» на панели управления**
  Элемент **Брандмауэр Windows** можно открыть с панели управления.

  Важно

  Изменения, произведенные в элементе **Брандмауэр Windows** на панели управления, применяются только к текущему профилю.На переносных компьютерах и других мобильных устройствах пользоваться элементом**Брандмауэр Windows** на панели управления нельзя, так как профиль может измениться при установлении соединения в другой конфигурации,в результате чего ранее настроенный профиль станет недоступен.Дополнительные сведения о профилях см. в разделе Руководство по началу работы с брандмауэром Windows в режиме повышенной безопасности.

  Элемент **Брандмауэр Windows** на панели управления позволяет настроить Ниже перечислены некоторые из них:
  - Включение и отключение элемента **Брандмауэр Windows** на панели управления.
  - Включение и отключение правил.
  - Предоставление исключений для портов и программ.
  - Задание некоторых ограничений области действия.

  Элемент **Брандмауэр Windows** на панели управления лучше всего подходит пользователям, которые не имеют опыта в настройке конфигурации брандмауэра, если необходимо настроить основные параметры брандмауэра для стационарного компьютера.Элемент **Брандмауэр Windows** на панели управления можно также открыть командой**run**, выполнив следующую процедуру.

  ### Открытие элемента «Брандмауэр Windows»

  5. В меню **Пуск** выберите команду **Выполнить** и введите команду `firewall.cpl`.
  6. Нажмите кнопку **OK**.

- **Консоль управления (MMC)**
  Оснастка «Брандмауэр Windows в режиме повышенной безопасности» позволяет настраивать дополнительные параметры брандмауэра.Эта оснастка представляет большинство параметров брандмауэра и в удобной форме, а также все профили брандмауэра.Дополнительные сведения см. в подразделе Брандмауэр Windows в режиме повышенной безопасности далее в этом разделе.
- **netsh**
  Программа **netsh.exe** позволяет администратору настраивать компьютеры с ОС Windows и наблюдать за ними из командной строки или с помощью пакетного файла**.** При

использовании средства **netsh** вводимые команды направляются соответствующим помощникам, которые и производят их выполнение.Помощник представляет собой DLL-библиотеку, расширяющую функциональность средства **netsh**, которая предоставляет возможности настройки, наблюдения и поддержки других служб, программ и протоколов.Все операционные системы, поддерживающие SQL Server, имеют модуль поддержки брандмауэра.Windows Server 2008 также содержит расширенный помощник брандмауэра **advfirewall**.В этом разделе не обсуждаются подробности использования программы **netsh**.Однако многие из описанных параметров конфигурации можно настроить и с помощью программы **netsh**.Например, выполните в командной строке следующий скрипт, чтобы открыть TCP-порт 1433:

```
netsh firewall set portopening protocol = TCP port = 1433 name =
SQLPort mode = ENABLE scope = SUBNET profile = CURRENT
```

Аналогичный пример, использующий брандмауэр Windows для модуля поддержки повышенной безопасности:

```
netsh advfirewall firewall add rule name = SQLPort dir = in protocol =
tcp action = allow localport = 1433 remoteip = localsubnet profile =
DOMAIN
```

Дополнительные сведения о программе **netsh** см. в следующих разделах.

- Использование средства Netsh.exe и параметров командной строки
- Использование контекста «netsh advfirewall firewall» вместо контекста «netsh firewall» для управления работой брандмауэра Windows в операционной системе Windows Server 2008 или Windows Vista
- Команда «netsh firewall» с параметром «profile=all» не настраивает открытый профиль на компьютере под управлением Windows Vista

Порты, используемые SQL Server

Следующие таблицы помогут выяснить, какие порты использует SQL Server.

Порты, используемые компонентом Database Engine

В следующей таблице перечислены порты, обычно используемые компонентом Компонент Database Engine.

Сценарий	Порт	Комментарии
Экземпляр SQL Server по умолчанию, работающий по протоколу TCP	TCP-порт 1433	Этот порт открывают в брандмауэре чаще всего.Он применяется для программных соединений с экземпляром компонента Компонент Database Engine по умолчанию или именованным экземпляром, который является единственным на данном компьютере(для именованных экземпляров следует учитывать ряд особых требований,подробнее о

		которых см. в подразделе Динамические порты далее в этом разделе).
Именованные экземпляры SQL Server в конфигурации по умолчанию	TCP-порт выделяется динамически в момент запуска компонента Компонент Database Engine.	См. подраздел Динамические порты далее в этом разделе.При использовании именованных экземпляров службе браузера SQL Server может потребоваться UDP-порт 1434.
Именованные экземпляры SQL Server, если они настроены для использования фиксированного порта	Номер порта настраивается администратором.	См. подраздел Динамические порты далее в этом разделе.
Выделенное административное соединение	TCP-порт 1434 предназначен для экземпляра по умолчанию.Другие порты используются для именованных экземпляров.Номер порта проверьте по журналу ошибок.	По умолчанию удаленные соединения по выделенному административному соединению (DAC) запрещены.Разрешить удаленное выделенное административное соединение можно при помощи средства настройки контактной зоны.Дополнительные сведения см. в разделе Настройка контактной зоны.
Служба «SQL Server, браузер»	UDP-порт 1434	Служба «SQL Server, браузер» прослушивает входящие соединения к именованному экземпляру и возвращает клиенту номер TCP-порта, соответствующего именованному экземпляру.Обычно служба «SQL Server, браузер» запускается при использовании именованного экземпляра компонента Компонент Database Engine.Если клиент

		настроен для соединения с именованным экземпляром по заданному порту, то службу «SQL Server, браузер» запускать не обязательно.
Экземпляр SQL Server, работающий через конечную точку HTTP	Может указываться во время создания конечной точки HTTP.По умолчанию используется TCP-порт 80 для данных CLEAR_PORT и порт 443 для данных SSL_PORT.	Используется для HTTP-соединения по URL-адресу.
Экземпляр SQL Server по умолчанию, работающий через конечную точку HTTPS	TCP-порт 443	Используется для HTTPS-соединения по URL-адресу.HTTPS представляет собой HTTP-соединение, защищенное по протоколу SSL.
Компонент Service Broker	TCP-порт 4022.Чтобы проверить используемый порт, выполните следующий запрос: `SELECT name, protocol_desc, port, state_desc FROM sys.tcp_endpoints WHERE type_desc = 'SERVICE_BROKER'`	Для компонента SQL Server Компонент Service Broker нет порта по умолчанию, но эта конфигурация принята в электронной документации для использования в примерах.
Зеркальное отображение базы данных	Порт, выбранный администратором.Чтобы определить порт, выполните следующий запрос. `SELECT name, protocol_desc, port, state_desc FROM sys.tcp_endpoints WHERE type_desc = 'DATABASE_MIRRORING'`	Для зеркального отображения базы данных нет порта по умолчанию, однако в примерах электронной документации используется TCP-порт 7022.Очень важно избегать прерывания используемой конечной точки зеркального отображения, особенно в режиме высокой безопасности с автоматической отработкой отказа.Конфигурация брандмауэра должна избегать прерывания кворума.Дополнительные

		сведения см. в разделе Указание сетевого адреса сервера (зеркальное отображение базы данных).
Репликация	Соединения с SQL Server для репликации используют порты, которые обычно использует компонент Компонент Database Engine (TCP-порт 1433 для экземпляра по умолчанию и т. д.) Веб-синхронизация и доступ через FTP/UNC к моментальному снимку репликации потребуют открытия в брандмауэре других портов.Передачу начальных данных и схемы из одного места в другое репликация осуществляет по протоколу FTP (TCP-порт 21) либо с помощью синхронизации через HTTP (TCP-порт 80) или общего доступа к файлам.Для общего доступа к файлам используются UDP-порты 137 и 138 и TCP-порт 139 (если используется NetBIOS).Совместное использование файлов использует TCP-порт 445.	Для синхронизации по протоколу HTTP в репликации используется конечная точка IIS (порты которой являются настраиваемыми, но порт 80 применяется по умолчанию), однако процесс IIS подключается к серверу базы данных SQL Server через стандартные порты (1433 для экземпляра по умолчанию). При веб-синхронизации через FTP-порт передача данных выполняется между службами IIS и издателем SQL Server, а не между подписчиком и службами IIS.
Отладчик Transact-SQL	TCP-порт 135 См. раздел Особые замечания относительно порта 135 Также может потребоваться исключение IPsec.	При использовании среды Visual Studio на Visual Studio главном компьютере в список исключений необходимо также добавить программу**Devenv.exe** и открыть TCP-порт 135. При использовании среды Среда Management Studio на Среда Management Studio главном компьютере

		необходимо также добавить в список исключений программу **ssms.exe** и открыть TCP-порт 135.Дополнительные сведения см. в разделеНастройка отладчика Transact-SQL.

Пошаговые инструкции по настройке брандмауэра Windows для компонента Компонент Database Engine см. в разделеНастройка брандмауэра Windows для доступа к компоненту Database Engine.

Динамические порты

По умолчанию именованные экземпляры (включая SQL Server Express) используют динамические порты.Это означает, что при каждом запуске компонент Компонент Database Engine находит доступный порт и занимает его.Если именованный экземпляр является единственным установленным экземпляром компонента Компонент Database Engine, то, скорее всего, он будет использовать TCP-порт 1433.При установке других экземпляров компонента Компонент Database Engine они будут использовать другие TCP-порты.Поскольку выбираемый порт может меняться при каждом запуске компонента Компонент Database Engine, настроить брандмауэр для разрешения доступа к нужному порту сложно.Поэтому, если используется брандмауэр, рекомендуется настроить компонент Компонент Database Engine на постоянное использование одного и того же порта.Такой порт называется фиксированным или статическим.Дополнительные сведения см. в разделе Настройка сервера для прослушивания указанного TCP-порта (диспетчер конфигурации SQL Server).

В качестве альтернативы настройке именованного экземпляра на прослушивание фиксированного порта можно создать в брандмауэре исключения для программы SQL Server, например **sqlservr.exe** (для компонента Компонент Database Engine).Это хороший выход из положения, однако номер порта не будет отображаться в столбце **Локальный порт** на странице **Правила для входящих подключений** оснастки «Брандмауэр Windows в режиме повышенной безопасности».В результате аудит открытых портов станет сложнее. Еще один нюанс заключается в том, что при применении совокупного обновления или пакета обновления может измениться путь к исполняемому файлу SQL Server, что сделает правило брандмауэра недействительным.

Примечание
Следующая процедура выполняется с помощью элемента **Брандмауэр Windows** на панели управления.В оснастке MMC «Брандмауэр Windows в режиме повышенной безопасности» поддерживается настройка дополнительных параметров брандмауэра.В их число входит настройка исключение службы, которая может оказаться полезной при обеспечении углубленной защиты.См. подраздел Использование оснастки «Брандмауэр Windows в режиме повышенной безопасности» ниже.

Добавление в брандмауэр исключения для программы при помощи элемента «Брандмауэр Windows» на панели управления

1. На вкладке **Исключения** элемента **Брандмауэр Windows** на панели управления нажмите кнопку **Добавить программу**.
2. Перейдите к экземпляру SQL Server, которому необходимо открыть доступ через брандмауэр, например к **C:\Program Files\Microsoft SQL Server\MSSQL12.<instance_name>\MSSQL\Binn**, выберите **sqlservr.exe**, а затем нажмите**Открыть**.
3. Нажмите кнопку **OK**.

Дополнительные сведения о конечных точках см. в разделах Настройка компонента Database Engine на прослушивание нескольких портов TCP и Представления каталога конечных точек (Transact-SQL).

Порты, используемые службами Analysis Services

В следующей таблице перечислены порты, обычно используемые службами Службы Analysis Services.

Компонент	Порт	Комментарии
Службы Analysis Services	TCP-порт 2383 для экземпляра по умолчанию	Стандартный порт для экземпляра служб Службы Analysis Services по умолчанию.
Служба «SQL Server, браузер»	Для именованного экземпляра служб Службы Analysis Services необходим только TCP-порт 2382	Запросы клиентского соединения к именованному экземпляру служб Службы Analysis Services, в которых не указан номер порта, направляются на порт 2382, который прослушивает служба «SQL Server, браузер».Браузер SQL Server затем перенаправляет запрос на порт, используемый запрошенным именованным экземпляром.
Службы Службы Analysis Services настроены для работы через протокол IIS/HTTP (служба PivotTable® Service использует протокол HTTP или HTTPS)	TCP-порт 80	Используется для HTTP-соединения по URL-адресу.
Службы Службы Analysis Services настроены для работы через	TCP-порт 443	Используется для HTTPS-соединения по URL-адресу.HTTPS представляет собой HTTP-соединение, защищенное по протоколу SSL.

протокол IIS/HTTPS (служба PivotTable® Service использует протокол HTTP или HTTPS)		

Если пользователи производят доступ к службам Службы Analysis Services через Интернет и службы IIS, необходимо открыть порт, который прослушивают службы IIS, и указать этот порт в строке соединения клиента.В этом случае необязательно иметь открытые порты для прямого доступа к службам Службы Analysis Services.Необходимо ограничить доступ к порту по умолчанию 2389, порту 2382 и другим портам, которые не нужны для осуществления доступа.
Пошаговые инструкции по настройке брандмауэра Windows для служб Службы Analysis Services см. в разделе Настройка брандмауэра Windows на разрешение доступа к службам Analysis Services.

Порты, используемые службами Reporting Services

В следующей таблице перечислены порты, обычно используемые службами Службы Reporting Services.

Компонент	Порт	Комментарии
Веб-службы Службы Reporting Services	TCP-порт 80	Используется для HTTP-соединения со службами Службы Reporting Services по URL-адресу.Не рекомендуется использовать стандартное правило **Службы Интернета (HTTP)**.Дополнительные сведения см. в разделе Взаимодействие с другими правилами брандмауэра ниже.
Службы Службы Reporting Services настроены для работы через протокол HTTPS	TCP-порт 443	Используется для HTTPS-соединения по URL-адресу.HTTPS представляет собой HTTP-соединение, защищенное по протоколу SSL.Не рекомендуется использовать стандартное правило **Защищенные службы Интернета (HTTPS)**.Дополнительные сведения см. в разделе Взаимодействие с другими правилами брандмауэра ниже.

Для соединения служб Службы Reporting Services с экземпляром компонента Компонент Database Engine или служб Службы Analysis Services необходимо также открыть соответствующие порты для этих служб.Пошаговые инструкции по настройке брандмауэра Windows для служб Службы Reporting Services см. в разделе настроить брандмауэр для доступа к серверу отчетов.

Порты, используемые службами Integration Services

В следующей таблице перечислены порты, используемые службой Службы Integration Services.

Компонент	Порт	Комментарии

Корпорация Майкрософт Удаленный вызов процедур (MS RPC) Используется средой выполнения служб Службы Integration Services.	TCP-порт 135 См. разделОсобые замечания относительно порта 135	Служба Службы Integration Services обращается к DCOM по порту 135.Диспетчер управления службами использует порт 135 для запуска и остановки службы Службы Integration Services, передачи управляющих запросов запущенной службе и выполнения других задач.Номер порта не может быть изменен. Это единственный порт, который должен быть открыт при соединении с удаленным экземпляром службы Службы Integration Services из среды Среда Management Studio или прикладной программы.

Пошаговые инструкции по настройке брандмауэра Windows для служб Службы Integration Services см. в разделе Настройка параметров брандмауэра Windows для доступа к службам SSIS.

Другие порты и службы

В следующей таблице перечислены порты и службы, от которых может зависеть SQL Server.

Сценарий	Порт	Комментарии
Инструментарий управления Windows (WMI) Дополнительные сведения о WMI см. в разделе Основные понятия о поставщике WMI для управления конфигурацией	Инструментарий WMI запускается в составе общего узла службы с назначением портов через DCOM.Инструментарий WMI может пользовать TCP-порт 135. См. раздел Особые замечания относительно порта 135	Диспетчер конфигурации SQL Server использует инструментарий WMI для просмотра и управления службами.Рекомендуется использовать стандартную группу правил **Инструментарий управления Windows (WMI)**.Дополнительные сведения см. в разделеВзаимодействие с другими правилами брандмауэра ниже.
Координатор распределенных транзакций (Майкрософт) (MS DTC)	TCP-порт 135 См. раздел Особые замечания относительно порта 135	Если приложение использует распределенные транзакции, то может потребоваться настройка брандмауэра таким образом, чтобы разрешить передачу данных координатора распределенных транзакций (Майкрософт) (MS DTC) между отдельными экземплярами MS DTC и между MS DTC и диспетчерами ресурсов (например SQL Server).Рекомендуется использовать

		стандартную группу правил **Координатор распределенных транзакций**. Если для всего кластера настроен единственный общий координатор MS DTC в отдельной группе ресурсов, следует добавить программу sqlservr.exe в список исключений брандмауэра.
Кнопка обзора в среде Среда Management Studio соединяется со службой SQL Server, браузер по протоколу UDP.Дополнительные сведения см. в разделе Служба обозревателя SQL Server (компонент Database Engine и SSAS).	UDP-порт 1434	Протокол UDP не сохраняет соединения. Свойство UnicastResponsesToMulticastBroadcastDisabled интерфейса INetFwProfile управляет работой брандмауэра по отношению к одноадресным ответам на широковещательные (или многоадресные) UDP-запросы.Возможны два варианта. • Если этот параметр имеет значение TRUE, то одноадресные ответы на широковещательные запросы запрещены.Перечисление служб завершится ошибкой. • Если этот параметр имеет значение FALSE (по умолчанию), то одноадресные ответы разрешены в течение 3 секунд.Время ожидания не настраивается.Если сеть переполнена, каналы имеют задержки или сервер работает в режиме высокой нагрузки, то при построении списка экземпляров SQL Server список может быть возвращен лишь частично и ввести пользователя в заблуждение.
Трафик по протоколу IPsec	UDP-порты 500 и 4500	Если политика домена требует выполнения сетевых соединения через протокол IPsec, необходимо добавить в список исключений UDP-порты 4500 и 500.Протокол IPsec можно включить при помощи **мастера создания правила для нового входящего подключения** в оснастке «Брандмауэр Windows».Дополнительные сведения см. в разделеИспользование оснастки «Брандмауэр Windows в режиме повышенной безопасности» ниже.

Использование проверки подлинности Windows в надежных доменах	Брандмауэр можно настроить для разрешения запросов проверки подлинности.	Дополнительные сведения см. в разделе Настройка брандмауэра для работы с доменами и отношениями доверия.
SQL Server и кластеризация Windows	Кластеризация требует открытия дополнительных портов, не связанных с SQL Server напрямую.	Дополнительные сведения см. в разделе Подготовка сети для работы кластера.
Пространства имен URL-адресов, зарезервированные в компоненте HTTP.SYS	Обычно TCP-порт 80, однако можно настроить для использования любого другого порта.Общие сведения см. в разделе Настройка протоколов HTTP и HTTPS.	Сведения о резервировании конечной точки компонента HTTP.SYS при помощи программы HttpCfg.exe, относящиеся к SQL Server, см. в разделе Сведения о резервировании и регистрации URL-адресов (диспетчер конфигурации служб SSRS).

Особые замечания относительно порта 135

При использовании в качестве транспортного протокола RPC через TCP/IP или UDP/IP входящие порты для системных служб часто выделяются динамически с номерами выше 1024.Иногда их называют «случайными RPC-портами». В этом случае RPC-клиент определяет порт, назначенный серверу, через модуль конечной точки RPC.Для некоторых служб, работающих через протокол RPC, можно настроить использование определенного фиксированного порта.Можно также ограничить диапазон портов, которые могут быть динамически назначены службой RPC независимо от службы.Поскольку порт 135 используется для многих служб, он часто подвергается атакам злоумышленников.В случае открытия порта 135 рекомендуется ограничить область действия правила брандмауэра.

Дополнительные сведения о порте 135 см. в следующих ресурсах.

- Общие сведения о службе и требования к сетевым портам в системе Windows Server
- Устранение неполадок модуля сопоставления конечной точки RPC при помощи средств поддержки, устанавливаемых с компакт-диска Windows Server 2003
- Удаленный вызов процедур (RPC)
- Настройка динамического выделения портов RPC для работы с брандмауэром

Взаимодействие с другими правилами брандмауэра

Настройка брандмауэра Windows производится на основе правил и групп правил.Каждое правило или группа правил обычно связаны с определенной программой или службой, которая может изменить или удалить это правило без участия пользователя.Например, группы правил **Службы**

Интернета (HTTP) и **Защищенные службы Интернета (HTTPS)** связаны со службами IIS.При включении этих правил будут открыты порты 80 и 443 и разрешены функции SQL Server, зависящие от этих портов.Однако администратор в процессе настройки служб IIS может изменить или отключить эти правила.Поэтому, если SQL Server использует порт 80 или 443, необходимо создать собственное правило или группу правил для поддержки необходимой конфигурации портов, не зависящей от служб IIS.
Оснастка «Брандмауэр Windows в режиме повышенной безопасности» пропускает весь трафик, соответствующий применимым разрешающим правилам.Если существует два правила для порта 80 (но с разными параметрами), будет разрешен любой трафик, соответствующий хотя бы одному из этих правил.Таким образом, если одно правило разрешает трафик по порту 80 из локальной подсети, а второе разрешает трафик с любого адреса, то будет разрешен любой трафик по порту 80, независимо от его источника.Чтобы обеспечить эффективное управление доступом к SQL Server, администратор должен периодически проверять все правила брандмауэра, разрешенные на сервере.

Общие сведения о профилях брандмауэра

Профили брандмауэра обсуждаются в разделе Руководство по началу работы с брандмауэром Windows в режиме повышенной безопасности, в подразделе **Брандмауэр узла, привязанный к местонахождению в сети**.Подводя итоги, операционная система определяет и запоминает каждую из сетей, к которым осуществлялось подключение, по обмену данными, соединениям и категории. Брандмауэр Windows в режиме повышенной безопасности делит сети на три типа.

- Домен.Windows может выполнить проверку подлинности доступа к контроллеру домена, в который включен компьютер.
- Открытая.В эту категорию первоначально попадают все сети, не входящие в домены.Сети, которые представляют прямые соединения с Интернетом, являются открытыми (аэропорты, кафе и другие места открытого доступа).
- Частная.Сеть, определенная пользователем или приложением как личная.Только доверенные сети могут быть определены как частные.Обычно в качестве частной сети определяется сеть малого предприятия, домашняя сеть и т. п.

Администратор может создать профиль для каждого типа сети и задать для этих профилей разные политики брандмауэра.Одномоментно применим только один профиль.Профили применяются в следующем порядке.

1. Если все интерфейсы прошли проверку подлинности к контроллеру домена, членом которого является компьютер, то применяется профиль домена.
2. Если все интерфейсы либо прошли проверку подлинности к контроллеру домена, либо соединены с сетями, которые определены как частные, применяется частный профиль.
3. В противном случае применяется открытый профиль.

Просмотреть и настроить профили брандмауэра можно с помощью оснастки «Брандмауэр Windows в режиме повышенной безопасности».Элемент **Брандмауэр Windows** на панели управления позволяет настраивать только текущий профиль.

Дополнительные параметры брандмауэра в элементе «Брандмауэр Windows» на панели управления

Исключения, добавляемые в брандмауэр, могут ограничить открытие портов для входящих соединений с определенных компьютеров или из локальной подсети.Метод ограничения области действия открытия портов способен сократить зону уязвимости компьютера, и поэтому рекомендуется к применению.

Примечание

Элемент **Брандмауэр Windows** на панели управления позволяет настроить только текущий профиль.

Изменение области действия исключения брандмауэра с помощью «Брандмауэра Windows» на панели управления

1. В элементе **Брандмауэр Windows** на панели управления выберите программу или порт на вкладке **Исключения** и нажмите кнопку **Свойства** или **Изменить**.
2. В диалоговом окне **Изменение программы** или **Изменение порта** нажмите кнопку **Изменить область**.
3. Выберите один из следующих параметров.
    - **Любой компьютер (включая Интернет)**
      Не рекомендуется.В этом режиме любой компьютер, который имеет доступ к данному узлу, сможет подключиться к программе или порту.Этот параметр может пригодиться для передачи данных анонимным пользователям Интернета, однако он повышает уязвимость компьютера.Уязвимость еще более повысится, если одновременно с этим параметром разрешить просмотр трансляции сетевых адресов (например при помощи параметра «Разрешить просмотр узлов»).
    - **Только моя сеть (подсеть)**
      Это более безопасный режим, чем **Любой компьютер**.Только компьютеры локальной подсети могут производить соединение с программой или портом.
    - **Особый список.**

    Соединение разрешено только компьютерам, имеющим перечисленные IP-адреса.Это еще более безопасный режим, чем **Только моя сеть (подсеть)**, хотя у клиентского компьютера, использующего DHCP, может измениться IP-адрес.После этого он уже не сможет установить соединение.Другой компьютер, которому доступ не предоставлялся, может получить перечисленный в списке IP-адрес, что позволит ему установить соединение.Параметр **Особый список** может пригодиться для хранения списка серверов, настроенных для использования фиксированного IP-адреса, однако эти адреса могут быть перехвачены злоумышленником.Эффект ограничения правил брандмауэра напрямую зависит от уровня защиты сетевой инфраструктуры.

Использование оснастки «Брандмауэр Windows в режиме повышенной безопасности»

Дополнительные параметры брандмауэра можно настроить при помощи оснастки «Брандмауэр Windows в режиме повышенной безопасности».Эта оснастка включает в себя мастер правил и дает доступ к дополнительным параметрам, которые недоступны через элемент **Брандмауэр Windows** на панели управления.В их число входят следующие параметры.

- Параметры шифрования.
- Ограничения служб.
- Ограничение соединений для компьютеров по именам.
- Ограничение соединений для определенных пользователей или профилей.

- Разрешение просмотра узлов для исключения маршрутизаторов NAT.
- Настройка правил исходящих соединений.
- Настройка правил безопасности.
- Требование протокола IPsec для входящих соединений.

Создание правила брандмауэра при помощи мастера создания правил

1. В меню «Пуск» выберите пункт **Выполнить**, введите WF.msc и нажмите кнопку **ОК**.
2. В левой части панели **Брандмауэр Windows в режиме повышенной безопасности** щелкните правой кнопкой мыши **Правила для входящих подключений** и выберите пункт **Создать правило**.
3. Завершите **мастер создания правила для нового входящего подключения**, задав все необходимые параметры.

Устранение неполадок настройки брандмауэра

Следующие средства и методы могут оказаться полезными при устранении неполадок брандмауэра.

- Действующее состояние порта является объединением всех правил, связанных с этим портом.Чтобы заблокировать доступ к порту, бывает полезно просмотреть все правила, в которых он упоминается.Чтобы сделать это, откройте оснастку «Брандмауэр Windows в режиме повышенной безопасности» и отсортируйте правила по номеру порта.
- Просмотрите порты, которые активны на компьютере, где запущен SQL Server.В процессе анализа необходимо проверить, на каких TCP/IP-портах осуществляется прослушивание, а также проверить состояние этих портов.
  Чтобы проверить, на каких портах осуществляется прослушивание, используйте программу командной строки**netstat**.Помимо активных TCP-соединений, программа **netstat** также выводит различную статистику и другие сведения о протоколе IP.

  ### Получение списка прослушиваемых TCP/IP-портов

  1. Откройте окно командной строки.
  2. В командной строке введите **netstat -n -a**.
     При наличии параметра **-n** программа **netstat** отображает адреса и номера портов активных соединений TCP в числовом виде.При наличии параметра **-a** программа **netstat** отображает порты TCP и UDP, прослушивание которых осуществляет компьютер.
- Программу **PortQry** можно использовать для вывода состояния портов TCP/IP (прослушивается, не прослушивается, фильтруется).В состоянии фильтрации порт может либо прослушиваться, либо не прослушиваться. Это состояние указывает, что программа не получила ответа от порта. Программу **PortQry** можно загрузить из Центра загрузки Майкрософт.

См. также

Общие сведения о службе и требования к сетевым портам в системе Windows Server